E.T.S. de Ingeniería Industrial,
Informática y de Telecomunicación

Renovación de la infraestructura de red de datos para soporte NAC (Network Access Control) de una empresa.

Grado en Ingeniería en Tecnologías de Telecomunicación

Trabajo Fin de Grado

Autor: Ruth González Novillo

Director: Eduardo Magaña Lizarrondo

Pamplona, 25 Junio del 2014

upna Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

ÍNDICE

RESÚMEN

Uno de los objetivos de este trabajo es describir los pasos seguidos por una empresa multinacional a la hora de realizar un cambio en su red de datos. Para ello es necesario analizar el estado actual de la red y los objetivos que se quieren conseguir tras la nueva instalación.

Se pretende analizar los reajustes realizados durante el proceso del proyecto del cambio de la infraestructura de la red de datos, así como los cambios tanto de plazo como técnicos que se vayan generando a lo largo de la ejecución del procedimiento.

Este proyecto pretende recoger la complejidad de la realización de un cambio global de la infraestructura de red de datos de una empresa del sector de la automoción, siguiendo los objetivos no sólo propuestos por la sede local, sino por los exigidos por el grupo multinacional en conjunto.

Tras el análisis del estado actual de la red de datos tanto el despliegue de fibra óptica como la electrónica de red, se procederá a indicar las características de la futura instalación mediante el análisis de las RFP (Request For Proposal) convocadas por la empresa para el cambio del tendido de fibra óptica y la electrónica de red.

Este trabajo, por cuestiones temporales, recoge todos los pasos del proyecto del cambio de la infraestructura de red de fibra óptica previos a la recepción de las ofertas por parte de los ofertantes. El estado final de la descripción y seguimiento termina con la publicación de la citada RFP. Los pasos no contenidos son por tanto la descripción de las ofertas recibidas y la selección de una de ellas para la implantación final.

Dentro del proceso de actualización de la red de datos, la empresa pretende incorporar el concepto de NAC (Network Access Control) y zonas seguras.

En lo referente a este concepto NAC, en este trabajo se explica el funcionamiento teórico de una arquitectura de red segura y los protocolos que intervienen para conformarla. Se describen las necesidades de NAC dentro de la empresa y los requerimientos necesarios para su implantación según los estándares oficiales de la multinacional. Además, a modo de solución alternativa se implementará una prueba de este concepto NAC mediante código OpenSource.

En este trabajo también se incluyen las tareas más importantes realizadas dentro del entorno de la empresa y relacionadas con la gestión de las redes de la misma.

Índice de figuras

Lista de palabras clave

A
Autentificación
Autorización
Acceso

B
-

C
Core

D
Distribución
DMLT

E
EAP
EAPOL

F
-
G
-
H
-
I
IST

J
-
K
-
L
-
M
MLT
MacroLAN

N
NAC

Ñ
-
O
-
P
Portal cautivo

Q
-
R
RADIUS
RFP

S
Saneamiento
SMLT
SNMP

T
-
U
-
V
VRRP

W
-
X
-
Y
-
Z
Zonas de seguridad

Capítulo 1 – Introducción.

La motivación principal para la renovación de la red de datos de la empresa es el fin del periodo de soporte de la electrónica de distribución en conjunto con el factor añadido de que la Infraestructura de redes actual de la empresa no cumple con los requerimientos para la implantación de NAC (Network Access Control) a nivel de la capa de enlace, ni la implantación de zonas seguras, exigidas por la matriz de la multinacional.

Dentro de los Programas de Seguridad de la empresa, se exige que haya una autenticación a nivel de puerto en la capa de enlace para el acceso a la Red. Esto exige la implantación de una infraestructura que cumpla estos requerimientos a nivel de enlace. Por otra parte el backbone de la red debe ser reemplazado por el fin de ciclo de vida. Esto implica finalmente la decisión por parte de la empresa de reemplazar toda la infraestructura existente por otra acorde con los estándares.

La idea inicial del trabajo era analizar la RFP realizada para el cambio del backbone de fibra óptica de la empresa y la electrónica de red de la parte corporativa, sin embargo, tras la decisión de la empresa de realizar en el mismo lote el cambio de la electrónica de red industrial, y separar la RFP inicial en dos, una dedicada al cambio de fibra óptica y otra a la electrónica de red, se decidió centrar el trabajo en el análisis del Lote 1, es decir, de la RFP realizada para el cambio del backbone de fibra óptica.

Al tratarse de un proyecto real de una empresa multinacional los plazos temporales han variado considerablemente desde el inicio del trabajo hasta su fin, es por este motivo que paralelamente al estudio del Lote 1 (RFP para el cambio de la infraestructura de fibra óptica) se ha decidido realizar un estudio teórico y una prueba práctica de otro de los objetivos principales de la multinacional en el ámbito de la seguridad de la red que se pretende implantar tras la actualización de la infraestructura de red, es decir, del NAC.

Los objetivos principales de este trabajo se resumen en los siguientes puntos:

- Descripción del estado actual de la red de datos de la empresa, tanto a nivel lógico como físico. Se describen las dos redes que forma la infraestructura de red de la empresa (red corporativa e industrial) y el backbone de fibra óptica. Se describen además las comunicaciones externas, las comunicaciones con los proveedores y el cambio de las líneas de comunicación con estos últimos.

- Analizar los reajustes realizados durante el proceso del proyecto del cambio de la infraestructura de la red de datos, así como los cambios tanto de plazo como técnicos que se vayan generando a lo largo de la ejecución del procedimiento.

- Explicar y describir las soluciones para el control de acceso 802.1X y NAC a nivel teórico. Describir las condiciones para su futura implantación en la empresa así como

los fabricantes considerados y admitidos por la empresa y las soluciones ofrecidas por los mismos.

- Búsqueda de alternativas OpenSource para la implementación del concepto NAC y elección de una de ellas.
- Prueba e instalación de una solución OpenSource del concepto NAC y comparación con las soluciones propietarias. Descripción del funcionamiento de la solución y de sus características.
- Descripción de las tareas más relevantes realizadas dentro de la empresa.

Capítulo 2 – Situación actual de la red de datos.

La empresa objeto del documento es una empresa multinacional dedicada a la producción de automóviles. Para dar soporte a todos los procesos productivos cuenta con una red de datos industrial que permite el control de todos los procesos relacionados con la producción y de los propios autómatas así como información sobre la localización de los vehículos en cada instante sobre la línea de producción.

Además de esta red, cuenta con otra prácticamente independiente dedicada a propósitos más generales y de gestión y encargada de soportar la red Wifi de la empresa. Esta red se usa principalmente para dar conexión a las oficinas de los diferentes departamentos de la empresa y procesos de gestión y acceso a Internet. Ambas redes descritas se interconectan entre sí por dos puntos mediante firewalls.

Estas dos redes diferenciadas cuentan cada una con un direccionamiento distinto, en ambas privado pero de diferente clase. En caso de la red industrial se utiliza una Clase B, mientras que en el caso de red corporativa, una Clase A. En ambos casos para la asignación de IPs se utiliza subnetting.

Como se ha comentado, se trata de una empresa multinacional, consecuentemente cuenta con múltiples sedes en diferentes localizaciones, para la comunicación entre las sedes se utiliza el rango de Clase A, es decir, la multinacional tiene asignado un rango dentro de ese direccionamiento Clase A a cada una de las sedes aplicando subnetting.

Como consecuencia, la red corporativa es directamente visible desde el resto de sedes mientras que la red industrial permanece oculta.

Para la conexión con el resto de redes se utilizan túneles MPLS. A través de estos también se accede a un proxy, situado en la sede central de la multinacional, que se encarga de permitir el tráfico a Internet.

El proyecto de la empresa está centrado en el cambio de las redes de datos corporativa e industrial descritas, tanto el tendido de fibra óptica como la electrónica de red de las redes corporativa e industrial.

A continuación se va a proceder a describir brevemente la infraestructura física de la empresa de forma que la futura descripción de la red de datos resulte más sencilla.

2.1 Localizaciones de la Red de Datos. Infraestructura.

La empresa, en lo referente a infraestructuras, está formada por diferentes naves dedicadas a la producción, algunas de ellas disponen de zona de oficinas. Existen también otros edificios de oficinas, depuradora, y otros con diferentes finalidades.

Las diferentes naves y edificios están interconectados entre sí mediante enlaces de fibra óptica intentando formar una red en estrella con enlaces redundantes para asegurar la fiabilidad de la red y la redundancia de caminos ante fallos.

En total dispone de 5 naves dedicadas en su mayor parte a distintos procesos relacionados con la producción. En algunos casos, estas naves están divididas a su vez en diferentes partes o segmentos que siguen la lógica de la cadena de producción del automóvil. En el siguiente esquema se pueden apreciar todas las naves así como los nodos de comunicación principales y los LDR (Local Data Room), salas donde se encuentra gran parte de la electrónica de red y los núcleos tanto de la red corporativa como industrial. En ellas se concentran los mayores equipos de conmutación, todos los servidores, firewalls y cabinas de discos.

En la siguiente Figura 1 se puede apreciar el plano de la empresa con sus diferentes naves y nodos de comunicaciones.

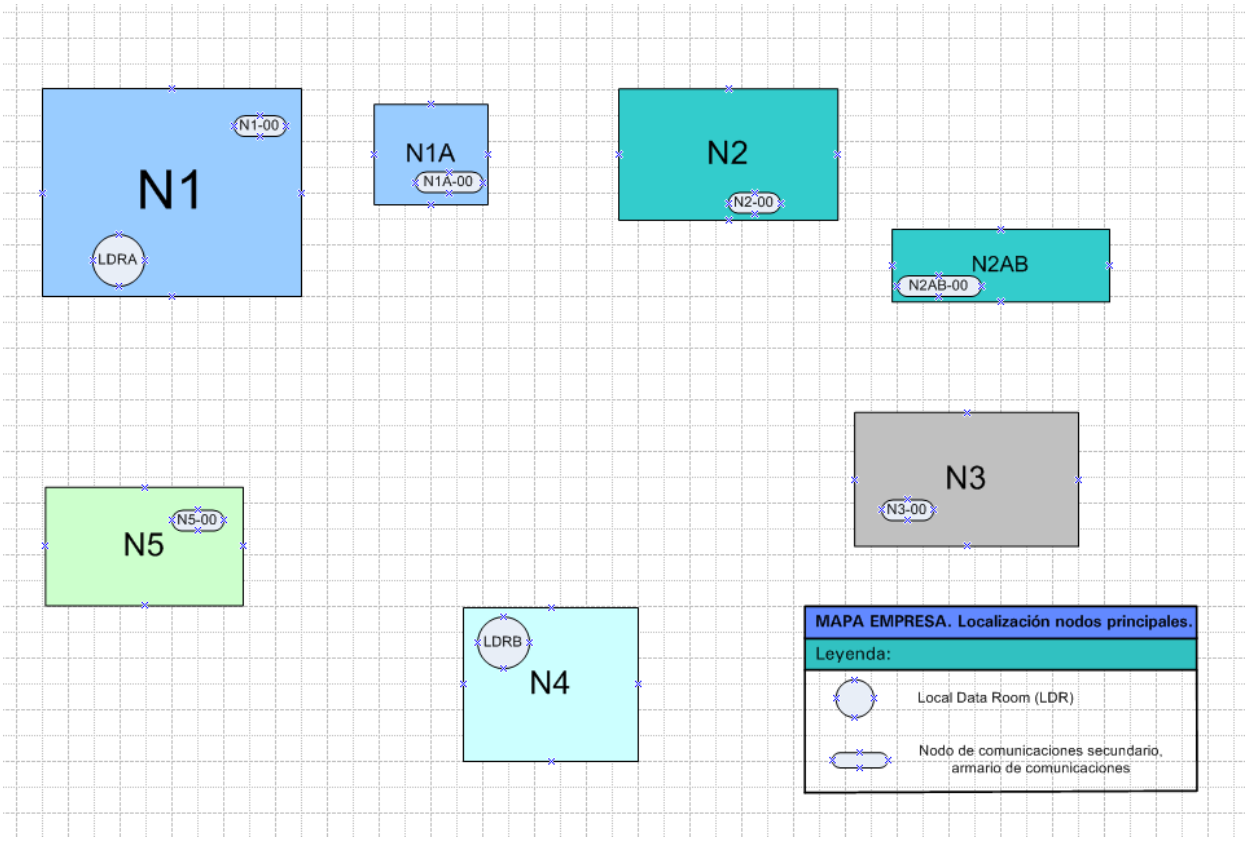


Figura 1-Plano naves y nodos de la empresa.

En dos de las naves (N1 y N4) se sitúan los LDR ya comentados, el LDRA (Local Data Room A) se sitúa en la nave N1 y es el LDR primario mientras que en la nave N4 se encuentra el LDRB (Local Data Room B) que actúa como sala secundaria, ambas salas funcionan simultáneamente y todo el equipamiento que se encuentra en una, está replicado en la otra de forma que si una

de las dos deja de funcionar, la otra sala tiene capacidad de absorber el trabajo de la otra aportando fiabilidad y redundancia.

Además de estos dos núcleos, se pueden encontrar nodos de comunicación principales en cada una de las naves excepto en N4 ya que esta nave depende directamente del LDRB. Estos nodos de comunicación principales dependen en la mayoría de los casos directamente de los LDR. La empresa cuenta con dos redes, la red corporativa y la red industrial. Esta última está dedicada a todos los procesos de producción. La estructura de ambas redes es similar y están unidas entre sí por dos enlaces protegidos por firewalls que unen los equipos que forman el núcleo de cada una de las redes o lo que se puede denominar Core, siendo esta la nomenclatura que se utilizará más adelante.

Además de los LDR y los nodos de comunicación principales de cada nave, existen diferentes armarios de comunicaciones repartidos por las diferentes naves que cuelgan o bien de uno de los dos LDR directamente o de uno de estos nodos de comunicación principales de cada nave.

Es decir, en cuanto a infraestructura de armarios y salas de comunicaciones se tendrían tres niveles:

- Armarios de comunicaciones distribuidos por las naves: Son armarios sencillos, normalmente están equipados con electrónica de red de la capa de acceso, es decir, a la que se conectan los usuarios finales. Estos armarios dependen de los nodos de comunicaciones principales de cada nave o en el caso de la nave N4 directamente del LDR. Todos los armarios cuenta con una pequeña SAI (Sistema de alimentación ininterrumpida) y puerta con llave.

- Nodos de comunicaciones principales: Son las salas de comunicación principales de cada nave. Generalmente contienen electrónica de red de la capa de distribución. Dependen normalmente de los LDR. Están compuestas por varios armarios, y cuentan con sistemas de alimentación ininterrumpida. El acceso a ellos está restringido a usuarios autorizados.

- LDR: Son las dos salas de comunicación principales, y a parte de albergar los servidores de la empresa, contienen electrónica de red tanto del núcleo (Core) como de la capa de distribución. Cuentan con sistemas de seguridad de acceso, SAIs y equipos de refrigeración.

2.2 Estructura lógica de la Red de Datos

Las redes de comunicaciones actuales de la empresa (industrial y corporativa) están estructuradas de forma jerárquica en tres capas: Core, Distribución y Acceso.

La capa de Core es el backbone de conmutación de alta velocidad de la red de datos. Su configuración tiene que ser sencilla, por este motivo opera en capa 2, sin enrutar. Está preparado para adaptarse con rapidez a cambios, es tolerante ante fallos y de alta fiabilidad permitiendo una conmutación a altas velocidades.

El Core se une con el nivel de Distribución mediante enlaces de fibra; la velocidad máxima alcanzable entre estas dos capas es de 1 Gbps. Este segundo nivel tiene diversas funcionalidades, las principales son: enrutamiento entre VLANs, definición de dominios de broadcast, aplicación de políticas de calidad de servicio, etc.

El tercer nivel y el más próximo al usuario es el de Acceso, que permite acceder a los usuarios a los recursos de la red.

Como se ha comentado, la empresa cuenta con dos LDR o también denominados CPD (Centro de Procesado de Datos). Esta duplicación permite asegurar el funcionamiento de la red de la empresa ante la caída de una de las dos salas o de alguno de los equipos de estas. Para conseguir esto, ambos LDR están interconectados entre sí mediante dos enlaces de fibra óptica monomodo 9/125 (uno de 24 fibras y otro de 48) y otro enlace multimodo 62.5/125 de 48 fibras. Estos enlaces se encargan de unir los dos equipos que conforman el Core de las diferentes redes (dos equipos para el Core industrial y dos para el Core corporativo) y que están situados uno en cada LDR.

2.3 Protocolos propietarios del fabricante

Para entender el funcionamiento de la disposición de la red es necesario definir ciertos protocolos propietarios del fabricante Avaya [1], que permiten la comunicación de los diferentes nodos de la red en los tres niveles que la conforman.

MLT (Multi-Link Trunking) es un mecanismo que permite agrupar dos o más puertos físicos de un mismo switch de forma que operen como un único puerto lógico. La distribución del tráfico entre los diversos enlaces físicos de MLT se hace mediante un algoritmo de hashing que tiene en cuenta las direcciones MAC origen y destino para tomar la decisión del puerto físico escogido para enviar tráfico. Permite ampliar el ancho de banda de interconexión entre dos equipos. Permite la agrupación de varios enlaces físicos Ethernet en un único enlace lógico para proporcionar tolerancia a fallos y enlaces de alta velocidad entre routers, switches y servidores.

DMLT (Distributed MLT) es un mecanismo que permite agrupar dos o más puertos físicos de dos o más Switches que forman parte de un mismo stack de forma que operen como un único puerto lógico.

Todos los puertos que formen parte de un MLT han de tener la misma configuración de VLANs, STP, velocidad, etc.

SMLT (Split MultiLink Trunking) es una extensión del estándar 802.3ad de la IEEE (link aggregation) de agregación de enlaces que proporciona un nivel superior de protección añadiendo la redundancia de nodo como principal funcionalidad. Esta redundancia de nodo se consigue haciendo que los enlaces del MLT terminen en dos nodos de agregación distintos.

Para que SMLT funcione adecuadamente, estos nodos de agregación se conectan entre sí usando IST (Inter Switch Trunk). IST es un protocolo que utiliza el puerto TCP 6000 tanto en

origen como en destino para establecer una sesión entre dos nodos de agregación, en este caso Switches Layer 2/3. Sobre esta sesión se intercambian información de estado y tablas de direccionamiento, permitiendo una rápida reacción ante fallos y aparecer así como un único equipo lógico.

Al utilizar SMLT con IST, esta configuración está inherentemente capacitada para evitar bucles de red, con lo que no es necesario ni aconsejable configurar STP (Spanning Tree Protocol) en los enlaces implicados.

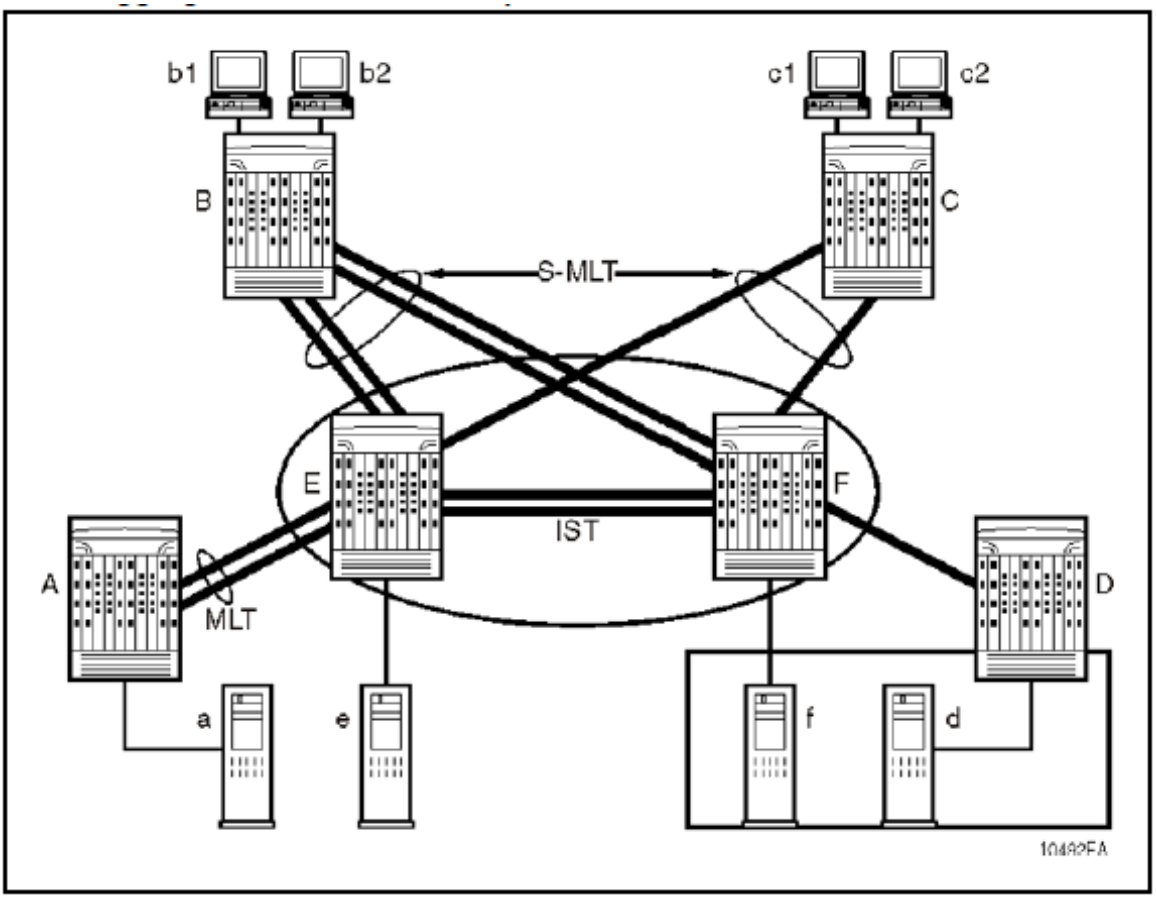


Figura 2-Esquema de protocolos propietarios de Avaya.

En la Figura 2 se pueden ver los diferentes protocolos descritos, MLT que permite la unión de dos enlaces físicos en uno lógico (Unión entre el equipo A y el E); SMLT que se puede ver por ejemplo en el equipo C donde los dos enlaces terminan en distintos equipos, E y F; y el protocolo IST que comunica a los equipos E y F consiguiendo que el equipo C los vea como un único nodo lógico.

2.4 Red Corporativa

En cuanto a electrónica de red, el nivel de Core de la red corporativa está formado por dos Switches L2/L3 situados uno en cada uno de los LDR. Son equipos modulares, y constan de dos fuentes de alimentación por temas de redundancia. Estos equipos se comunican entre sí utilizando un protocolo propietario del fabricante Avaya, IST (Inter Switch Trunk) permitiendo intercambiar información entre ellos y que aparezcan como un único equipo lógico.

Dentro de la capa de Distribución de la red corporativa se tienen cuatro puntos principales formados por dos Switches capa 2/3 modulares cada uno (nodos de distribución principales o distribuidores principales). Esta agrupación de dos conmutadores capa 2/3 está unida mediante dos enlaces de fibra óptica multimodo LX configurados en MLT (agregación de enlaces) y se comportan mediante un único nodo lógico gracias a IST. Estos cuatro distribuidores principales formados por dos equipos cada uno se encuentran en el LDRA, LDRB, y en los nodos de comunicación principales de las naves N1 y N3 (N1-00 y N3-00).

De estos cuatro puntos cuelgan en muchos casos Switches capa 2 que forman parte del nivel de acceso y a los que se conectan directamente los usuarios finales. Estos Switches de acceso se unen en la mayor parte de los casos mediante dos enlaces multimodo uno a cada equipo de la pareja que forme su punto de distribución. Hay casos en los que sólo se utiliza un solo enlace de unión entre el Switch y uno de los distribuidores.

Según la localización de los conmutadores de acceso, su nodo de distribución varía. Para configurar este tipo de enlaces se utiliza MLT en los conmutadores de acceso y SMLT en los Switches de agregación.

La red de distribución está también compuesta de Switches capa 2, Switches distribuidores, que están conectados a su vez a uno de los puntos de distribución principales y también a Switches de acceso a los que los usuarios finales se podrán conectar. Estos equipos están situados en los nodos principales de cada una de las naves.

En general, los Switches de acceso conectados directamente a los distribuidores principales son los que pertenecen a oficinas. Los Switches de acceso distribuidos por las naves, al ser mayor cantidad y para hacer la red escalable, se conectan a Switches distribuidores los cuales se conectan a su vez a uno de los cuatro nodos de distribución principales.

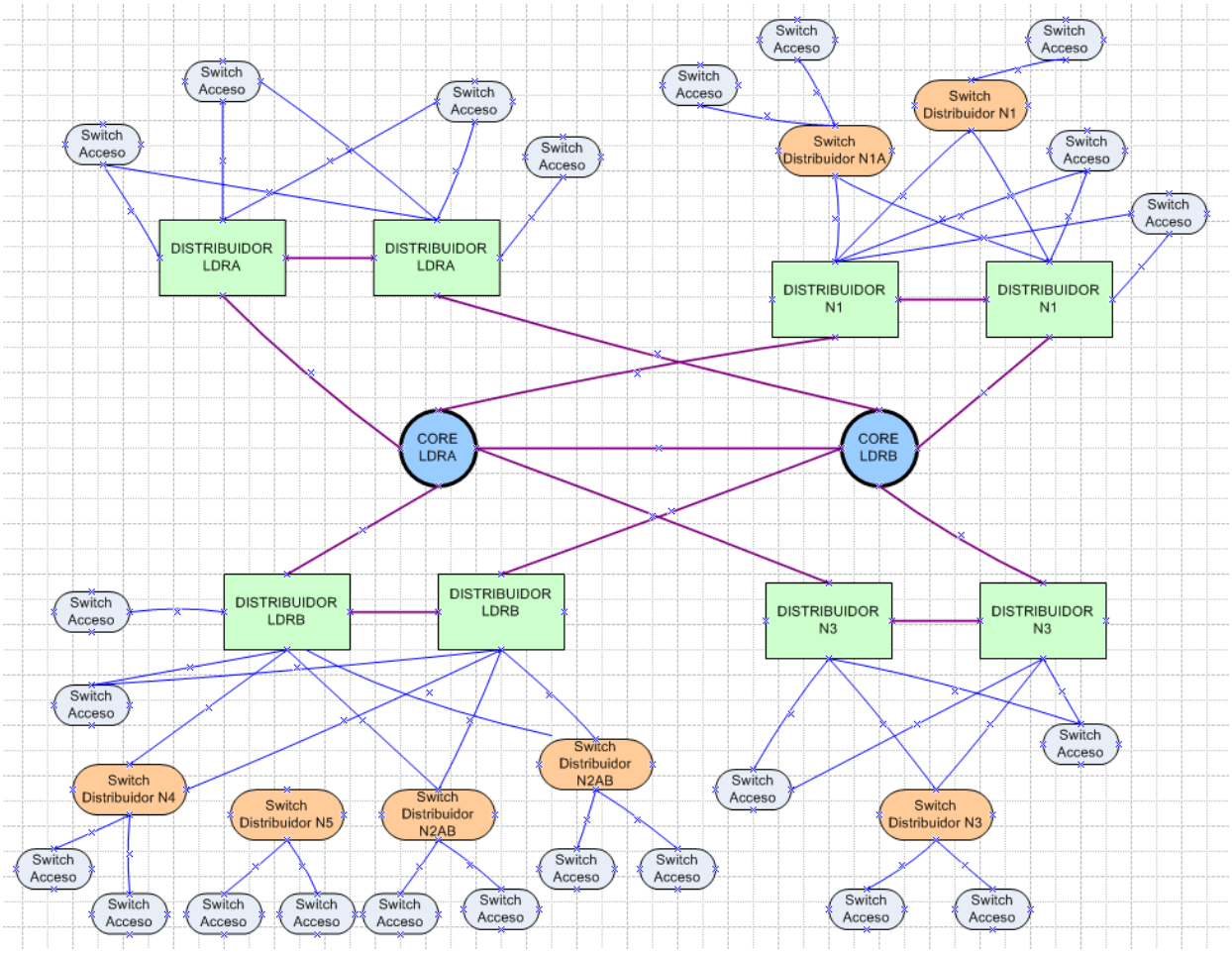


Figura 3-Topología física de la red corporativa

Como se ha descrito anteriormente, existe un nodo principal en cada una de las naves (N1-00, N1A-00, N2-00, N2AB-00, N3-00, N5-00) y en estos se sitúan los conmutadores denominados Switches distribuidores que se conectan a los conmutadores de acceso, siguiendo así la jerarquía de tres niveles descrita anteriormente, la cual se puede apreciar en la Figura 3. Se pueden ver Switches distribuidores en las naves N4, N5,N2AB, N3, N1 y N1A.

Esta Figura 3 anterior permite ver claramente lo descrito en este apartado, se pueden apreciar los dos equipos que forman el Core corporativo, los cuatro puntos de distribución formados cada uno por dos equipos físicos que mediante protocolos propietarios forman un único equipo lógico, se aprecian también los Switches distribuidores de los cuales penden Switches de la capa de Acceso.

La topología lógica resultante de la red de datos corporativa es una estrella, siendo el Core el centro de ella y los cuatro puntos de distribución sus ramas principales. Tras los nodos de distribución principales se encuentran otros conmutadores de distribución o directamente conmutadores de acceso. En cuanto a topología física, el resultado no sería exactamente una estrella puesto que tanto el Core como los cuatro nodos de distribución principales están formados por dos equipos físicos que se comportan como uno lógico gracias a configuraciones y protocolos propietarios del fabricante los cuales se han descrito con anterioridad.

2.5 Red Industrial

Como se ha comentado, la red de datos está conformada por dos redes diferenciadas unidas entre sí mediante dos puntos que unen los Core de las distintas redes y cuya unión está protegida por un Firewall y un IPS (Intrusion Prevention System). En esta unión redundante está activa únicamente una, siendo la segunda el backup en caso de que la primera no funcione. La red industrial es la dedicada a todos los procesos de producción.

El hecho de contar con dos redes separadas, una de ellas dedicada exclusivamente a los procesos de producción, permite garantizar una mayor seguridad en las redes. Sólo la red corporativa tiene comunicación con el resto de sedes de la empresa y esta emplea un rango de direccionamiento asignado por la sede principal de forma que es visible por el resto de sedes, mientras que la red industrial es una red interna de la sede actual y no visible por el resto de sedes de la multinacional. Además, este hecho hace que por contar con un direccionamiento no gestionado por el consorcio multinacional, no puede salir al exterior por la red WAN MPLS y tampoco ser accedida desde la misma. El hecho de contar con dos redes diferenciadas con todas sus capas Core, Distribución y Acceso duplicados permite además mejorar la escalabilidad. Tener una electrónica de red diferente en ambas redes permite adecuarla al tipo de uso que se le va a dar, y facilita la gestión de los dispositivos. Además, los equipos industriales son más robustos y aguantan mejor condiciones adversas (las fuentes de alimentación son externas y duplicadas, están en muchos casos formados en módulos cambiables en caliente, soportan mayores temperaturas, etc.) por lo que de esta forma se evita que se conviertan en un punto crítico de fallo en la producción.

Al igual que la red corporativa, la red industrial está estructurada de forma jerárquica en tres niveles: Core, Distribución y Acceso. El Core está formado por dos equipos, cada uno localizado en uno de los LDR. La conexión entre los LDR se realiza mediante dos enlaces a 10 Gbps usando fibra óptica monomodo. A cada equipo de Core se le conecta un Switch apilable mediante MLT con dos enlaces 1000BASE-T.

La estructura de distribución es similar a la de la red Corporativa descrita anteriormente. En este caso se disponen de tres puntos de distribución formados por dos equipos cada uno y unidos con los protocolos propietarios descritos con anterioridad formando un único punto lógico, es decir, la conexión con los Switches de las diferentes localizaciones se hace mediante SMLT y entre los equipos de distribución mediante IST, de forma que cada Switch de acceso se conecta a cada uno de los dos equipos que forman su punto de distribución.

En el caso del nodo de distribución localizado en N1-00, aparte de distintos Switches de la capa de Acceso, se conecta a él un Switch distribuidor de la nave N1A, situado en el nodo N1A-00.

Al nodo de distribución localizado en N3-00 se le conecta un Switch distribuidor que da comunicación a la nave N4 y el cual está situado en esta misma nave, en concreto en el LDRB ya que como se ha comentado esta nave no cuenta con nodo principal de comunicaciones. El tercer nodo de distribución se encuentra en la nave N2AB (N2AB-00).

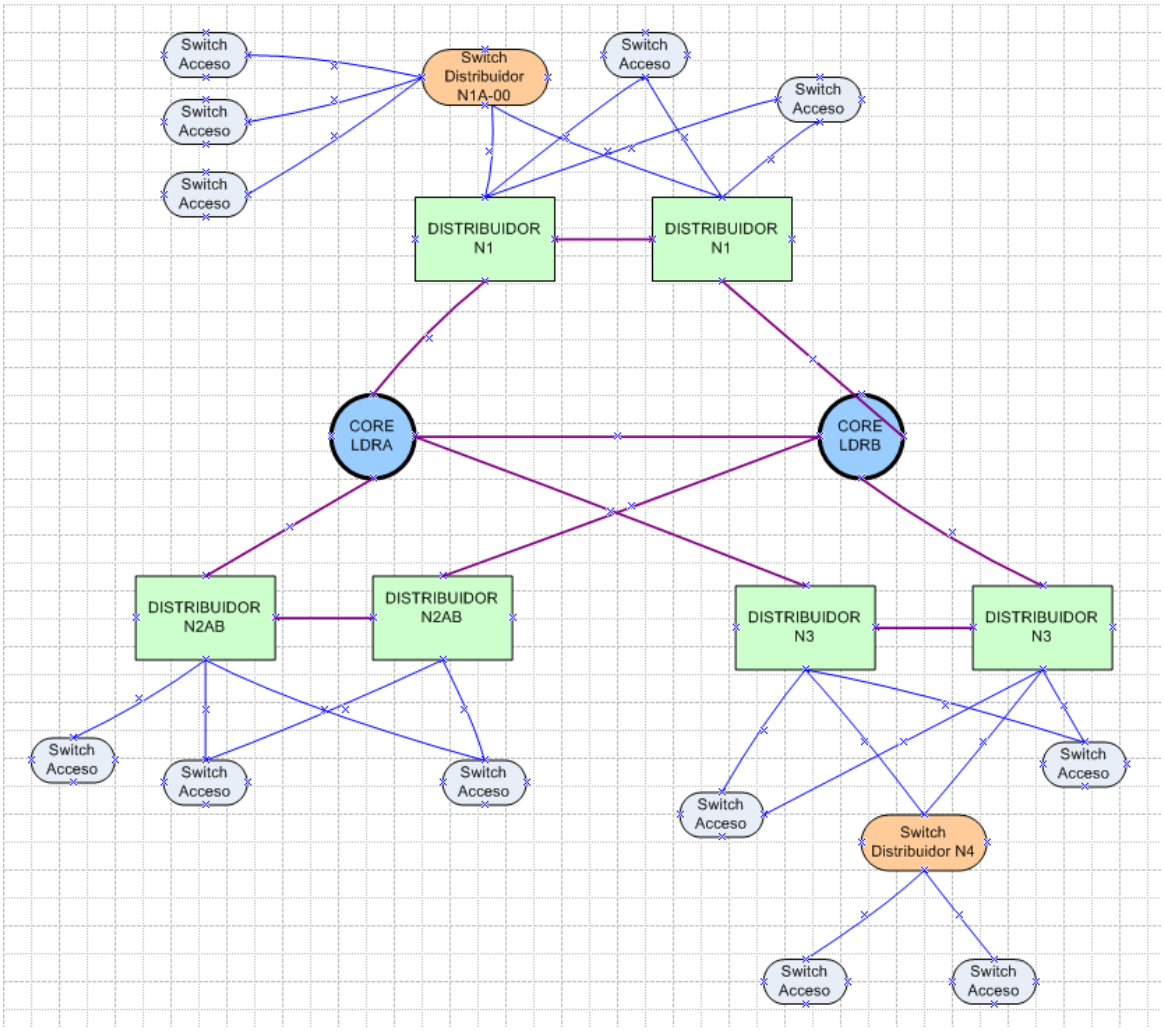


Figura 4-Esquema de la red industrial

En la Figura 4 se puede ver el esquema de la red industrial con los diferentes distribuidores principales y Switches de distribución y acceso conectados a ellos.

2.6 Comunicaciones externas

Al ser una empresa multinacional, dispone de sedes en diferentes localizaciones. Para la comunicación de la empresa con otras sedes y con Internet se dispone de dos enlaces hacia el exterior mediante una red WAN y tecnología MPLS. El direccionamiento que se emplea es privado y mediante el túnel MPLS se pueden conectar con este rango privado con las otras sedes de la multinacional. Para la conexión a Internet se utiliza un proxy situado en otra sede que se encarga de gestionar el paso de IP privada a pública, actúa como NAT asignando direcciones públicas reservadas de la empresa.

La gestión de la conexión a Internet se realiza de dos mediante dos formas diferentes, en el caso de la red WIFI corporativa se realiza mediante autentificación de certificados. El usuario para conectarse a internet necesita una tarjeta con un chip que contiene un certificado este es validado por un servidor RADIUS el cual comprueba la validez de este certificado y permite o

deniega el acceso al usuario. Esto es así puesto que para WIFI se tiene implementado el concepto de control de acceso a la red que se definirá en un capítulo aparte. Como concepto importante, el certificado del usuario autentifica al equipo como conocido y perteneciente al grupo por lo que se le autoriza el acceso a Internet.

En el caso de la red cableada, para la conexión a Internet se necesita un usuario y contraseña pertenecientes a la empresa. Esta información de usuarios está centralizada a nivel multinacional, es decir, para todas las sedes, en un servidor de directorio LDAP (Lightweight Directory Access Protocol).

A este servidor se accede mediante el protocolo LDAP que opera sobre TCP/IP (Transmission Control Protocol/Internet Protocol) y utiliza SSL (Secure Socket Layer). Por tanto nos permite operar sobre Internet. Cuando un usuario quiere acceder a Internet, el navegador solicita sus credenciales y este debe de introducir su usuario y contraseña. Esos son enviados mediante SSL (permite crear un túnel para evitar que la información sea visible por otros usuarios) al servicio de directorio centralizado, se comprueban si estos se encuentran en ese servidor y si es así se le autoriza el acceso.

Para la autentificación de los dispositivos en las tomas de red, se utilizan listados con las direcciones MAC de los dispositivos autorizados, de esta forma se evita que un dispositivo desconocido acceda a la intranet al conectarse a una de las tomas de red que se encuentran distribuidas en los diferentes puntos de la empresa. La gestión de este sistema es manual.

2.7 Comunicaciones con los proveedores.

Además de las comunicaciones externas con las otras sedes de la empresa e Internet, la sede dispone de conexiones directas a todos sus proveedores. La mayoría de estos están situados en lo que se denomina “parque de proveedores” y se encuentran próximos a la empresa. El resto de proveedores se encuentran todos en la misma provincia excepto uno que se sitúa a 180Km en una provincia cercana. La conexión con estas empresas se ha modificado durante el transcurso de este trabajo.

Las tecnologías usadas en un principio para la conexión de los proveedores eran Frame Relay como red principal y R.D.S.I (Red Digital de Servicios Integrados) como backup. La velocidad conseguida mediante estas tecnologías era de 64Kbps.

Actualmente se ha modificado la conexión con todos los proveedores de la empresa de forma que se emplea como red principal una MacroLAN y como backup un ADSL empresarial.

La empresa cuenta con 12 proveedores con los que se quiere conectar. Como se ha comentado la red principal será un a MacroLAN y el Backup un ADSL. Esto es así en 10 de las 12 sedes, para las dos restantes debido a las reducidas de necesidades se emplea únicamente un ADSL.

2.7.1 MacroLAN.

Una MacroLAN [2] es un servicio de Red Privada Virtual del proveedor Telefónica en el que se hace routing del tráfico IP del cliente entre sus distintas sedes. El servicio permite realizar el transporte de tráfico Ethernet entre diferentes sedes del mismo cliente ubicadas en distintos puntos del territorio como si las sedes estuviesen conectadas mediante una red de área local. El servicio MacroLAN es la solución de Telefónica de altas prestaciones y velocidad para la interconexión de Redes Privadas Virtuales.

La red MacroLAN utiliza la infraestructura MAN (Metropolitan Area Network) como medio de acceso a la red IP/MPLS (Multi Protocol Label Switching), la cual sirve de infraestructura tanto para la interconexión de las sedes de un cliente a nivel provincial como con la conexión con la red IP/MPLS que proporciona comunicación entre sedes a nivel nacional comunicando sedes ubicadas en diferentes provincias.

Sobre la cobertura del servicio hay que distinguir dos ámbitos:

- Provincial: El servicio se apoya en la infraestructura de la MAN.
- Nacional: Además de la MAN, se utiliza la infraestructura IP/MPLS y tecnología de VPN IP.

La arquitectura de la MacroLAN está formada por diferentes elementos:

- EDC (Equipo en domicilio de cliente): Es el equipo que se instala en la sede del cliente proporcionando la conectividad a la red MAN. Este está gestionado remotamente por el ISP (Telefónica). En el lado de los proveedores el equipo instalado es un Juniper SRX100-Cu-TE que se conecta al proveedor mediante el puerto 0.
- Circuito de acceso a la MAN: El router Juniper tiene el puerto RJ45 (puerto 7) conectado a un conversor de medios (cobre a fibra óptica), el otro extremo de fibra óptica es el que proporciona el acceso a la MAN.
- Conexión entre MAN y IP/MPLS: Son conexiones compartidas por múltiples clientes.
- Caudales: No son elementos físicos en sí mismos, son los anchos de banda para el acceso las diferentes redes que el cliente debe de contratar. En este caso la empresa sólo necesita dos tipos:
    - Caudal Metro: Es el caudal o ancho de banda que el cliente contrata para acceder a la MAN.
    - Caudal Nacional Agregado: Es el caudal que el cliente contrata en cada provincia, en la conexión con la red IP/MPLS. El que controla el tráfico entre la MAN de una provincia y la otra.

La MacroLAN de Telefónica define tres clases de servicio que pueden ser contratadas por el cliente: Plata, Oro y Multimedia; más una clase interna adicional para la gestión de los EDCs que es transparente para el cliente.

El servicio Plata está orientado al tráfico Intranet del cliente. Su prioridad es normal. Es la clase de servicio que se asigna por defecto cuando no se contrata calidad de servicio.

El servicio Oro está orientado al tráfico Intranet del cliente de aplicaciones críticas. Su prioridad es normal. Los SLAs (Service Level Agreement o Acuerdo a nivel de servicio) son más exigentes que los de la clase Plata.

El servicio Multimedia está orientado a tráfico muy sensible de retardo y jitter y tiene prioridad máxima.

En el caso de la empresa se ha contratado el servicio Plata.

En la Figura 5 se puede apreciar la estructura de una red MacroLAN con sus elementos. Se ven los equipos colocados en las instalaciones del cliente, las redes MAN y la red IP/MPLS.

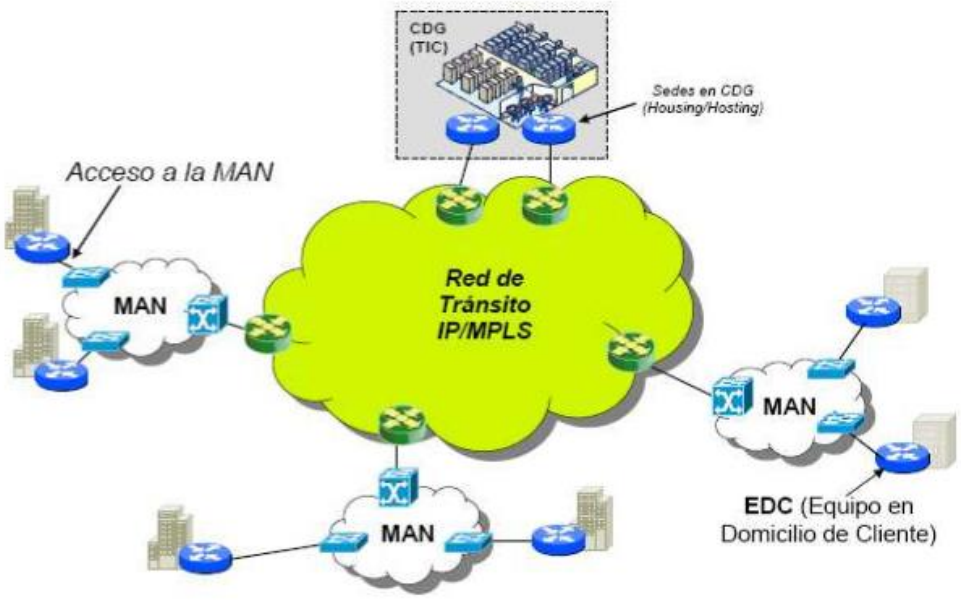


Figura 5-Estructura de una MacroLAN

En cada una de las 10 sedes que cuentan con una conexión mediante MacroLAN se instala un router Juniper SRX100-Cu-TE, este va conectado a un conversor de medios (cobra a fibra óptica) y este extremo de fibra óptica es el que se conecta con los equipos de la MAN a través del proveedor de servicios (ISP) que en este caso es, como se ha comentado, Telefónica.

Las sedes se unen a la MacroLAN mediante el caudal metropolitano (caudal metro) cuya velocidad es de 2Mbps para cada uno de las 10 sedes. Esta velocidad es la que ha sido contratada por la empresa y se define a la salida de los EDC, en este caso el router Juniper.

La velocidad anterior (64 Kbps) era lenta para la comunicación de algunos de los proveedores ya que muchos de los programas usados por las sedes se comunican con servidores situados en los LDR de la empresa y por tanto la carga de los mismos y su funcionamiento eran lentos.

En la parte de la sede de la multinacional se disponen de dos routers situados cada uno en un LDR (LDRA y LDRB), en concreto se tienen instalados dos routers Juniper SRX210-Cu-TE. El caudal metropolitano contratado es de 40Mbps para el situado en el LDRA. El router del LDRB no cuenta con pago por caudal adicional puesto que se usa como respaldo del primero. Ambos routers se conectan a la red por MacroLAN.

En total se cuenta con 10 sedes cuya velocidad máxima es de 2Mbps lo que hace un total de 20Mbps. Las otras dos sedes restantes que se comentan a continuación tienen una velocidad máxima de 4Mbps. En total el tráfico máximo generado por las 12 sedes es de 28Mbps. La velocidad contratada en la empresa para evitar convertirse en un cuello de botella es de 40Mbps lo que proporciona un margen para poder incluir nuevas sedes o nuevos aumentos de velocidad en alguna de las existentes sin tener que aumentar la velocidad contratada.

2.7.2 ADSL.

El ADSL se utiliza en 10 de las 12 sedes como medio de backup con una velocidad contratada de 2Mbps. En las otras dos sedes restantes se utiliza como medio de comunicación principal y la velocidad contratada es de 4Mbps. Se contrata un ADSL para empresas que utiliza los caudales plata. El equipo ADSL instalado en cada una de las sedes es un Cisco 887VA-M-K9.

2.7.3 VRRP

Los routers Cisco y Juniper colocados en las sedes de los proveedores se conectan a un Switch a través del cual se envían mensajes VRRP (Virtual Router Redundancy Protocol) de forma que cuando el router principal de la MacroLAN MPLS falle, el router ADSL sea capaz de cursar el tráfico a través de él.

El protocolo utilizado para ello es VRRP (Virtual Router Redundancy Protocol) [53]. VRRP es un protocolo de redundancia no propietario definido en el RFC 3768 [3], está diseñado para aumentar la disponibilidad de la puerta de enlace por defecto de una red. El aumento de fiabilidad se consigue mediante el anuncio de una dirección IP virtual como una puerta de enlace por defecto en lugar de la dirección IP de un router físico.

Los routers físicos se configuran para recibir paquetes en esa dirección IP virtual. Puede haber dos o más routers físicos, cada uno tiene su propia dirección IP real. Si el router físico configurado como principal que está realizando el enrutamiento falla, el otro router físico negocia para sustituirlo. Se denomina router maestro al router físico que realiza realmente el enrutamiento y routers de respaldo a los que están en espera de que el maestro falle.

En la Figura 6 se puede ver un ejemplo de funcionamiento de una estructura VRRP. Los routers se conectan a la LAN interna mediante un Switch, el host de esta LAN tiene como puerta de enlace la dirección virtual de los routers. Cuando el router principal o maestro está activo el tráfico circulará a través de él, pero en el momento que este deje de funcionar pasará a circular por el router secundario.

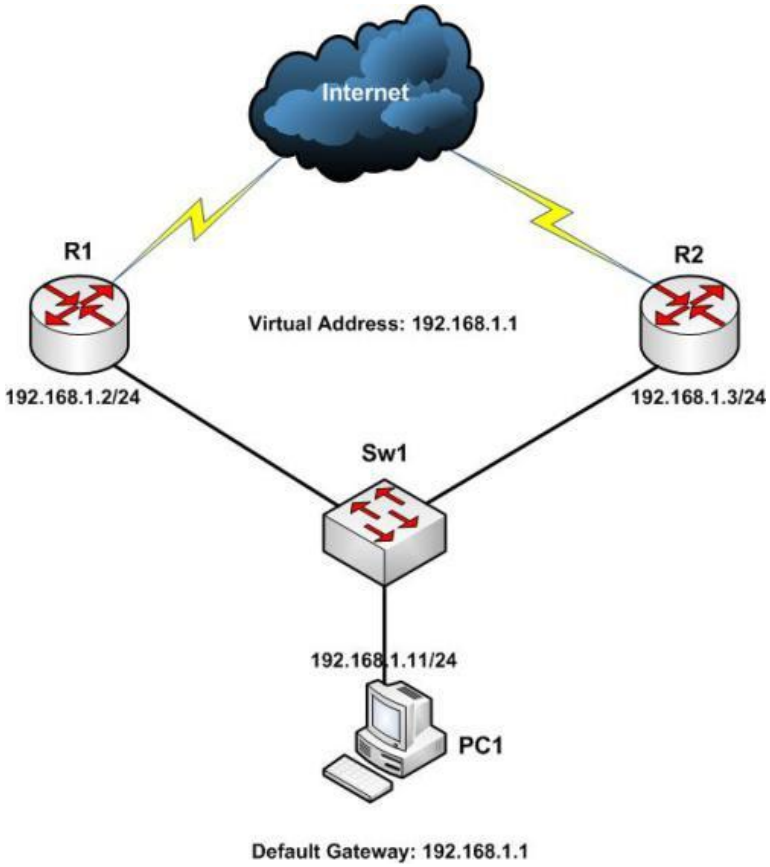


Figura 6-Estructura VRRP [4]

Como se ha comentado, durante el desarrollo de este trabajo se realizó el cambio de las líneas con los proveedores, de forma que nos fuimos desplazando a cada uno de ellos para realizar las nuevas conexiones.

Como los equipos pertenecen al proveedor de servicios, la instalación de los mismos así como la tirada de fibra óptica necesaria para la comunicación es responsabilidad de este, por lo que la configuración de los equipos la realizaba Telefónica de forma remota.

Las sedes de los proveedores cuentan con un direccionamiento privado interno distinto que el que utiliza la empresa multinacional. Para que la comunicación sea posible es necesario convertir estas direcciones en otras que pertenezcan a la empresa. En concreto la empresa dispone de una VLAN únicamente dedicada a los proveedores. Esta se ha subnateado en redes de 30 host (32 si se cuenta la dirección de red y la de broadcast), es decir, subredes con máscara "/27". Estas direcciones son nateadas de forma estática en los routers de las sedes de los proveedores de forma que una dirección IP interna al proveedor corresponda a otra dirección IP de la VLAN de proveedores.

Como se ha comentado que los equipos EDC son responsabilidad de telefónica, es este el que se encarga de configurar el nateo en los mismos.

En cada uno de los proveedores se ha realizado la misma prueba DRP (Disaster Recovery Plan): se ha conectado un PC a un Switch al cual también se le han conectado los dos routers. Al PC

se le ha asignado una dirección IP interna de la sede correspondiente a una de las IPs nateadas y se ha probado su conexión con la red de la multinacional mediante los comandos ping y traceroute. Una vez comprobado el funcionamiento se ha desconectado el cable con el router principal (Juniper) y tras unos segundos de pérdida de conexión esta se reestablece a través del router secundario Cisco (mediante ADSL). Tras esta desconexión es necesario esperar 5 minutos puesto que si las líneas flapean, es decir, la conexión por ADSL pasa a MPLS y viceversa demasiado rápido más de tres veces, se bloquea una línea.

La conexión ADSL es únicamente de backup, no se usan las dos conexiones simultáneamente puesto que el caudal contratado es de 2Mbps y no de 4Mbps, que es de lo que se dispondría si se utilizarán las dos tecnologías a la vez. Además, el tráfico por ADSL es más lento por lo que no interesa que circule por este excepto en caso de fallo del principal.

Una vez conectado el cable al router principal se debe comprobar que se reestablece la conexión por el mismo. Cabe destacar la diferencia de tiempos de ping entre las dos tecnologías, en el caso de la MacroLAN MPLS el tiempo ronda en torno a unos 2ms, mientras que por ADSL son entre 42 y 43ms.

Una vez realizada la prueba con un ordenador, llega el punto de migrar las líneas, lo que supone cortar las comunicaciones del proveedor con la empresa. En algunos casos esto era crítico y era necesario esperar a que el proveedor contase con suficiente información como para no necesitar conexión durante al menos 10 minutos.

La migración consistía principalmente en desconectar el cable RJ45 del interfaz del router Frame Relay y conectarlo al router Juniper de la MacroLAN y lo mismo con el cable RJ45 del router R.D.S.I con el router Cisco del ADSL.

En algunos casos era necesario modificar las direcciones internas de la sede o la puerta de enlace predeterminada de estos para ajustarlos a la nueva.

Durante la realización de las pruebas han surgido diferentes problemáticas, desde dificultades para realizar la conexión física de los equipos, mala configuración del nateo o problemas a nivel de aplicación.

Tras el cambio de las líneas ha sido necesario modificar unos parámetros de un programa propio de la empresa (desarrollado por un miembro del departamento IT) encargado de monitorizar las conexiones con los proveedores. El cambio a realizar era indicarle al programa las nuevas direcciones IP de los routers a monitorizar en cada sede, para ello era necesario cambiar un fichero de texto plano (con extensión .txt) y modificar en este las direcciones IP reemplazando las antiguas direcciones de los routers RDSI y Frame Relay por las de los routers de la MPLS y el ADSL.

2.8 Backbone de la red.

Toda la empresa está conectada mediante un backbone de fibra óptica que finaliza en paneles de parcheo donde se decide si la fibra formará parte de la Red Corporativa o Industrial.

El backbone de la red está formado por fibra óptica de tres tipos distintos, monomodo de 9/152, multimodo de 50/125 y multimodo de 62.5/125. Los dos nodos principales LDRA y LDRB se unen mediante dos enlaces monomodo y otro multimodo de 62.5. La empresa cuenta con seis nodos secundarios, situados uno en cada nave (N1, N1A, N2, N2AB, N3 y N5) a excepción de una de ellas (N4) la cual depende directamente del LDRB. Estos nodos principales de cada nave cuelgan en su mayoría directamente de uno de los dos LDRs y en bastantes casos, de los dos LDRs, en todos los casos tienen como mínimo dos enlaces desde diferentes nodos.

Como se ha comentado, las redes de la empresa están estructuradas de forma jerárquica, tanto la red corporativa como la industrial. En ambas, el nivel más cercano al usuario final es el de Acceso y, su función es permitir a los usuarios conectados en las diferentes ubicaciones su interconexión y el acceso a la granja de servidores y recursos conectados a su nodo de distribución, así como a los usuarios, servidores y recursos conectados a otros nodos de distribución a través del Core. Esta capa de Acceso está formada básicamente por conmutadores capa 2 a los que se conectan los latiguillos de los usuarios finales a una velocidad de 100Mbps.

Hay que aclarar que el backbone de fibra óptica es común para las redes industrial y corporativa, esto significa que la tirada de fibra que une los diferentes nodos o armarios de comunicaciones y finaliza en un panel de parcheo de fibra en los extremos, puede usarse para una red u otra independientemente, sin embargo, la estructura de la electrónica de red tiene pequeñas variaciones entre la red industrial y la corporativa, aunque la jerarquía de los niveles Core, Distribución y Acceso se cumple en ambas.

Como se ha comentado, la fibra óptica que compone el backbone de la red puede ser de tres tipos: monomodo (9/125), multimodo (62.5/125) y multimodo (50/125).

El conjunto de enlaces de fibra óptica permite comunicar las naves y edificios entre sí. La unión directa entre LDRA y LDRB sólo se realiza mediante un único camino, aunque está previsto añadir uno redundante de forma que se asegure el funcionamiento de la red ante incidencias en ese camino.

Del LDRA y LDRB salen múltiples enlaces de fibra a distintos armarios de comunicaciones donde hay switches de acceso y también enlaces a los nodos principales de cada nave.

Del nodo LDRA cuelgan los nodos de comunicación principales N1-00, N2-00, N3-00, N2AB-00. Del nodo LDRB cuelgan los nodos principales N5-00, N2AB-00 y N3-00. El nodo principal N1A-00 cuelga de los nodos principales N1-00 y N3-00.

De cada uno de los nodos de comunicación principales de cada nave cuelgan distintos armarios de comunicaciones que se distribuyen por cada una de las naves.

En cuanto a velocidades, se dispone de conexiones a 1 Gbps entre las capas Core y Distribución, y Distribución y Acceso, y conexiones de 100 Mbps entre la capa de Acceso y los puestos de usuario.

Para fibra óptica se utilizan conectores de tipo LC para monomodo, ST para multimodo de 62.5/125 y tanto LC como SC para fibra óptica multimodo de 50/125.

Para facilitar la conexión de los elementos, las fibras acaban en paneles de parcheo, en el caso de que estas no se usen, en este debe colocarse el correspondiente protector. Para la unión de los paneles a los equipos finales se utilizan latiguillos.

En el caso de par trenzado de cobre, utilizado para la capa de Acceso, también se utilizan paneles de parcheo, que se unen con los dispositivos finales mediante los correspondientes latiguillos con conector RJ45.

2.9 Comunicación entre redes.

Para el enrutamiento interno, entre los distribuidores se utiliza el protocolo OSPF (Open Shortest Path First). Este es un protocolo IGP (Interior Gateway Protocol) de tipo Link State basado en el algoritmo de Dijkstra. Las razones principales de uso de este protocolo en el ámbito interno de la empresa es su estabilidad, su estandarización y aparición en diversas RFCs y que por lo general la cantidad de tráfico generado es pequeña en comparación con otros protocolos como RIP.

OSPF, al tratarse de un protocolo dinámico requiere de poca carga administrativa, pues al añadir o quitar subredes, el protocolo lo detecta y actualiza sus tablas e informa a sus vecinos de forma automática e inmediata.

Capítulo 3- Procesos Intermedios. Pasos previos al proyecto.

La planificación inicial de la empresa respecto al cambio de las redes y la implantación del concepto NAC era realizar la migración de forma independiente para cada una de las dos redes, corporativa e industrial, y una vez realizada esta migración implementar pruebas piloto con NAC hasta finalmente incluir el concepto como solución en toda la red.

Para la realización de este cambio, uno de los primeros pasos fue el desarrollo del documento RFI (Request For Information) para el cambio de únicamente la electrónica de la red corporativa y el backbone de fibra óptica.

Este documento tenía por objeto solicitar información sobre propuestas de renovación de la red y poder obtener así un presupuesto aproximado del coste de la obra e instalación final. Es decir, obtener una valoración tanto técnica como económica de las tareas a realizar. Se pretendía mediante la elaboración de este documento solicitar a los proveedores interesados la presentación de soluciones técnicas y funcionales para desarrollar la actualización de la red de datos de la empresa.

Este documento tenía dos lotes definidos, el Lote 1 que incluía el cambio de la infraestructura de fibra óptica de la red corporativa y la introducción de nuevos armarios de comunicaciones, y el Lote 2, que incluía todo lo relacionado con la electrónica de red. Dentro de este documento se especificaban los requerimientos a cumplir para la posterior implantación de un sistema de control de acceso basado en puertos (NAC).

Una vez realizado este documento, se decidió cambiar a la vez la electrónica de red de las redes industrial y corporativa argumentando que a un volumen mayor el precio conjunto se reduciría.

Al ser una empresa de producción, el proceso de migración e instalación de nuevos equipos debe de hacerse en días no laborables, por lo que, por temas temporales, la decisión final fue separar el Lote 1 que hace referencia al cambio de la infraestructura de fibra óptica, del cambio de la electrónica de red tanto de las redes corporativa e industrial. De esta forma hablando en plazos temporales, la consecución del proyecto evitaba atrasarse más tiempo de forma que se impidiese la instalación de la infraestructura de fibra en periodo vacacional.

Tras el giro en el proyecto de actualización de la red de datos, el siguiente paso a realizar fue la elaboración de una RFP (Request For Proposal) que englobase únicamente el Lote 1 (cambio de la infraestructura de fibra óptica de la empresa), dejando el Lote 2 para más adelante. El presente capítulo se va a centrar principalmente en el desarrollo de la ejecución de este Lote 1.

3.1 RFP Lote 1. Fibra óptica.

Para la renovación de la estructura de la red de datos mediante una consultora externa se ha elaborado una RFP. Como se ha comentado en el apartado anterior, se ha elaborado una RFP individual para el Lote 1 (Renovación de fibra óptica), dejando el Lote 2 (Electrónica de red) para más adelante.

3.1.1 Objetivo.

El objetivo del Lote 1 es la renovación de la infraestructura de cableado (fibra óptica) que componen las redes de la empresa. La RFP resultante está dirigida a los proveedores potenciales que tengan experiencia en la prestación de dichos servicios.

Mediante el documento de la RFP, se solicita a los proveedores interesados, la presentación de soluciones técnicas y funcionales respecto las diferentes estrategias y soluciones ofrecidas por el mercado, para desarrollar la actualización de la red corporativa de la empresa, siendo las tareas a acometer las siguientes:

- Diseño de la nueva infraestructura de cableado de fibra óptica, que cubra con las diferentes especificaciones indicadas, y que permita a la empresa disponer de una infraestructura capacitada para los futuros.

- Propuesta de tipología de fibra que más se adapte a los requerimientos especificados en la RFP.

- Valoración de los costes relativos al suministro, instalación y certificación de la infraestructura física de red de fibra, así como elementos pasivos necesarios para cubrir con las necesidades de la empresa.

- Valoración de los costes asociados a la retirada de la infraestructura de fibra obsoleta, en función de las especificaciones marcadas por la empresa.

- Documentación de las diferentes actuaciones realizadas durante la ejecución de las actividades descritas en el presente lote, en función de los estándares la empresa.

- Valoración de los costes asociados a la adquisición de dos nuevos armarios de comunicación, así como repuestos para otros tres armarios. A su vez, en función del nuevo diseño, se deberá valorar los costes de la adquisición de cualquier otro armario que sea requerido.

- Realización de una auditoría de cableado (fibra óptica), que garantice la consecución de los objetivos marcados en el presente pliego, y verifique la idoneidad del diseño de la arquitectura de la red de la empresa.

- Documentación e integración de toda la infraestructura instalada en la documentación existente en formato HLS (*Hallem Layout System*) [54] en la empresa. Es un formato propietario de la empresa para la gestión y visualización de planos y documentos.

3.1.2 Condiciones de la propuesta.

Dentro del documento de la RFP se definen diferentes apartados que concretan el formato de la respuesta por parte de los proveedores tanto en los elementos técnicos, económicos y temporales.

En cuanto a plazo temporal, el adjudicatario del lote 1, debe disponer de la infraestructura física de fibra necesaria, lista para ser desplegada en un plazo máximo de un mes desde la firma del pedido resultante del pliego de prescripciones técnicas.

La totalidad del proyecto deberá realizarse en los plazos establecidos previamente con la empresa y quedando supeditados al calendario productivo de la organización.

En el documento se establecen diferentes condiciones obligatorias de proceso a cumplir por todos aquellos proveedores con interés en ofertar.

Estas condiciones se establecen en forma de hitos siguiendo el siguiente orden:

1. Visita conjunta por parte de los proveedores a las instalaciones de la empresa.
2. Recepción de preguntas por parte de los proveedores a la empresa.
3. Respuesta de preguntas.
4. Recepción de la oferta técnica y económica.
5. Estudio de las ofertas de los proveedores.

Respecto a la presentación de las ofertas, en el documento RFP se detalla el formato y el modo de recepción de las mismas, permitiendo tanto correo electrónico como convencional.

El diseño de la nueva infraestructura de fibra óptica que pretende dar servicio a la empresa debe garantizar que se alcancen los objetivos marcados en el documento de la RFP.

Por ello, los proveedores deberán presentar una propuesta de diseño, o actualización de la infraestructura de fibra actual garantizando los mayores niveles de calidad, optimizando costes y cumpliendo en todo caso con los requerimientos especificados a tal efecto por la empresa.

En función de la estructura actual existente, se pretende reemplazar la totalidad de la fibra 62.5/125 Multimodo, por la fibra más adecuada en función de la tirada necesaria.

Aun así la empresa está abierta a recibir propuestas en este sentido, que garanticen el cumplimiento de los objetivos marcados, reduciendo costes.

Dentro del documento de la RFP se facilita al ofertante información sobre las tiradas actuales de fibra, así como el número de fibras nuevas a instalar por tirada y una estimación de los metros.

Al tratarse de estimaciones, el ofertante deberá asumir hasta un 15% de diferencia entre las mismas y la situación real, Por ello, dicha información a su vez deberá ser ajustada antes del inicio del proyecto, en la fase de replanteo del mismo.

En caso de que la diferencia sea mayor que el 15%, se debe comunicar este hecho a la empresa antes de la realización del proyecto para que la misma aporte una solución al respecto.

3.1.3 Requerimientos tecnológicos y especificaciones de servicio.

En cuanto a características técnicas del nuevo tendido de fibra, se especifica que estos deben ser:

- Tendidos de fibra de 9 / 125 Monomodo, para interconectar las diferentes Naves existentes.
- Tendidos de fibra de 50 / 125 Multimodo para comunicar los armarios de comunicaciones de las naves.

La nueva fibra empleada deberá disponer, como mínimo, de las siguientes características:

- Deberá ser fibra del tipo OM3 y OS2
- Deberá disponer de protección anti-roedores.
- Deberá disponer de protección anti-tracción (kevlar).
- No deberá propagar halógenos.
- Deberá estar libre de silicona.
- Deberá poder emplearse tanto en exteriores como en interior.
- Deberá poder emplearse en los diferentes medios de canalización existentes en la empresa, siendo estas bandejas interiores, aéreas o canalizaciones subterráneas (tanto sumergidas como no sumergidas), entre otros. En aquellos casos en que se requieran nuevas canalizaciones (canaletas, bandejas, etc.), estas deberán ser propuestas por el proveedor, y su instalación deberá ser aprobado la empresa.

La instalación de la fibra únicamente puede ser desarrollada por empresas que dispongan de la certificación correspondiente del fabricante ofertado, la cual les permita diseñar, instalar y certificar infraestructuras de fibra.

Respecto dicha instalación, todas las conexiones de la fibra deberán realizar mediante fusionado con pigtail, debiéndose valorar en la propuesta de manera independiente los costes asociados a dichas fusiones (3000 fusiones en total). Un pigtail es un latiguillo de fibra óptica el cual cuenta con una fibra descubierta en uno de los extremos para ser empalmado a la fibra del cable principal mediante fusión. En el otro extremo cuenta con un conector que sirve de interfaz con los equipos. Cuando se afirma que todas las conexiones de fibra deben realizarse mediante fusionado con pigtail, a lo que se hace referencia es a la fusión de este latiguillo de fibra con el cable de fibra principal, el conector del pigtail termina por tanto en los paneles de parcheo de fibra del armario de comunicaciones en el que finalice.

En función de las nuevas tiradas de fibra dimensionadas por la empresa (53), se deberán valorar los costes asociados al suministro e instalación de los elementos de interconexión necesarios para el correcto funcionamiento de la infraestructura.

Respecto los Patchs Panels, pigtails, y conectores estos deberán ser del mismo fabricante que la fibra ofertada. Los conectores a emplear en los mismos serán LC.

Toda la instalación de cableado deberá estar certificada, por el fabricante de la misma, de extremo a extremo, aportando la documentación que garantice el correcto funcionamiento de la misma.

Dicha certificación deberá realizarse por los estándares de IEEE, de TIA/EIA, o de ISO/IEC y deberá de tratarse de una certificación completa, de nivel 1 (régimen básico de control) y 2 (régimen extendido de control).

La certificación del cableado de nivel 1 deberá ser realizada con un medidor de potencia (el cual deberá disponer de los certificados de calibración anuales) y una fuente luminosa o un conjunto de comprobación de pérdida óptica, para medir la pérdida absoluta del enlace y compararla con los límites del estándar. Dichas certificaciones deberán poderse leer y gestionar con el software LinkWare de Fluke Networks.

La certificación de nivel 2 y la solución de problemas deberán llevarse a cabo con un OTDR.

En ambos casos, la certificación deberá incluir la longitud de la fibra y la pérdida óptica en dos fibras a dos longitudes de onda diferentes, indicando la pérdida máxima permitida, y especificando si dicha fibra PASA o FALLA los controles del estándar seleccionado.

En todos los casos, la certificación deberá ser positiva, y en aquellos casos contrarios, será responsabilidad del proveedor, realizar las tareas necesarias para mitigar esta situación, asumiendo los costes que se puedan desprender.

En cuanto a las fibras antiguas, el proveedor deberá presentar un plan para la retirada de la fibra obsoleta.

Este plan deberá contemplar tanto la retirada de la fibra sin uso, como las actuaciones necesarias para aquellas fibras que no puedan ser retiradas por la complejidad técnica que podría suponer (por ejemplo, en los casos de fibras que pasan por arquetas inundadas o incluso cerradas).

En estos casos, como norma general se procederá al corte físico de la misma, y al etiquetado de la fibra tanto en origen como en destino. Dicho etiquetado deberá garantizar la durabilidad de la información contenida, y deberá indicar como mínimo el origen y final de la tirada, fecha del corte, tipología de la fibra, y la finalidad para la que se empleó.

3.1.4 Contenido y estructura de la respuesta

Dentro del documento de la RFP se especifica la estructura de la respuesta técnica y económica para facilitar el análisis y evaluación de las mismas.

Las contestaciones presentadas deberán contener todos los elementos de información especificados en la RFP. La empresa se reserva el derecho de excluir todas aquellas propuestas que no se adecuen al formato y condiciones descritas.

El ofertante podrá adjuntar a su contestación toda la información complementaria a la solicitada que considere de interés.

Los entregables mínimos a presentar son un resumen ejecutivo, la oferta técnica, prestaciones superiores o complementarias a las exigidas, referencia de la empresa y credenciales profesionales y la oferta económica.

Como se ha comentado, la propuesta debe incluir un breve resumen ejecutivo que contendrá las principales ventajas y beneficios de la solución propuesta. Debe contener una visión general de la solución presentada incluyendo los puntos clave y el enfoque utilizado. En este resumen debe incluirse también una breve presentación del proveedor así como de sus experiencias más destacadas en proyectos similares. Se incluirán también los responsables de la gestión del proyecto.

En cuanto a la oferta técnica, se redactará un breve resumen de la solución propuesta respecto a los requerimientos tecnológicos y especificaciones de los servicios especificados en la RFP y resumidos en este documento.

Dentro de la oferta técnica, a parte del resumen de la solución propuesta, se redactará un informe descriptivo detallado de las características técnicas de la solución propuesta.

Este informe incluirá la siguiente información:

- Planificación global del presente lote, indicando los tiempos necesarios para el desarrollo de cada una de las tareas que los compone, en formato Project.
- Descripción del diseño de la infraestructura de fibra propuesto, así como las características del mismo.
- Planificación de la auditoría de cableado (fibra óptica), y especificaciones técnicas de la misma.
- Descripción de la tipología de fibra a emplear, especificando las características de la misma.
- Detallar las características del proceso de instalación de la fibra, especificando una estimación de los tiempos necesarios. En este apartado se deberá incluir de manera independiente las características y planificación del proceso de fusionado, y los aspectos relativos a la instalación de los elementos pasivos necesarios.
- Indicar la propuesta de plan de pruebas y contingencias, que garanticen la continuidad de los servicios de la empresa durante la ejecución del proyecto.
- Detallar las especificaciones de retirada de la fibra obsoleta, y las diferentes especificaciones para los escenarios coexistentes en la empresa.
- Costes específicos de cada una de las actividades que componen el presente lote.

La oferta técnica incluirá cualquier información gráfica (esquemas, gráficos, planos, etc.) que el ofertante considere necesarios para describir la propuesta presentada.

En la oferta económica se presentarán los precios globales y detallados de la oferta, presentados en EUROS (€).

3.2 Seguimiento del Lote 1. Análisis.

Tras la elaboración del Lote 1, el cual se ha descrito en el apartado anterior, se ha elaborado una lista con una serie de fabricantes introduciendo en ella a instaladores de fibra locales. Esta lista se ha reenviado a la sección de compras de otra sede de la multinacional en España y de ahí a la sede central de la multinacional en conjunto con la RFP para su revisión.

Este proceso es costoso y debido a ello hay que realizar un replanteo de las fechas. La publicación de la RFP prevista no depende de la sede local sino de la sede central y del departamento de compras el cual es el encargado de publicar esta RFP.

El factor tiempo es importante en la ejecución de este lote puesto que la realización de la instalación de fibra requiere en muchos casos el paro de la producción por lo que hay que aprovechar para realizarla en el mes de vacaciones durante el cual la empresa carece de procesos productivos.

Tras todos los procedimientos reglamentarios se ha conseguido lanzar la RFP del lote con un retraso temporal de tres meses a la prevista instalación de la fibra. El parón vacacional se realiza del día 1 de Agosto hasta el 25 del mismo mes. La publicación de la RFP se realizó el 28 de Abril.

Para la posible participación de los ofertantes se les obliga a realizar una visita conjunta a las instalaciones de la empresa la cual se realizó finalmente el día 9 de Mayo.

El plazo establecido para la recepción de preguntas por parte de los proveedores se concretó en el día 16 de Mayo y el plazo para su contestación por parte de la empresa el día 23 de Mayo. Como fecha final para la entrega de la oferta por parte de los proveedores se establece como fecha límite el día 30 de Mayo.

Para la elaboración de la RFP y su correspondiente publicación intervienen gran cantidad de personas de diferentes departamentos y empresas. Como se ha comentado esta RFP ha sido realizada con la ayuda de una consultoría externa situada en otra localidad. Para la puesta en marcha de la RFP se necesita además lanzar un procedimiento interno que se tiene establecido dentro de la empresa para la aprobación de la consecución de proyectos, en el cual es necesario presentar un proyecto de inversión con los posibles costes del proyecto. Una vez aprobado internamente, para su correcta publicación se ha contado con el departamento de compras de otra sede nacional de la multinacional puesto que esta había renovado anteriormente su infraestructura de red y ya contaba con experiencia en este tipo de proyectos.

Todas estas colaboraciones exigen una fuerte coordinación y una comunicación constante entre el personal involucrado en la realización del proyecto por lo que semanalmente se han realizado reuniones y multiconferencias para poder mantener esta coordinación.

Durante todo el procedimiento se puede apreciar claramente la importancia de dos aspectos a la hora de la realización del proyecto.

El primer aspecto es el plazo temporal, es un concepto que se ha degradado fácilmente conforme la elaboración del proyecto. Se ha dado un retraso muy considerable entre la fecha de publicación de la RFP inicialmente prevista y la real. Esto ha sido principalmente debido a los reajustes realizados durante el proceso. Estos cambios o reajustes incluyen la modificación de la RFI inicial que contenía los dos lotes para obtener una RFP final únicamente dedicada al lote de fibra. Inicialmente en la RFP realizada en Marzo, la fecha para la visita de los proveedores a la empresa se había previsto para el día 11 de Abril cuando finalmente se realizó el 9 de Mayo, lo que significa que todos los procesos y etapas establecidas en el proyecto han tenido un retraso de un mes.

El segundo aspecto es la coordinación y necesidad de comunicación entre los miembros del grupo de trabajo. Al intervenir tantos miembros es necesario mantener un flujo constante y correcto de información entre ellos para la correcta puesta en marcha del proyecto. El hecho de necesitar la intervención de tantos miembros de diferentes sedes o empresas puede ser un factor posible al favorecimiento de la degradación del objetivo temporal.

Como se ha comentado, el día 9 de Mayo se realizó la visita a las instalaciones por parte de los proveedores. El total de empresas que acudieron fueron 6, menos de las invitadas inicialmente:

- Abast Systems
- Ampers Sistemas
- Cenorma S.L
- Fibratel
- NET Quality 2
- Orbe

Previamente a esta visita se concertó una reunión entre los miembros del proyecto en la sede de la multinacional, en la cual se intentó planificar las posibles preguntas de los proveedores, asegurando de esta forma la eficacia a la hora de responderlas.

La reunión del día 9 de Mayo con los proveedores constó de tres partes. La primera parte consistió en una presentación de los miembros asistentes tanto por parte de la multinacional como de los proveedores.

Por parte de la multinacional cabe destacar la presencia de cada una de las partes implicadas, es decir, acudió un miembro de la consultoría externa encargada de elaborar la RFP, miembros del departamento de IT de la empresa encargados del proyecto y un representante de la sección de compras de la sede ayudante de la multinacional.

En esta primera fase de la reunión se presenta un poco que es lo que la empresa quiere y se explica la RFP brevemente, reforzando los puntos clave de esta y aquellos que puedan ocasionar algún tipo de duda al proveedor.

Esta reunión es de gran utilidad a la hora de aclarar futuras dudas y permite establecer un primer contacto con los posibles ofertantes finales.

La segunda fase consiste en una visita a algunas de las instalaciones principales de la empresa como son el LDRA y el nodo N1-00 en el que se debe instalar un nuevo armario. Se visitan también brevemente las instalaciones de la empresa para que puedan ver cómo están las canalizaciones de fibra óptica y puedan calcular los costes asociados a la implementación de esta y la maquinaria necesaria como pueden ser elevadoras.

En la tercera fase se reunió a los proveedores para la resolución de dudas. De este proceso cabe destacar que no hubo ninguna. Para no favorecer a ningún proveedor y tratar de realizar el proceso de la forma más transparente posible se les comentó que la respuesta a las dudas que tuviesen se facilitaría a todos los proveedores de forma que todos tuviesen a su disposición la misma información.

Durante el proceso del proyecto del Lote 1 se pueden apreciar desviaciones frente a lo previsto y lo realizado finalmente. Esto se puede ver en dos puntos distintos, la propia RFP y la visita a las instalaciones por parte de los proveedores.

En el primer punto, la RFP, cabe comentar que tras ser publicada y adquirida por los proveedores invitados fue necesario realizar algunas modificaciones sobre ella las cuales fueron explicadas a los proveedores durante la reunión del día 9 de Mayo. Principalmente los cambios fueron dos:

-Camino redundante: En la RFP del Lote 1 se indicaba que la tirada de fibra entre el LDRA y el LDRB debía realizar por dos caminos distintos, tirando dos mangueras de 120 fibras por cada uno de ellos, sin embargo, esto finalmente no se va a realizar de esta forma. Los proveedores deberán instalar únicamente una manguera de 120 fibras por un único camino. Se ha tomado esta decisión por la ausencia de un camino redundante y por la existencia de un proyecto de la empresa que consiste en la construcción de una nueva nave la cual también estará conectada con los LDR y por tanto es una buena opción para crear el camino redundante entre los nodos principales. Es decir, la construcción de un camino redundante para los nodos principales LDRA y LDRB se realizará en un proyecto a parte que el actual.

-Auditoría de cableado: En la RFP se anexa un documento para la realización del presupuesto de la oferta económica que es estándar de la multinacional. Este constaba con un apartado destinado a la auditoría del cableado. Los proveedores debían presupuestar el coste de la realización de una auditoría de fibra óptica a las fibras ya presentes en la multinacional, sin embargo, para poder realizar esta auditoría es necesaria la desconexión de las fibras y este factor es inviable a no ser que se pare la producción. Como decisión final se les comunicó a los proveedores que este apartado no debía tenerse en cuenta. Durante el transcurso de la reunión los miembros del departamento de IT de la empresa decidieron una solución alternativa, la realización de una auditoría únicamente de las fibras instaladas pero no en uso. Tras esta decisión se rectificó lo acordado con los proveedores comunicándoles el nuevo cambio.

El segundo punto de cambios frente a lo previsto se realizó durante la visita a las instalaciones. Se tenía previsto visitar dos nodos principales de nave y el LDRA, además de dar una vuelta de reconocimiento a la nave N1 para que los proveedores pudiesen tener una idea genérica de la infraestructura actual de redes. Finalmente sólo se visitó el LDRA y un nodo principal de nave, y sobre la visita a la nave N1, se realizó de manera breve puesto que no se disponía de calzado de seguridad para los proveedores, el cual es necesario llevar por normativa de la empresa.

Como solución se decidió realizar un reportaje fotográfico de las instalaciones por parte del departamento de IT de forma que los proveedores pudiesen tener una mejor idea de la infraestructura a actualizar. Además quedó pendiente la idea de poder realizar visitas en grupos reducidos de proveedores de forma que el desplazamiento por las naves fuese más fácil y viable. Finalmente con el documento fotográfico fue suficiente.

Tras la reunión con los proveedores se reenvió a los mismos el documento de la RFP incluyendo las modificaciones comentadas, es decir, la auditoría de cableado y quitando el camino redundante entre el LDRA y LDRB.

Una de las fechas establecidas en el documento RFP era la recepción de preguntas. Cabe destacar que de los 6 proveedores que acudieron a la reunión sólo dos proveedores han enviado consultas. En la siguiente Figura 7 se puede apreciar el documento con las preguntas formuladas por los ofertantes.

Nº Pregunta	RFP	Consulta
1	1 (Documentación)	¿El plano de recorridos tiene que ser dibujado en formato HLS con los nombres de archivo y capas específicos del grupo o basta con que esté dibujado en MicroStation? - En caso que la respuesta sea en HLS, proporcionarán los planos base de fábrica para poder dibujar o hay que realizarlo en sus instalaciones o subcontratarlo?
2	4.1.1	¿Qué se valora como mejora técnica?
3	4.1.1	¿Qué peso tienen en el proceso de adjudicación de la oferta?
4	4.1.1	¿Cómo se deben incluir los costes adicionales de la mejora en la oferta? ¿Cómo ampliación de la oferta base?
5	4.1.1.3. (Fusionado con pigtail)	En los costes separados de las fusiones, ¿Se deben incluir aquí los costes de las certificaciones?
6	4.1.1.3 (Servicios)	¿Nos pueden facilitar el precio del alquiler de la caseta de obra que será necesaria disponer en las dependencias de la empresa?
7	4.1.1.4. (Elementos de interconexión)	¿Hay que incluir los latiguillos de fibra óptica? - En caso afirmativo, cuantos y de que longitud?
8	4.1.1.7. (Retirada de FO)	¿En qué fecha tiene que estar toda la infraestructura de fibra certificada y operativa para que se pueda empezar a instalar la nueva electrónica de red?
9	4.1.1.7. (Retirada de FO)	¿En qué fecha estará toda la nueva electrónica de red operativa para empezar a desinstalar la fibra obsoleta?
10	4.1.1.7. (Retirada de FO)	¿Hay plazo de tiempo para terminar la desinstalación de fibra?
11	4.1.1.8. (Otras Actuaciones)	Los nuevos Armarios a instalar, ¿Deben ir electrificados?
12	4.1.1.8. (Otras Actuaciones)	¿En caso afirmativo, del mismo modelo y potencia de rPDU que tienen?
13	4.1.1.8. (Otras Actuaciones)	¿El del LDR.B tiene que ser redundante de los dos SAI's?
14	4.1.1.8. (Otras Actuaciones)	¿Hay que conectarlas a la Red y Configurarlas en el sistema de gestión?
15	6.2.1 (Auditoría)	Referente a la auditoria del estado de las fibras se solicitará la certificación o medición e de potencia, o ambos documentos como en los tendidos nuevos. Las mediciones se realizarán en ambos sentidos o en un único sentido de los tendidos FO?
16		¿Existen zonas donde sea obligatorio disponer de medios de elevación tipo diésel o especiales, y que no sean utilizables en los interiores de los talleres?
17		Cuanta canalizacion adicional se estima que habra que instalar?
18	5.3	Que diferencia hay entre la criticidad de los armarios?

Figura 7-Consultas RFP de los ofertantes.

En la primera columna se encuentra el número de pregunta, en la segunda el apartado de la RFP al que se hace referencia, y en la tercera columna la pregunta formulada por el proveedor.

Tras la recepción de preguntas se organizó una reunión con los miembros del grupo para decidir la respuesta de las mismas.

Se han recibido un total de 16 preguntas. Las dos últimas preguntas fueron añadidas por la empresa con el fin de aclarar conceptos que no se creía que estuviesen claros.

La pregunta 1 hace referencia a la documentación, en la RFP se especifica que los planos deben entregarse en formato HLS, el cual es propio de la multinacional. En respuesta a esto la empresa ha contestado que la documentación debe ser en HLS según la normativa del grupo, la empresa proporcionará la documentación y los planos base. Además ha añadido que para la aceptación se deberá presentar una certificación por una empresa homologada por la multinacional (T-Systems ó IPS) y que se permite la subcontratación.

En la segunda pregunta, como mejora técnica la empresa valora soluciones para ahorrar cableados en los LDR como puede ser la pre-conectorización o una forma alternativa de gestión de cableado. En cuanto al peso, la empresa contesta que estas serán tenidas en consideración.

Los costes referentes a la mejora de la oferta técnica deberán, según la empresa, entregarse como ampliación de la oferta base en el formato que la sección de compras de la multinacional considere oportuno. La sección de compras entregará un documento estándar para la presentación de los presupuestos este se puede ver en el Anexo 1.

En cuanto a la pregunta 5 referente a las fusiones de los pigtail, sí se deben incluir los costes de las fusiones individuales de los pigtail junto con las certificaciones.

La pregunta 6 está relacionada con los servicios a la hora de realizar la obra del proyecto, la empresa no proporciona la caseta. En este sentido, sólo aporta las características de la misma y el lugar de su ubicación. Se cobra por los servicios en caso necesario de agua, luz, telefónica, dato, etc. La caseta debe ser alquilada por el ofertante que a su vez correrá con los gastos de transporte, montaje y desmontaje.

En cuanto a los latiguillos se ha decidido que se valore la instalación de 700 de 3 metros cada uno con conectores LC en ambos extremos. (100 monomodo y 600 multimodo de 50/125). Aunque en la instalación real se van a encontrar necesidades de latiguillos de mayor medida estos van a ser muy pocos y la mayoría serán de 3 o menos metros.

Como fecha límite para la terminación de la infraestructura de fibra óptica se ha decidido el 2 de Noviembre del 2014 y la electrónica de red se afirma que estará operativa el 19 de Enero del 2015. En cuanto al plazo de tiempo de desinstalación de la fibra óptica la empresa estima que debería estar terminado para el 31 de Diciembre del 2015, ya que se realizará una vez se acabe también el proyecto del cambio de la electrónica de red. Pero esta fecha dependerá también de los proyectos vinculados a las instalaciones donde se procederá a realizar la retirada.

La respuesta para las preguntas 11, 12, 13 y 14 es afirmativa en todas ellas.

La respuesta a la auditoría del estado de las fibras se afirma que debe de ser la misma que se especifique para las fibras nuevas.

Sobre elevadoras especiales se explica que no se necesitarán tipo diésel puesto que no se van a realizar trabajos por el exterior por tanto deben de ser eléctricas. Y se puntualiza la

posibilidad de necesitar algún tipo de elevador especial por altura o por menor ancho de cesta y la posible necesidad de instalar andamios homologados.

Sobre la canalización se ha estimado la necesidad de 1000 metros de canaleta de 300x100 sin tapa y con soportería puesto que se sabe que parte de la canalización existente está estropeada y otra parte no es accesible y por tanto no se va a poder realizar el tendido de fibra por la existente.

En cuanto a la criticidad de los armarios se ha adjuntado como respuesta la siguiente tabla aclaratoria:

Criticidad	Definición	Especificaciones
Alta	Contiene elementos críticos que pueden afectar a la producción de la empresa a corto plazo.	Se deberá disponer de un plan específico de implantación. La actuación se deberá planificar conjuntamente con otros mienbros de la empresa con riesgo de verse afectados. La actuación se debera realizar fuera de los horarios productivos
Media	Contiene elementos críticos que pueden afectar a la prodicción de la empresa a medio plazo	Puede requerir la planificación conjunta con otras aeras de la empresa. Deberá analizarse el caso y determinar una ventana de actuación concreta.
Baja	Contiene elementos que no tienen ningún tipo de afectación en la producción.	Se puede realizar la implantación en horario productivo

Paralelamente a la publicación de la RFP del lote 1 se ha realizado mediante la ayuda de la consultoría externa la RFP del Lote 2, incluyendo en lo que ya se tenía antes de separar el documento inicial en dos RFPs la parte de electrónica de red de la parte industrial.

Para poder incorporar esto al lote del cambio de la electrónica de red ha sido necesario realizar una estimación de las bocas ocupadas en los equipos de acceso, para poder realizar esta tarea de una forma sencilla se dispone de un programa propietario del fabricante, que como se ha comentado es Avaya (Actual Nortel) el cual permite ver gráficamente el switch de forma remota además de configurarlo, por tanto, mediante esta aplicación se ha obtenido la información necesaria para el cálculo.

Capítulo 4- NAC, 802.1X y Zonas de Seguridad.

Uno de los motivos de la actualización de la infraestructura de red es la incorporación de la solución NAC (Network Access Control). Para la implantación de este concepto de seguridad es necesario tener una electrónica de red compatible, esta es una de las motivaciones del cambio.

Este sistema tiene como objetivo asegurar que todos los dispositivos que se conectan a las redes corporativas de una organización cumplen con las políticas de seguridad establecidas para evitar amenazas como la entrada de virus, salida de información, etc.

El fenómeno BYOD (Bring Your Own Device) en el que los empleados utilizan sus propios dispositivos (tabletas, portátiles, smartphones) para acceder a los recursos corporativos está acelerando la adopción de las tecnologías NAC para autenticar al dispositivo y al usuario.

Cuando una empresa tiene una red a la que se pueden conectar usuarios, tiene como objetivo controlar el acceso de los usuarios a esta y a qué servicios puede acceder, o al menos asegurar que sólo los usuarios autorizados tienen acceso a la red. Esto es exactamente lo que las aplicaciones NAC permiten hacer.

El concepto de NAC se basa en la norma 802.1X [5] de la IEEE para el control de acceso a la red basada en puertos, este estándar permite la autentificación de los dispositivos conectados a un puerto de un conmutador. En la actualidad se ha extendido y se usa también en redes wireless. La norma 802.1X es un vínculo de autentificación estándar que se encarga de agregar la autentificación RADIUS (Remote Authentication Dial-In User Service) y EAP (Extensible Authentication Protocol – Protocolo de autentificación extensible).

EAP especificado en la RFC2284, es un protocolo utilizado para el transporte de la información de identificación del usuario. Este protocolo permite transmitir información entre el suplicante y el servidor de autentificación.

Hay varios protocolos soportados por el estándar 802.1X pero el que destaca sobre todo los demás es EAP. De hecho EAP es sólo un estándar para intercambiar mensajes con información de autentificación entre los distintos elementos de un proceso de autentificación basado en 802.1X.

En la comunicación definida por el estándar 802.1X intervienen tres elementos (Figura 8):

-Un controlador de acceso llamado autenticador, que se encarga de otorgar o denegar a un usuario el acceso a la red. El controlador de acceso es un firewall básico que actúa como intermediario entre el usuario y el servidor de autentificación.

-El usuario o cliente de este sistema recibe el nombre de solicitante o suplicante.

-Servidor de autentificación (generalmente RADIUS).

El suplicante y el autenticador envían mensajes EAP mediante un software instalado en los dispositivos. El autenticador y el servidor de autentificación envían mensajes mediante el protocolo RADIUS, encargado de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1812 UDP para establecer sus comunicaciones.

En la Figura 8 se pueden apreciar los tres elementos que conforman la comunicación 802.1X así como los protocolos utilizados para comunicarse entre ellos.

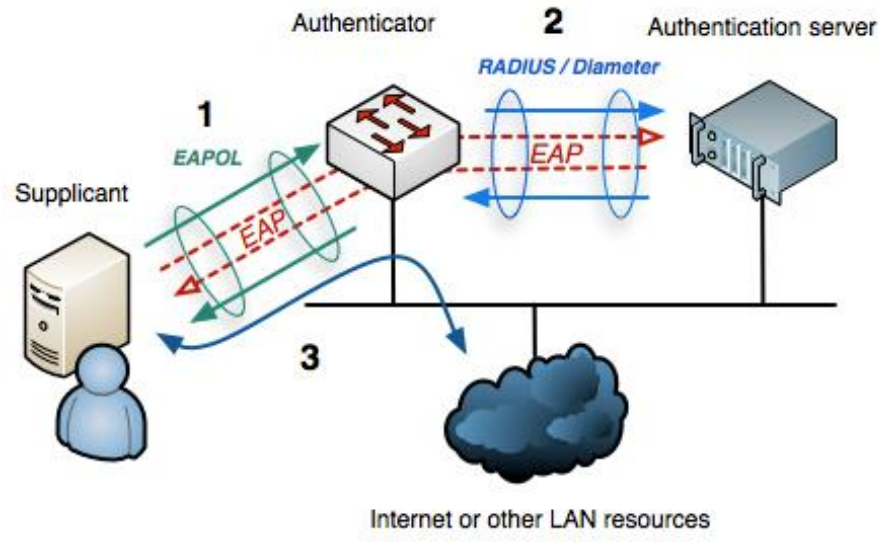


Figura 8- Esquema del proceso de autentificación NAC. [6]

Los datos EAP [7] primero se encapsulan en tramas EAPOL (EAP sobre Ethernet) que se envían entre el suplicante y el autenticador, luego son reencapsuladas generalmente en RADIUS para ser enviadas al servidor de autentificación. Los protocolos nombrados se describen a continuación.

4.1 Protocolo EAP

Como se ha comentado, EAP se utiliza en el proceso de autenticación para intercambiar información entre suplicante y servidor de autenticación. Consiste en un encapsulado que puede correr sobre diferentes niveles de enlace. Las tramas deben ser soportadas por el suplicante y el servidor de autentificación, para ello, en el caso del estándar 801.1X se utiliza EAPOL (EAP Over LAN), que permite transportar EAP directamente sobre el nivel de Ethernet. Esta es la utilización de EAP para redes de área local (LAN) y es la que se va a definir.

Cuando este protocolo es soportado por estos tres elementos, el suplicante, el autenticador y el servidor de autentificación, entonces es más sencillo adquirir los credenciales de autentificación. El autenticador sólo permite el paso de mensajes de tipo EAP del suplicante que quiere conectarse a la red, filtrando cualquier otro tipo de tráfico hasta que no se haya completado la autorización.

EAP proviene de las tecnologías PPP y del acceso por línea conmutada (Dial Access). Se definió por primera vez en la IETF RFC 2284 en el año 1998.

La siguiente Figura 9 muestra el formato de la trama EAP:

Figura 9-Trama EAP

El campo de código (Code) indica el tipo de paquete EAP. Los distintos tipos son:

1	Request
2	Response
3	Success
4	Failure

El campo de ID (Identificador) es un byte que permite identificar las solicitudes (request) con las respuestas (response).

El campo Length (Longitud) es el número de bytes del paquete EAP incluyendo el campo de código, ID, el de longitud y los datos.

El formato del campo de datos varía dependiendo del campo de código. Los tipos 3 y 4, Success y Failure no tienen campo de datos (0 bytes). Los tipos 1 y 2 comparten el mismo formato. Este se reduce a un código que indica el tipo de datos, y otro campo que son los propios datos. El paquete EAP con datos (Tipos 1 y 2) quedaría de la siguiente manera:

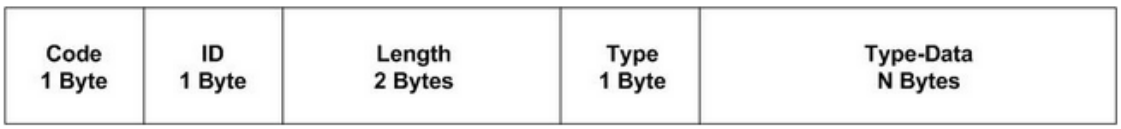


Figura 10-Trama EAP con datos.

4.1.1 EAPOL

En un medio LAN, el estándar 802.1X necesita alguna forma de permitir la comunicación entre el suplicante y el autenticador. Esto ocurre directamente sobre la capa de enlace (Layer2). El protocolo utilizado es EAPOL que permite la encapsulación de EAP sobre una red LAN.

Si tenemos en cuenta el formato de la trama a nivel de Ethernet que se aprecia en la Figura 11, la posición del paquete EAP se colocaría dentro del campo de datos (Data).

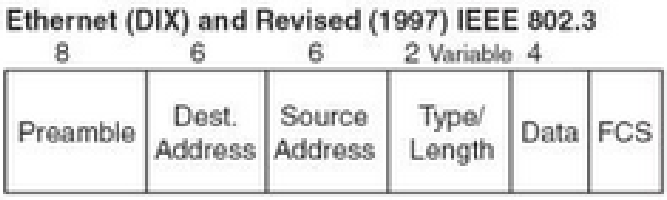


Figura 11-Trama Ethernet

Por tanto la trama EAPOL (EAP encapsulado en Ethernet) quedaría de la siguiente manera:

Destination MAC 6 Bytes	Source MAC 6 Bytes	EtherType Code 2 Bytes	Protocol Version 1 Byte	Packet Type 1 Byte	Body Length 2 Bytes	Packet Body
		0x888e	1		# of bytes	

Figura 12-Trama EAPOL.

Como se puede ver en la imagen, los tres primeros campos pertenecen a la cabecera de Ethernet. El campo Ethertype indica que protocolo se encapsula dentro de la trama Ethernet, en este caso es EAP. Esta asignación de protocolos se puede comprobar dentro de los documentos de la IEEE (http://standards.ieee.org/develop/regauth/ethertype/eth.txt).

Se puede apreciar que ha desaparecido del paquete EAP encapsulado el campo ID de cabecera que permitía identificar una respuesta a una petición, esto se debe a que al ir sobre el nivel de enlace ya se pueden identificar los extremos mediante sus direcciones MAC, por lo que este campo no es necesario.

Los siguientes campos pertenecen a la trama EAP. El primero indica la versión del protocolo. El segundo campo indica qué tipo de paquete EAP contiene. Existen los siguientes tipos:

0	EAP Packet
1	EAPOL Start
2	EAPOL Logoff
3	EAPOL Key
4	EAPOL Encapsulated ASF Alert

El tipo de paquete EAP “Key Packet” se usa para variantes del protocolo que permiten una llave (Key) de encriptación.

El tipo de mensaje “ASF Alert EAP” se utiliza por ejemplo para enviar trazas SNMP (Simple Network Management Protocol) por un puerto donde el resultado de la autentificación ha sido no autorizado.

Como se ha comentado, EAPOL permite encapsular paquetes de tipo EAP para enviarlos sobre una red LAN, es decir, funciona como un contenedor para estos paquetes, por lo que en el campo de datos del paquete EAPOL se tendrá un paquete EAP con el formato similar al especificado anteriormente.

La siguiente Figura 13 muestra el modo de funcionamiento del protocolo. Básicamente este proporciona un contenedor en capa 2 para transportar la información EAP entre el suplicante y el autenticador. El autenticador utiliza un protocolo estándar, normalmente RADIUS, para reenviar la información desde y para el servidor de autentificación, encapsulando los paquetes EAP dentro de este protocolo.

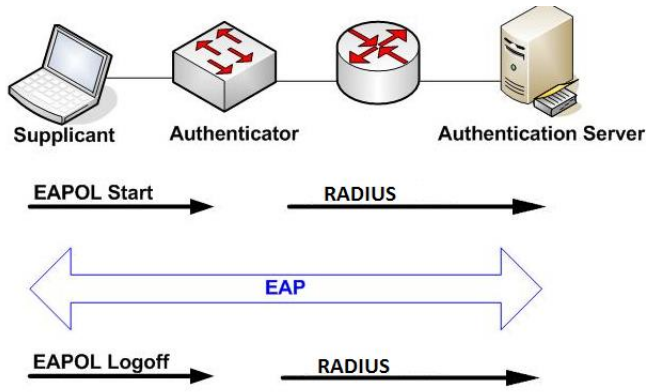


Figura 13-Esquema transmisión EAP sobre EAPOL

Inicialmente los mensajes entre el suplicante y el autenticador se transmiten mediante EAPOL y el autenticador los convierte en paquetes RADIUS que envía al servidor de autentificación. Este servidor entonces negocia el tipo de autentificación EAP que son capaces de aceptar tanto el suplicante como el propio servidor y comienza a comunicarse mediante mensajes EAP para continuar con el proceso de autentificación. Algunos autenticadores no soportan todos los tipos de EAP por lo que pueden actuar como una pasarela de forma que los suplicantes se conecten directamente con los servidores de autentificación.

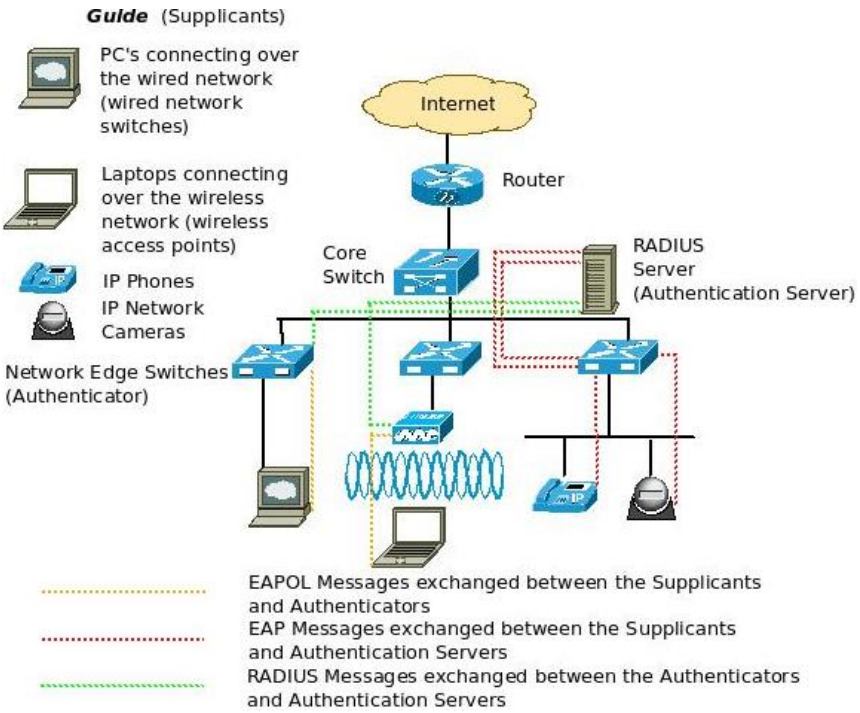


Figura 14-*Estructura de una red aplicando el concepto NAC. [8]*

En la Figura 14 anterior se aprecia como hay paquetes sobre EAPOL y RADIUS y otros que mediante EAP comunican directamente extremo a extremo.

4.1.2 Tipos de EAP

EAP es un protocolo de autentificación muy flexible que permite diferentes mecanismos de autentificación, el administrador puede elegir cuál de ellos o qué combinación usar para autentificar a los usuarios que esperan conectarse a la red. EAP permite combinar distintos tipos de autentificaciones, por ejemplo, se puede combinar una autentificación basada en Usuario-Contraseña y otra basada en dirección MAC, un dispositivo que se quiera conectar a la red, sólo tendrá acceso si tanto el usuario y contraseña como la dirección MAC coinciden con los valores almacenados previamente en el servidor de autentificación. Hay varios tipos de métodos de autenticación que se pueden encapsular por encima de EAP, ya que como se ha comentado, este en realidad es un marco para distintos protocolos de autentificación. A continuación se van a describir algunos de los más conocidos [9]:

4.1.2.1 EAP-MD5 (EAP- Message Digest 5)

Es uno de los métodos básicos de autentificación. Utiliza el mecanismo de usuario contraseña para autentificar los credenciales. El autenticador envía un reto al suplicante (una cadena), y este tiene que probar que conoce el password haciendo un hash de la cadena enviada y de su contraseña. El suplicante prueba su identidad haciendo un hash del reto enviado y de su contraseña mediante MD5(Message-Digest Algorithm 5). MD5 es un algoritmo que permite crear hashes.

Este tipo de autentificación no suele ser usada cuando se requiere cierto nivel de seguridad puesto que es sensible a ataques 'man-in-the-middle' y a ataques de diccionario. Ofrece una protección básica.

4.1.2.2 EAP-TLS(EAP- Transport Level Security)

Es un método de autentificación basado en mecanismos criptográficos. En este método, tanto el cliente como el servidor de autentificación necesitan tener preinstalados certificados de tipo PKI (Public Key Infraestructure) para poder autentificarse mutuamente.

Al sistema que se requiere para proporcionar encriptado de clave pública (public key) y los servicios de firma digital se denomina PKI. El propósito de una infraestructura de clave pública es gestionar claves y certificados. La PKI proporciona un certificado digital que puede identificar a un individuo u organización.

La infraestructura de clave pública utiliza criptografía de clave pública, en este tipo de criptografía, la autoridad certificadora (CA) crea simultáneamente una clave pública y una privada usando el mismo algoritmo. La clave privada se le proporciona sólo a la entidad de terceros que solicita el certificado, mientras que la clave pública queda disponible en un directorio donde todas las entidades pueden acceder. La clave privada nunca se comparte con nadie ni se envía por Internet, esta se usa para desencriptar lo que manden los demás usuarios a la entidad y que ha sido encriptado con la clave pública correspondiente a la clave privada de la entidad.

Además de encriptar, permite autentificarse: esto se realiza mediante la firma de su certificado digital [10] mediante la clave privada. Cuando el resto de entidades reciben este certificado, pueden usar la clave pública la cual es conocida para desencriptarlo y verificar la firma y por tanto a la entidad. Cuando se recibe un certificado, se desencripta la firma de este mediante la clave pública y esta firma es un hash del certificado. Para comprobar la identidad de la entidad, se compara el hash obtenido al desencriptar la firma y el hash realizado del documento, si son iguales se ha verificado la identidad. En definitiva, un certificado digital es un documento electrónico que asocia una clave pública con la identidad de su propietario.

El la Figura 15 se puede ver el proceso de creación y verificación de una firma digital la cual es la base para el funcionamiento de los certificados digitales, puesto que para verificar la veracidad e integridad de un certificado es necesario comprobar la firma de la entidad que lo ha emitido.

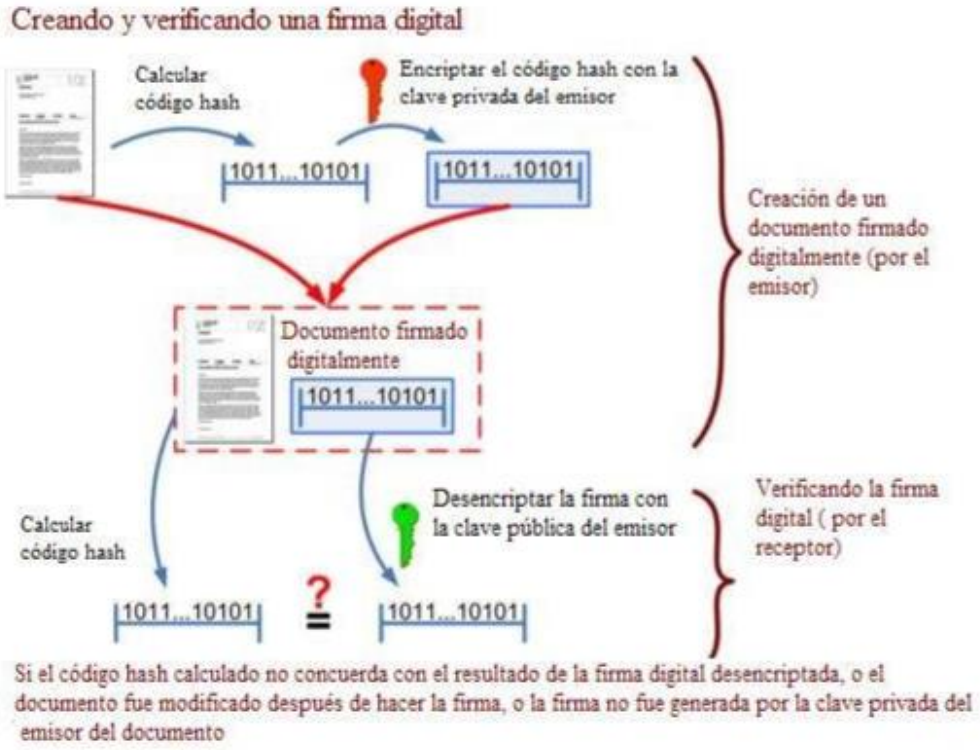


Figura 15-Esquema de firma digital. Verificación de identidad. [10]

Los certificados contienen generalmente:

- *Número de versión:* La versión del estándar X.509 a la que se atiene el certificado si usa este estándar.
- *Número de serie:* Un número que identifica de manera única al certificado y que está emitido por la entidad emisora de certificados.
- *Algoritmo de firma del certificado:* El algoritmo utilizado para crear la firma.
- *Entidad emisora:* La entidad que verifica la información y emite el certificado.

- *Destinatario:* Persona o entidad identificada.
- *Validez:*
    - Fecha de Inicio (Valid-From): La fecha en la que el certificado ha comenzado a ser válido.
    - Fecha de Fin (Valid-To): Fecha de caducidad.
- *Uso de la clave o asunto:* Propósito de la clave pública.
- *Información de la clave pública del sujeto:*
    - La clave pública.
    - Algoritmo de la clave pública.
- *Extensiones:* Información adicional del certificado.
- *Thumbprint Algorithm (Algoritmo de la huella digital*): El algoritmo utilizado para realizar un hash del certificado.
- *Thumbprint (Huella digital):* El hash del certificado.
- *Valor de la firma:* La firma actual de la entidad emisora para verificar que proviene de esta. Es la huella digital encriptada con la clave privada.

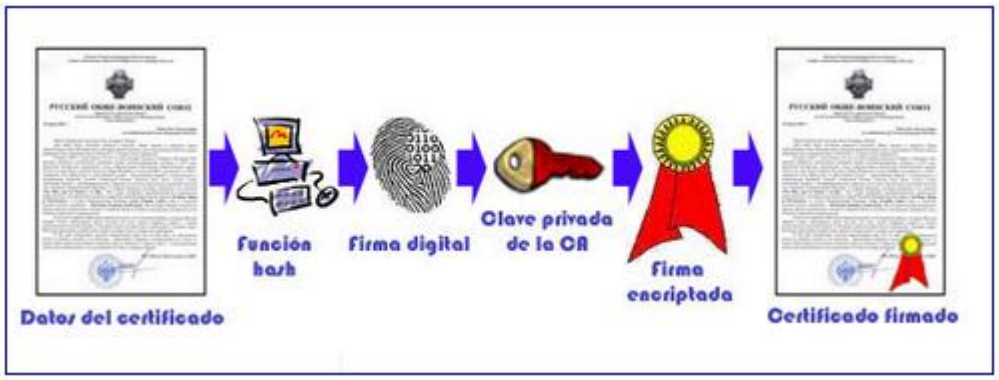


Figura 16-Creación de certificado firmado [55]

En la Figura 16 se puede ver el proceso de creación de un certificado digital a partir de un hash del certificado y de la clave privada de la autoridad certificadora.

Ya se ha explicado qué es un certificado digital, cómo se firman y cómo se verifican así como el funcionamiento de la encriptación de clave pública o asimétrica, tras esto se puede definir el concepto de PKI.

Una infraestructura de clave pública es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública. Una PKI está formada por:

- Una autoridad certificadora (CA) que emite y verifica los certificados digitales.
- Una autoridad registradora (RA) que actúa como verificador de la autoridad certificadora antes de que el certificado digital sea emitido al solicitante.
- Uno o más directorios donde los certificados con sus claves públicas son almacenados.
- Un sistema de gestión de certificados.

EAP-TLS que se basa en infraestructuras PKI, funciona de la siguiente manera:

1. El suplicante envía un mensaje de inicio EAPOL (start message).
2. El autenticador solicita la identidad del solicitante.
3. El suplicante le envía el identificador de acceso a la red (NAI) al autenticador mediante EAPOL.
4. El identificador de acceso se encapsula en RADIUS y se envía al servidor de autenticación.
5. Como se necesita un túnel encriptado, el servidor envía su certificado al suplicante.
6. Si el cliente confía en el certificado lo utiliza para encriptar los mensajes de autenticación. Dentro de esta comunicación segura en un solo sentido (del suplicante al servidor), el suplicante envía su certificado al servidor.
7. El servidor autentica al cliente y permite desbloquear el puerto del cliente.
8. El cliente recibe la información necesaria para poder comunicarse. Se le autoriza el acceso.

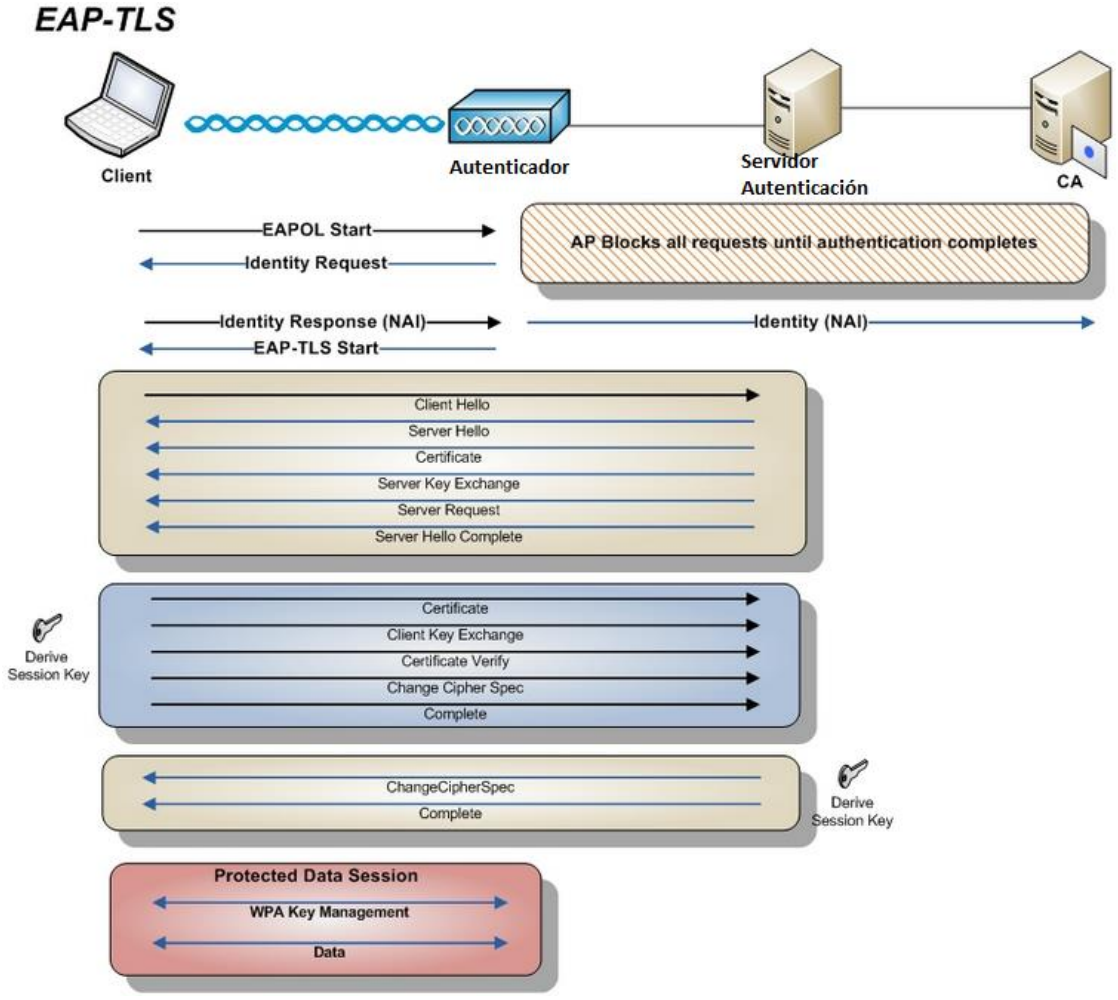


Figura 17-Esquema EAP-TLS. [56]

En la Figura 17 se pueden ver los diferentes pasos que se realizan en una autenticación EAP-TLS y que han sido descritos anteriormente.

4.1.2.3 EAP-TTLS (EAP- Tunneled TLS)

Es semejante al caso EAP TLS, la diferencia con este es que no se requieren certificados PKI por parte del cliente, es suficiente con que los clientes autentifiquen a los servidores. El servidor envía su certificado y este se utiliza para establecer un túnel de comunicación seguro entre el cliente y el servidor. La autenticación del cliente se realiza mediante usuario y contraseña transportados por este túnel seguro.

4.1.2.4 Protected EAP (PEAP)

PEAP usa seguridad de la capa de transporte (TLS) para crear un canal cifrado entre un cliente de autenticación PEAP y un autenticador PEAP. No especifica ningún método de autenticación, sino que proporciona seguridad adicional para otros protocolos de autenticación EAP.

4.1.2.5 EAP-OTP (One Time Password)

Es similar a EAP-MD5, pero en este caso no se utilizan retos si no contraseñas que sólo son válidos una vez.

4.2 RADIUS

El protocolo RADIUS [11] permite la gestión AAA (Authentication, Authorisation, Accounting) de la red y es el transporte para el protocolo EAP entre el autenticador y el servidor de autentificación.

- ✓ Authentication (Autenticación): Es el procedimiento por el que el cliente envía una petición de acceso a la red sobre la capa de enlace. Esta petición contiene los credenciales del usuario o su certificado. El autenticador empaqueta esta información en el formato RADIUS como un mensaje de tipo “Access Request” (petición de acceso). Como en este trabajo se está hablando de la aplicación del concepto NAC mediante EAP, lo que se encapsulará en RADIUS será el la trama EAP. Este mensaje de petición se reenvía al servidor de autenticación RADIUS. Este servidor comprueba su base de datos de usuarios para encontrar si es válido o no y autenticar así al usuario. Hay diferentes tipos de mensajes, Access Reject (Deniega al usuario), Access Accept (Autentifica al usuario) y Access Challenge (Pide más información).

- ✓ Authorisation (Autorización): El servidor RADIUS estipula los términos de acceso para el usuario.

- ✓ Accounting (Recuento, seguimiento): Cuando un usuario accede, se suelen querer estadísticas e información. Los servidores RADIUS permiten estos procesos, esta funcionalidad tiene que ser permitida por el autenticador emitiendo un “Accounting Start Request” al servidor RADIUS. Como consecuencia de esto, se le enviarán paquetes indicando información como por ejemplo la duración de la sesión del usuario. El proceso de “Accounting” termina cuando se envía una trama del tipo “Accounting Stop Record” al servidor.

El protocolo RADIUS utiliza los puertos UDP 1812 para Autorización y 1813 para el seguimiento (Accounting).

La trama RADIUS [12] tiene la siguiente estructura:

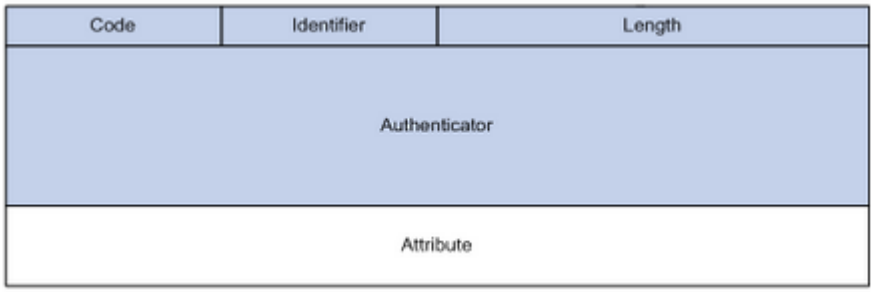


Figura 18-Trama RADIUS.

El campo de Code indica el tipo de paquete RADIUS:

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

El identificador (Identifier) permite conectar los mensajes de petición con su respuesta. Permite identificar a que conversación corresponden los paquetes.

El campo longitud (Length) indica la longitud total del paquete, la cual varía entre 20 y 4096 bytes.

El campo autenticador (Authenticator) contiene información que el cliente y el servidor utilizan para autenticarse mutuamente.

El campo de atributos (Attributes) contiene información específica sobre la autenticación y autorización además de detalles de configuración. Dentro de este campo se encapsulan los atributos los cuales cumplen el siguiente formato:

- Tipo (Type): Indica el tipo de atributo, los posibles atributos se pueden encontrar en las RFC-2869 y RFC-2865.
- Longitud (Length): Longitud del atributo.
- Valor (Value): El tamaño de este campo varía y contiene información específica del atributo.

En la siguiente Figura 19 se puede ver el formato del campo atributo dentro de una trama RADIUS.

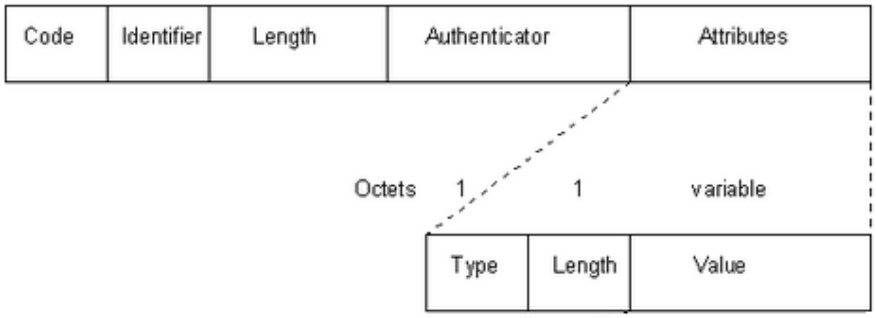


Figura 19-Trama RADIUS y atributos.

El atributo 26 (Vendor-Specific) permite al proveedor definir atributos para implementar funciones que el protocolo RADIUS estándar no tiene. En la siguiente Figura 20 se puede ver un fragmento de un paquete RADIUS con este atributo.

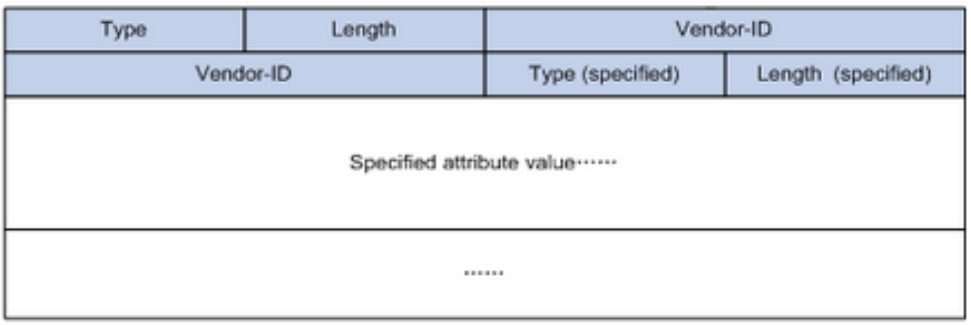


Figura 20-Trama RADIUS. Atributo Vendor-Specific.

Como se ha comentado, para transmitir la información entre el autenticador y el servidor de autentificación (RADIUS) se necesitan encapsular paquetes EAP sobre RADIUS. Para ello se utilizan los atributos “EAP-Message” y “Message-Authenticator”.

EAP-Message: Este atributo se utiliza para encapsular paquetes EAP. El valor del campo tipo es 79. El campo de string o valor puede tener un tamaño máximo de 253 bytes, si el paquete EAP es mayor, entonces puede ser fragmentado y encapsulado en múltiples paquetes RADIUS con el atributo EAP-Message. Se puede ver como se encapsulan los paquetes EAP en atributos de RADIUS en la Figura 21.

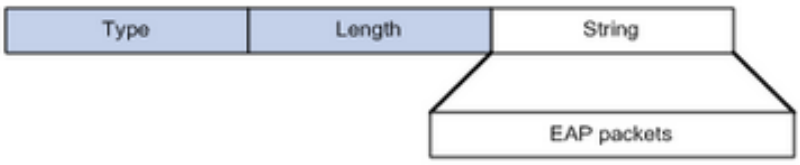


Figura 21-Atributo EAP-Message

Message-Authenticator: Este atributo se utiliza para prevenir a las peticiones de acceso de ser vistas durante la autentificación EAP. Permite verificar la integridad de los paquetes y es obligatorio en todos los paquetes RADIUS que contengan el atributo "EAP-Message".

4.3 Proceso de autentificación

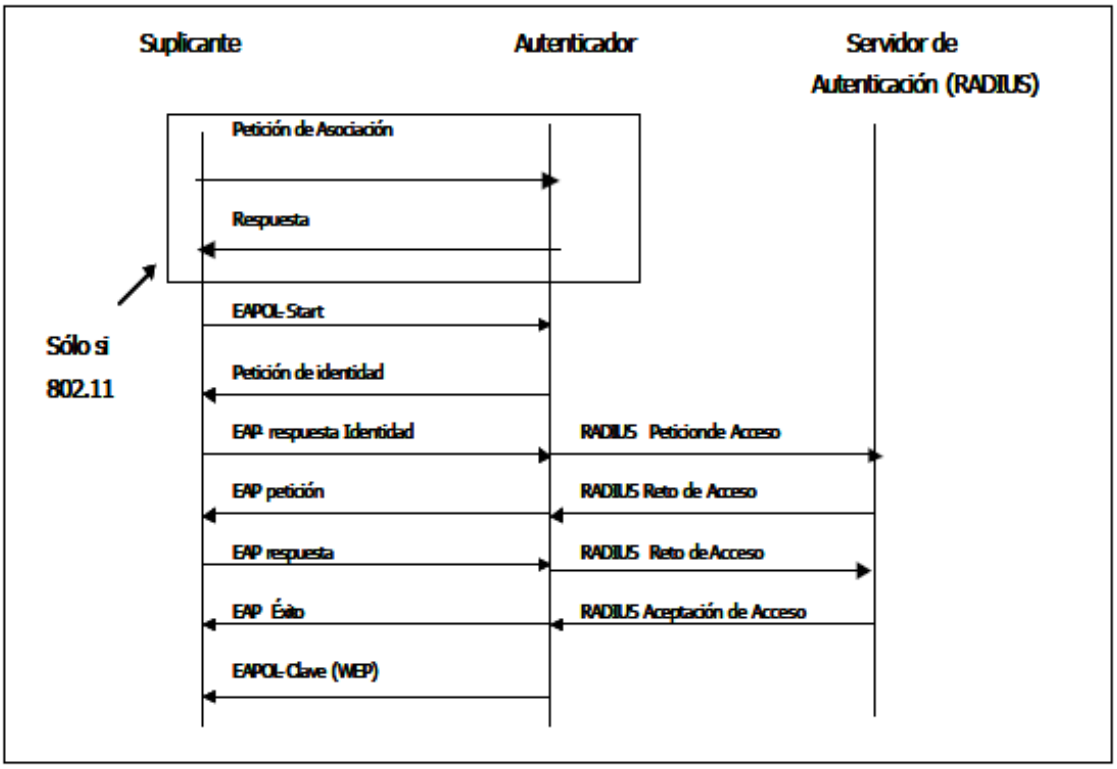


Figura 22- Diálogo de Autentificación EAPOL con/sin asociación 802.11.

En la Figura 22 se puede ver el proceso de autentificación descrito por el estándar 802.1X. El usuario, con el software suplicante realiza una petición al controlador (Autenticador) este le responde con una solicitud de autentificación. El usuario responde con su identidad y esta mediante el protocolo RADIUS llega al servidor de autenticación. Se establece un reto de acceso, hay diferentes métodos de autentificación. Si el cliente es válido, el servidor de autentificación permite el acceso del cliente.

4.4 Concepto NAC

El estándar 802.1X descrito anteriormente es una forma básica de realizar el control de acceso a la red (NAC). [13]

NAC es una solución de red que utiliza un conjunto de protocolos para definir e implementar políticas que describen como proporcionar seguridad de acceso en los nodos de red cuando los dispositivos se conectan a ésta.

802.1X es un estándar perteneciente a la IEEE (Institute of Electrical and Electronics Engineers) para el acceso a la red basado en puerto. Su propósito principal es proporcionar un mecanismo de autenticación para los dispositivos y usuarios que pretendan conectarse a redes LAN (cableadas o inalámbricas) para que solamente permitir usuarios autorizados.

NAC es un término que ha sido adoptado para nombrar a las soluciones que proveen autentificación de usuarios y dispositivos (como 802.1X) y además permite la validación de las políticas de seguridad de los dispositivos que se intentan conectar a la red. Puede haber confusión sobre las funciones y beneficios de 802.1X y las soluciones NAC. Normalmente una combinación de ambas soluciones permite proporcional un buen nivel de seguridad, control y visibilidad de la red.

A diferencia de 802.1X no hay actualmente un estándar NAC, y las soluciones mayormente comerciales utilizan arquitecturas y tecnología propietaria. La mayoría de las soluciones NAC incorporan 802.1X y añaden nuevas funcionalidades. La autenticación de los usuarios y dispositivos en NAC es muy parecida a 802.1X, de hecho muchas soluciones como se ha comentado, pueden implementar autenticación 802.1X y también otros estándares ya desarrollados en la mayoría de las redes (Directorio Activo, LDAP, etc.).

Los elementos que forman un sistema NAC varían un poco en los empleados para el estándar 802.1X aunque mantienen cierta simetría:

- Access Requestor (AR): Es el dispositivo final que pide acceso a la red. Toma un papel similar al suplicante de 802.1X
- Policy Enforcement Point (PEP): Es el elemento que permite o bloquea el acceso. (Autenticador en 802.1X).
- Policy Decision Point (PDP): El verificador o el elemento que decide si garantiza el acceso. (Servidor de autenticación en 802.1X).

A pesar de la similaridades entre 802.1X y NAC, una de las diferencias clave entre estas soluciones es el concepto del cumplimiento de las posturas de seguridad de los dispositivos finales como parte del proceso de decisión de acceso a la red. Esto significa que no sólo el usuario tiene que ser válido mediante un proceso de autenticación, sino que además debe cumplir con todas las normas de seguridad que se especifiquen, permitiendo a la solución NAC aplicar una mayor restricción mediante nuevas reglas.

Este cumplimiento de las normas de seguridad puede basarse en simples comprobaciones sobre la versión del sistema operativo (OS) o puede ser mucho más exhaustivo basándose en el tipo de dispositivo, aplicaciones instaladas, etc. Las soluciones NAC normalmente incluyen la funcionalidad de comprobar la presencia de antivirus o herramientas anty-spyware y de asegurarse de que están actualizadas y denegar o no el acceso en función de esta información. Algunas soluciones NAC incluso son capaces de comprobar la existencia de aplicaciones prohibidas u obligatorias, ficheros o tipos de ficheros completos, etc.

La parte del control de acceso de NAC puede ser realizada de diferentes formas, desde activar o desactivar un puerto físico de un switch o puntos de acceso (tal como se hace en 802.1X) hasta incluso la habilidad de activar políticas de acceso muy específicas.

Muchas soluciones NAC incorporan políticas de acceso basado en roles, esto se realiza mediante el uso de VLANS (igual que en 802.1X), permitiendo cambiar dinámicamente al puerto del switch o punto de acceso WIFI de VLAN en función del rol o grupo al que pertenezca.

Además de la validación del cumplimiento de las políticas de seguridad para permitir el acceso, NAC incorpora también los conceptos de cuarentena (o aislamiento) y saneamiento. Cuando un dispositivo final no cumple con las políticas de seguridad definidas por la empresa (por ejemplo no dispone de algún parche de seguridad para su SO), el dispositivo puede ser aislado de la red. Se considera que este dispositivo es un riesgo y se le aísla para su tratamiento.

Las principales semejanzas entre 802.1X y NAC son:

- Fuertes mecanismos de autenticación: tanto 802.1X y NAX hacen uso del estándar.
- Pre-conexión: Todos los puertos son no autorizados hasta que se hayan autenticado con éxito.
- Control de acceso basado en roles: Permite la asignación dinámica de VLANS para controlar el nivel de acceso para los diferentes tipos de usuarios.

Las principales diferencias entre 802.1X y NAC nos:

- NAC proporciona la validación del cumplimiento de directivas de seguridad para determinar el acceso.
- NAC es independiente del software en los clientes, aunque algunas soluciones sí emplean agentes en los clientes, sobre todo para las funcionalidades avanzadas.
- NAC proporciona una monitorización y control posterior a la conexión, permite asegurar el correcto funcionamiento, el cumplimiento de las políticas y reaccionar a estímulos de seguridad que pueden proporcionar los equipos de inspección de paquetes (IPS) u otros elementos. Permite la gestión y monitorización de la autenticación de forma centralizada.

La implementación NAC se puede realizar de diferentes formas, hay diferentes arquitecturas empleadas por las soluciones NAC, las más comunes incluyen Out-Of-Band, Inline y basada en agentes.

- ✓ **Basadas en 802.1X:** Algunas soluciones NAC confían principalmente en 802.1X y añaden la verificación de las políticas de seguridad vía agentes en los clientes o servidores que realizan escaneos.
- ✓ **Out-Of-Band:** Permite controlar la infraestructura de red de una forma similar a 802.1X sin la dependencia de los suplicantes o que los dispositivos soporten el estándar 802.1X. La verificación de las políticas de seguridad se pueden realizar vía

agentes en los clientes o servidores que realizan escaneos. Es una solución escalable y flexible, aunque algunas soluciones sólo funcionan con un tipo de fabricante concreto.

- ✓ **Inline:** Usan servidores o aplicaciones que se implementan directamente en el camino de los datos por lo que todo el tráfico de red debe pasar a través de ellos. No es una solución escalable y pueden requerir la implementación de un número considerable de servidores, además su implementación puede requerir de cambios en los esquemas de direccionamiento IP y otros cambios en el diseño de la topología de la red.
- ✓ **Hibrido:** Se pueden combinar varias implementaciones de forma que se logre una estructura más escalable y segura.

4.5 Implementación NAC en la empresa

Dentro de la empresa, el objetivo es la implantación de este concepto NAC y de Zonas seguras. La red de datos está expuesta a diversos riesgos especialmente derivados de la conexión de dispositivos no autorizados a la red de la empresa. Es por ello, que para proteger a las redes de éstos intentos de accesos internos no autorizados, para ello se pretende implementar un control de acceso a red (NAC).

De este modo, se incrementará el nivel de seguridad de la organización. La solución NAC debe proteger la conectividad de dispositivos finales ajenos a la empresa a las diferentes zonas de la empresa. Este concepto será aplicado a todos los dispositivos que actualmente ya están conectados, incluyendo PCs, impresoras, dispositivos multi-funcionales, y futuros teléfonos IP.

En la sede de la empresa se pretende aplicar NAC a nivel 2, es decir, únicamente la autentificación del usuario a nivel de enlace para obtener acceso a la red. Aunque algunos sistemas propietarios NAC ofrecen conectividad a la red basándose en niveles superiores de la torre OSI (Open System Interconnection), en este caso la empresa realiza este filtrado a nivel de firewall por lo que este tipo de implementaciones NAC no son de interés.

Cabe decir que ya se tiene implementada una solución de este tipo para el caso de la red de WIFI, y el objetivo final de la multinacional es obtener el mismo resultado para la red cableada. Como muestra de concepto se va a explicar muy brevemente el concepto de NAC implementado en la empresa para Wireless.

A lo largo de la empresa se reparten múltiples puntos de acceso (Access Point –AP), estos equipos carecen de inteligencia y se encargan simplemente de emitir las ondas en las dos frecuencias WIFI disponibles y actuar como una pasarela entre los clientes WIFI (Suplicantes) y el autenticador. En este caso concreto el autenticador del sistema es un controlador de la marca Cisco, este es el encargado de denegar el tráfico hasta que se haya realizado la autenticación. Como servidor de autenticación se utiliza RADIUS. Para la implementación de la infraestructura NAC de WIFI se ha utilizado Cisco ISE [14] mediante el uso del estándar 802.1X, por lo que es el servidor RADIUS ISE el encargado de comunicarse con el controlador para decirle que permita o deniegue el tráfico de un cliente.

El punto de acceso cuando recibe algo del usuario lo envía directamente al controlador WLC (Wireless LAN Controller). En el caso de que sea una petición de autenticación, tras producirse el proceso de asociación, el cual no supone que el usuario tenga acceso a la red, se inicia el

envío de paquetes EAPOL entre el suplicante (cliente WIFI) y el controlador Cisco. Mediante el uso de EAP-TLS, el controlador verifica la identidad del usuario mediante peticiones a RADIUS. En el caso de que el usuario sea correcto se realiza una petición DHCP y se le asigna una dirección IP al cliente lo que le permite la conexión a la red. En el caso de clientes que no admitan el uso de certificados, la autenticación se hace mediante una reserva de MAC. La gestión de los usuarios se realiza mediante RADIUS ISE, el servidor encargado de la autenticación y que permite gestionar a los administradores los usuarios autenticados.

Como soluciones propietarias para la implantación de la NAC únicamente se tienen en cuenta la gama de productos Enterasys Access Management [24], en su versión Netsight V4 [25] o mayor o Cisco ISE [14] en el caso de que la solución elegida a nivel equipamiento sea Cisco. Esto es así debido al libro de estándares de la empresa multinacional, el cual contiene los fabricantes admitidos y las características de los equipos de los mismos que son susceptibles de ser instalados.

A continuación, se identifican brevemente algunos de los servicios que se incluirán dentro de cada una de las zonas de seguridad determinadas por los estándares de la empresa que se muestran a continuación:

- Comunicaciones externas:
    - Módulos de acceso conectando las redes internas y externas (servicios de interconexión con otras redes del grupo). Todos aquellos dispositivos que comuniquen las redes internas con las externas formarán parte de esta zona de seguridad.

- No gestionados:
    - Los clientes y servidores no clasificados como conocidos o de confianza por la NAC (por ejemplo usuarios invitados).

- Clientes clasificados:
    - Clientes clasificados como conocidos y de confianza por NAC.
    - Servicios relacionados con el cliente (por ejemplo, Active Directory, servicios de impresión, servidor de buzón de correo, VozIP) se pueden asignar a los clientes clasificados de la zona de seguridad, siempre y cuando no se incumplan los criterios de seguridad especificados.
    - Estos clientes deben estar validados a través del uso de certificados (PKI-Public Key Infrastructure).

- Público:
    - Contiene las aplicaciones que se pueden utilizar sin autenticación, utilizando una identidad de la empresa.
      Nota: La presente zona de seguridad se puede considerar como una típica zona desmilitarizada (DMZ).

- Restringido:
    - Contiene equipos que sólo pueden autentificarse a través de la MAC, y no permiten el uso de certificados. Red de servidores.

- Administración / Gestión
    - Esta red se utilizará para proveer los servicios de administración y gestión de equipos (gestión de los equipos de red, gestión de servidores, etc.) principalmente red de IT.

- Servicios de infraestructura / CPD:
    - Servicios que no requieren un acceso directo del usuario, por ejemplo, DNS (Domain Name System), NTP (Network Time Protocol), etc.

- Producción: Equipos de la red de producción.

En el diseño de la nueva red corporativa se deberá tener en consideración todas las zonas de seguridad para la implementación de los nuevos firewalls. Se pretende separar cada una de las zonas mediante firewalls. Estos deberán ir conectados a los routers de la capa de Distribución.

El concepto de zonas seguras permite separar las zonas descritas a nivel 3 mediante firewalls, evitando el acceso a los usuarios a otras zonas mediante el filtrado IP-puerto. En la actualidad la red de la empresa está dividida en dos grandes redes, industrial y corporativa separadas mediante firewalls. Lo que se pretende con este concepto es dentro de la red corporativa incorporar un mayor nivel de seguridad, separando esta red en zonas y restringiendo el acceso a ellas. La red industrial pasaría a formar parte de la zona de producción.

Para ello es necesario configurar los routers de forma que encaminen el tráfico de las redes pertinentes al firewall, el cual se encarga de realizar el filtrado de los paquetes pertinentes y reenviar los aceptados de vuelta al router para que este los reenvíe a la red correspondiente.

Falta aclarar que en la empresa no se utilizan diferentes LANs (Local Area Network) sino VLANs (Virtual Local Area Networks), por lo que el firewall se encargará de filtrar los paquetes entre las diferentes zonas en función de las VLANs.

Como se ha comentado, las dos alternativas para la implementación del sistema NAC son ISE Cisco y Netsight de Enterasys. A continuación se describen las principales características de los mismos.

4.5.1 Solución ISE Cisco

Cisco Identity Services Engine (ISE) [15][22] es una solución propietaria de Cisco para la implementación del control de acceso NAC. Es un producto que permite la creación y el refuerzo de la seguridad y políticas de acceso para los dispositivos extremos conectados a los switches o APs de una empresa. Su propósito es simplificar la gestión del proceso de identificación de los diversos dispositivos y aplicaciones funcionando en la red.

ISE es un componente principal de la arquitectura de la solución Cisco para BYOD. Esta incluye varios servicios, entre ellos [16]:

- Portales de autogestión de registros y altas

- Autenticación

- Autorización
- Creación de perfiles de dispositivos
- Registro y aprovisionamiento de dispositivos
- Inscripción de certificados
- Definición de políticas
- Interfaz con almacenes de identidad (por ejemplo, Active Directory)
- Creación de informes y lista negra de dispositivos perdidos o robados
- Permite autenticar y autorizar los dispositivos finales conectados mediante cable, red inalámbrica o VPN (Virtual Private Network) con las políticas seleccionadas por la empresa.
- Permite la conexión de usuarios invitados reduciendo la carga de trabajo.
- Ofrece visibilidad de la red descubriendo, clasificando y controlando automáticamente los puntos finales conectados a la red para permitir los servicios de seguridad apropiados a cada uno de estos dispositivos finales.
- Aborda vulnerabilidades de las máquinas de usuarios, las evalúa y ayuda proactivamente a tratar virus, gusanos o spyware.
- Permite reforzar la seguridad bloqueando y aislando máquinas que no cumplen los requisitos sin necesidad de la intervención de un administrador.
- Permite identificar los dispositivos de la red mediante un escáner activo de dispositivos finales (Active Endpoint Scanning).
- Permite gestionar los dispositivos mediante EPS (Endpoint Protection Service), un servicio de protección de dispositivos finales, que permite administrar un dispositivo final concreto. Por ejemplo, el administrador puede especificar un dispositivo final concreto, seleccionar una acción como por ejemplo cambiarlo a una nueva VLAN o aislarlo de la red.
- SGA (Security Group Access): Permite a los clientes traducir sus objetivos de negocios en las decisiones del control de acceso a la red. SGA combina el control de acceso basado en roles con una autorización consistente y estable. En vez de usar control de acceso basado en listas IP (ACL-Access Control List) se basa en listas basadas en roles. Esta solución es más escalable, es independiente de la topología y más fácil de administrar que las ACL basadas en direcciones IP. Es decir, puede asignar la VLAN en función de a qué departamento pertenece ese dispositivo o persona.
- Emplea RADIUS como protocolo para autentificación, autorización y seguimiento. Soporta un amplio rango de protocolos de autenticación como PAP, MS-CHAP, EAP-TLS o PEAP entre otros. Ofrece una política basada en reglas o atributos para crear un control de acceso flexible.

- La solución Cisco ISE es capaz de actuar en una infraestructura multi-fabricante (Ej: routers, Switches, puntos de acceso…) ya que soporta 802.1X, el estándar de seguridad de la IEEE [17].

- Permite un ciclo de vida completo para la gestión de usuarios invitados los cuales sólo pueden acceder a la red según las especificaciones que la empresa quiera definir para ellos, por ejemplo permitirles únicamente un tiempo de conexión limitado, o portales cautivos de acceso.

Una de las funciones más importantes de Cisco ISE es que permite tener una única ubicación para el registro de dispositivos, un punto centralizado de control. Al conectarse un dispositivo a la red por primera vez, se le puede redirigir a un portal de autogestión de registro en el que el usuario puede registrar el dispositivo, darlo de alta y recibir auto-aprovisionamiento en el equipo. Este servicio es esencial para reducir la carga de los administradores de la red (IT), de modo que no tengan que registrar y pre-aprovisionar cada dispositivo conectado a la red de forma manual. Asimismo, brinda a IT visibilidad de los dispositivos que acceden a la red.

Cisco ISE permite a los administradores tomar acciones correctivas como el apagado o cuarentena de equipos y autorización de servicios mediante un interfaz gráfico web. Permite a los administradores configurar, gestionar, establecer políticas, autentificar y autorizar servicios de forma centralizada mediante una consola gráfica web. Además, Cisco ISE incluye una consola web para la gestión y la creación de reportes para identificar rápidamente los problemas.
En la siguiente Figura 23 se puede ver la consola de gestión que mantiene el control de los dispositivos activos, el perfil de los dispositivos y el cumplimiento de las políticas.

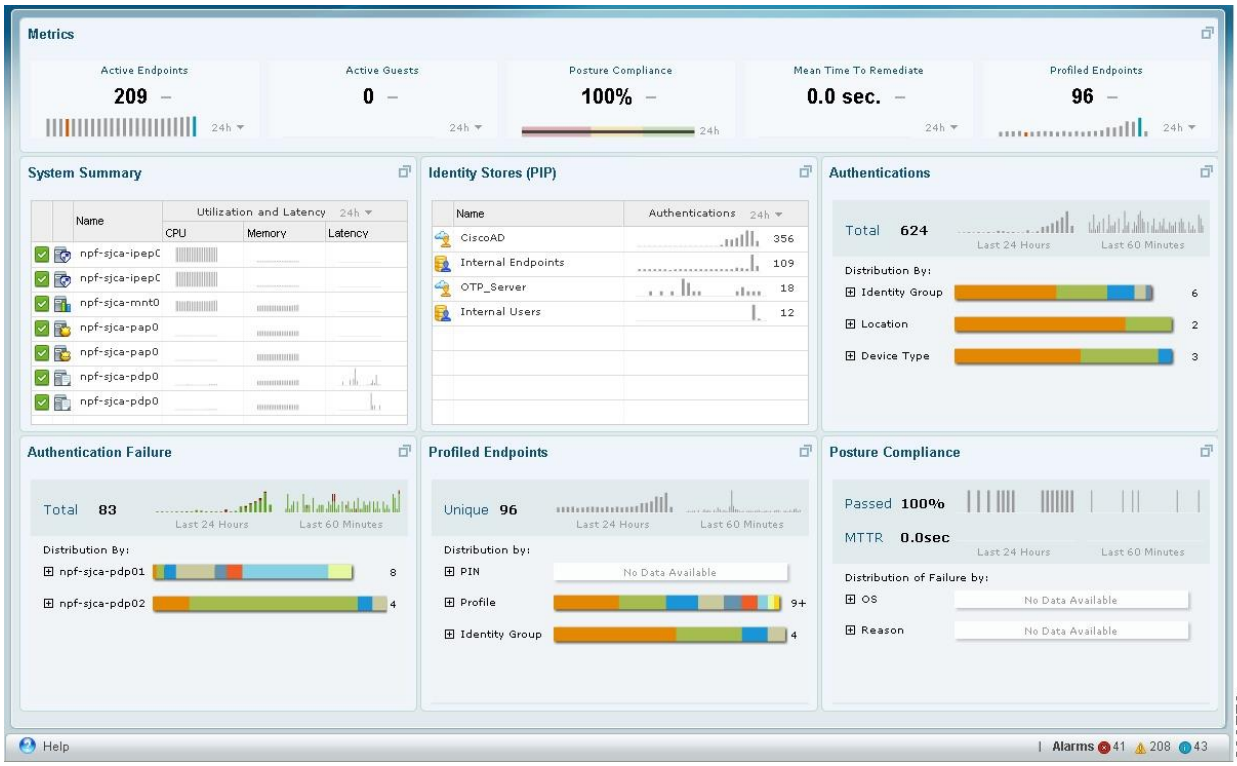


Figura 23-Consola de gestión

4.5.1.1 Especificaciones Hardware:

Cisco ISE está disponible tanto de forma física o virtualizada y se disponen de tres tipos de aplicaciones físicas y tres virtuales basadas en VMware [23] en función del hardware del servidor. En la siguiente Figura 24 se pueden ver las especificaciones requeridas en cada caso.

	Cisco Identity Services Engine Appliance 3315 (Small)	Cisco Identity Services Engine Appliance 3355 (Medium)	Cisco Identity Services Engine Appliance 3395 (Large)
Processor	1 x QuadCore Intel Core 2 CPU Q9400 @ 2.66 GHz	1 x QuadCore Intel Xeon CPU E5504 @ 2.00 GHz	2 x QuadCore Intel Xeon CPU E5504 @ 2.00 GHz
Memory	4 GB	4 GB	4 GB
Hard disk	2 x 250-GB SATA HDD	2 x 300-GB SAS drives	4 x 300-GB SFF SAS drives
RAID	No	Yes (RAID 0)	Yes (RAID 0+1)
Removable media	CD/DVD-ROM drive	CD/DVD-ROM drive	CD/DVD-ROM drive
Network Connectivity			
Ethernet NICs	4 x Integrated Gigabit NICs	4 x Integrated Gigabit NICs	4 x Integrated Gigabit NICs
10BASE-T cable support	Cat 3, 4, or 5 unshielded twisted pair (UTP) up to 328 ft (100 m)	Cat 3, 4, or 5 UTP up to 328 ft (100 m)	Cat 3, 4, or 5 UTP up to 328 ft (100 m)
10/100/1000BASE-TX cable support	Cat 5 UTP up to 328 ft (100 m)	Cat 5 UTP up to 328 ft (100 m)	Cat 5 UTP up to 328 ft (100 m)
Secure Sockets Layer (SSL) accelerator card	None	Cavium CN1620-400-NHB-G	Cavium CN1620-400-NHB-G
Interfaces			
Serial ports	1	1	1
USB 2.0 ports	4 (two front, two rear)	4 (one front, one internal, two rear)	4 (one front, one internal, two rear)
Video ports	1	1	1
External SCSI ports	None	None	None
System Unit			
Form factor	Rack-mount 1 RU	Rack-mount 1 RU	Rack-mount 1 RU
Weight	28 lb (12.7 kg) fully configured	35 lb (15.87 kg) fully configured	35 lb (15.87 kg) fully configured
Dimensions	1.69H x 17.32W x 22 in.L (43 x 440 x 55.9 mm)	1.69H x 17.32W x 27.99 in.L (43 x 42.62 x 711 mm)	1.69H x 17.32W x 27.99 in.L (43 x 42.62 x 711 mm)
Power supply	350W	Dual 675W (redundant)	Dual 675W (redundant)
Cooling fans	6; non-hot plug, nonredundant	9; redundant	9; redundant

Figura 24- Especificaciones hardware para CISCO ISE [18].

4.5.1.2 Tipos de licencias Cisco ISE:

Cisco ISE cuenta, como se ha comentado, con múltiples funcionalidades las cuales pueden implementarse o no en función de las necesidades del cliente y de la licencia que este adquiera.
Para la implementación de Cisco ISE se requieren licencias que permiten activar los diferentes servicios, en concreto hay tres tipos de licencias de Cisco ISE:

- ISE BASE (Básica): Sirve para activar los servicios básicos como autentificación, autorización, gestión de invitados, gestión y resolución de problemas de servicio.
- ISE ADVANCED (Avanzada): Añade funcionalidades a la licencia básica. Permite activar servicios para el establecimiento de políticas de seguridad, profiling (creación de perfiles de los dispositivos), EPS y SGA.
- ISE WIRELESS (Inalámbrica): Activa todos los servicios ISE pero únicamente para puntos de acceso inalámbricos.

4.5.1.3 Autenticación y autorización:

Las políticas de autenticación de Cisco ISE permiten proporcionar autenticación a los usuarios a través del uso de diferentes protocolos de autentificación como pueden ser PAP, CHAP, PEAP o EAP. Cisco ISE específica el protocolo o protocolos permitidos que están disponibles para los dispositivos de red con los que los usuarios tratan de autenticarse, y especifica las fuentes de identificación o almacenes de identidad que realizan la validación de la identidad del cliente. Estas fuentes de identidad son las que almacenan la información para autenticar a los usuarios, almacenan información que permite verificar los credenciales de los usuarios en el proceso de autenticación. Estas fuentes pueden ser internas (Cisco ISE almacena información en una base de datos) o externas (Directorio activo, LDAP, RADIUS).

En la siguiente Figura 25 se pueden ver los protocolos de autentificación disponibles en función de la fuente donde se almacenen las credenciales del cliente.

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP1	RADIUS Token Server or RSA
EAP-GTC2, PAP3 (plain text password)	Yes	Yes	Yes	Yes
MS-CHAP4 password hash: MSCHAPv1/v25 EAP-MSCHAPv26 LEAP7	Yes	Yes	No	No
EAP-MD58 CHAP9	Yes	No	No	No
EAP-TLS10 PEAP-TLS11 (certificate retrieval) **Note** For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required but can optionally be added for authorization policy conditions.	Yes	Yes	Yes	No

Figura 25-Protocolos de autenticación en función de la fuente de identidad. [19]

Cisco ISE soporta 802.1X, autenticación MAC y autentificación basada en web mediante el registro en un navegador tanto para redes cableadas como inalámbricas.

Una vez que el usuario se autentica de forma correcta, si está configurada la opción, se procede a la autorización del usuario mediante la verificación del cumplimiento de las políticas de seguridad. El resultado de este paso es que Cisco ISE asigna un perfil que define los privilegios que tendrá el usuario una vez autenticado con Cisco ISE. En los siguientes apartados se va a explicar que son estas políticas y el funcionamiento de los perfiles.

4.5.1.4 Incorporación de la evaluación de las políticas de seguridad en el cliente y saneamiento de los dispositivos finales (Posture and Health Compliance and Remediation):

Cisco ISE permite crear políticas de seguridad y verificar los cumplimientos de estas políticas en todos los dispositivos finales de los usuarios conectados a la red. La verificación de las políticas en el cliente trabaja vía un agente persistente instalado en los equipos o a un agente web temporal para validar que el dispositivo final es conforme con las políticas de seguridad de la empresa. Proporciona la capacidad de crear fuertes políticas que incluyen la verificación de los últimos parches para sistemas operativos, antivirus, etc. ISE soporta auto-saneamiento del

cliente así como verificaciones periódicas de que el cliente no viola ninguna de las políticas de seguridad de la empresa. EPS permite a los administradores tomar rápidamente medidas correctivas (Cuarentena, apagado, etc.) en los dispositivos de riesgo para incrementar la seguridad en la red. Refuerza el cumplimiento de las políticas de seguridad de los dispositivos proporcionando medidas y evaluando los dispositivos finales que se conectan a la red incluyendo los entornos 802.1X.

Para asegurar que las medidas impuestas de seguridad en la red son efectivas, Cisco ISE permite al administrador de IT validar y mantener las capacidades de seguridad en cualquier máquina que acceda a la red. La evaluación de los dispositivos para la comprobación del cumplimiento de las políticas de seguridad se realiza mediante el uso de uno de los siguientes tipos de agentes Cisco ISE disponibles [20]:

- Cisco NAC web-agent: Un agente vía web. Es un agente temporal que el usuario instala en su propio sistema cuando inicia sesión y finaliza cuando esta termina. Permite la evaluación de los dispositivos finales de forma temporal en las máquinas cliente. Los clientes lanzan el agente ejecutable que instala los ficheros del agente web en un directorio temporal del cliente. Cuando el usuario termina la sesión, el agente web desregistra al usuario de la red. El agente web obtiene los requerimientos configurados para ese rol y ese sistema operativo del servidor ISE de cisco, comprueba el registro del host, sus procesos, aplicaciones y servicios y envía el report al servidor Cisco ISE. Si los requerimientos se cumplen en el cliente, este puede acceder a la red, si no cumple se le proporcionan las instrucciones para cumplir estos requisitos. En la siguiente Figura 26 se muestra la instalación y el uso del agente web de Cisco. Cuando el usuario abre el navegador es redirigido a una página de login. El usuario introduce sus credenciales en la web de registro y se le redirige al instalador del agente web. Una vez completada la instalación, el agente Web NAC de Cisco comprueba automáticamente si el sistema del cliente cumple con los requisitos de seguridad para ese dispositivo. Si el usuario cumple se le proporciona acceso a la red, si no cumple se le da la opción de tener acceso restringido (esto es configurable) o un diálogo con las instrucciones a seguir para el cumplimiento de las políticas establecidas.

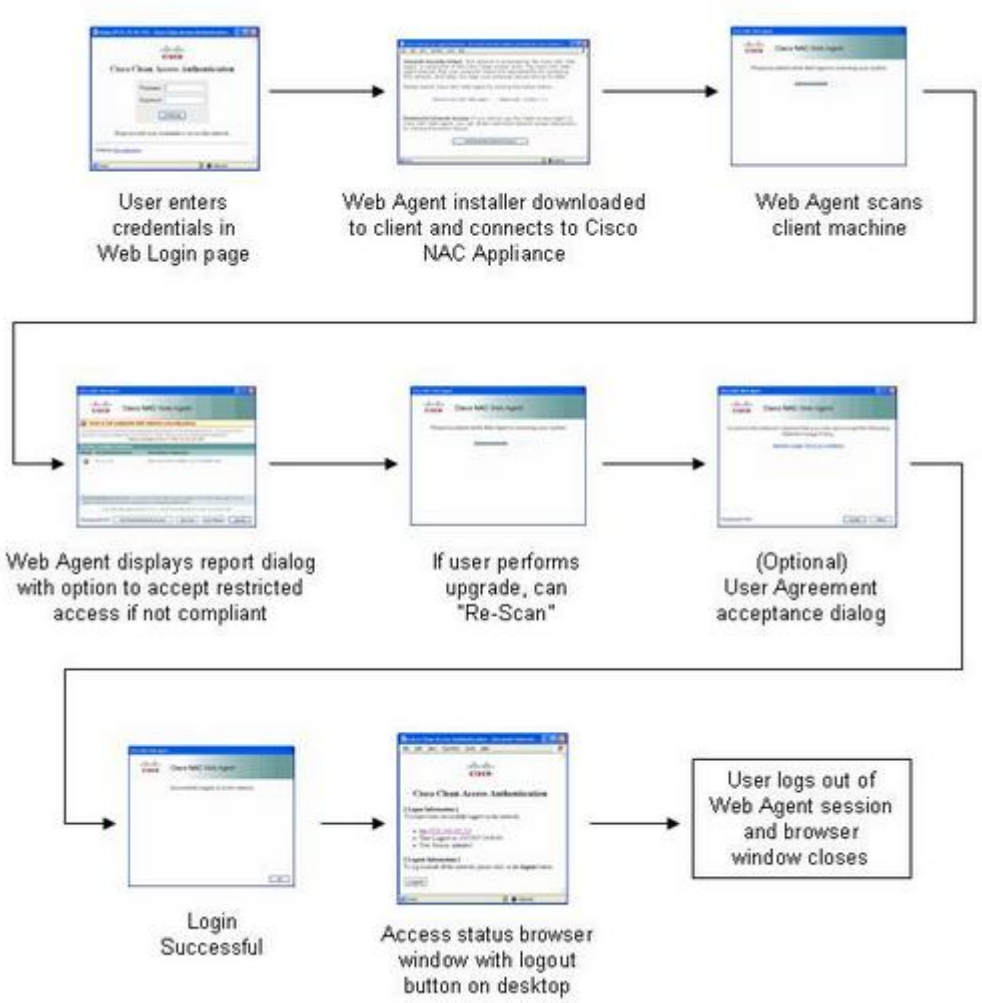


Figura 26-Ejemplo de instalación y uso del agente web de Cisco.

El agente web NAC de Cisco proporciona un portal web para la autenticación temporal de usuarios. Su propósito es la autorización a la red de usuarios invitados.

- Cisco NAC Agent: Este es persistente y una vez instalado permanece en el dispositivo. Para usarlo se necesita que el equipo sea compatible. Los sistemas operativos compatibles son los siguientes: Windows 8 Basic, Windows 8 Professional, Windows 8 Enterprise, Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise, Windows Vista Home, Windows 7, Windows XP Professional, Windows XP Home, Windows XP Media Center Edition, Windows XP Tablet PC; Mac OS X (v10.5.x, v10.6.x, v10.7.x and v10.8.x).

  Una vez instalado, el usuario introduce sus credenciales en el agente para entrar en la red de forma similar al registro mediante página web. Si hay varias formas de realizar la autenticación el usuario puede elegir cual (interna, directorio activo, LDAP). En la Figura 27 se pueden ver dos modelos distintos de pantalla de entrada de este agente, en uno de ellos se puede elegir la fuente de autenticación.

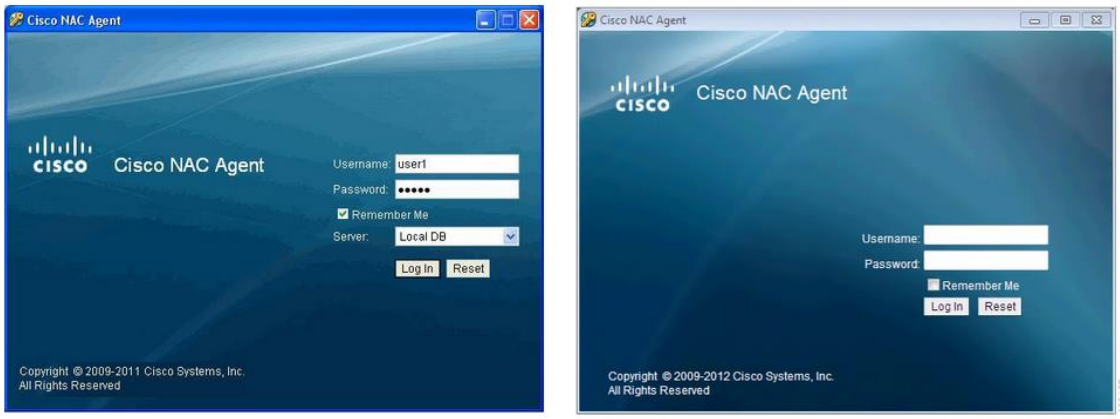


Figura 27-Ejemplos del agente NAC persistente.

Los agentes NAC comentados, se instalan en el cliente e interaccionan con el servicio de políticas de Cisco ISE. Estos agentes NAC refuerzan la seguridad permitiendo o denegando el acceso a los equipos si no cumplen con la normativa.

Estos agentes se usan para algunas políticas de seguridad relacionadas con el estado de los dispositivos y sirven como método de autenticación para usuarios temporales. En la Figura 28 se puede ver la jerarquía del sistema Cisco ISE. En el nivel del cliente se encuentran los agentes NAC utilizados para la supervisión de los equipos y para la autenticación de usuarios temporales. En el nivel de cliente también se encuentra el suplicante 802.1X que puede ser el embebido por el propio sistema operativo del dispositivo o AnyConnect, el cual es propio de Cisco y permite realizar funciones similares a los agentes NAC a la hora de evaluar el dispositivo final. Hay que diferenciar entre el agente, el cual se usa para evaluar las políticas de seguridad de un dispositivo, y el proceso de autenticación mediante el suplicante 802.1X. En el nivel intermedio se encuentran los equipos Cisco que soportan 802.1X y la implementación de ISE. En el nivel superior se encuentra ISE como punto único de creación y gestión de políticas de acceso a la red.

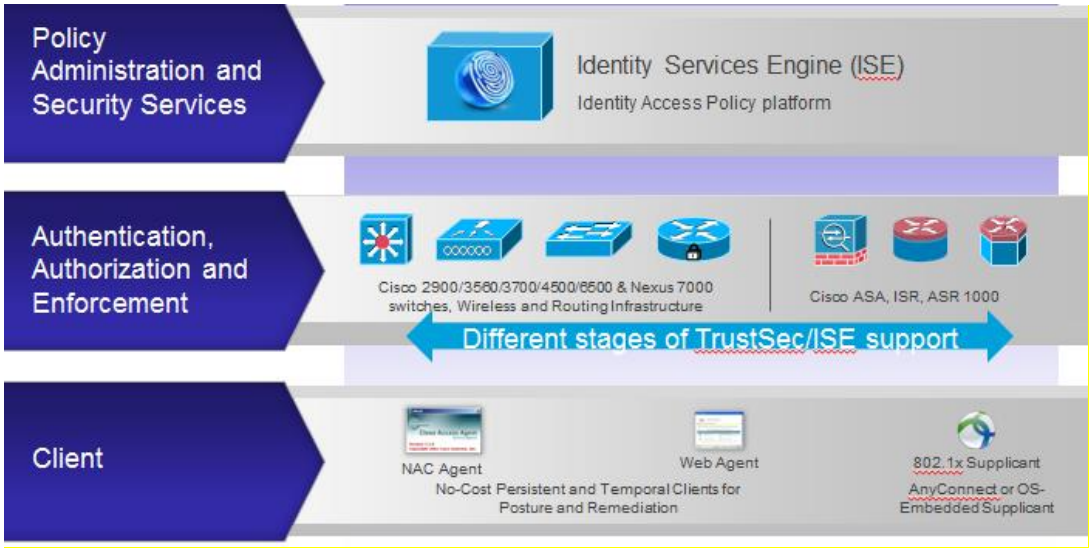


Figura 28-Jerarquía Cisco ISE

Cisco ISE es el motor del sistema BYOD de Cisco, en la siguiente Figura 29 se puede ver un esquema con la implementación completa de la solución NAC de Cisco.

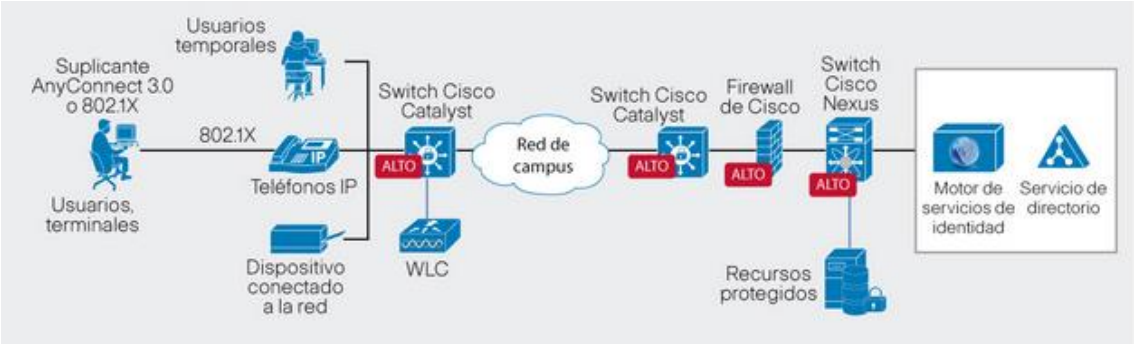


Figura 29-Esquema BYOD de Cisco

Cisco ISE es integrable con el Software de monitorización Cisco Prime Infraestructure mediante el cual se puede monitorizar la red y a los usuarios completando la solución ISE propuesta.

4.5.1.5 Creación de perfiles:

Además de las funciones principales, como autenticación y autorización, Cisco ISE brinda inteligencia acerca de los dispositivos que se conectan a la red mediante perfiles de dispositivos. Los perfiles de dispositivos pueden usarse para detectar, localizar y determinar el tipo y las funciones de los terminales conectados a la red, a fin de denegar o aplicar ciertas reglas de autorización o políticas de seguridad en función del tipo de dispositivo. A esto se le llama “profiling” [21].

Por ejemplo, un mismo usuario puede conectarse a la red mediante un equipo corporativo al que se le garantiza todo el acceso, si este mismo usuario en vez de conectarse mediante un equipo corporativo lo hace mediante uno propio, esto se puede detectar y se le puede restringir el acceso a una parte de la red o a lo que se quiera especificar mediante la asignación de una VLAN u otra.

Como se ha comentado, contiene plantillas o perfiles predefinidos para una amplia gama de dispositivos, los administradores pueden crear sus propias plantillas para dispositivos. Estas plantillas se usan automáticamente para detectar y clasificar los dispositivos cuando se conectan a la red.

El servicio de creación de perfiles permite identificar, localizar y determinar las capacidades de todos los dispositivos finales de la red (a esto se le conoce como “identities” en Cisco ISE), independientemente del tipo de dispositivo de forma que se pueda asegurar y mantener un acceso apropiado a la red. Cisco ISE en su funcionalidad de creación de perfiles (Cisco ISE Profiler function) realiza pruebas para obtener información de los dispositivos de la red, una vez obtenidos los datos se realiza un análisis que permite clasificar el dispositivo final de acuerdo con las políticas asociadas e este tipo de dispositivos.

En otras palabras, tiene la capacidad de recoger información de los dispositivos y tras esto, mediante el uso del estándar RADIUS enviar esta información a ISE para la clasificación de los

dispositivos finales en función de políticas. (Ej: No permitir la conexión de teléfonos móviles con cierto sistema operativo).

En la Figura 30 se puede ver un ejemplo de lo que es "profiling". Un usuario se conecta a red utilizando un dispositivo. Mediante diferentes técnicas es capaz de crear perfiles de los dispositivos, a estos perfiles se les asigna una política, en el caso del ejemplo se puede ver que al dispositivo personal le coloca en la VLAN 20 y sólo tiene acceso a Internet mientras que al dispositivo corporativo lo coloca en la VLAN 10 y tiene acceso a los recursos de la organización.

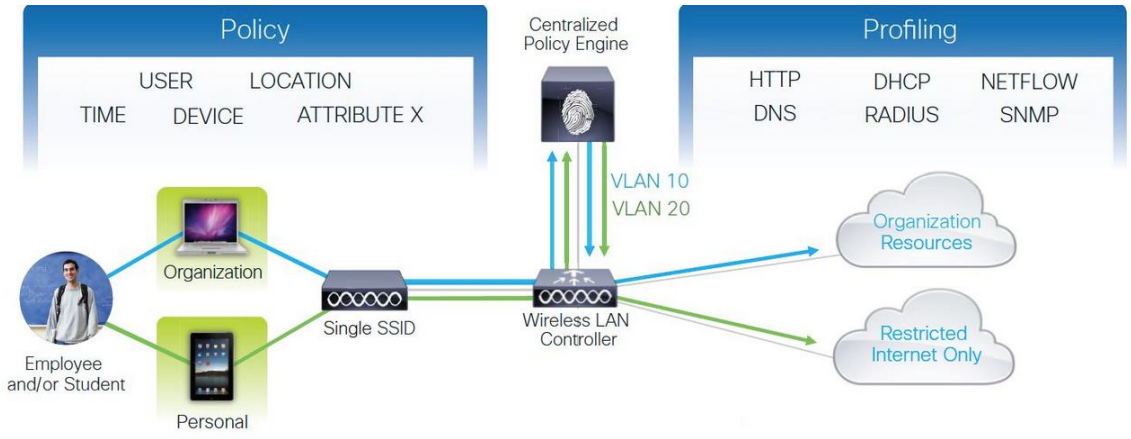


Figura 30-Ejemplo profiling [52]

4.5.1.6 Creación de políticas:

Una política en este entorno hace referencia a una regla que se crea con el fin de conseguir una red más segura y un acceso más restringido a la misma.

Cisco ISE soporta la configuración de políticas de seguridad. Permite al administrador configurar políticas de autenticación y autorización.

Permiten definir políticas de autorización y configurar perfiles de autorización para usuarios o grupos específicos que accedan a la red.

La autorización de las políticas de red asocia reglas con usuarios y grupos de usuarios para crear perfiles.

4.5.2 Solución Enterasys.

El control de acceso a la red que proporciona la solución de Enterasys NAC [26] se basa en los estándares y proporciona interoperabilidad entre vendedores tanto para redes inalámbricas como cableadas y VPN. Utilizando la aplicación NAC de Enterasys [24] junto con el software de gestión, monitorización y configuración NetSight [25] los administradores de IT pueden desarrollar una solución para asegurar que sólo los usuarios correctos acceden a la información correcta en el debido instante de tiempo. La ventaja de Enterasys NAC es que

proporciona control sobre los usuarios individuales y aplicaciones en una infraestructura formada por componentes de distintos fabricantes. Permite proteger la infraestructura existente sin requerir la instalación de nuevos equipamientos hardware ni de la instalación de agentes en todos los sistemas finales.

Ofrece flexibilidad para elegir entre restringir o no el acceso para los usuarios invitados a los servicios de Internet y cómo manejar los usuarios o dispositivos autenticados que no superan la evaluación de las posturas de seguridad. La capacidad de NAC para evaluar los peligros alerta a los usuarios cuando necesitan actualizar su sistema y se puede permitir un periodo de transición antes de que sean puestos en cuarentena.

Enterasys NAC consta de diferentes políticas para permitir, denegar, priorizar, etiquetar, limitar la tasa, redirigir o auditar el tráfico de la red en función de la identidad del usuario, el tiempo, la localización y el tipo de dispositivo entre otras variables.

Sus principales características son:

- ✓ BYOD y registro de invitados: Permite la implantación del concepto BYOD (Trae tu propio dispositivo) proporcionando un registro automático a los usuarios para registrar su propio dispositivo con sus credenciales sin la intervención de IT.
- ✓ Opciones de configuración: Permiten multitud de opciones, tipos de autentificación, grupos de usuarios, sistemas operativos y dispositivos finales.
- ✓ Disponible de forma física o virtual.
- ✓ Arquitectura abierta para evaluaciones: Permite una integración fácil con herramientas de gestión de terceros para MDM (Mobile Device Management es un tipo de software que permite asegurar, monitorear y administrar dispositivos móviles sin importar el operador de telefonía o proveedor de servicios.) tratamiento de amenazas, sistemas de prevención de intrusión, y gestión de eventos entre otros.
- ✓ Proporciona funcionalidades relacionadas con la identidad del usuario, como por ejemplo descubrimiento, autentificación y control de acceso basado en roles. Los procesos de gestión del ciclo de vida del usuario (Ej: Inscripción, cambios de rol, terminación) puede ser automatizados y unidos a otros procesos mediante integración LDAP y RADIUS.
- ✓ Monitorización: Proporciona capacidades para determinar las políticas de seguridad de los dispositivos conectados. Evalúa si se cumplen o no las reglas de seguridad establecidas. Puede funcionar con múltiples servidores de evaluación, servidores de autenticación y agentes de seguridad software para alcanzar las necesidades de las organizaciones las cuales ya tengan probablemente tecnología de evaluación.

4.5.2.1 Escaneo de los hosts finales:

Todos los dispositivos finales deberían incorporarse en el sistema de control de acceso para que este sea más efectivo. Enterasys proporciona evaluación de las capacidades de los clientes

para determinar su seguridad de dos formas, mediante agentes instalados en los dispositivos finales o sin ellos. Enterasys NAC trabaja con diferentes servidores de evaluación, servidores de autenticación y agentes software para cubrir las necesidades de las empresas las cuales pueden tener ya instalada otra tecnología de evaluación.

La funcionalidad sin agente no necesita de la instalación de ningún software en los dispositivos finales y se usa típicamente en ordenadores invitados, teléfonos, cámaras e impresoras IP. Esta funcionalidad realiza escaneos para ver el tipo de sistema operativo y las vulnerabilidades de las aplicaciones instaladas.

La funcionalidad de monitorizado de extremos finales basada en agente sí requiere la instalación de un software adicional en el dispositivo final. El agente permite realizar escáneres sobre los antivirus, el estado del firewall, parches de seguridad en los sistemas operativos o aplicaciones de tráfico P2P. Los agentes pueden mirar cualquier proceso o registro de entrada y automáticamente sanearlo. La combinación de las dos funcionalidades (con agente y sin agente) permite proporcionar una solución de gestión y creación de reportes más eficiente.

Los sistemas operativos soportados para los dispositivos finales conectados a la red a los que se les pueden instalar los agentes para la evaluación de la seguridad son los siguientes:

- Windows 2000, Windows 2003, Windows 2008, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1.

- Mac OS X – Tiger, Leopard, Snow Leopard, Lion, Mountain, Lion, y Mavericks.

4.5.2.2 Gestión NAC NetSight:

El software de gestión NetSight permite la creación y el seguimiento de las políticas de seguridad NAC. Permite al personal de IT configurar y controlar la solución NAC desde un punto centralizado simplificando el desarrollo y la administración. Además, también incluye la realización de estadísticas sobre la conectividad de la red y las vulnerabilidades así como auditar las actividades de acceso a la red y proporcionar reportes detallados de las vulnerabilidades en la red. La gestión está simplificada mediante una estructura jerárquica. La gestión NAC proporciona un valor añadido debido a su integración con otros productos de Enterasys.

El software de gestión NetSight permite al personal de IT, desde un punto centralizado, configurar y controlar la solución NAC simplificando el desarrollo y la administración. La gestión NAC también agrega la conectividad de la red y estadísticas de vulnerabilidad, audita las actividades de acceso a la red y proporciona reportes detallados de las vulnerabilidades en la red. Permite una gestión consistente tanto de redes inalámbricas como cableadas desde un solo interfaz. El usuario puede acceder a los datos de la red y a los reportes mediante un interfaz gráfico.

Permite la creación centralizada de políticas que deben seguir los usuarios y dispositivos sobre la red. Estas no están atadas a la red física y pueden cambiar en función del usuario, el dispositivo, la localización o el tipo de conexión.

Contiene un sistema de alarmas y eventos inteligente capaz de avisar a IT cuando ocurren problemas dentro de la red y desaparecen cuando estos se solucionan. Permite además definir umbrales de avisos para enviar notificaciones antes de que los sistemas fallen. Permite una solución de problemas fácil. Introduciendo el nombre de usuario se puede descubrir donde se encuentra, donde está conectado a la red, el tipo de dispositivo que utiliza y más. Permite además gestionar dispositivos de terceros para obtener una imagen completa de la infraestructura de red en un entorno heterogéneo.

Las herramientas que componen la solución NAC de NetSight son:

- NetSight gestión: Proporciona una configuración y un control unificado para las redes inalámbricas y cableadas desde un punto centralizado.
- Identidad y acceso: El interfaz especializado OneView™ proporciona control, facilidad de uso e información detallada de los sistemas y usuarios conectados.
- Network Access Control (NAC) Management (Gestión): Gestiona las soluciones NAC proporcionando una control granular y basado en políticas sobre los usuarios y dispositivos finales así como reportes de alto nivel y vistas sobre todas las políticas de seguridad.
- Inventory Management (Gestión de inventario): Automatiza el inventario y los cambios de gestión, los cambios en el seguimiento y en los reportes de la configuración de red y simplifica la configuración de backups y actualizaciones del firmware.
- OneView™: Proporciona un acceso web unificado para la creación de reportes, análisis de la red, solución e problemáticas (troubleshooting). Incluye dashboards (consola gráfica donde el usuario puede administrar el software), reports, información de la gestión de las identidades y el acceso, control de mapas de topología, dispositivos y gestión de alarmas y eventos.
- Gestión móvil (Mobile Management): Optimiza la gestión de la red y ayuda en la solución de los problemas desde cualquier sitio y a cualquier hora permitiendo el acceso a la información crítica desde dispositivos móviles.
- Automated Security Management (Gestión de seguridad automatizada): Permite la integración con NAC.

4.5.2.3 Autenticación. Identidad y Acceso.

NAC de Enterasys es una solución de control de acceso multi-vendedor basada en los estándares. Usando las aplicaciones de identidad y acceso (en su opción virtual o no) junto con el software de configuración y gestión NetSight se convierte en una completa solución NAC.

La aplicación de identidad y acceso controla la autenticación de los extremos, la evaluación de los dispositivos y la autorización en la red. Para los servicios de autenticación, la aplicación de identidad y acceso (Identity & Access appliance) actúa como un proxy RADIUS o servidor RADIUS para la autenticación MAC que se comunica con los servicios de autenticación RADIUS

de la organización (Microsoft Active Directory, LDAP, etc.). Soporta autenticación 802.1X (EAP), MAC, basada en web y Keberos.

Para la evaluación de los dispositivos finales, la aplicación de identidad y acceso se conecta con múltiples servidores de evaluación y agentes. En el caso de los servicios de autorización, la aplicación comunica los atributos RADIUS al switch autenticador. Esto permite al switch autorizar dinámicamente y colocar a los dispositivos finales en función de los resultados de evaluación de los dispositivos.

Además, permite almacenar información sobre la configuración NAC y la localización física de los dispositivos finales. Es escalable y soporta redundancia y grandes desarrollos NAC. Los diferentes modelos cumplen con las necesidades de implementaciones de diferentes tamaños.

La evaluación o escaneo de los dispositivos (Ver apartado 4.5.2.1) tiene un licencia independiente que incluye las evaluaciones basadas en agentes como las que no.

4.5.2.4 Versiones de NAC Enterasys:

La solución NAC propuesta por Enterasys está compuesta por diferentes elementos y tiene diferentes posibles configuraciones en función del grado de funcionalidad que se requiera.

Las principales funcionalidades que ofrece son:

- Detección: Identifica cuando y donde se conecta un dispositivo a la red.
- Autenticación: Verifica la identidad del usuario o dispositivo conectado a la red. Enterasys NAC soporta autenticación “pass through” (delegando en un servidor secundario RADIUS) de 802.1X, basada en web, y autentificación MAC.
- Evaluación (Assessment): Determina si el dispositivo cumple con la seguridad corporativa y los requerimientos de seguridad como por ejemplo revisión de los parches de seguridad de los sistemas operativos, antivirus, etc.
- Autorización: Determina la red de acceso apropiada para conectar cada dispositivo basándose en la autenticación y/o en los resultados de evaluación. El nivel de autorización puede basarse en la localización del usuario, su dirección MAC, posturas de seguridad (como por ejemplo los resultados de la evaluación del dispositivo), en la identidad del usuario o del dispositivo. El dispositivo final puede ser autorizado para acceder a la red usando diferentes técnicas. Se puede implementar de forma “inline” (el tráfico atraviesa el dispositivo), y “Out-of-Band” (el tráfico no atraviesa el dispositivo) y cada una utiliza diferentes técnicas para autentificar los sistemas.
- Saneamiento: Permite a los usuarios sanear de forma segura sus dispositivos finales sin impactar sobre las operaciones de IT. Con esta funcionalidad los usuarios son notificados cuando su sistema entra en cuarentena porque no cumple con las políticas de seguridad de la red. El proceso de saneamiento incluye actualizaciones del dispositivo para el cumplimiento de los requerimientos de seguridad.

La solución NetSight proporciona diferentes modelos con diferentes funcionalidades. Existen tres modelos:

- NMS-BASE-XX: Incluye la gestión básica de las redes cableada e inalámbrica así como la gestión de inventario, gestión de políticas y OneView básico (solo para la gestión de los dispositivos, alarmas y administración). Además de las conexiones de usuarios ilimitados a OneView se incluyen tres conexiones remotas.

- NMS-XX: Incluye la gestión básica de las redes cableada e inalámbrica así como la gestión de inventario, gestión de políticas, gestión NAC, Automated Security Management, gestión móvil, y el interfaz OneView completo. Incluye 25 clientes remotos.

- NMS-ADV-XX: NMS-XX: Incluye la gestión básica de las redes cableada e inalámbrica así como la gestión de inventario, gestión de políticas, gestión NAC, Automated Security Management, gestión móvil, y el interfaz OneView completo. Además incluye gestión avanzada de las redes inalámbricas, la posibilidad de instalar un servidor secundario y el desarrollo completo para las aplicaciones NAC. Incluye 25 clientes remotos.

4.6 Instalación y configuración de una alternativa open source: PacketFence.

Para comprobar el funcionamiento de un sistema NAC se ha seleccionado un software gratuito. La solución NAC de código abierto elegida es PacketFence. [28]

Existen diferentes alternativas gratuitas como son por ejemplo Opennac [29], FreeNac [30], sin embargo se ha decidido implementar PacketFence por ser una de las más conocidas y más implementadas, se adapta a grandes escenarios, dispone de una gran cantidad de funcionalidades y métodos de autenticación, es compatible con bastantes fabricantes, soporta diversos mecanismos de autenticación y cuenta con unos portales de monitorización y gestión gráficos muy intuitivo. Al ser una de las soluciones más implementadas la cantidad de información sobre su funcionamiento, instalación y reparación de bugs es mayor que con el resto de soluciones.

A parte de soluciones NAC, existen otras menos completas que simplemente se basan en portales cautivos, estos son programas que vigilan el tráfico HTTP y HTTPS forzando a los usuarios a pasar por una página especial si quieren navegar de forma normal por Internet.

El programa vigila y captura todo el tráfico web hasta que el usuario es autenticado, entonces deja de interceptar su tráfico y le permite acceder a la web de manera convencional. Ejemplos de soluciones de este tipo OpenSource son: ChilliSpot [31], Wifidog [32], PepperSpot [33].

Existen soluciones FireWall gratuitas como PfSense [34] y Zeroshell [35] que incluyen portales cautivos para impedir que cualquiera se conecte a la web y que incluye autenticación de usuarios mediante servidores RADIUS.

PacketFence es una solución gratuita que permite la gestión y el control centralizado de acceso de usuarios a una red ya sea inalámbrica o cableada proporcionando una solución para el concepto BYOD. Soporta el estándar 802.1X y el aislamiento a capa 2 de dispositivos problemáticos. Se puede usar tanto para redes pequeñas como grandes.

Es un sistema NAC OpenSource basado en Linux que proporciona control de acceso a la red, monitorizado y detección de intrusión. Proporciona diversas funcionalidades a la red como pueden ser:

- Portal cautivo: Puede usarse para registrar a los usuarios que acceden a la red o para proporcionar instrucciones al usuario, bloqueando cualquier otro tipo de tráfico.
- Detección de Malware y alertas: Puede trabajar con sensores como Snort.
- Escáneres de vulnerabilidad con Nessus [39] u OpenVAS [40].
- Aislamiento de dispositivos problemáticos.
- DCHP fingerprinting: Permite obtener información del tipo de dispositivo usando únicamente información básica de la transacción DCHP.

PacketFence tiene dos mecanismos de funcionamiento posibles:

- Out-Of-Band
- Inline

4.6.1 Out-Of-Band deployment (VLAN enforcement)

Permite una mayor escalabilidad y resistencia ante fallos. Para utilizar este método es necesario disponer de una electrónica de red adecuada [41] es decir, disponer de dispositivos compatibles con PacketFence. Los dispositivos pueden ser compatibles por uno o varios de los siguientes mecanismos:

- SMMP (Simple Network Management Protocol): Facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas.
- Autenticación MAC: No todos los dispositivos soportan 802.1X. Para que estos dispositivos se puedan usar en un entorno seguro se proveen mecanismos alternativos para poder autenticarlos. Uno de estos mecanismos es MAB (MAC Authentication Bypass). Cuando MAB se configura en un puerto, este primero trata de comprobar si hay algún dispositivo compatible con 802.1X conectado. Si no se recibe ninguna información del dispositivo conectado tratará de autenticarlo a través del servidor de autenticación usando la dirección MAC del dispositivo conectado como usuario y contraseña. Los administradores de red deben configurar el servidor de autenticación para que permita autenticar esas MACs.
- 802.1X

Hay una gran cantidad de dispositivos compatibles los cuales se listan en la documentación la cual además proporciona la configuración necesaria de los equipos para su correcto funcionamiento. [42]

PacketFence gestiona los dispositivos mediante estos mecanismos ordenando al equipo de acceso (Switch o AP) que deje pasar el tráfico de cierto dispositivo y que lo asigne a cierta VLAN. Esto se puede hacer en función de la MAC y el estándar 802.1X o vía SNMP:

-Mediante SNMP: Todos los puertos de los Switches deben de estar configurados para enviar traps SNMP al servidor PacketFence, este recibe las notificaciones, las reformatea y las escribe en un fichero de logs (/usr/local/pf/logs/snmptrapd.log). El servidor contiene un demonio que lee estos datos del fichero plano del log y responde a ellas ajustando al puerto del switch en la VLAN adecuada.

-Mediante 802.1X y/o MAB: En este contexto PacketFence se encarga de ejecutar el demonio del servidor de autenticación (FreeRADIUS) y devuelve la VLAN apropiada al switch. El módulo que incorpora FreeRADIUS realiza una llamada remota a PacketFence para obtener información.

MAB es un nuevo mecanismo que introducen algunos vendedores para manejar casos donde no existe un suplicante 802.1X. Tras un periodo de tiempo cuando un dispositivo no soporta 802.1X, el Switch deja de funcionar en 802.1X y empieza a funcionar en MAB. Este funcionamiento tiene las mismas ventajas que 802.1X sólo que lo que se envía es la MAC del usuario en vez de su nombre y que la conversación sobre EAP no es extremo a extremo sino entre el Switch y el extremo final.

Para el modo de funcionamiento “OUT-OF-BAND” se necesitan crear como mínimo dos VLANS, “Registration VLAN” a la que se asignarán los dispositivos no registrados y “Isolation VLAN”, en la que se colocarán los dispositivos aislados, es decir aquellos que no cumplan con alguna política de seguridad definida como por ejemplo que tienen algún virus, o no es un dispositivo válido. El resto de VLANS que es necesario crear dependen de la configuración de la red del usuario, es decir, son las VLANS en las que se quieren comunicar los dispositivos autorizados. Se pueden establecer políticas para asignar un dispositivo a una VLAN u otra.

Con un solo servidor con figurado en este modo se pueden conseguir cientos de Switches seguros y miles de nodos conectados a ellos. En este modo PacketFence es el servidor encargado de asignar las VLANs o roles a los dispositivos. Este mecanismo sólo se usa cuando se tienen dispositivos manejables. Es el propio servidor PacketFence el que se encarga de introducir a los usuarios en una VLAN u otra. Dichas VLANs tienen diferentes características y normas para el acceso a la red permitiendo separar a los usuarios.

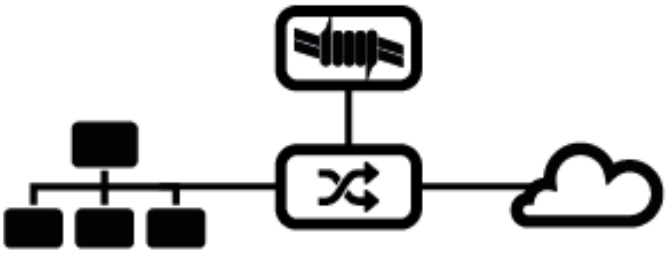


Figura 31-Esquema VLAN Enforcement

En la figura se aprecia como PacketFence se comunica con la electrónica de red para asignar los roles a los dispositivos. PacketFence se sitúa “Fuera de banda”, es decir no se coloca como un elemento en el camino sino que se comunica con estos para configurarlos dinámicamente.

La asignación de VLANS se puede realizar mediante diferentes técnicas. Estas técnicas son compatibles entre sí pero no dentro del mismo Switch, lo que significa que puedes usar las últimas y más seguras técnicas en los Switches que lo soporten y otras más antiguas en los que no. Como el nombre del método implica, “VLAN assignment” o “VLAN enforcement” significa que PacketFence es el servidor que asigna las VLANS a los dispositivos. Estas VLANs pueden ser una de las VLANS que el usuario ya tenga creadas en su red u otra especial en la que PacketFence muestre un portal cautivo para su autenticación.

Este modo de funcionamiento permite aislar efectivamente los hosts o dispositivos finales de la red a nivel 2 de la torre OSI.

PacketFence soporta distintas maneras de realizar esta asignación de VLANS, cabe decir que no todos los equipos soportan todos los métodos, pero como se ha comentado, estos son compatibles entre sí. Los métodos disponibles, cuyo funcionamiento se ha descrito anteriormente, son los siguientes:

- ✓ Seguridad por puerto y SNMP
- ✓ 802.1X + Autentificación MAC para redes cableadas
- ✓ 802.1X + Autentificación MAC para redes inalámbricas

4.6.2 Inline deployment (Inline enforcement)

Este modo de funcionamiento es compatible para dispositivos inalámbricos y cableados no gestionables por el servidor, es decir que son incapaces de comunicarse con este. Es menos escalable puesto que el sistema se coloca en medio de la comunicación lo que hace que todos los paquetes lo atraviesen aumentando su carga. Es un método conveniente para obtener control NAC sobre hardware incapaz de realizar asignaciones en VLANS o no es compatible con PacketFence. Sin embargo dispone de un inconveniente, los dispositivos son visibles dentro de

la LAN interna por lo que el NAC sólo se realiza cuando la conexión es hacia el exterior ya sea otra LAN o Internet. Sin embargo, como en general el uso del mecanismo “inline” sólo se realiza como último recurso, cuando se dispone de equipos no compatibles, y la LAN o VLAN en la que los equipos quedarían visibles entre sí estaría formada únicamente por aquellos hosts detrás de este Switch o AP no gestionable. Este modo de funcionamiento permite aislar los dispositivos a nivel 3 de la torre OSI.

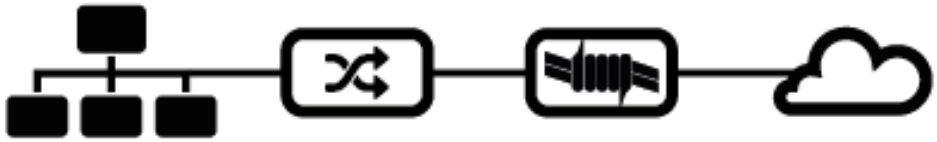


Figura 32-Esquema Inline Enforcement

Como se puede ver en la imagen, PacketFence se convierte en la puerta de salida de la red y permite hacer NAT al tráfico entrante utilizando IPTables hacia internet o hacia otra sección de la red. No se necesita ninguna configuración especial en los dispositivos, sólo se necesita asegurar que el dispositivo se comunica con la VLAN “inline”. En esta configuración todo el tráfico pasa por PacketFence puesto que es la puerta de salida (Gateway) para esta VLAN.

El control de acceso para el funcionamiento en línea se basa completamente en IPTables. Cuando un usuario no está registrado y se conecta en la VLAN “inline”, PacketFence le proporciona una dirección IP correspondiente a la red interna. A partir de este punto se marca al usuario como no registrado en el firewall y su tráfico es denegado hasta que este usuario no se haya autenticado. Una vez que el usuario se ha registrado, PacketFence cambia las reglas del firewall (en este caso de las IPTables) para permitir a la dirección MAC del usuario pasar a través de él.

El modo de gestión inline debido a su naturaleza tiene varias limitaciones de las que es necesario ser consciente. Todos los usuarios que se encuentras tras un interfaz inline se encuentran en la misma capa 2 de la LAN. Cada paquete de los usuarios autorizados atraviesa el servidor de PacketFence incrementando la carga del servidor considerablemente. Además, esto convierte a PacketFence en un único punto de fallo para el acceso a Internet. No permite gestionar redes enrutadas, sólo funciona a nivel 2.

Existe un modo de funcionamiento híbrido que permite la coexistencia le los dos mecanismos anteriormente descritos, “inline” y “Out-Of-Band”.

Tanto para el método “inline” como “Out-Of-Band” cuando un usuario no se autenticado aún, todo su tráfico web es redirigido a un portal cautivo, cualquier otro tráfico generado es bloqueado.

Un portal cautivo funciona interceptando el acceso HTTP a páginas web y redirigiendo a los usuarios a una aplicación web que proporciona instrucciones y herramientas para la actualización del ordenador o el acceso a internet.

4.6.3 Características

PacketFence proporciona un completo sistema de control de acceso a redes que cuenta con múltiples características, las más destacables son las siguientes [43]:

- Cuenta con un sitio web cautivo para autenticación y registro de dispositivos que solicitan el acceso a la red. Un portal único externo ofrecido por un dispositivo NAC para la autenticación inalámbrica y por cable, elimina la necesidad de crear varios portales, y consolida los procesos de políticas de gestión.
- Permite la detección de actividades de la red anormales.
- Puede realizar exploraciones preventivas de vulnerabilidades.
- Permite el aislamiento de los dispositivos problemáticos.
- Servicio de DHCP.
- Permite un control de acceso basado en roles.
- Integración con escáneres de vulnerabilidades diferentes y soluciones de detección de intrusos.
- Soporte 802.1x con FreeRadius incluido.
- Gestión centralizada de las redes tanto cableada como inalámbrica.
- Integración con el sistema para la detección de intrusos y vulnerabilidades SNORT y NESSUS.
- Soporte VLAN y aislamiento de redes.
- En cuanto a la Autenticación, PacketFence tiene soporte para: Microsoft Active Directory, Novell eDirectory, OpenLDAP, Cisco ACS, RADIUS (FreeRADIUS, Radiator, etc.), fichero local (htpasswd file), FaceBook, SMS, LADP, email, Google y Github.
- PacketFence se integra de forma perfecta a las redes inalámbricas a través del módulo FreeRadius. Esto permite asegurar las redes cableadas e inalámbricas de la misma manera usando la misma base de datos de usuarios y el mismo portal cautivo, proveyendo de una experiencia consistente para los usuarios.

PacketFence se ha creado utilizando estándares abiertos para evitar el tener que centrarse en un solo vendedor. Los estándares usados y soportados son los siguientes:

- 802.1X
- Simple Network Management Protocol (SNMP)
- Standard SNMP management information base (MIB) como por ejemplo BRIDGE-MIB, Q-BRIDGE-MIB, IF-MIB, IEEE8021-PAE-MIB
- RADIUS
- Netflow / IPFIX
- Wireless ISP Roaming (WISPR)

Además posee algunos puntos de extensión que le permiten ser customizado por el propio cliente mediante código PERL.

En la Figura 33, en color azul se pueden apreciar todos los componentes que componen PacketFence.

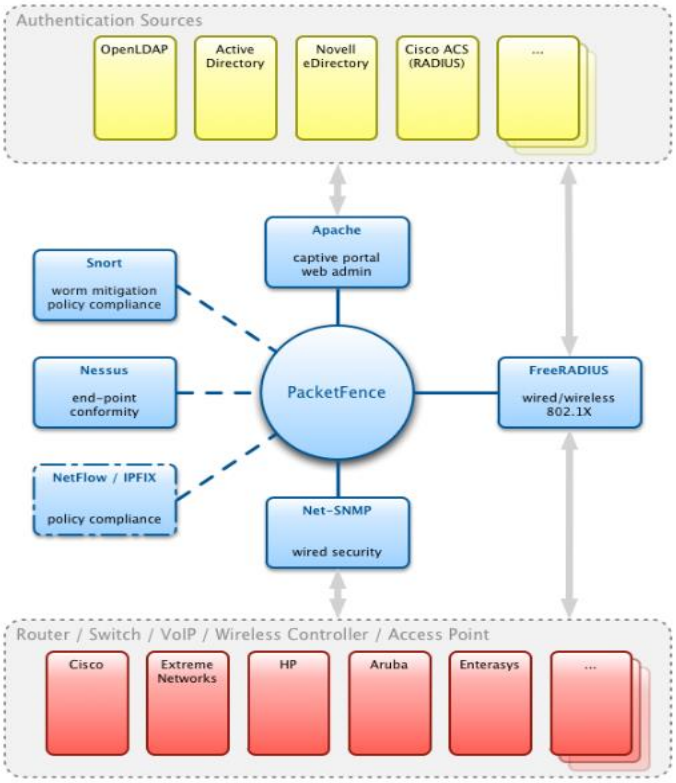


Figura 33-Componentes de PacketFence.

4.6.4 Instalación de PacketFence.

Antes de instalar el servidor es necesario asegurar que se disponen de los medios necesarios, para ello se tienen que cumplir diferentes condiciones descritas a continuación.

Componentes necesarios a instalar:

- ✓ Base de datos MySQL
- ✓ Servidor WEB Apache
- ✓ Servidor DHCP
- ✓ Servidor RADIUS

Requisitos mínimos Hardware:

- ✓ Intel o AMD CPU 3 Ghz
- ✓ 4 Gb de RAM
- ✓ 100 Gb de espacio libre en disco (RAID-1 recomendado)
- ✓ 1 tarjetas de red Servicio

Requisitos mínimos de Sistema Operativo:

- ✓ Red HAT Enterprise Linux 6.X
- ✓ CentOS 6.X
- ✓ Debian 7.0
- ✓ Ubuntu 12.04 LTS

Se ha decidido instalar PacketFence 4.2.0 sobre una máquina virtual concretamente VirtualBox [36] con sistema operativo Ubuntu 12.04 LTS, por tanto antes de realizar la instalación de la solución NAC se ha realizado la instalación de la máquina virtual y del correspondiente sistema operativo, pasos que no se recogen en este proyecto. A continuación se va a describir el procedimiento adecuado para la instalación de PacketFence en un sistema operativo Ubuntu, que es el procedimiento que se ha seguido en este caso.

Para la instalación de PacketFence se han seguido los siguientes pasos [44]:

1. Lo primero que hay que hacer es añadir el repositorio "Inverse" en la localización "*/etc/apt/sources.list.d/*" , para ello en esta dirección hay que crear un fichero llamado "packetfence.list" el cual debe contener la siguiente línea:

   ```
   deb http://inverse.ca/downloads/PacketFence/ubuntu precise precise
   ```

2. Tras añadir el repositiorio es necesario introducir las claves para la descarga mediante el siguiente comando:

   ```
   sudo apt-key adv --keyserver keys.gnupg.net --recv-key 0x810273C4
   ```

3. Una vez añadidas las claves se actualizan los repositorios y se instala PacketFence:

   ```
   sudo apt-get update

   sudo apt-get install packetfence
   ```

4. Si se quiere usar el modo inline es necesario instalar IPTables:

   ```
   Sudo apt-get install xtables-addons-source xtables-addons-commons

   Sudo module-assistant auto-install xtables-addons-source
   ```

   Durante el proceso de instalación, el cual incluye todas las dependencias necesarias para el correcto funcionamiento del servidor, se pedirá la clave de la base de datos MySQL, la cual es necesario recordar para la posterior configuración del servidor.

4.6.5 Configuración en modo Inline

En primer lugar se ha procedido a realizar las pruebas en modo puramente Inline utilizando PacketFence como puerta de salida para los dispositivos. Este modo de funcionamiento no es escalable para grandes redes como las que podría tener una empresa, pero si escala para ámbitos más locales como pequeñas oficinas, negocios o redes domésticas. Esta configuración

va a permitir ver su funcionamiento usando routers ADSL domésticos los cuales se pueden encontrar en una gran cantidad de hogares como medio de acceso a Internet.

Para las pruebas de la solución NAC se necesitan los siguientes componentes:

- PC donde se instalará el servidor y las máquinas virtuales.
- VirtualBox
- Router ADSL

Para poder probar la solución NAC hay que simular un escenario real, para ello se han empleado máquinas virtuales utilizando Virtualbox.

Para simular un escenario "inline" se necesita una red interna formada por los hosts que quieren ser autenticados y su electrónica de red en nivel 2, un servidor PacketFence que actúe como gateway y firewall entre la red interna y la externa, un router ADSL y conexión a Internet. El escenario simulado se muestra en la siguiente Figura 34.

Figura 34-Estructura de la red.

En la imagen se ve la red interna con direccionamiento 10.0.0.0/24, esta LAN estará formada como se ha comentado, por hosts virtuales. Para poder implementarla mediante VirtualBox hay que configurar las máquinas para que su interfaz de red sea de tipo "Red Interna". VirtualBox tiene diferentes mecanismos de funcionamiento para sus interfaces de red, este en particular permite crear redes independientes del host anfitrión, es decir, independientes del ordenador donde se han instalado las máquinas virtuales. Se ha creado por tanto una red interna en VirtualBox a la que se configurarán todos los interfaces de red de los hosts finales.

El servidor PacketFence cuenta con dos interfaces uno de ellos debe configurarse en la red interna al igual que en los hosts y el otro se debe configurar en modo "Adaptador-Puente", este modo de funcionamiento del interfaz de red de la máquina virtual permite que esta funcione como si fuese un equipo real conectado a la red, para ello utiliza la tarjeta física del ordenador anfitrión. Este interfaz por tanto estará conectado a la red real (192.168.1.0/24) y por tanto tiene que tener una dirección IP dentro de este rango. Este además será el

encargado de realizar la traducción de IP de la red interna a otra IP de la red externa (192.168.1.0/24).

En este caso tras el servidor de NAC se encuentra un router ADSL convencional el cual se encarga de realizar el nateo entre direcciones privadas y públicas.

En general en esta instalación se tiene una red interna (10.0.0.0/24) otra externa (192.168.1.0) y el acceso con Internet.

Una vez instalado el sistema y configurada la máquina virtual del servidor PacketFence como se ha descrito anteriormente, para acceder a su configuración de este, es necesario introducir la siguiente URL en el navegador desde cualquier máquina de la LAN externa del servidor o desde el propio servidor.

https://IPdelServidor:1443/configurator/

En el caso particular de ejemplo, se cuenta con un router ADLS Amper ASL-26555 [46], este está configurado para ejercer las funciones de servidor DHCP asignando direcciones IP privadas de la red 192.168.1.0/24 a las máquinas que se encuentran en esta red. Además de funcionar como servidor local DHCP, el router se encarga de realizar las funciones de NAT convirtiendo la dirección privada de la red local del rango 192.168.1.0/24 a una dirección pública proporcionada por el proveedor de servicios (ISP), que en el caso del ejemplo es Telefónica.

Como conviene que la dirección IP del servidor en la red externa sea fija, mediante la página de configuración del router (Introduciendo en el navegador la dirección IP 192.168.1.1) se ha reservado la IP 192.168.1.42 para el interfaz eth2 del servidor de PacketFence en esa red. De esta forma esta dirección será estática a pesar del servidor DHCP del router.

Como dirección de IP del interfaz de la red interna se ha tomado la dirección 10.0.0.1 la cual hay que configurar en el interfaz de la máquina de forma manual. Para ello, teniendo cuenta que el sistema operativo de la máquina virtual del servidor es Ubuntu es necesario introducir el siguiente comando:

```
Sudo ifconfig eth1 10.0.0.1/24
```

Por tanto ahora que las direcciones IP del servidor de PacketFence son conocidas se puede acceder a la web de configuración del mismo mediante cualquier máquina conectada a una de las dos redes introduciendo una de las siguientes URLs en el navegador:

https://192.168.1.42:1443/configurator/

https://10.0.0.1:1443/configurator/

En la siguiente Figura 35 se puede ver la topología física que tendría que tener una implementación real del sistema NAC de PacketFence en su modo de funcionamiento “inline” y como se puede ver no se diferencia demasiado de la creada mediante máquinas virtuales en este trabajo. En ambos escenarios aparecen tres tramos de conexión, el primero entre la red interna y el servidor, el segundo une el servidor con el router, y el tercero es el que permite el

acceso a Internet. En nuestro caso al tener todo realizado mediante máquinas virtuales no se dispone de equipamiento físico a nivel dos ni se pueden realizar pruebas mediante APs reales como se aprecia en la figura nombrada.

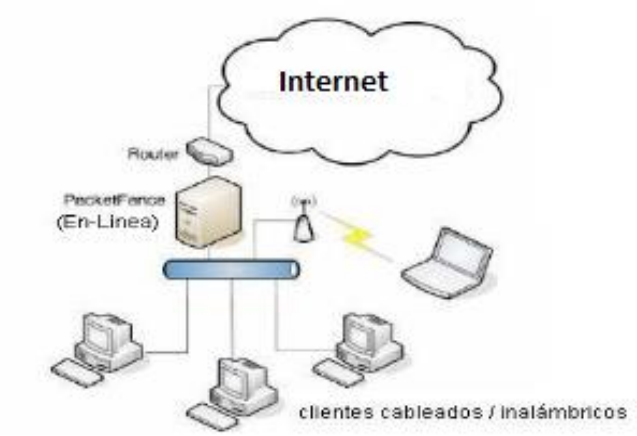


Figura 35-Estructura de escenario real.

Como se ha comentado, tras la instalación del servidor, queda una URL disponible por la que se accede a la web de configuración, dentro de esta web, el primer paso es seleccionar el tipo de mecanismo en el que debe funcionar PacketFence. Como no se dispone de equipos compatibles, se ha seleccionado el mecanismo "Inline".

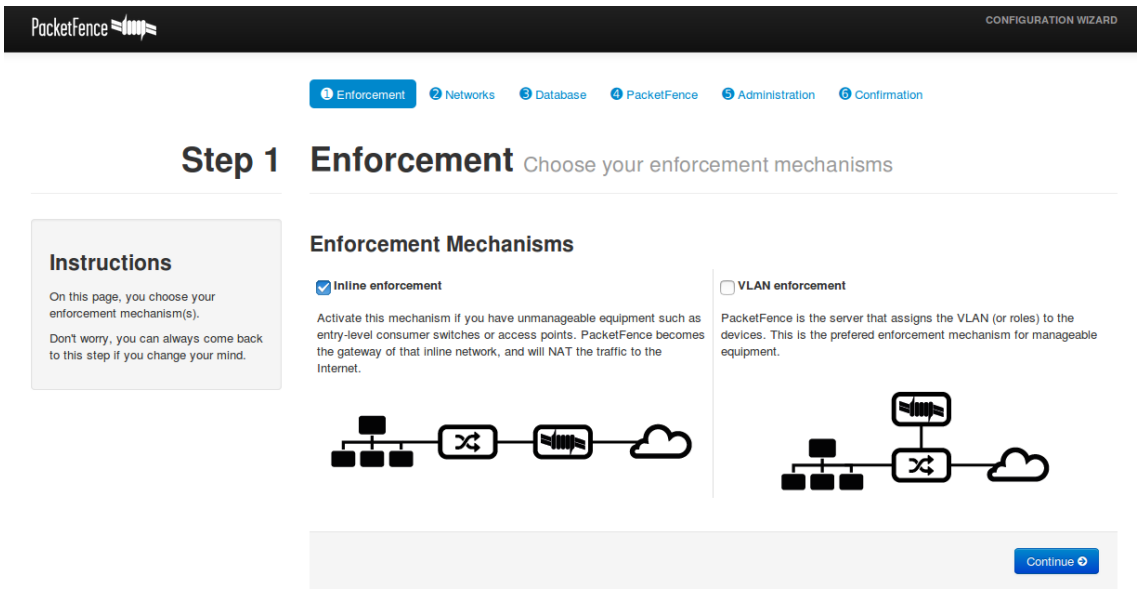


Figura 36-Paso 1 configuración PacketFence

El segundo paso es comprobar la dirección IP de los interfaces, en este caso se tienen dos, el interfaz eth1 cuya dirección IP es 10.0.0.1 y el interfaz eth2 con dirección 192.168.1.42.

El primer interfaz debe configurarse en modo “inline”, este debe de estar en la red del router, mientras que el segundo debe configurarse en modo “inline”. Para configurar cada interfaz hay que clicar en su nombre. En el caso de eth1 se selecciona el modo “inline” y se le asigna como servidor de DNS el que se tenía por defecto en la LAN antes de instalar el servidor, el cual en este caso es el servidor de DNS del ISP cuya dirección IP es 80.58.61.250. Esto es así puesto que en el modo “inline” el servidor actúa como un elemento intermedio que hace las veces de firewall y proxy NAT.

Como puerta de salida hay que configurar la dirección IP del router en la LAN que es la que nos permitía anteriormente conectarnos a Internet, en este caso es 192.168.1.1. Hay que poner la dirección del interfaz del router en esta red, y es a través del cual le llegará todo el tráfico proveniente de la red interna. En el modo Inline, PacketFence realiza el nateo de la red interna a la externa y se comunica con la externa mediante el default Gateway.

El segundo interfaz debe configurarse en modo “management” y este será el que nos permita el acceso a la consola de configuración basada en web del servidor PacketFence. Este interfaz además es también el encargado de realizar el nateo.

Por lo tanto para el modo inline se necesitan dos interfaces:

-Management: Es el interfaz al que se conecta el servidor para poder gestionarlo bien por SSH o HTTPS. Se encarga de realizar el nateo. Se encuentra en la red externa.

-Inline: Es el interfaz que actúa como puerta de enlace para la red interna. Se encuentra en la red interna.

Esta configuración se puede ver en la siguiente Figura 37.

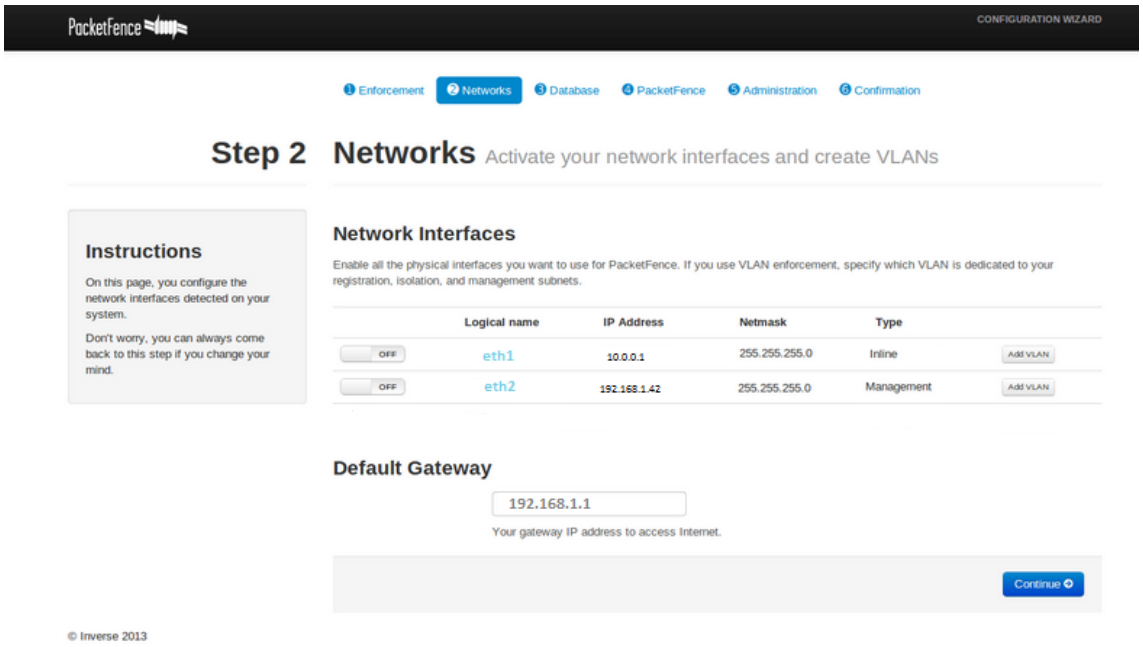


Figura 37-Paso 2 configuración PacketFence

El tercer paso en el proceso de configuración del servidor PacketFence es la base de datos. Lo primero que hay que hacer es comprobar el funcionamiento de MySQL, para ello hay que introducir la contraseña de MySQL que se ha solicitado durante el proceso de instalación de PacketFence. En este caso se ha decidido que esta sea “mysql”. El nombre del usuario se deja por defecto “root”. Una vez introducida esta contraseña se comprueba si es correcta clicando el botón “Test”.

Una vez comprobada la correcta instalación y acceso a MySQL se procede a crear la base de datos, el nombre por defecto de esta es “pf”. Si se clica en el botón “Create database and tables” se procede a crear la base de datos con sus correspondientes tablas.

Por último es necesario crear el usuario para la base de datos, en este caso se ha dejado el nombre que venía por defecto “pf”, y como contraseña se ha introducido “packetfence”.

En la siguiente figura se puede ver la pantalla de configuración de este tercer paso.

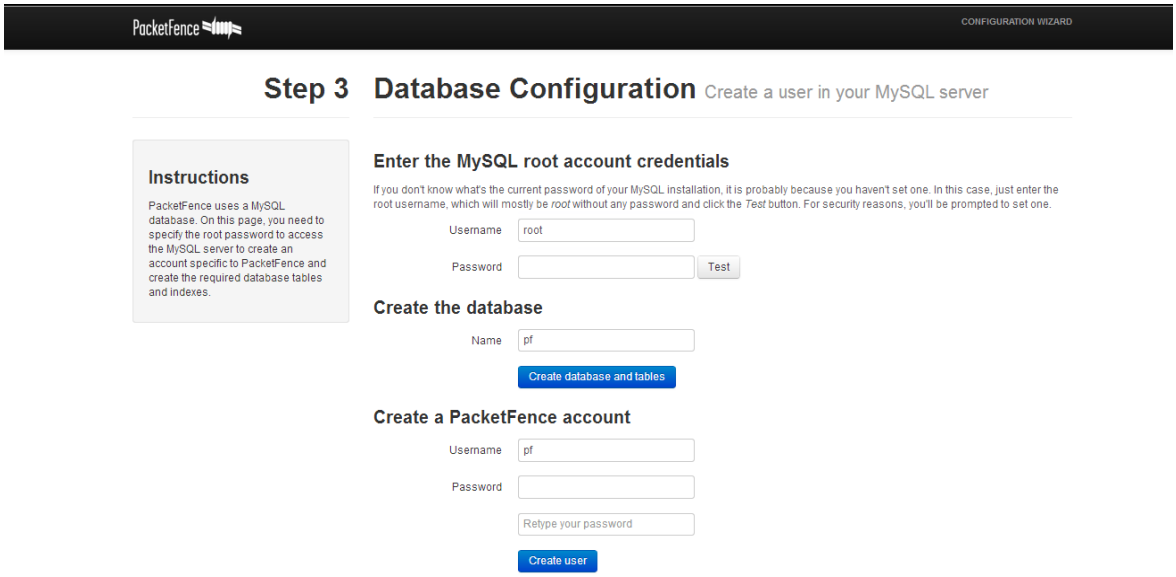


Figura 38-Paso 3 Configuración PacketFence

Al crear esta base de datos se crean una serie de tablas que se pueden ver en la Figura 39, estas se usan para almacenar datos referentes al programa que luego aparecen en el dashboard o tablón de gestión. Por ejemplo se almacenan en la tabla “node” todos los nodos detectados por PacketFence y si están registrados o no. En la tabla “person” se almacena información de los usuarios administradores. También contiene información sobre los logs como por ejemplo en la tabla traplog que almacena información de los traps enviados por el servidor a los switches o puntos de acceso que gestione en caso de que funcione en modo Out-Of-Band.

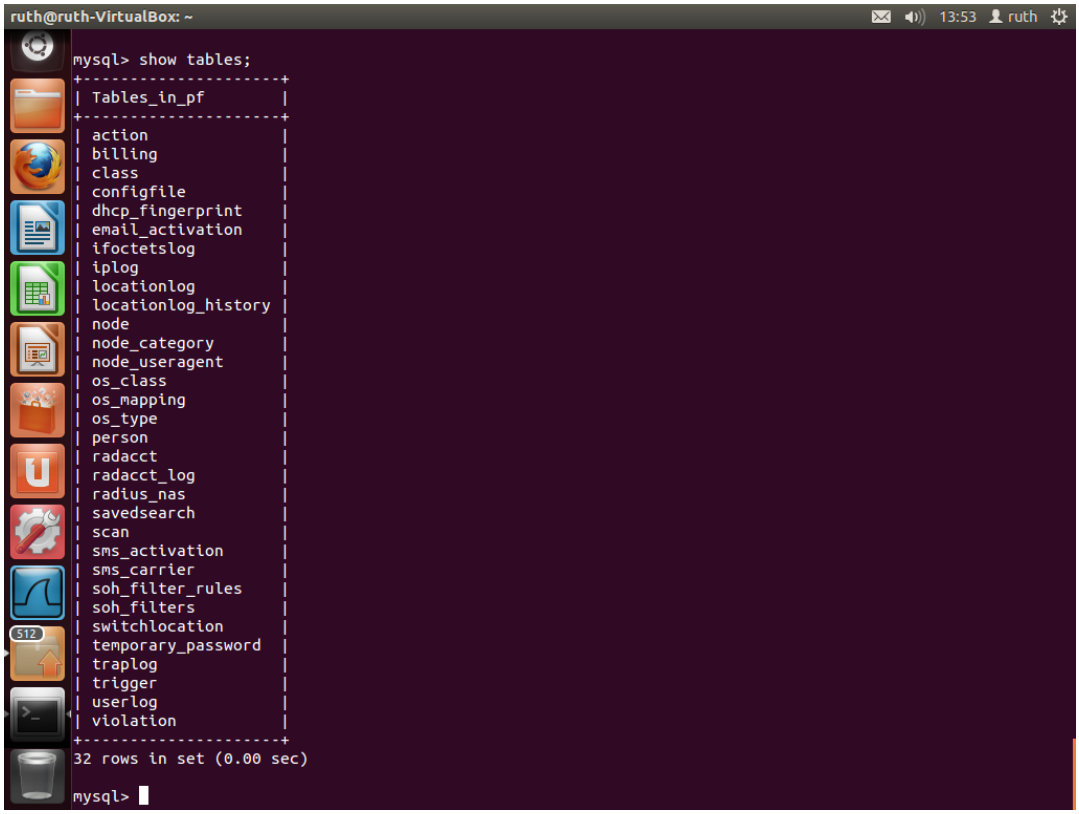


Figura 39-Tablas de la base de datos pf.

El cuarto paso para la configuración del servidor es establecer su dominio, el nombre del host, el servidor DHCP de la red y la dirección de correo a la que enviar alertas.

En este caso como dominio se ha elegido pf.org, el hostname es pfserver y como servidor DHCP se va a usar el propio módulo de DHCP que incorpora el servidor PacketFence por lo que como dirección IP hay que configurar es la del servidor en la red interna: 10.0.0.1

Este último paso en la configuración es el responsable de que cuando un usuario de la red interna se conecte a esta adquiera sus parámetros de configuración de red como su dirección IP y su puerta de enlace. Además, la implementación del servidor DHCP que incorpora PacketFence permite la actualización del servidor de DNS (Domain Name System) del host por lo que le asigna el servidor de DNS propio de PacketFence. Esto hace posible que el equipo final del usuario sea capaz de resolver el dominio elegido para el servidor PacketFence.

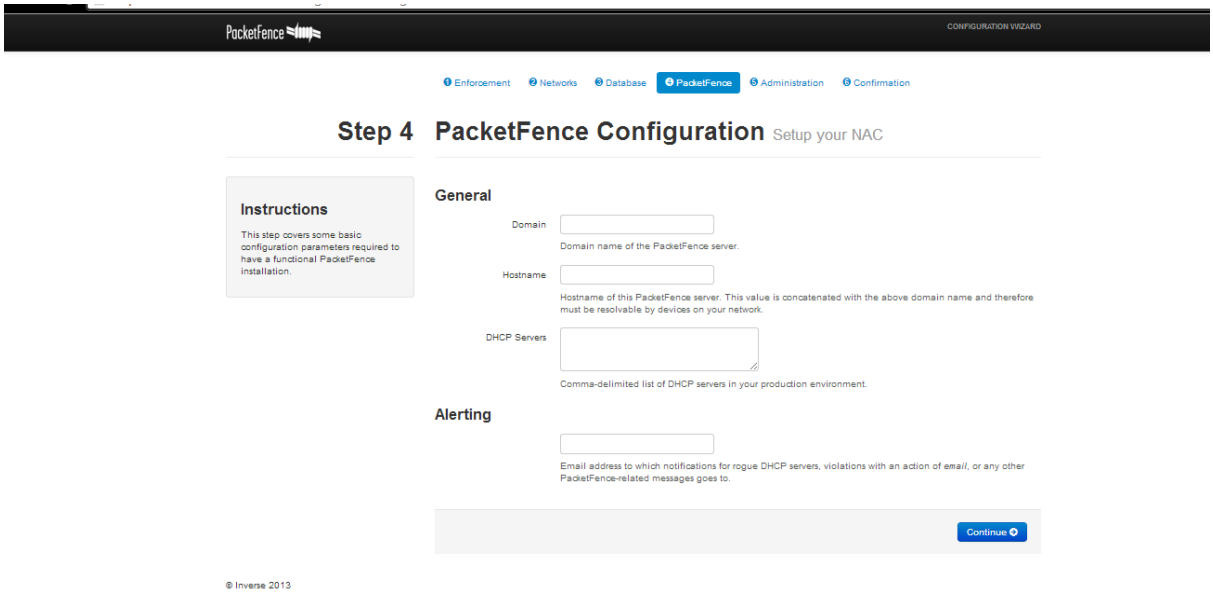


Figura 40- Paso 4 Configuración PacketFence

El paso número 5 consiste en configurar el administrador del sistema, para ello hay que introducir nombre de usuario y contraseña. En este caso el usuario es “admin” y la contraseña “admin”

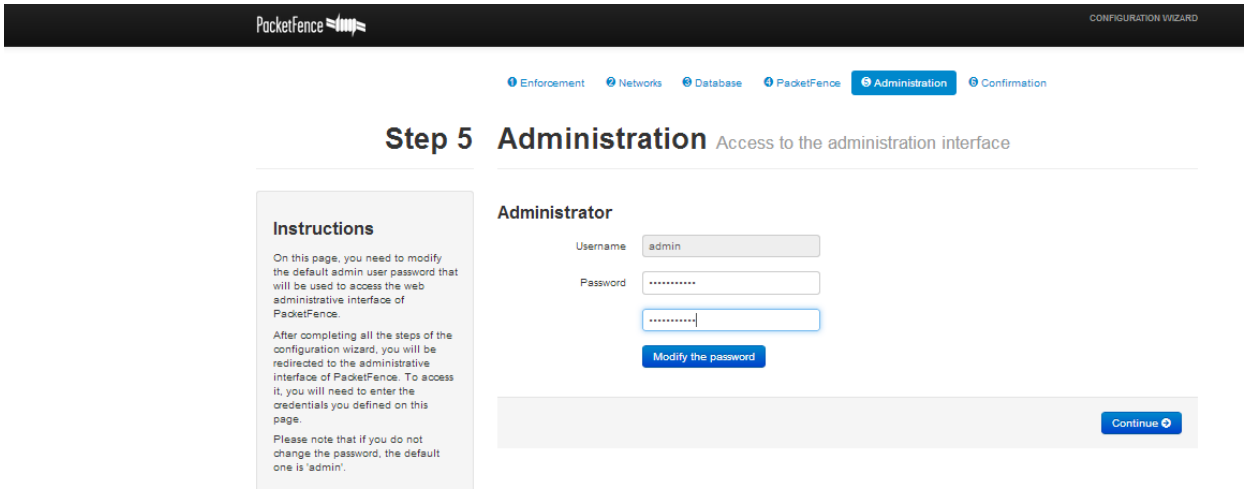


Figura 41-Paso 5 Configuración PacketFence

El último paso para el correcto funcionamiento del servidor es iniciar los servicios clicando en el botón “Start PacketFence”.

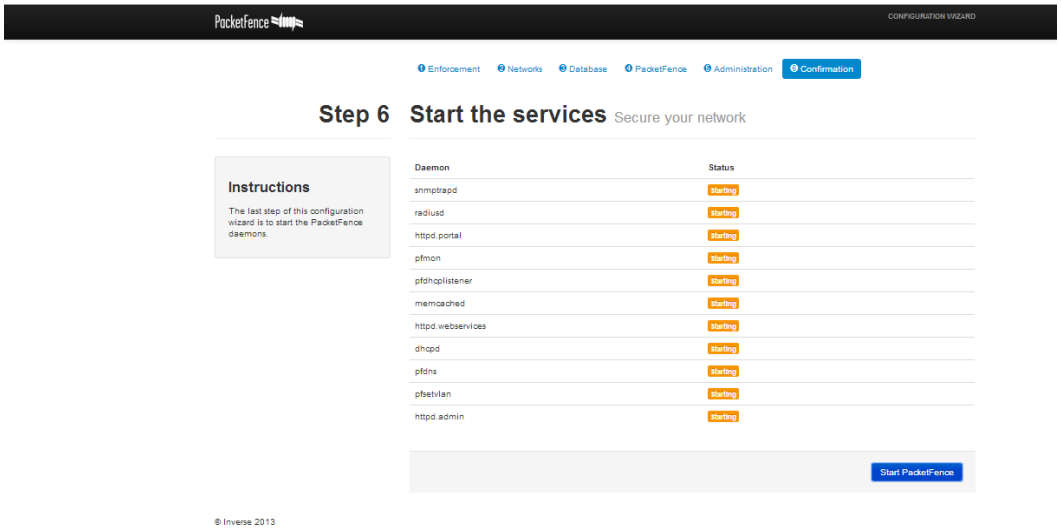


Figura 42-Paso 6 Configuración PacketFence

Para el correcto funcionamiento del servidor en el modo "inline" es necesario que el servidor sea capaz de enrutar entre el tráfico de la red interna y externa, para ello hay que activar "IP forwarding". Para hacer esto de forma permanente hay que modificar el fichero "/etc/sysctl.conf" y asegurarse que la siguiente línea está descomentada y tal como aparece a continuación:

```
net.ipv4.ip_forward = 1
```

Es necesario que el servidor enrute puesto que todos los paquetes que se envíen por la red interna deben pasar a la red externa por lo que el servidor tiene que ser capaz de enrutar estos paquetes hacia a la IP del router.

Una vez realizado este paso se puede dar por finalizada la configuración general del servidor y se puede acceder a la interfaz web de gestión del servidor a través de cualquier máquina conectada a la red en la que se encuentra el interfaz de gestión (192.168.1.0/24) o en el propio servidor, mediante la dirección IP del interfaz de gestión que en este caso es 192.168.1.42 Para acceder a esta interfaz es hay que introducir la siguiente URL en el navegador:

```
https://192.168.1.42:1443
```

Esta dirección nos dirigirá a la página de entrada del interfaz web de gestión del servidor que es la que se aprecia en la siguiente figura.

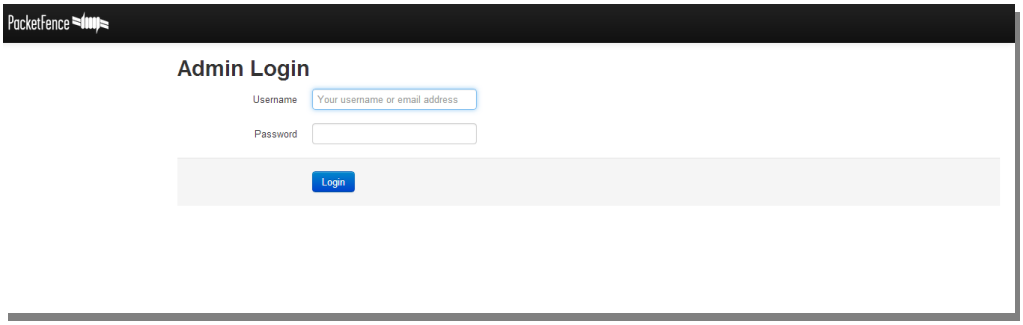


Figura 43-Interfaz web de gestión de Packetence

Como se puede comprobar por ejemplo en la Figura 44 da error de HTTPS (Hypertext Transfer Protocol Secure) esto es debido a que los certificados del servidor PacketFence no están emitidos por una entidad certificadora válidos si no que se han generado localmente. Como han sido creados localmente son fiables pero estos se podrían sustituir por unos con validez más global si se quisiera.

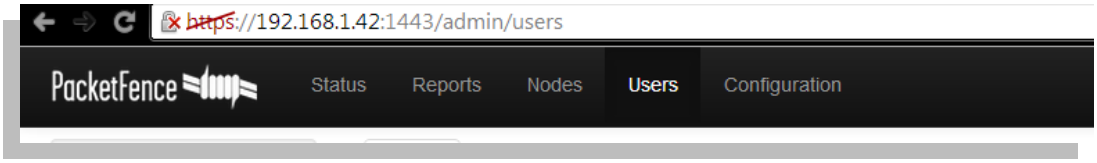


Figura 44-Https PacketFence

4.6.6 Interfaz web de administración.

Como se ha comentado este interfaz es accesible a través de la dirección IP de gestión del servidor y a través del puerto 1443. Tiene diversas opciones y a partir de él se configura de forma gráfica el servidor.

La interfaz web consta de un menú superior horizontal con los siguientes apartados:

- Status: Se muestra el estado de la red. Tiene dos campos, el" Dashboard" (Figura 45) que indica la cantidad de nodos registrados, los nodos nuevos, cuántos son inalámbricos y cuantos cableados, además de si se ha producido algún incumplimiento de alguna regla establecida para realizar la conexión. Y el segundo campo es "Services" (Figura 46) en el que aparecen todos los servicios que corren el servidor y la posibilidad de pararlos.

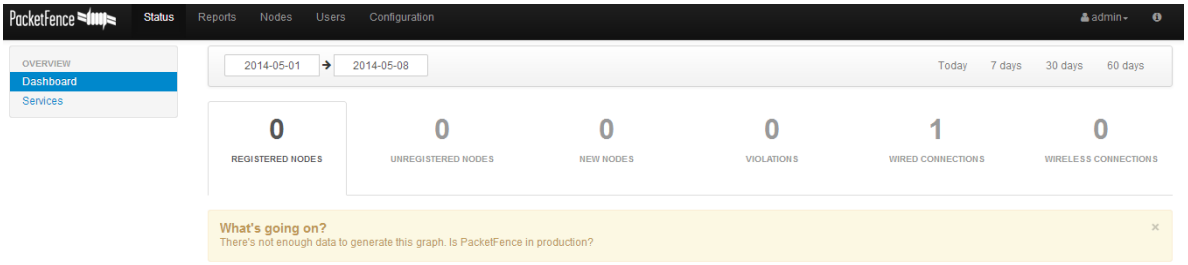


Figura 45-Dashboard

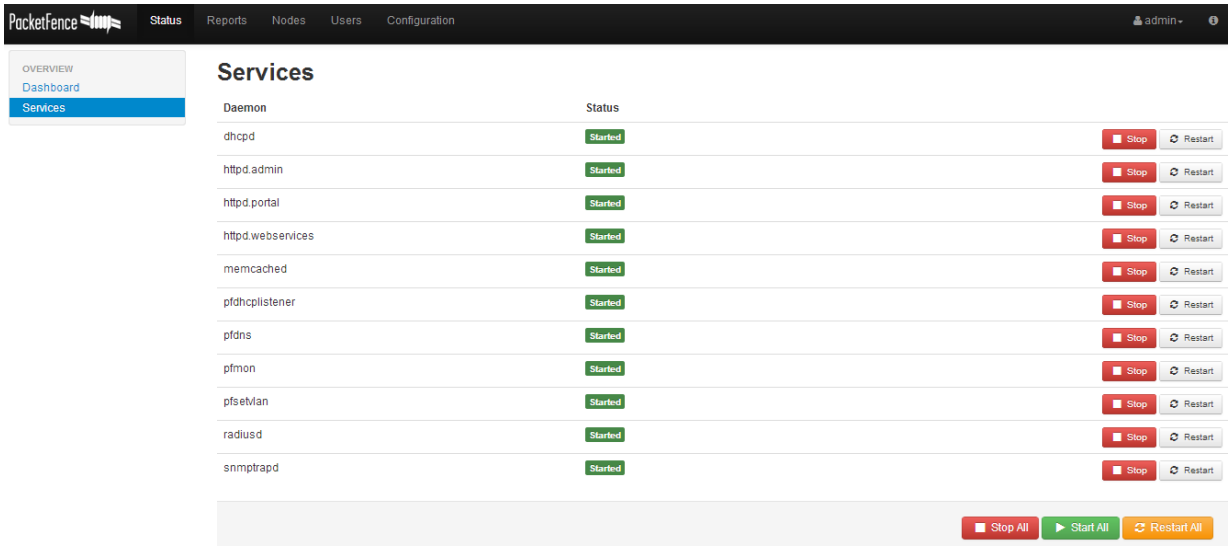


Figura 46-Services

- Reports: Permite realizar informes sobre el estado de los nodos, su sistema operativo, las violaciones de seguridad producidas por estos. Contiene una parte de seguimiento (Accounting) que permite ver qué clientes consumen más ancho de banda.

- Nodes: Permite introducir nodos manualmente o importarlos a través de un fichero en formato CSV. Esta pestaña permite configurar los nodos, se les puede asignar roles, bloquear, ver su MAC, su IP y la fecha de última conexión, etc. Esto se puede apreciar en la Figura 47.

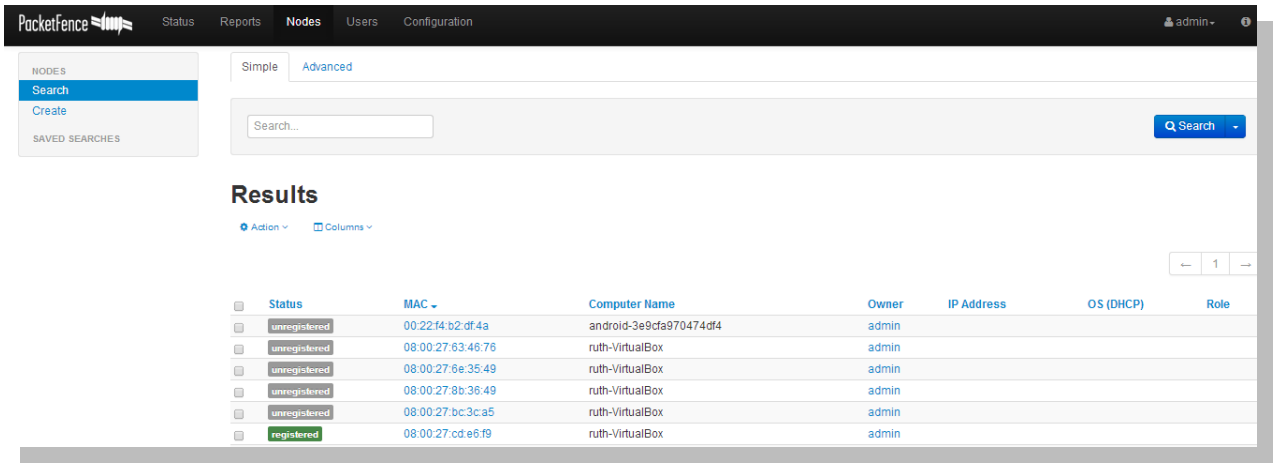


Figura 47-Pestaña Nodes

- Users: Se refiere a los usuarios del servidor, los encargados de gestionarlo y gestionar la red. Permite añadir nuevos y buscar. Al crear nuevos usuarios de administrador se les puede dar acceso a la configuración parcial o total del servidor controlando de esta forma sus privilegios.

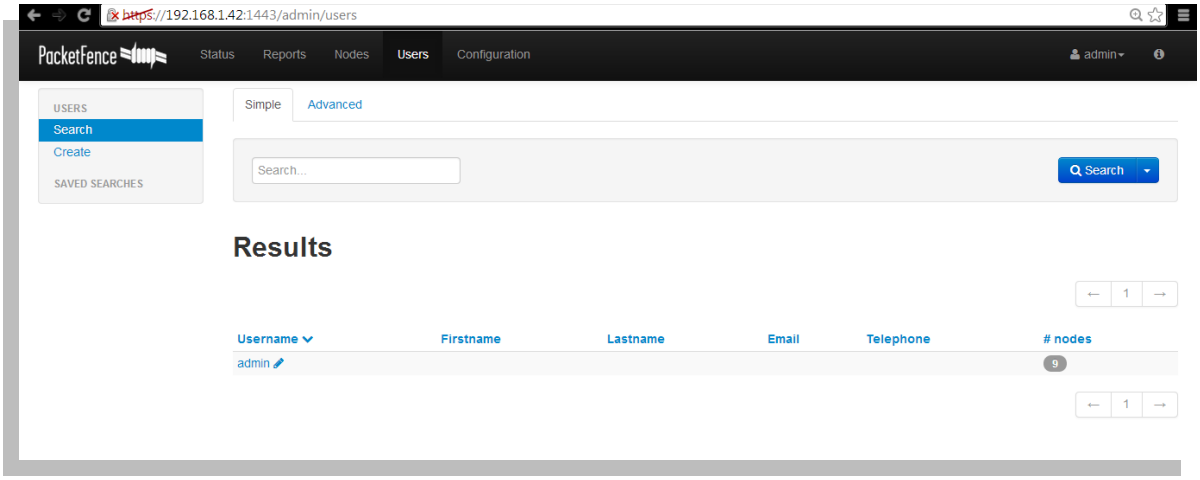


Figura 48-Pestaña Users

- Configuration: En esta opción se configura el servidor de NAC PacketFence. Cuenta con un menú lateral dividido en diferentes secciones cada una referente a una parte de la configuración del servidor:

    - Main: Es la configuración general del servidor, cuenta con muchos subapartados en los que se puede configurar la IP del servidor, sus interfaces, su dominio, configurar la IP del servidor DHCP, cambiar los servidores de DNS, configurar el acceso del administrador, monitorización de la red, el portal cautivo, etc.

    - Network: Permite configurar nuevos Switches a PacketFence, nuevos APs y los interfaces que tiene el servidor en la red.

    - Users: Permite configurar dos cosas, los roles que se les da a cada usuario y la fuente de autentificación para los mismos. Los roles sirven para clasificar los usuarios. Se pueden asignar manualmente o automáticamente al ser autenticados.

    - Compliance: En esta sección hay dos campos, “violations” y “Statement of health”. En la primera sección aparece una lista con las reglas más comunes, con las violaciones de seguridad más comunes y se pueden activar para denegar el tráfico o el acceso a la red del host que las incumpla. Un ejemplo de esto es el tráfico P2P. PacketFence se integra con programas de detección de paquetes como Snort [37] o Suricata [38] lo que le permite ver que tráfico circula por la red y aplicar políticas como el filtrado del tráfico P2P que se ha comentado entre otras. También se pueden establecer otro tipo de políticas como la denegación de la conexión a algún sistema operativo en concreto. PacketFence es capaz de detectar actividades anormales en la red (virus, gusanos, spyware, tráfico denegado por el establecimiento de alguna política, etc.) mediante el uso de sensores remotos (Snort o Suricata). Más allá de la simple detección, PacketFence tiene sus propios mecanismos de alertas y supresión para cada tipo de alerta. Contiene un conjunto configurable de

acciones para cada violación las cuales están disponibles para los administradores. PacketFence soporta tanto Nessus [39] como OpenVas [40] como motores de escaneo para la evaluación de las vulnerabilidades de los dispositivos. Según el resultado de estos escáneres se pueden establecer políticas de seguridad y nuevas violaciones de la misma.

En el apartado "Statement of Health" se hace referencia a la salud de los equipos. El "Statement of Health" (SoH) es un producto que fue desarrollado por Microsoft al que ellos denominan Network Access Protection (NAP). En las versiones de Windows hay un servicio NAP instalado que puede transmitir información sobre su salud (actualizaciones de antivirus, su estado, actualizaciones del sistema, etc.) a un servidor DHCP o RADIUS. Esto puede servir para crear políticas de nuevas violaciones en caso de que por ejemplo un equipo no tenga activado el antivirus.

PacketFence puede crear políticas de seguridad sin necesidad de tener un agente instalado en el cliente apoyándose en otros softwares como pueden ser Snort, Suricata, OpenVas o Nessus.

- Identification: PacketFence puede combinar diferentes mecanismos para bloquear de manera efectiva el acceso a la red de aquellos dispositivos que no se quieran admitir:

    - DHCP Fingerprint: PacketFence puede bloquear dispositivos en función de sus huellas DHCP. Cada sistema operativo tiene unas huellas DHCP únicas. Basándose en esto se pueden bloquear por ejemplo Videoconsolas, puntos de acceso o teléfonos VoIP (Voz sobre IP).

    - User-Agent: PacketFence puede bloquear usuarios en función de su agente de usuario. (Dispositivos Apple, si usan una versión antigua del navegador, etc.)

    - MAC Addresses: PacketFence puede bloquear el acceso a la red de dispositivos que tengan un patrón específico de dirección MAC. Usando esto, por ejemplo se pueden bloquear todos los dispositivos de un fabricante en concreto.

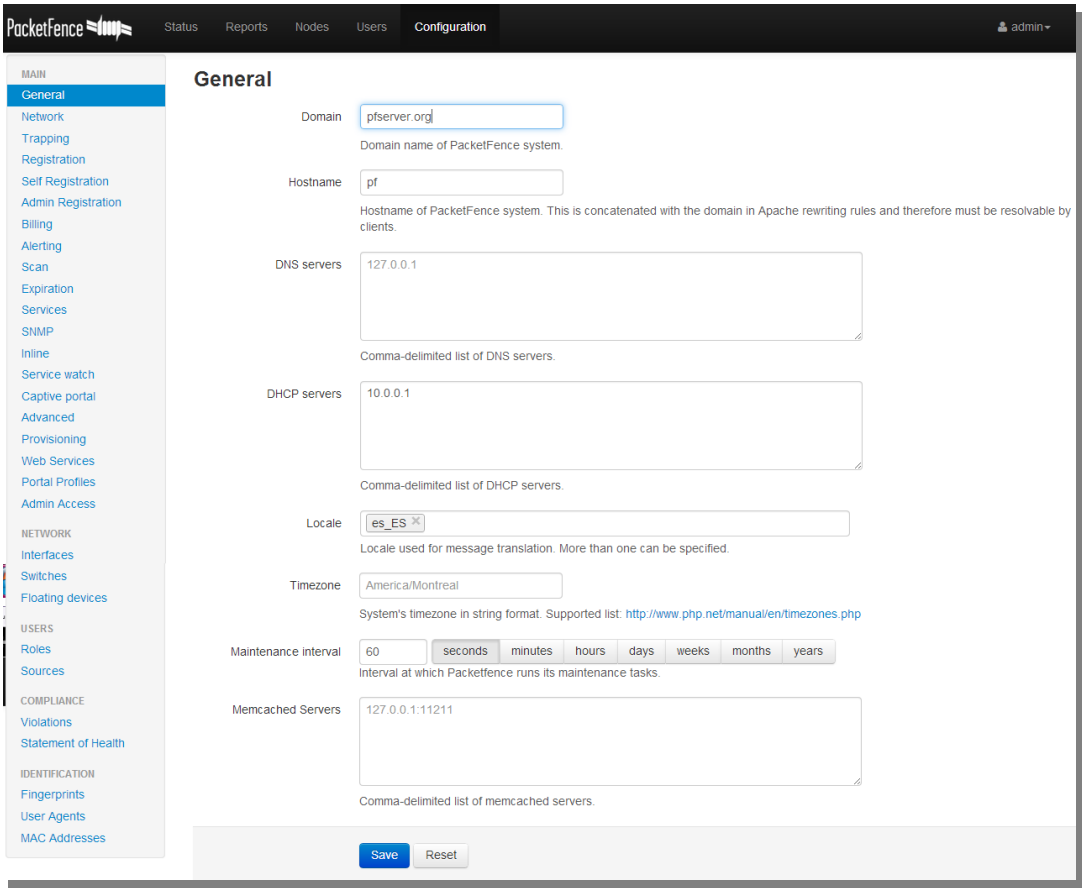


Figura 49-Pestaña Configuración

4.6.7 Portal cautivo.

Cuando un usuario intenta acceder a Internet es redirigido automáticamente al portal cautivo. Este tiene la opción de permitir a los usuarios registrarse utilizando diferentes medios. También incluye los campos usuario y contraseña para permitir al usuario autenticarse.

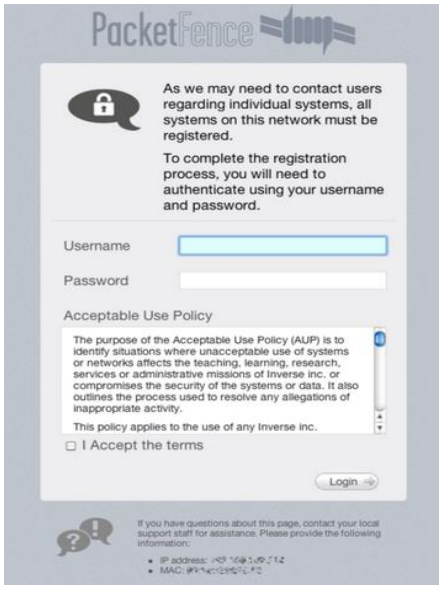


Figura 50-Imagen del portal cautivo.

Este portal cautivo puede modificarse de forma que cada empresa pueda personalizando añadiendo por ejemplo su logo y modificando las políticas de aceptación. Está creado a partir de plantillas XHTML creadas a partir de Toolkit [http://template-toolkit.org/]. Todos los ficheros están localizados en "/usr/local/pf/html/captive-portal/templates" y se pueden editar libremente. [47]

Si se quiere personalizar el portal modificando más que el código HTML, por ejemplo añadiendo nuevas variables hay que modificar los ficheros que se encuentran "/usr/local/pf/lib/pf/web/custom.pm" que consiste en un módulo Perl que permite sobrescribir el comportamiento por defecto del módulo predefinido /usr/local/pf/lib/pf/web.pm.

Muchos de los cambios se pueden realizar modificando únicamente los ficheros CSS guardados en /usr/local/pf/html/captive-portal/content/styles.css.

Otra forma más sencilla e intuitiva de realizar las modificaciones del portal cautivo es a través de la interfaz de configuración web del servidor. Dentro del apartado configuración, en el menú izquierdo lateral hay un enlace llamado "Portal Profiles", en este se encuentran los ficheros del portal cautivo.

Se pueden configurar perfiles de portal, es decir que aparezca un portal cautivo diferente en función de diferentes parámetros configurables como puede ser Switch por el que el usuario se conecte, SSID de la red WIFI, VLAN o fuente de autenticación.

Por defecto PacketFence tiene creado un perfil de portal cautivo que se aplica para todas las opciones.

En la Figura 51 se puede apreciar el apartado de configuración del portal cautivo por defecto. En la pestaña "Settings" se pueden configurar las políticas que se han comentado, es decir, cuando se quiere que se muestre ese portal cautivo. En la pestaña "Files" se encuentran los archivos. Estos se pueden pre-visualizar y editar online.

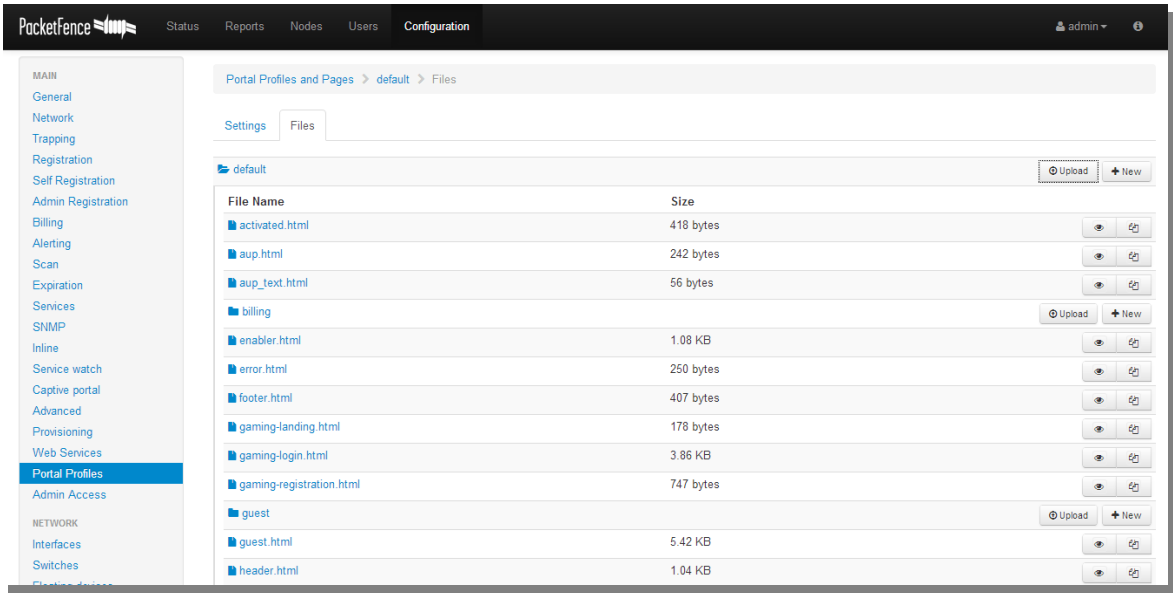


Figura 51-Ejemplo de archivos de portal cautivo.

El fichero aup_text.html contiene el texto mostrado en el portal cautivo. Este debería contener las políticas de seguridad que el usuario debe aceptar antes de entrar a la red. Se ha editado este texto de forma online con el editor html proporcionado por el servidor tal y como se puede ver en la Figura 52.

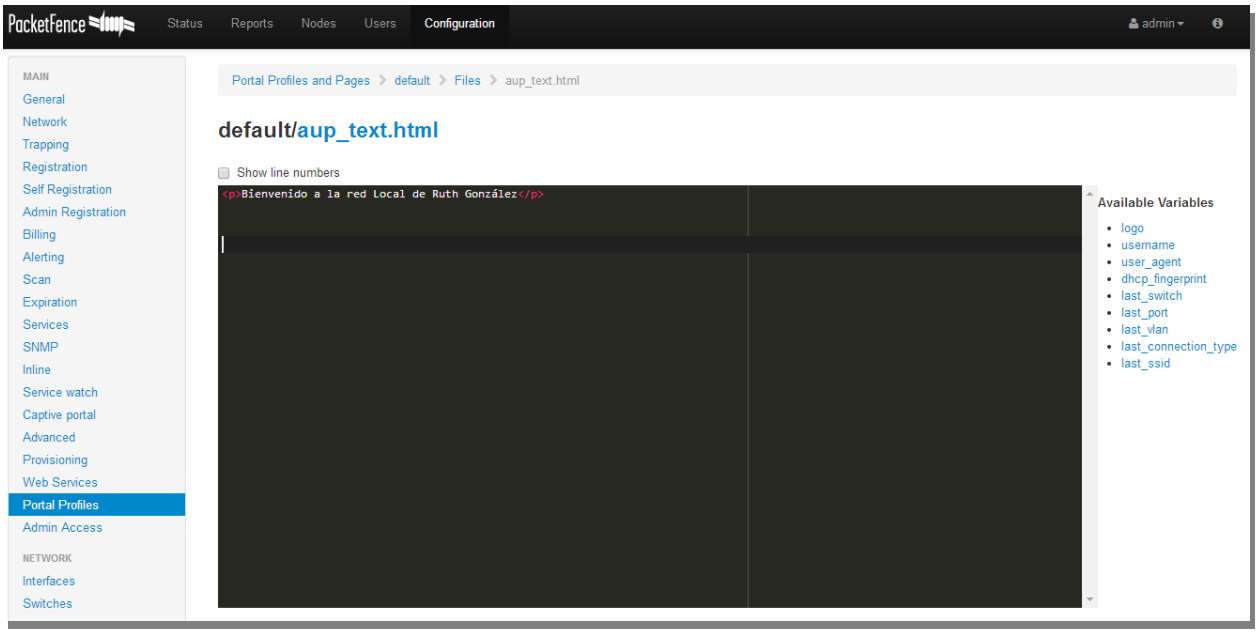


Figura 52-Ejemplo de edición en línea.

En la siguiente Figura 53 se puede ver el resultado del portal cautivo tras la modificación del fichero html. Como se puede apreciar ya no aparece el texto de la Figura 50 que venía predeterminado, sino que aparece el que se ha introducido a través del portal de configuración.

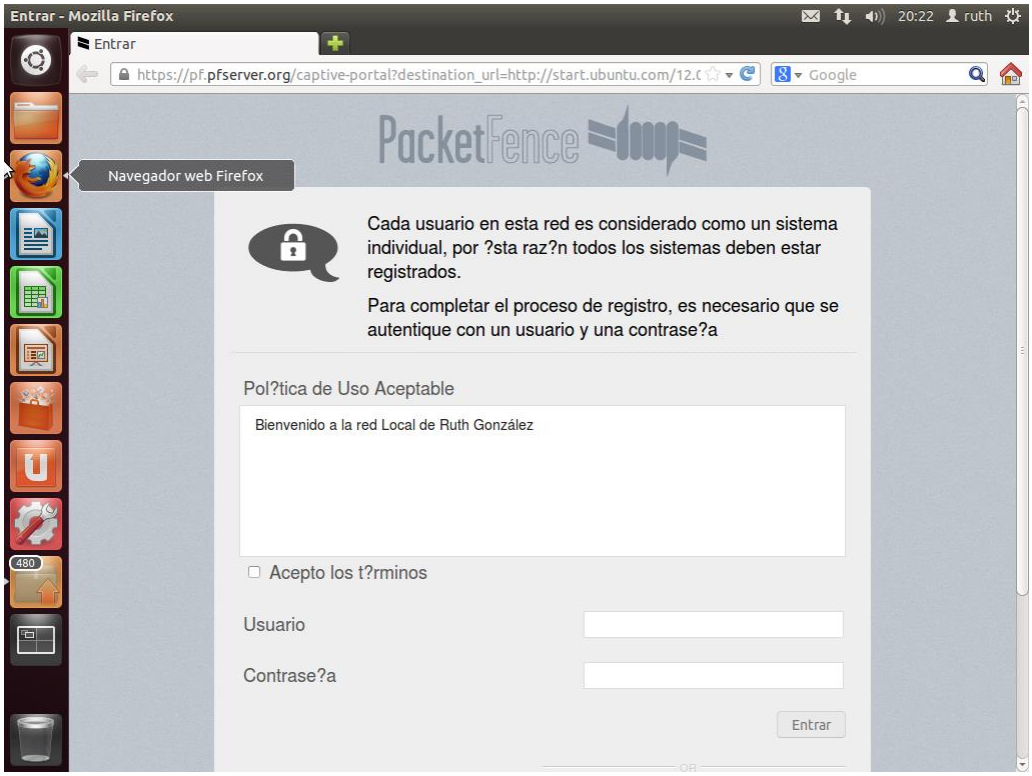


Figura 53-Portal cautivo personalizado

4.6.8 Configuración de autenticación.

Como se ha comentado en el apartado de características, PacketFence tiene diversos mecanismos de autentificación que se pueden clasificar en internos o externos en función de si forman parte del módulo del servidor o no.

Internos se tiene autenticación mediante RADIUS (FreeRadius) y mediante fichero local (htpasswd file). La autenticación mediante fuentes externas puede realizarse mediante Microsoft Active Directory, Novell eDirectory, OpenLDAP, Cisco ACS, FaceBook, SMS, LADP, email, Google y Github.

Como inicio para la prueba del sistema se ha decidido comenzar por el más básico, autentificación mediante usuario y contraseña en un fichero local del servidor protegido mediante htpasswd.

Dentro del portal web de configuración, en el apartado “Configuration“, en el menu lateral en el apartado referente a usuarios “users“ está la opción “Sources“, en esta se puede configurar la forma en la que se quiere realizar la autentificación de los usuarios. Por defecto viene creada una fuente de autentificación mediante htpasswd, en el caso de que esta no estuviese se puede crear mediante el botón “add source“.

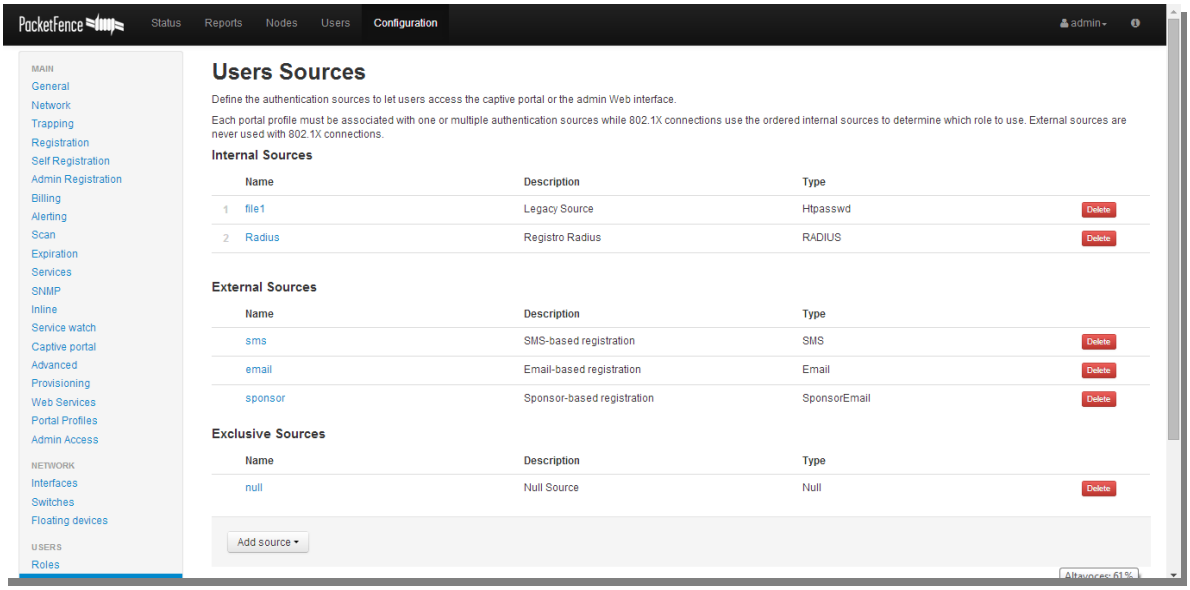


Figura 54-Menu sources

En la primera línea del apartado “Internal Sources” se puede comprobar la fuente de autenticación mediante “Htpasswd”. Clicando en esta se puede configurar.

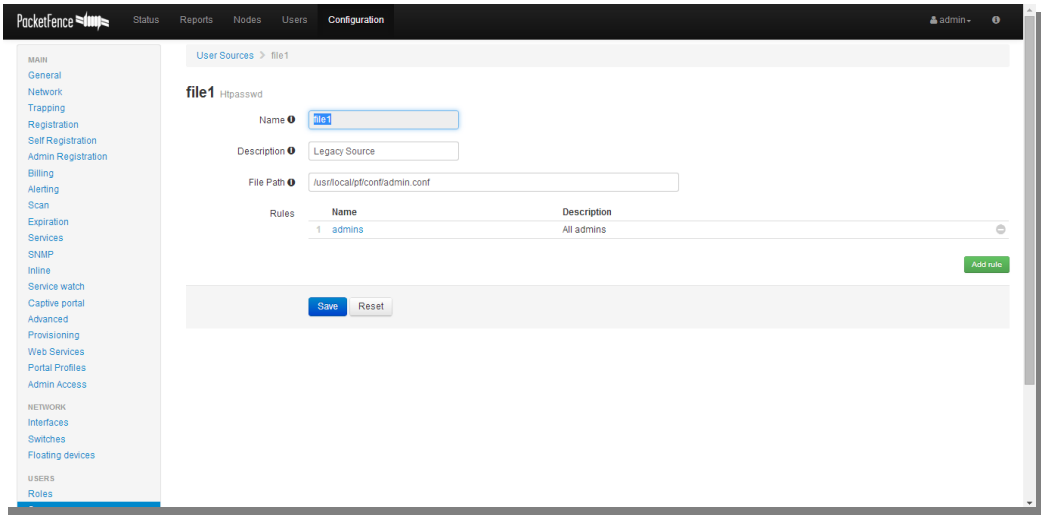


Figura 55-Configuración autenticación htpasswd

Como se ve en la figura, el fichero que contiene los usuarios y contraseñas se localiza en la dirección “/usr/local/pf/conf/admin.conf“. Se pueden añadir reglas, como por ejemplo el tiempo de conexión que se les quiere permitir, asignarle un papel (usuario invitado, usuario con privilegios, etc.), denegar el acceso a según qué usuarios, o a según qué hora se produzca la conexión. En este caso no se ha decidido configurar ninguna regla.

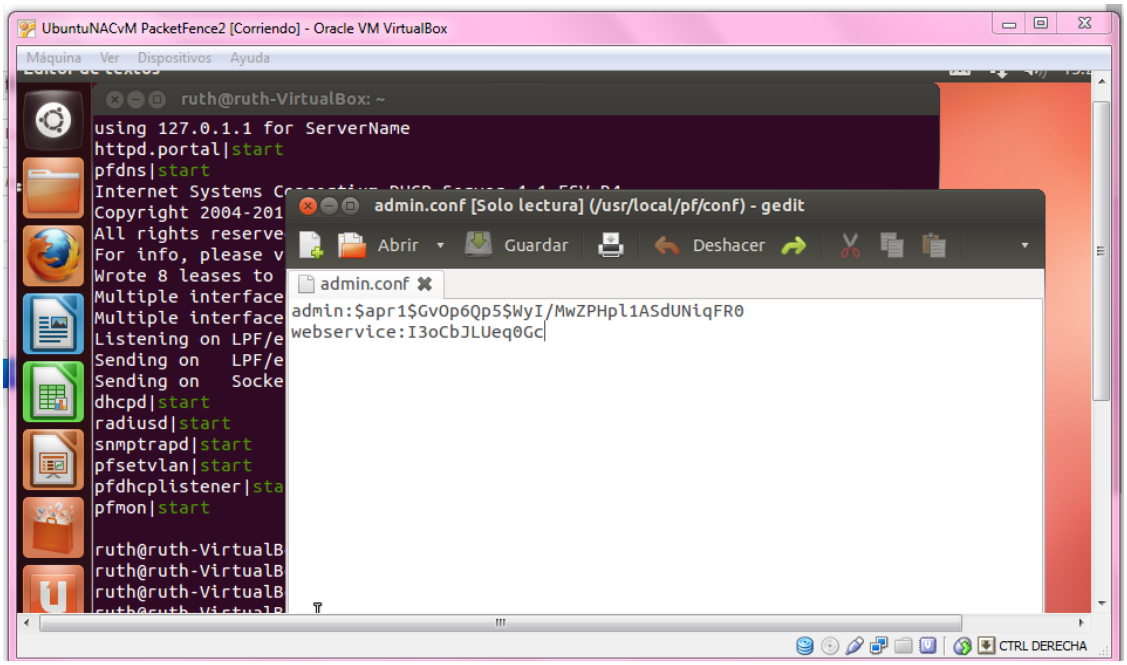


Figura 56-Imagen del fichero de contraseñas del servidor PacketFence

Para crear un nuevo usuario hay que introducir el siguiente comando:

```
Sudo htpasswd -d /usr/local/pf/conf/admin.conf nombre_usuario
```

Donde "nombre_usuario" es el nombre del usuario que se quiere introducir. Mediante esta acción creamos parejas de usuario y contraseñas válidas para que los usuarios puedan acceder a internet a partir del portal cautivo de PacketFence.

Una vez creado el usuario se ha procedido a comprobar el funcionamiento del mismo, para ello en uno de los hosts virtuales se ha intentado acceder a internet, y como era de esperar se le ha redirigido al portal cautivo.

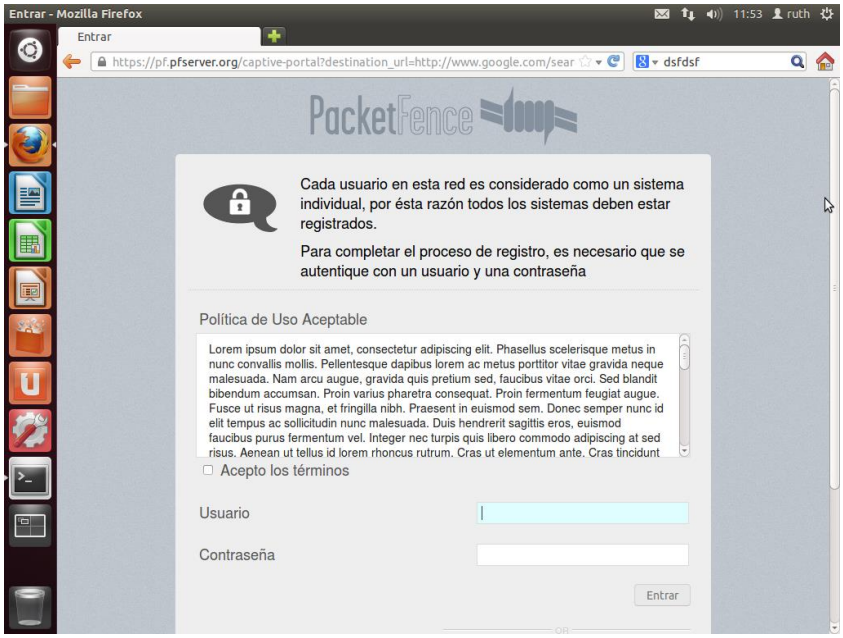


Figura 57-Redirección al portal cautivo

Para acceder a internet es necesario que el servidor nos de autorización ya que este es nuestra puerta de enlace, en modo Inline el servidor actúa como un firewall intermedio y cuando se nos permite el acceso, mediante IPTables enruta el tráfico hasta la puerta de enlace del router. Si por ejemplo se intenta hacer un traceroute a la dirección de Google cuando el usuario todavía no se ha autenticado se obtiene el resultado de la Figura 58:

```
ruth@ruth-VirtualBox:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.0.0.1 (10.0.0.1)  2.230 ms  1.922 ms  1.743 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
```

Figura 58-Traceroute a Google.

Como se puede ver, cuando se intenta conectar con Google, nos quedamos atascados en la puerta de enlace de la red interna (en el interfaz del servidor en la red interna) sin poder acceder ni siquiera a la red externa.

La redirección al nombre del servidor PacketFence es posible gracias a un módulo interno del servidor que actúa como servidor DNS y es configurado en el host de la red interna cuando este mediante DHCP solicita una dirección IP a PacketFence.

Para acceder a Internet hay que introducir el usuario y la contraseña que anteriormente se han configurado en el fichero htpasswd del servidor PacketFence, una vez realizado este paso aparece la siguiente pantalla que se muestra en la Figura 59.

En esta se puede apreciar un mensaje de habilitación de la red al usuario, la dirección IP de este que pertenece a la red interna y la dirección MAC del host que se está autenticando.

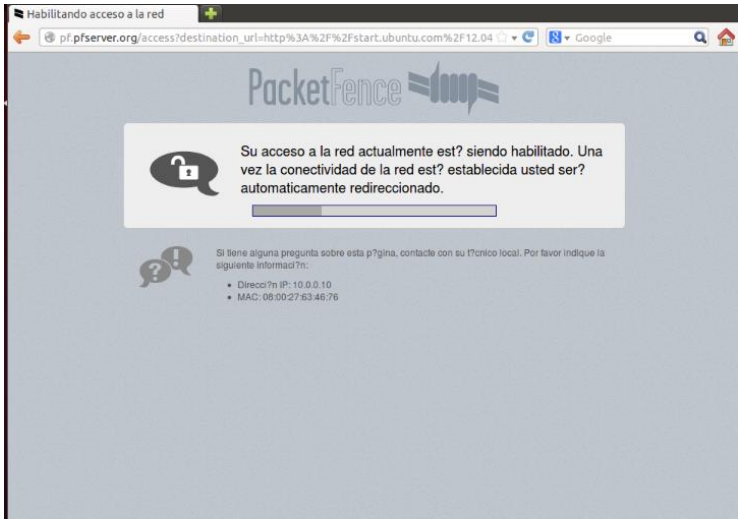


Figura 59-Autenticación PacketFence

Tras esto, el usuario es capaz de acceder a Internet, y en la web de administración del servidor se puede ver como se tiene un nuevo usuario registrado tal como se muestra en la Figura 60.

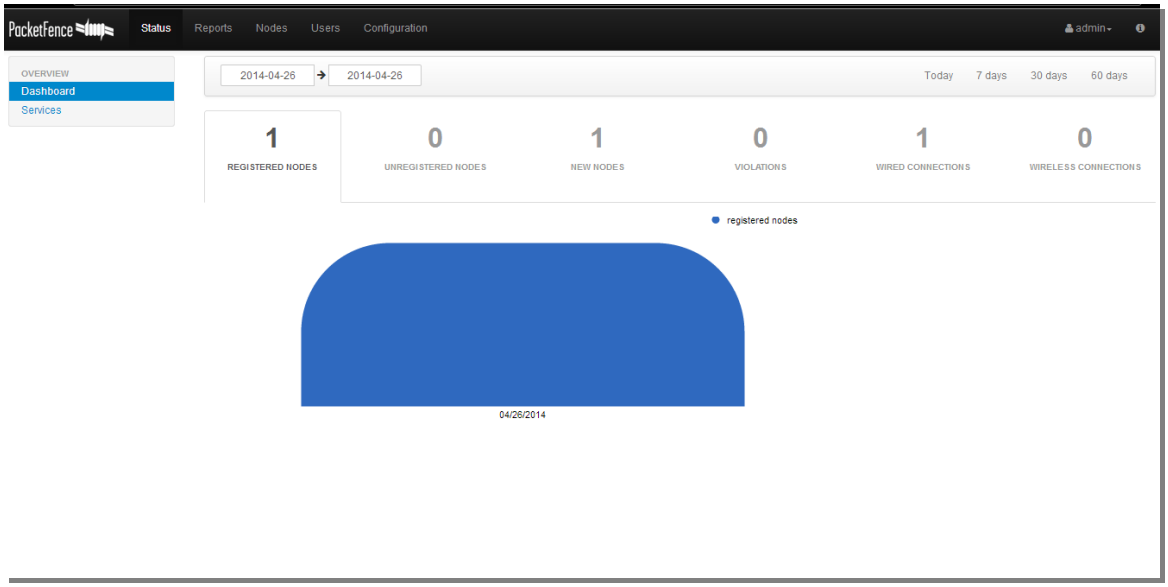


Figura 60-Verificación de nodo registrado.

Como no se ha añadido ninguna regla, y el servidor almacena a los usuarios en función de su dirección MAC, el nodo registrado tendrá a partir de este momento conexión a Internet sin necesidad de volverse a autentificar, esto puede modificarse añadiendo reglas en la pantalla de configuración de la fuente de autenticación.

Como se puede apreciar en la Figura 61 mediante traceroute ahora el usuario autenticado es capaz de llegar a internet, en este caso a Google. Se puede ver como a través de una dirección de la red interna llega al interfaz del servidor en esta red (10.0.0.1) y de ahí sale hacia internet gracias al nateo del servidor, el cual convierte la dirección interna del host en una del rango 192.168.1.0/24, el router de telefónica hace NAT a esta dirección para poder salir a internet con un direccionamiento público. En la Figura 34 que se mostraba al describir la configuración en modo Inline se pueden apreciar los saltos que se tienen que dar para poder establecer la comunicación.

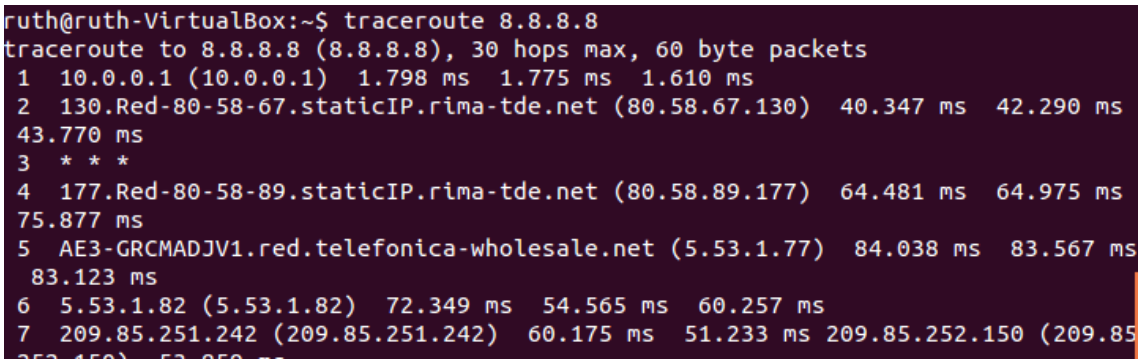


Figura 61-Traceroute a Google con usuario autenticado.

4.6.9 Configuración VLAN enforcement.

Como se ha comentado, PacketFence tiene dos modos de funcionamiento, hasta ahora sólo se había podido probar el modo Inline por falta de equipamiento.

El modo de funcionamiento VLAN enforcement puede trabajar usando diferentes técnicas. Estas técnicas son compatibles entre sí pero no en el mismo equipo. Esto significa que puedes usar las técnicas más modernas en los equipos que lo soporten y otras más antiguas en los que no. En este modo, PacketFence es el servidor encargado de asignar la VLAN al dispositivo final. Esta VLAN puede ser una de las actuales de la red del cliente o una propia de PacketFence (Isolation o Registration) donde PacketFence presenta al usuario un portal cautivo para autenticarse o con las instrucciones para el saneamiento del dispositivo.

Este modo de funcionamiento permite aislar los dispositivos finales a nivel de capa 2 de la torre OSI sin tener que realizar grandes modificaciones en la red actual.

En el modo VLAN enforcement existen dos formas de comunicar el servidor con el Switch, mediante 802.1X (y MAB si lo soporta) o SNMP (Simple Network Management Protocol) tal como se ha descrito en el apartado 4.6. En este caso se ha decidido probar por sencillez en primer lugar la configuración mediante SNMP, concretamente con la opción Port Security.

En el modo Port-Security se asigna una dirección MAC falsa a cada uno de los puertos, de esta forma cualquier dirección MAC que se conecte generará una violación de la seguridad y se

enviará un evento (trap) al servidor de PacketFence. El sistema autorizará la dirección MAC y colocará al puerto en la VLAN adecuada.

Cuando PacketFence trabaja mediante SNMP, todos los puertos del conmutador deben configurarse para enviar traps al servidor PacketFence. En el servidor se utiliza snmptrapd como el receptor de trazas SNMP. Cuando recibe una traza la reformatea y la escribe en un fichero plano (/usr/local/pf/logs/snmptrapd.log), entonces un demonio (pfsetvlan) lee estas trazas del fichero plano y responde a ellas colocando al puerto del Switch en la VLAN correcta. Dependiendo de las capacidades del Switch, el demonio pfsetvlan actúa con diferentes tipos de traps SNMP.

Se necesita crear una VLAN de registro con un servidor DHCP en la que PacketFence colocará a los dispositivos no registrados. Este servidor DHCP es el encargado de asignar a los usuarios una dirección IP correspondiente a la VLAN de registro lo que les permitirá a los usuarios tener conectividad con el servidor de NAC para poder autenticarse. Si además, se quiere aislar a los ordenadores que violen alguna norma de seguridad hay que crear otra VLAN para su aislamiento.

La Figura 62 muestra la estructura de funcionamiento de la comunicación SNMP. Los equipos se conectan a un Switch, este envía trazas SNMP que son escuchadas por el demonio que corre en PacketFence (snmptrapd) y se almacenan en un fichero de logs. Otro demonio (pfsetvlan) es capaz de leer esas trazas y mediante los datos de configuración del Switch (switches.conf) donde se encuentra información sobre las VLANS que hay, la dirección IP del Switch o la versión SNMP de este entre otras, es capaz de responder con peticiones SNMP al Switch para asignar las VLANS a los equipos finales.

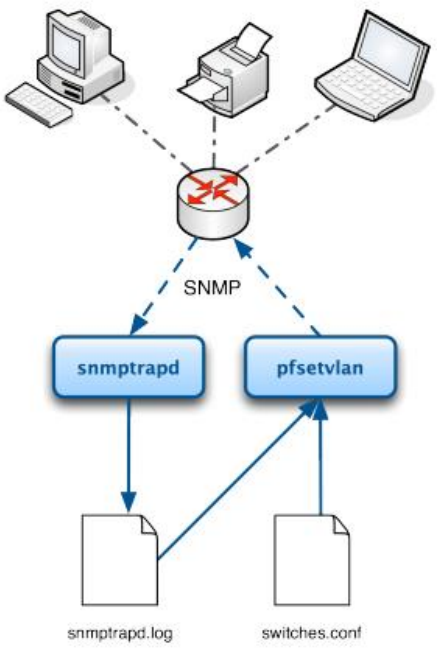


Figura 62-Estructura de comunicación SNMP de PacketFence.

Como se ha descrito, en el servidor de PacketFence corre un demonio SNMP capaz de leer los logs con las trazas SNMP que el Switch le envía y de esta forma responderle colocando al puerto y por tanto al dispositivo en la VLAN adecuada. En este modo de funcionamiento, el Switch se comunica con el servidor y viceversa de forma que cuando el equipo final se autentica es introducido en la VLAN correspondiente y a partir de este momento puede acceder a la red. La diferencia con el modo Inline es que en este caso el servidor NAC no es un elemento intermedio y los paquetes no tienen que pasar a través de él, sino que actúa como un controlador del acceso a la red comunicándose con el Switch para denegar o permitir el acceso de los host finales.

A parte del modo de funcionamiento SNMP mediante traps Port-Security, existen otros dos tipos de traps SNMP que se pueden usar, linkUp/linkDown y MacNotification. Se recomienda usar el modo Port-Security en primer lugar si el conmutador lo soporta antes que cualquiera de las otras dos opciones. El por qué es debido a que una vez que una dirección MAC es autorizada en un puerto y es la única conectada, el Switch no enviará trazas si el dispositivo se reinicia, enchufa o desenchufa, lo que disminuye drásticamente el número de interacciones SNMP entre los conmutadores y PacketFence.

Cuando se activan las trazas port-security en un conmutador no es recomendable activar las trazas linkUp/linkDown ni las MACNotification.

4.6.9.1 Consideraciones previas

En el modo Inline se había instalado el servidor en una máquina en el sistema operativo Ubuntu mediante una máquina virtual VirtualBox, esta instalación no es compatible para el modo VLAN enforcement debido a los problemas para manejar VLANs en modo bridge de VirtualBox.

En la configuración anterior, como se ha descrito, se tenía configurada la máquina virtual para que actuase como una máquina más conectada a la red, es decir, el adaptador de red estaba en modo puente o bridge. El problema surge con el etiquetado de las VLANS en VirtualBox. Los paquetes que salen del VirtualBox llevan correctamente la etiqueta 802.1Q, sin embargo las respuestas aparecen sin esta etiqueta y por tanto no sabe a qué interfaz va este paquete lo que hace imposible la comunicación. Es decir, en la máquina virtual donde se tenía instalado el servidor se habían creado ciertas VLANS con sus corrientes subinterfaces en cada una de ellas. Concretamente la VLAN 100 en el subinterfaz virtual eth2.100. Esta máquina se había conectado al Switch 2950 de Cisco en un interfaz en modo trunk para que pudiesen pasar todas las VLANS a través de él.

A la VLAN 100 se le había asignado una dirección IP de gestión en el Switch de forma que se pudiese verificar hasta donde llegan los paquetes. Al realizar un ping desde el interfaz eth2.100 de la máquina virtual a la dirección IP de gestión del Switch en esa VLAN 100 no se recibía

respuesta. Si se observaba el tráfico en el interfaz eth2 de la máquina virtual se veía como los ARP request enviados por la máquina virtual contenían la etiqueta 802.1Q con el identificador de VLAN 100 lo cual es correcto, sin embargo los ARP response que le enviaba el Switch Cisco venían sin etiqueta por lo que no podían llegar al subinterfaz eth2.100 y por tanto la comunicación no se establecía. Tras no poder solucionar este problema se decidió instalar el servidor en una máquina Ubuntu real. El sistema operativo sobre el que se ha instalado es el mismo que el que se tenía en la máquina virtual y los pasos de instalación son los mismos por lo que no se va a proceder a describirlos. En este caso ya no necesitamos una red interna como se tenía en el modo Inline por lo que la red 10.0.0.0/24 desaparece. La dirección IP del interfaz de managemet se mantiene (192.168.1.42). En el caso VLAN enforcement no es necesario activar IP forwarding en el servidor pues este este no va a enrutar tráfico como hacía en el modo Inline, Si es necesario configurar una puerta de enlace por defecto (default Gateway) para el interfaz de managemet para que este tenga acceso al resto de la red.

4.6.9.2 Elementos necesarios y estructura de la red.

Los elementos necesarios para la realización de estas pruebas han sido:

- Cisco Catalyst 2950
- Cable de consola
- Adaptador puerto serie a USB
- PC con sistema operativo Ubuntu (PacketFence)
- PC Windows 8
- Router ADSL Amper-26555
- Cables RJ45
- Minicom para la configuración del Switch mediante puerto serie.

En la siguiente Figura 63 se puede ver la topología física de la red. Los puertos del switch con el servidor (Fa0/1) y el router (Fa0/2) se han configurado en el Switch Cisco en modo trunk mientras que los puertos correspondientes a los clientes o dispositivos finales que se quieran conectar a la red deben configurarse en modo acceso. En este caso se va a utilizar un PC conectado al puerto Fa0/3.

Como se puede apreciar en este caso el servidor no es un elemento intermedio si no que cuelga del Switch al igual que lo hacen el resto de equipos finales.

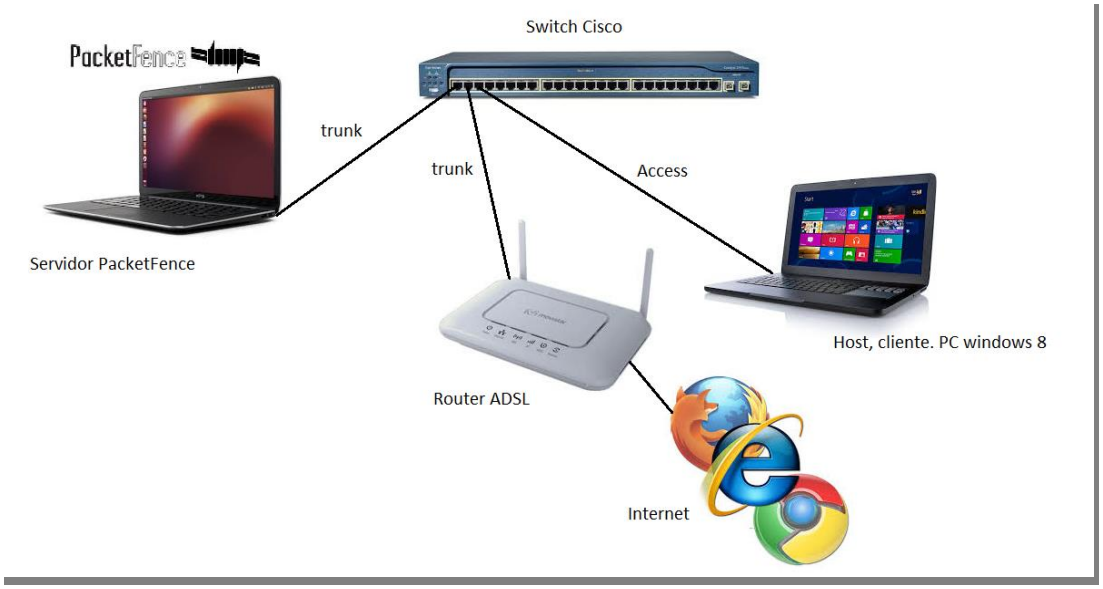


Figura 63-Estructura física de la red.

4.6.9.3 Creación de interfaces y VLANS

Para la implementación del escenario es necesario configurar diferentes VLANS tanto en el Switch como en el servidor. Son necesarias como mínimo cuatro VLANS, en este caso se han creado las siguientes:

- VLAN 100: Es la VLAN de registro (Registration Vlan), donde se colocan los dispositivos que no han sido registrados todavía. A esta VLAN se le ha asignado la red 10.100.0.0/24. Al interfaz del servidor en esta VLAN se le ha dado la dirección IP 10.100.0.1.

- VLAN 200: Es la VLAN donde se asignan los dispositivos que no cumplen con las políticas de seguridad o que se consideran críticos, (Isolation VLAN). La red asignada para ella ha sido la 10.200.0.0/24 y al interfaz del servidor en esta VLAN se le ha configurado la IP 10.200.0.1.

- VLAN 4: Esta VLAN es la de detección de MAC (MAC Detection VLAN), es una VLAN utilizada por el servidor PacketFence cuando se configura su comunicación con el Switch mediante SNMP. No tiene que tener nada configurado. A esta VLAN se asignan los interfaces del Switch inicialmente.

- VLAN 1: Es la VLAN por defecto a la que se asignarán los dispositivos una vez se hayan registrado. En este caso se ha elegido la VLAN 1 como VLAN nativa de forma que una vez que se autentiquen y se asignen a esta VLAN los paquetes no llevarán encapsulado 802.1Q. Esto se ha realizado de esta forma para que sean compatibles con el router ADSL que tiene que encargarse de natear los paquetes de la VLAN 1 para enrutarlos a Internet. Esta VLAN tiene el rango 192.168.1.0/24 que es el mismo en el que se encuentra la puerta de enlace del router ADSL (192.168.1.1) y el interfaz de

management del servidor (192.168.1.42). Se podría tener una red de management o gestión en una VLAN a parte y se podrían configurar distintas VLANS a las que asignar los diferentes equipos finales en función de diversas políticas como puede ser por ejemplo el tipo de autenticación elegida, el SSID o el Switch al que se han conectado, el nombre del equipo, etc. Como en este caso el router ADSL sólo va a realizar el nateo a direcciones públicas de la red 192.168.1.0/24, sólo se ha configurado esta VLAN para asignar a los dispositivos autenticados.

Primero se ha procedido a configurar el Switch [45] añadiéndole las cuatro VLANS descritas y tras esto se ha configurado SNMP Port-Security:

```
snmp-server enable traps port-security

snmp-server enable traps port-security trap-rate 1

snmp-server host 192.168.1.42 version 2c public port-security
```

Una vez configurado el servidor con el que se van a comunicar mediante SNMP, y activar SNMP port-security, hay que configurar los puertos. El puerto Fa0/1 y el puerto Fa0/2 del Switch hay que configurarlos en modo trunk, puesto que en el primero se conectará el servidor y en segundo actuará como puerto uplink del Switch conectándolo en nuestro caso con el router. En el caso concreto del ejemplo sólo circularán por este uplink paquetes pertenecientes a la VLAN 1 y como ésta se ha seleccionado como VLAN nativa los paquetes no llevarán etiquetado 802.1Q. Sin embargo si el router que se tuviese conectado a este uplink fuese compatible con VLANS se podrían tener configuradas varias VLANS para usuarios registrados y todas ellas circularían por este enlace uplink con su correspondiente etiquetado 802.1Q indicando el identificador de la VLAN a la que pertenecen. Por tanto, como sólo se tiene una VLAN (VLAN 1) a la que asignar los dispositivos autenticados no haría falta en este caso esta configuración de enlace uplink en modo trunk, aun así se ha decidido hacer de este modo.

En cada uno del resto de puertos del Switch hay que configurar lo siguiente:

```
switchport mode access

switchport access vlan 4

switchport port-security

switchport port-security violation restrict

switchport port-security mac-address 0200.0000.00xx
```

Es decir, se configuran en modo acceso, se asignan a la VLAN 4 y se active la seguridad por puerto. Donde pone xx se configura el número de interfaz desde 1 hasta los 24 puertos que tiene el Switch.

Como se ha comentado, en el modo Port-Security se asigna una dirección MAC falsa a cada uno de los puertos, de esta forma cualquier dirección MAC que se conecte a un puerto generará una violación de la seguridad y se enviará un evento (trap) al servidor de PacketFence. Para mantener un orden en la asignación de las falsas MAC a los puertos se utiliza un mapeo del número del puerto en los dos últimos dígitos de la dirección MAC.

Una de las VLANS del Switch debe de tener dirección IP para poderse comunicar con el servidor mediante SNMP ya que este protocolo va sobre el nivel de transporte UDP. Para ello a la VLAN 1 se le ha colocado la dirección IP de gestión 192.168.1.44/24.

Una vez creadas en el Switch, es necesario crearlas en el servidor. Para crear las VLANS en la GUI de administración del servidor, dentro de la pestaña de configuración hay un subapartado que hace referencia a los interfaces. Se tiene únicamente un interfaz físico, eth0 y sobre este es donde se configurarán los subinterfaces virtuales para cada una de las VLANS. En la Figura 64 se ve el resultado de cómo deben quedar los interfaces en el servidor. Como se puede ver se tiene un interfaz en la VLAN 100, otro en la 200 y otro en la 4 además del físico que pertenece a la VLAN nativa (VLAN 1),

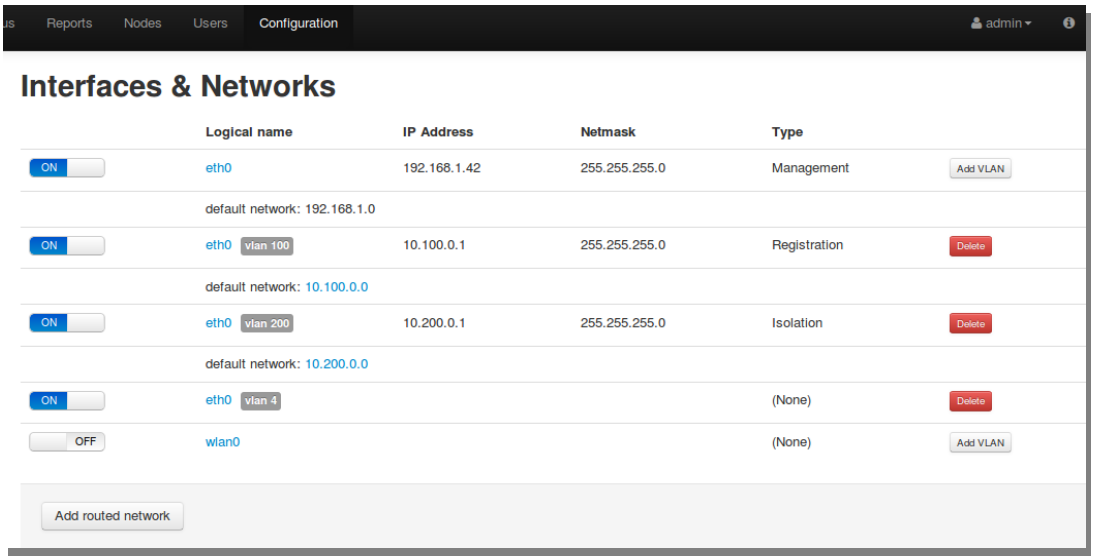


Figura 64- Configuración de interfaces VLAN enforcement en PacketFence

Al crear los subinterfaces en el servidor se crean automáticamente en la máquina puesto que al instalar el servidor se instalan los componentes necesarios para el soporte de VLANs en Ubuntu. En la Figura 65 se aprecian los interfaces en la consola de Ubuntu y como se puede ver, tras crear las VLANs en la consola web de administración se han creado en el propio sistema operativo también.

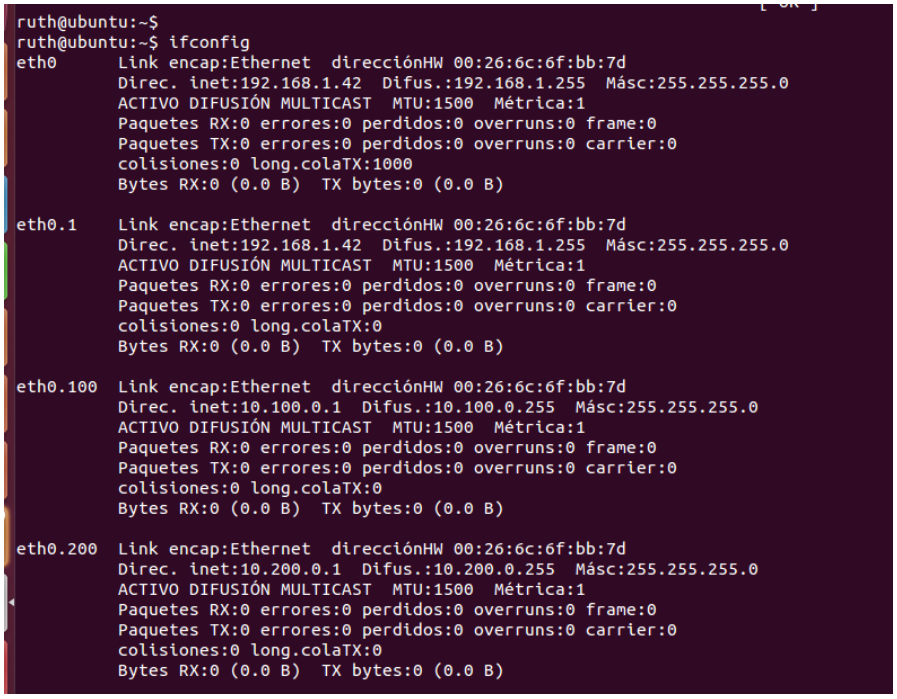


Figura 65-Interfaces en Ubuntu

4.6.9.4 Configuraciones en el servidor. Configuración del Switch y las VLANs.

Una vez configurados los interfaces en el Switch y en el servidor es necesario añadir el Switch al servidor para decirle que se tiene que comunicar con este, cómo lo tiene que hacer y qué es exactamente lo que tiene que gestionar. Para ello en la GUI dentro del apartado de configuración se encuentra un subapartado dedicado a switches. Dentro de este se encuentra una plantilla por defecto en la que se encuentran los valores que se asignarán por defecto a todos los switches. Si se quiere especificar un valor diferente para cada conmutador hay que realizarlo dentro de la plantilla individual de cada uno. Es decir, las configuraciones individuales de los equipos tienen prioridad sobre las configuraciones en el conmutador por defecto.

Para añadir el conmutador se añade una plantilla, al crearla se nos solicita la dirección IP del Switch, en este caso es la IP de gestión de la VLAN 1, 192.168.1.44. Una vez creada la plantilla se puede proceder a configurar los valores del conmutador. En la Figura 66 se muestran algunos parámetros que hay que introducir. Es importante introducir el modelo de conmutador que se está utilizando y el método de desautenticación en nuestro caso SNMP. También existen tres formas de funcionamiento, hay que seleccionar “production” puesto que es el modo en el que el servidor realmente actúa como NAC, el resto son formas de configurar el servidor y ver cómo funcionaría sin que afectase al resto de equipos de la red, lo que es útil si se tiene que instalar en la red de una empresa y se quiere ver su rendimiento sin comprometer a los equipos y la red de esta empresa.

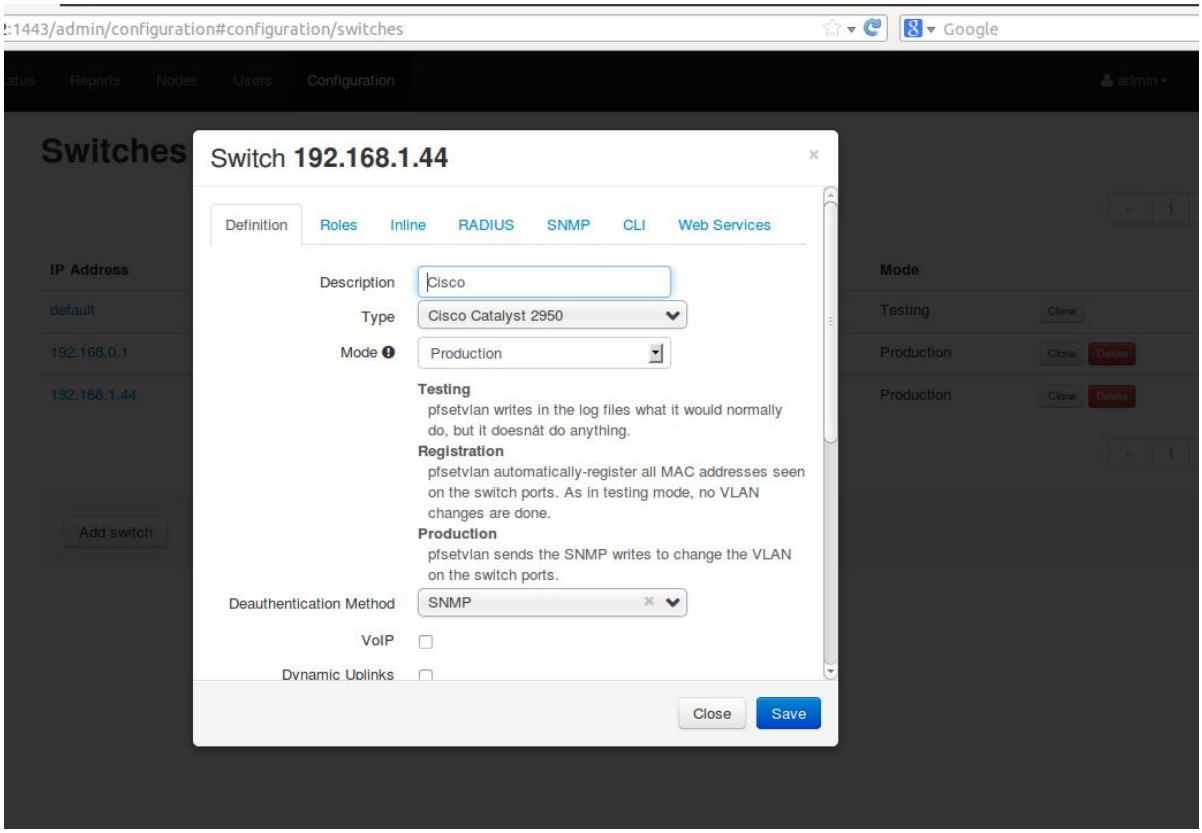


Figura 66-Configuración del Switch

Otros parámetros importantes a configurar son los puertos que no va a gestionar el servidor, es decir aquellos en los que no va a realizar el control de acceso como pueden ser puertos uplink a otros conmutadores o routers de una capa superior o el propio puerto donde está conectado el servidor. En este caso se tendrán los puertos 1 y 2 como uplinks puesto que en el primero se conectará el servidor, y en el segundo el router. Esto se puede apreciar en la Figura 67.

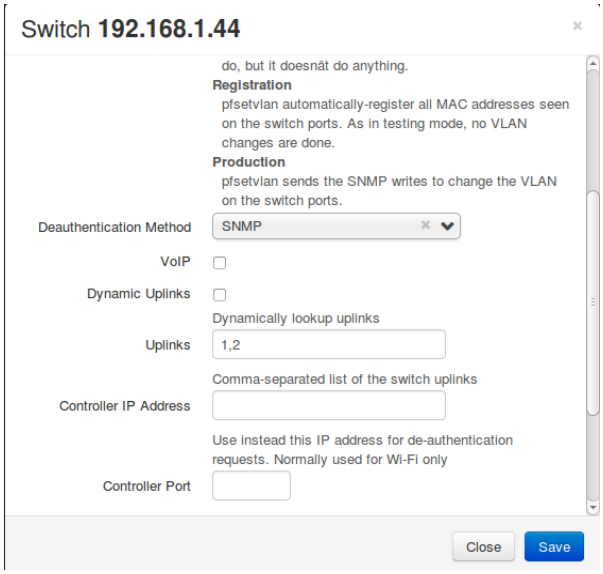


Figura 67-Configuración del Switch, uplinks.

En el apartado SNMP es donde se establecen las comunidades para SNMP, se han dejado públicas tal y como venían el conmutador por defecto. El apartado RADIUS no concierne en esta configuración puesto que se ha decidido realizar el NAC mediante SNMP y no mediante 802.1X.

En la pestaña "roles" hay que configurar las VLANS que se han definido previamente, esto se puede ver en la Figura 68. En nuestro caso nos interesan únicamente las VLANS 100, 200, 4 y 1 a las cuales se les han asignado los roles "registration", "isolation", "macdetection" y "default".

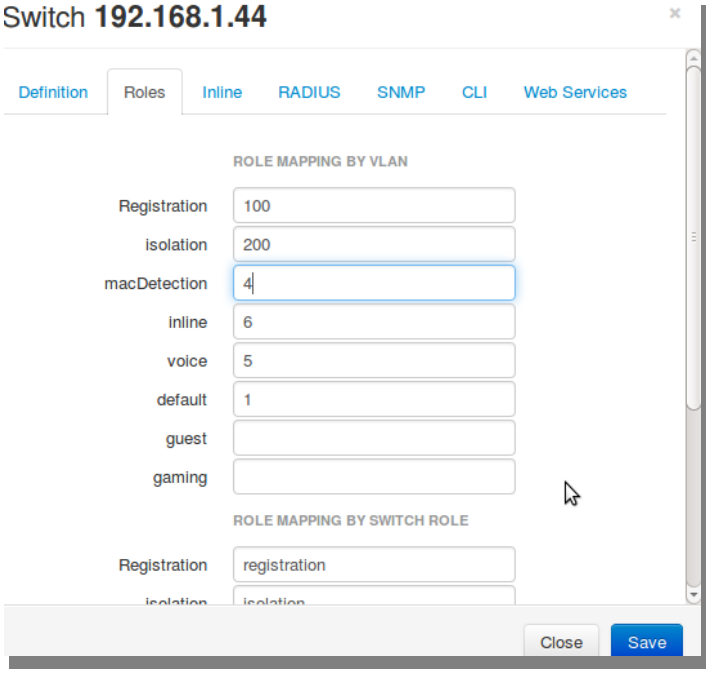


Figura 68-Selección de roles en el Switch.

Una vez configurado el servidor, hay que configurar los servidores DHCP. Se van a utilizar 3. Para dos de ellos se va a utilizar el servidor DHCP que tiene PacketFence, colocando un servidor DHCP en las direcciones IP del servidor en las VLANS 100 (Registro) y 200 (Aislamiento), concretamente en las direcciones 10.100.0.1 y 10.200.0.1. El tercer servidor DHCP estará en la dirección 192.168.1.1, es decir, es el router ADSL que nos da la comunicación a Internet y el encargado de traducir las direcciones privadas en públicas. Los tres servidores deben de configurarse en el servidor de PacketFence, aunque sólo para los dos primeros este será el encargado de contestar a las peticiones DHCP.

El último paso para poder tener el servidor NAC funcionando es configurar las fuentes de identidad, es decir, cómo se va autenticar el usuario, qué fuente de identidad va a usar. Al igual que en la configuración en modo Inline se va a usar como almacén de identidades un fichero local encriptado y protegido mediante htpasswd almacenado en el propio servidor. Se ha decidido usar el mismo fichero que se tenía en la configuración Inline, sin embargo, para poder utilizarlo hay que realizar un pequeño cambio en la configuración de esta fuente de autenticación. Para acceder a la configuración de la fuente de autenticación se siguen los mismos pasos explicados en el apartado 4.6.8. Una vez se ha accedido a la configuración de la

fuente de autenticación o almacén de identidades hay que añadir una regla (rule) para decir que a todos los que se autentiquen mediante este fichero local se les asigne a la VLAN 1 o lo que es lo mismo al rol que se ha configurado para esta “default”. Además se obliga a añadir una regla con el tiempo que se le permite al usuario estar conectado sin necesidad de volverse a autenticar. Esta configuración final puede apreciarse en la Figura 69.

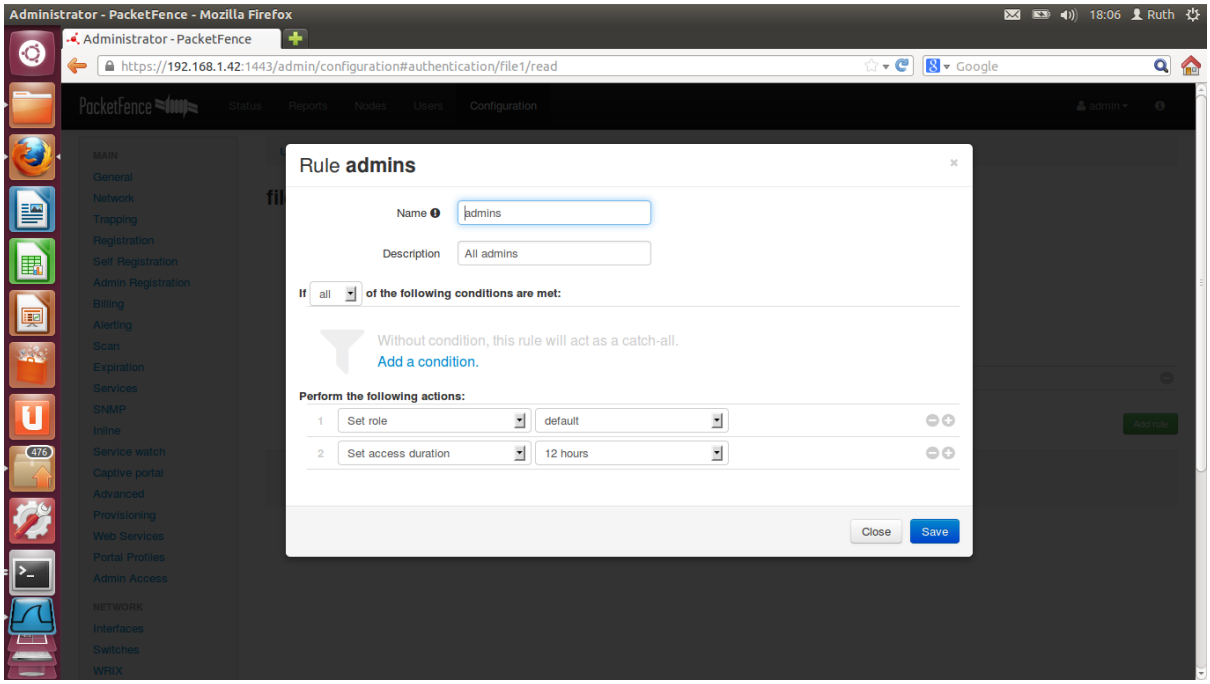


Figura 69-Configuración fuente de autenticación.

Si en el conmutador se ejecuta el comando “show snmp” se debería ver la configuración de la Figura 70 en la que se puede ver la dirección IP del interfaz del servidor PacketFence con la que se comunica el Switch, el número de paquetes enviados y recibidos, y que SNMP está activado.

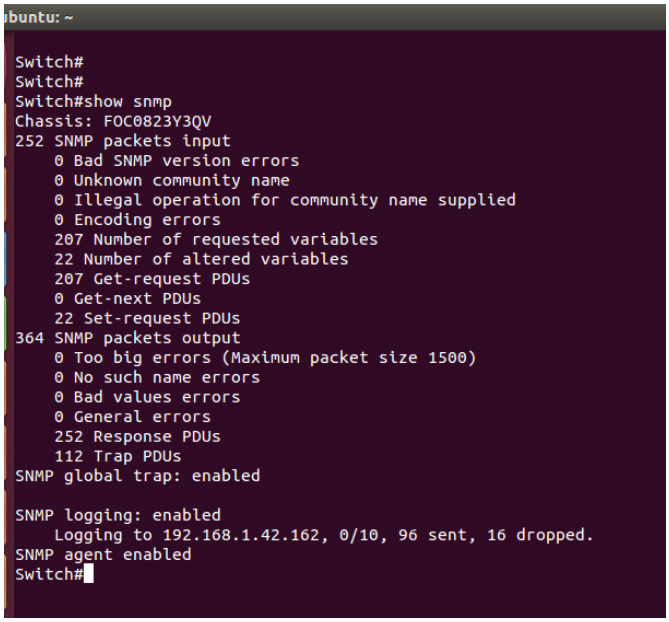


Figura 70-Show SNMP

Toda la configuración del servidor PacketFence puede hacerse de dos formas, mediante la interfaz gráfica o mediante ficheros. Los ficheros de configuración de este escenario se adjuntan en la sección de anexos.

El fichero donde aparece la configuración de los switches es switches.conf y se puede encontrar en el Anexo 2.

El fichero donde aparece la configuración general de PacketFence es pf.conf y se puede encontrar en el Anexo 3.

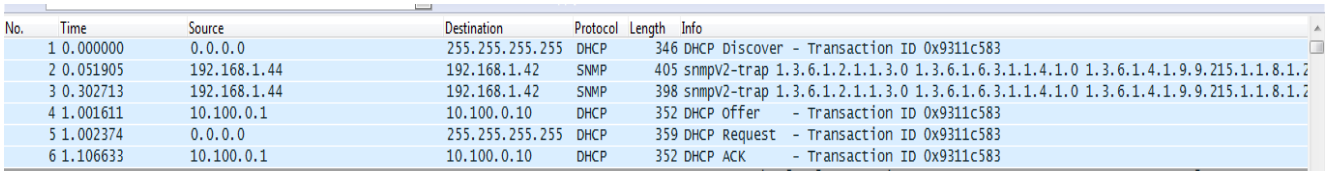
El fichero donde aparece la configuración de la autenticación es authentication.conf y se puede encontrar en el Anexo 5.

4.6.9.5 Comunicación entre servidor PacketFence, Switch y PC.

La comunicación entre el Switch de Cisco y el servidor PacketFence, como se ha comentado se realiza mediante SNMP sobre la capa de transporte UDP. Se ha realizado una captura del tráfico en el interfaz físico del servidor (eth0) mediante Wireshark de todo el proceso de autenticación del dispositivo, es decir, desde que se conecta un dispositivo al Switch hasta que este recibe el acceso a Internet. A continuación se van a comentar los resultados obtenidos.

En primer lugar, al conectar el dispositivo al conmutador, este no dispone de dirección IP por lo que lo primero que realiza el PC conectado es realizar una petición DHCP. En la Figura 71 se puede apreciar esta petición. En el paquete número 1 el PC sin dirección IP envía una petición a broadcast. En el paquete 4, el servidor PacketFence mediante la dirección IP del interfaz en la

VLAN 100 (VLAN de registro), mismo interfaz en el que se encuentra el servidor DHCP para esta VLAN, le contesta al PC asignándole la dirección IP 10.100.0.10. En los dos siguientes paquetes se completa esta asignación y a partir de ese momento el PC se encuentra en la VLAN de registro.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x9311c583
2	0.051905	192.168.1.44	192.168.1.42	SNMP	405	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.1.9.9.215.1.1.8.1.2
3	0.302713	192.168.1.44	192.168.1.42	SNMP	398	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0 1.3.6.1.4.1.9.9.215.1.1.8.1.2
4	1.001611	10.100.0.1	10.100.0.10	DHCP	352	DHCP Offer - Transaction ID 0x9311c583
5	1.002374	0.0.0.0	255.255.255.255	DHCP	359	DHCP Request - Transaction ID 0x9311c583
6	1.106633	10.100.0.1	10.100.0.10	DHCP	352	DHCP ACK - Transaction ID 0x9311c583

Figura 71-Petición DHCP inicial.

Las trazas SNMP que se pueden ver en los paquetes 2 y 3 son trazas enviadas por el Switch (192.168.1.44) a PacketFence (192.168.1.42) y hacen referencia al sysUpTime (1.3.6.1.1.1.3.0) [48] y a la gestión de equipos Cisco, todos los OID (Object Identifier) que cuelgan del OID 1.3.6.1.4.1.9.9 se encargan de la gestión de equipos de Cisco (ciscoMgmt) [49]. Para saber que significan se ha utilizado la MIB de Cisco [50].

En este caso los OID avisan de que ha habido un cambio en una dirección MAC de un puerto y te dicen cuál es la nueva dirección MAC aprendida. En la Figura 72 se puede apreciar como el Switch le envía la dirección MAC aprendida. El OID 1.3.6.1.4.1.9.9.215.1.1.8.1.2 hace referencia al objeto “cmnHistMacChangedMsg” y está formado un string de 11 octetos (01 00 64 70 54 d2 d8 2d 43 00 03) el cual se puede apreciar en el campo “value” de la captura de Wireshark. El primer octeto (01) indica que se ha aprendido una nueva dirección MAC, los dos siguientes octetos (00 64) indican la VLAN a la que pertenece esta MAC, que en este caso si traducimos de hexadecimal a decimal obtendremos la VLAN 100, la de registro. Los siguientes 6 octetos son la dirección MAC del PC (70:54:d2:d8:2d:43) que si se comprueban en el propio PC se ve que estos son correctos. Por último, los dos octetos finales (00 03) indican el interfaz donde se ha aprendido la nueva MAC, en este caso en el puerto 3 del conmutador que es en el que se tiene conectado el dispositivo final.

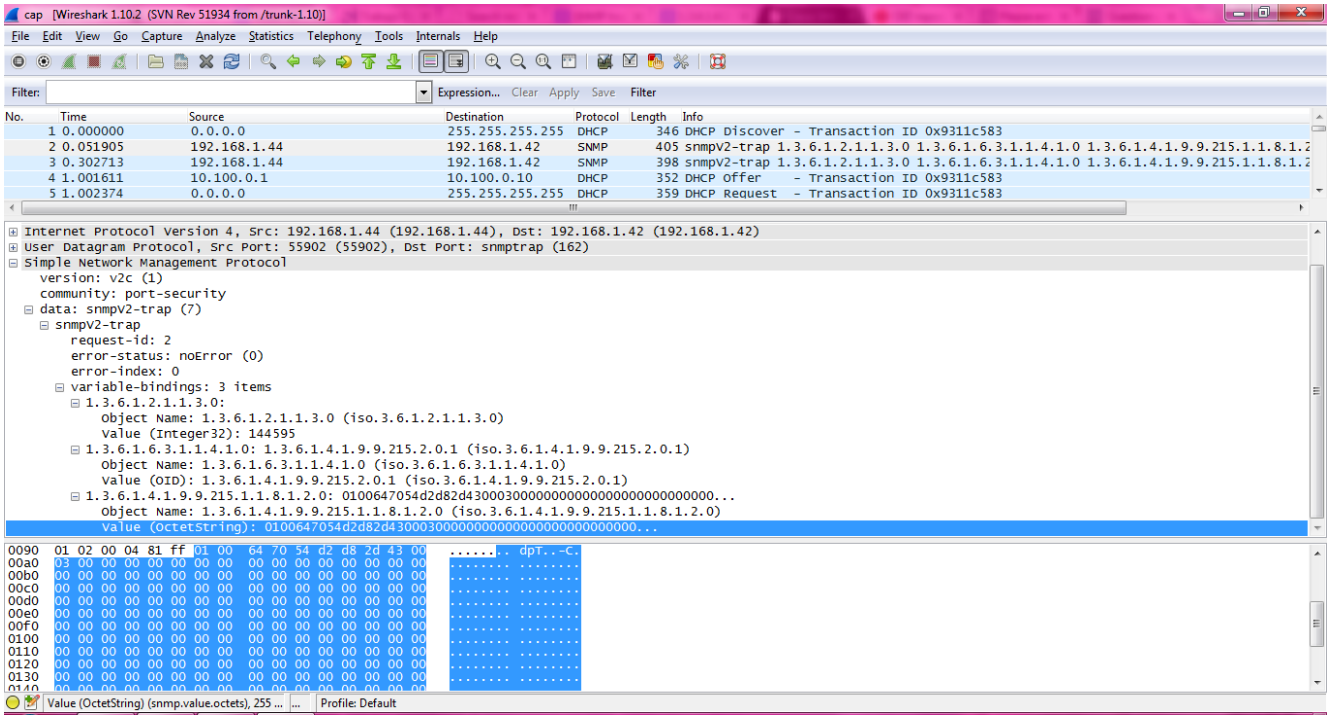


Figura 72- Trap SNMP de aprendizaje de nueva MAC en el conmutador.

Por el momento el usuario tiene una dirección IP en la VLAN de registro, y el servidor PacketFence ha aprendido la MAC del nuevo dispositivo conectado. A partir de este momento, cuando el usuario abra el navegador será redirigido al portal cautivo de PacketFence.

A partir de este momento la comunicación con el servidor va sobre TLS (Transport Layer Security) sobre tráfico web (HTTPS). Al instalar el servidor se crean los certificados los cuales pueden cambiarse por unos aceptados por la organización.

En la Figura 73 se puede ver que tras adquirir la dirección IP en la VLAN de registro y abrir el navegador se establece una comunicación http entre cliente y servidor que redirige al navegador a la url: https://pf.pfserver.org/captive-portal?destination_url=\r\n.

Como es una página segura lo siguiente que se ve es la comunicación TLS y el envío del certificado por parte del servidor.

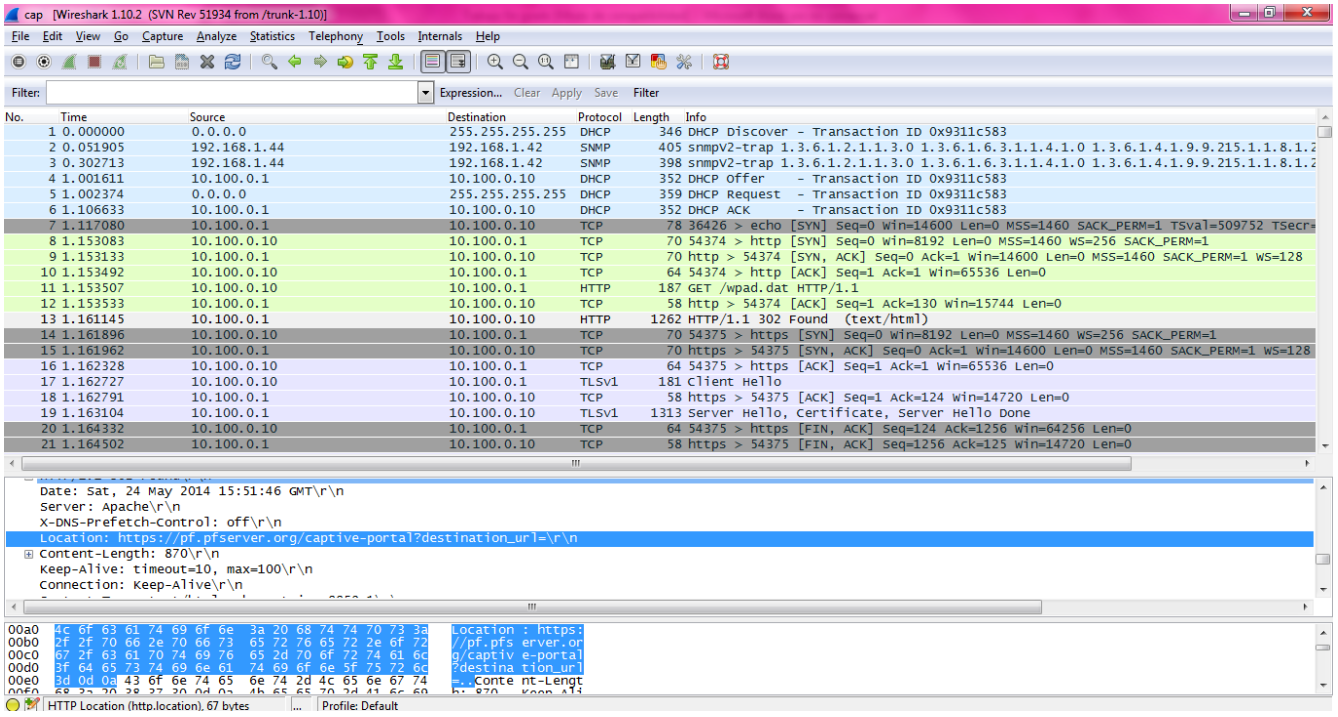


Figura 73-Paquetes TLS, HTTPS y HTTP.

Una vez en el portal cautivo el usuario se autentifica enviándole al servidor los datos de forma encriptada tras ser verificado el usuario, el servidor PacketFence envía una petición SNMP para cambiar al puerto de VLAN.

Durante el proceso de autenticación el servidor PacketFence envía peticiones de lectura para preguntar en que VLAN está ese puerto, cuando por se da por autenticado el usuario le envía una traza de escritura para cambiarlo de VLAN. En la Figura 74 se puede apreciar el OID (1.3.6.1.4.1.9.9.68.1.2.2.1.2.3) y en el campo “value” se le asigna el valor de la VLAN, en este caso es la VLAN 1 que es la que da acceso al usuario a la red.

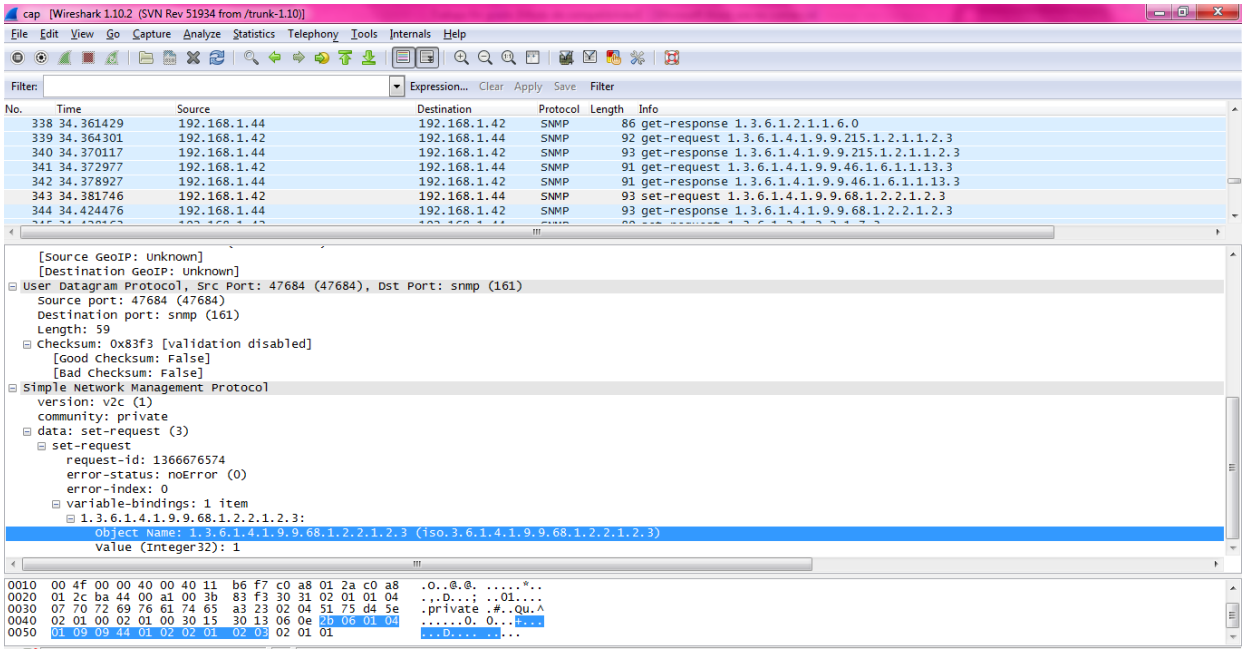


Figura 74-Traza SNMP de cambio de VLAN

La Figura 75 se ha obtenido de la MIB de Cisco, como se puede apreciar se describe el objeto de lectura y escritura de VLAN que utiliza PacketFence. En el caso de lectura el valor será nulo mientras que en escritura, el valor será un entero con el identificador de la VLAN tal y como se veía en la Figura 74.

Si nos fijamos, en el OID enviado por el servidor aparece un dígito más al final del OID, este indica el puerto al que se le está realizando la lectura o escritura.

```
1.3.6.1.4.1.9.9.68.1.2.2.1.2 (CISCO-VLAN-MEMBERSHIP-MIB)
vmVlan  OBJECT-TYPE
        SYNTAX     INTEGER(0..4095)
        MAX-ACCESS read-write
        STATUS     current
        DESCRIPTION                "The VLAN id of the VLAN the port is assigned to
                when vmVlanType is set to static or dynamic.
                This object is not instantiated if not applicable.

                The value may be 0 if the port is not assigned
                to a VLAN.

                If vmVlanType is static, the port is always
                assigned to a VLAN and the object may not be
                set to 0.

                If vmVlanType is dynamic the object's value is
                0 if the port is currently not assigned to a VLAN.
                In addition, the object may be set to 0 only."
        ::= { vmMembershipEntry 2 }
```

Figura 75-MIB Cisco cambio y lectura de VLAN [51]

Tras ser cambiado de VLAN se produce otro intercambio DHCP (Figura 76) esta vez entre el PC y el router de Movistar (192.168.1.1) en el que se le asigna al PC la dirección IP 192.168.1.26 con la que tiene pleno acceso a Internet

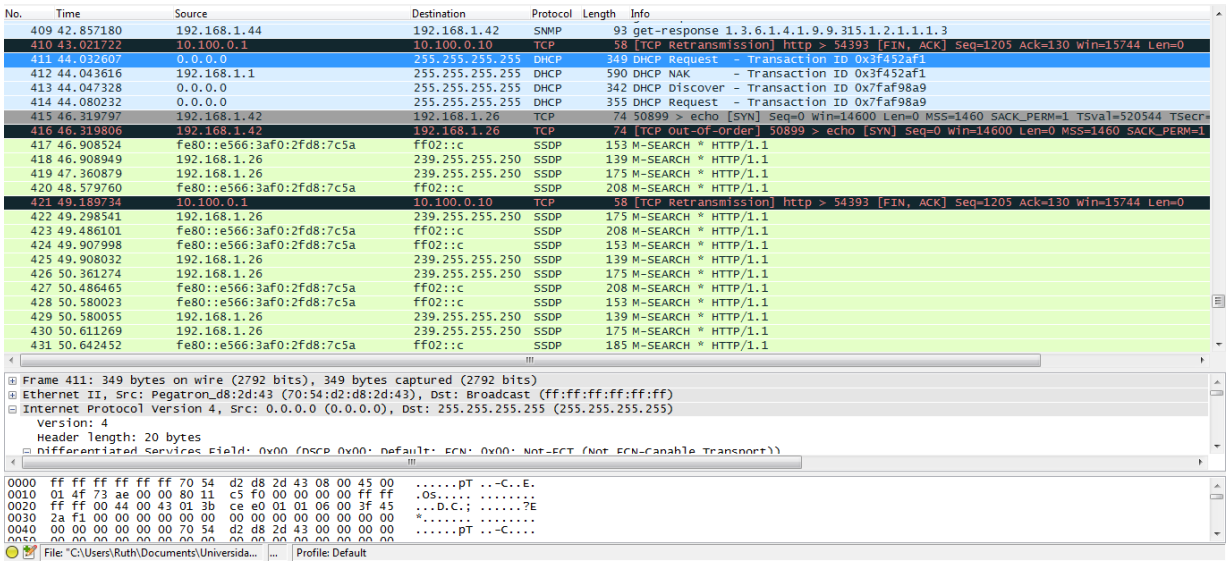


Figura 76-Establecimiento de comunicación

4.7 Comparación entre PacketFence, Cisco ISE y NetSight.

En este apartado se va a proceder a valorar y comparar las tres soluciones NAC que se han descrito en este trabajo.

Las tres opciones para la implantación del control de acceso basado en puerto que se han descrito son ISE de Cisco, Enterasys Management con NetSight y PacketFence.

De las tres opciones sólo la última de ellas, PacketFence es gratuita mientras que las otras dos son de pago. Las tres opciones son válidas para escenarios grandes y pequeños, aunque por temas económicos para escenarios muy pequeños la opción más viable sería la gratuita.

Las tres opciones son compatibles con el estándar 802.1X lo que hace que puedan interaccionar con dispositivos de distintos fabricantes, sin embargo, tan sólo la solución de Enterasys y la de PacketFence están orientadas principalmente a este fin. PacketFence es la más orienta a una infraestructura compuesta por diversos fabricantes permite la gestión de la autenticación mediante SNMP además de 802.1X.

Por el contrario la solución de Cisco ISE aunque soporta una infraestructura multi-fabricante pierde la mayoría de sus añadidos dejando una solución básica de NAC.

En lo respectivo a evaluación de los dispositivos finales para el establecimiento de las políticas de restricción de acceso a la red y saneamiento de los dispositivos Cisco lo realiza mediante la instalación de agentes en los equipos finales, Enterasys proporciona las dos posibilidades, con agente y sin él aportando diferentes funcionalidades con cada uno, las más dedicadas a la evaluación del propio dispositivo se realizan mediante el agente. PacketFence por el contrario no necesita agentes de escaneo en los dispositivos finales puesto que se integra con programas de escaneo de vulnerabilidades como pueden ser Nessus y OpenVAS. Esto es una

ventaja en el sentido de compatibilidad de dispositivos sin embargo es un punto más de gestión, configuración y aprendizaje por parte de los administradores IT.

Otro aspecto destacable es que tanto Cisco ISE como NetSight soportan integración mediante máquinas virtuales mientras que PacketFence presenta una mayor problemática puesto que no tiene un módulo especializado para ese fin como es el caso de las otras dos soluciones.

Las tres soluciones son capaces de distinguir los tipos de dispositivos conectados a la red y establecer diferentes políticas en función de cada uno. Cisco ISE denomina a esta funcionalidad "profiling".

Las tres soluciones son centralizadas mediante la gestión de una consola gráfica. Son capaces de aislar los dispositivos que no cumplan con las políticas de seguridad y proporcionarles soluciones de saneamiento.

En cuanto a la autenticación las tres soluciones son integrables con diferentes almacenes de identidades como LDAP o directorio activo. Las tres implementaciones proporcionan una solución de portal cautivo para el tratamiento de los usuarios invitados.

La soluciones Cisco ISE y NetSight proporcionan un mayor nivel de gestión pudiéndose integrar con otros Software propietarios y generar gráficas y estadísticas de los usuarios y la red. Se integran con otros Software de control de seguridad implementando en conjunto una mayor funcionalidad.

Cisco ISE proporciona además MDM (Mobile Device Management) que permite establecer políticas de seguridad en los dispositivos móviles, así como un seguimiento en tiempo real de la localización de los sistemas.

Capítulo 5- Otras tareas desarrolladas en la empresa

5.1. Reportes y seguridad WIFI.

Una de las actividades realizadas durante la estancia en la empresa ha sido la realización de un seguimiento de los puntos de acceso WIFI desconocidos existentes.

Según la normativa, el departamento de IT tiene que gestionar todos los puntos de acceso y ADSL que se encuentren en la sede, unificando y centralizando así el control y la responsabilidad. Como consecuencia se ha elaborado un documento de seguridad en el que recoge la normativa y el responsable de cada punto de acceso desconocido se hace responsable del mismo y bajo conocimiento de la normativa. De esta forma se pretende evitar que un mismo dispositivo pueda conectarse a la red interna de la empresa y a un punto de acceso a Internet independiente de la misma para evitar así ataques y puntos de intrusión en el sistema.

El despliegue WIFI reglamentario está realizado mediante puntos de acceso Cisco conectados a dos controladores funcionando en alta disponibilidad, siendo uno el redundante del primario. Estos APs son capaces de detectar otros APs o dispositivos 3G que emitan señales WIFI y obtener información de su potencia y SSID, de esta forma se pueden realizar reportes con información de los dispositivos no conocidos.

Una de las primeras tareas a realizar es la obtención de los reportes. Se comenzó obteniendo reportes diarios durante una semana. A partir de este punto se procedió a sacar reportes por semanas de los 7 días durante un mes. Una vez finalizado el mes se estableció como protocolo la obtención de los reportes de forma mensual con los datos de todo el mes. Estos informes se obtienen mediante el programa Cisco Prime Infraestructure el cual es el encargado de monitorizar el sistema WIFI de la empresa.

Cada reporte obtenido ha necesitado ser filtrado. El primero filtro aplicado ha sido en función del RSSI (Received Signal Strength Indicator) o indicador de fuerza de la señal recibida. Este es en realidad una escala de referencia (en relación a 1 mW) para medir el nivel de potencia de las señales recibidas por un dispositivo en las redes inalámbricas. El valor de -80dBm hace referencia a la señal mínima aceptable para establecer la conexión. Por tanto cada reporte ha sido inicialmente filtrado permitiendo separar los dispositivos emitiendo en una potencia menor que -80dBm, considerados externos a la empresa y los dispositivos emitiendo con potencias mayores de -80dBm, en este caso internos.

Sobre esta clasificación inicial, dentro del conjunto de dispositivos considerados internos (RSSI mayor que -80dBm) se han clasificado en tres grupos distintos atendiendo el SSID. Por un lado los dispositivos considerados teléfonos móviles o USB, en otro lado los ADSL de movistar y por último los APs desconocidos.

Esta clasificación se ha realizado así por varios motivos, el primero de ellos es que los dispositivos móviles son difíciles de encontrar puesto que no están fijos en un punto ni

conectados siempre. Por otra parte, el motivo de aislar los ADSL de movistar es que estos, a pesar de no ser gestionados por IT, sí que son conscientes de los mismos.

Estos reportes contienen en sus columnas el SSID del dispositivo WIFI, la potencia con la que emite, el AP de la empresa que lo ha visto, la zona de la empresa donde se ha visto, la MAC del dispositivo, el tipo de protocolo WIFI que emite, etc.

Realizando estas clasificaciones con todos los reportes obtenidos durante tres meses se puede obtener una primera información sobre los dispositivos WIFI existentes, para poder ver esta información de una forma rápida y visual se ha procedido a elaborar un Excel resumen de todos los reportes.

Este Excel se ha ido mejorando y retocando conforme se iban añadiendo reportes y obteniendo resultados de forma que la información final mostrada fuese lo más correcta posible. El formato final es un libro de Excel con diferentes hojas en las que se recopilan los datos de los reportes filtrados, una tabla con los responsables de la WIFI en cuestión y una tabla dinámica resumen. El Excel cuenta concretamente con las siguientes hojas:

- Hoja de responsables: Esta está formada por dos columnas, la primera indica el SSID del dispositivo y la segunda el nombre del responsable del mismo.

- Hoja de reportes de dispositivos móviles y 3G poco repetidos: En esta se encuentran recogidos los datos de los teléfonos móviles y 3G (no repetidos) de todos los reportes realizados. Se añaden dos columnas, una para indicar la fecha y otra con el responsable.

- Hoja de reportes de APs: En esta se encuentran recogidos los datos de los APs móviles de todos los reportes realizados. Se añaden dos columnas, una para indicar la fecha y otra con el responsable.

- Hoja de reportes de dispositivos 3G repetidos: En esta se encuentran recogidos los datos de los dispositivos 3G que se repiten durante los reportes realizados. Se añaden dos columnas, una para indicar la fecha y otra con el responsable. Esta hoja se ha ido modificando en función se realizaban nuevos reportes quitando datos de la hoja de dispositivos no repetidos y colocándolos en esta de forma que se obtuviese una información y una clasificación más precisa.

- Hoja de reportes de WIFI Movistar: En esta se encuentran recogidos los datos de los dispositivos WIFI de Movistar que se repiten durante los reportes realizados. Se añaden dos columnas, una para indicar la fecha y otra con el responsable.

- Tabla dinámica: Esta permite mostrar el número de veces que aparece cada dispositivo. Cuando se añaden nuevos datos de reportes se actualiza el resultado de forma que no es necesario estar pendiente de generar tablas resumen cada vez que se realizan nuevos reportes. Permite ver en qué mes se ha visto cada SSID, con que potencia y en qué zona de una forma fácil y resumida sin tener que acudir a las hojas de reportes. Esta tabla está realizada con ayuda de una macro programada mediante

VisualBasic, en la parte superior de la misma se encuentran cuatro botones, en relación con las cuatro hojas de datos descritas, al pulsar cada uno de ellos, la tabla dinámica muestra la información relativa a cada uno de los filtros aplicados (WFI de Movistar, APs, 3G repetidos o dispositivos móviles y 3G no repetidos). En la primera columna de la tabla dinámica aparece el SSID, en las siguientes el AP que lo ha visto, la zona, la potencia y el protocolo de WIFI. Tras estas columnas aparecen los meses en los que se han hecho los reportes. En el caso de las primeras semanas los meses se pueden expandir y se pueden ver las repeticiones diarias o semanales, en función de los reportes realizados. Para cada mes aparece el número de repeticiones de ese APs. En el caso de los reportes mensuales sólo aparece una vez si se ha visto, puesto que lo que captura el programa que genera los reportes (Cisco Prime Infraestructure) es información de los dispositivos vistos durante el periodo que se le especifique, por tanto, aunque un dispositivo haya estado conectado durante todos los días de un mes, el reporte lo contendrá sólo una vez. Es por esto que durante los meses en los que se han tomado más datos se tiene información más precisa de cuando estaba conectado cada dispositivo y aparecen un mayor número de repeticiones.

Otro dato a destacar del Excel está relacionado con la hoja de responsables. Dicha hoja está directamente relacionada mediante fórmulas con las columnas dedicadas a los responsables situadas en cada una de las hojas de reportes, de forma que cuando se inserte un SSID y un responsable, el nombre de este se sitúe en las hojas de reporte en las celdas dedicadas a los responsables que correspondan a ese SSID.

En la Figura 77 se puede ver el código creado en la macro mediante VisualBasic, este es el encargado de que al pulsar el botón referente a los dispositivos móviles y 3G poco repetidos se carguen los datos correspondientes a estos. Además se encarga de realizar la suma de SSIDs totales encontrados. Existe una función igual para cada uno de los botones existentes.

```
Sub Boton_moviles()
ActiveSheet.PivotTables("INFOAPs").ChangePivotCache ActiveWorkbook.PivotCaches. _
        Create(SourceType:=xlDatabase, SourceData:="Moviles", Version:= _
        xlPivotTableVersion10)

        ActiveSheet.Range("G2").Font.Bold = True
ActiveSheet.Range("G2").Font.Size = 18
ActiveSheet.Range("G2").HorizontalAlignment = xlCenter
        ActiveSheet.Range("G2").VerticalAlignment = xlCenter
ActiveSheet.Range("G2") = "INFO dispositivos 3G no repetidos o moviles"
ActiveSheet.Range("C2").FormulaR1C1 = _
        "=SUMPRODUCT(('RSSI>-80dBm 3G (moviles)'!R2C8:OFFSET('RSSI>-80dBm 3G (moviles)'
        !R1C8,1,0,COUNTA('RSSI>-80dBm 3G (moviles)'!C8),1)<>"""")/
        (COUNTIF('RSSI>-80dBm 3G (moviles)'!R2C8:OFFSET('RSSI>-80dBm 3G (moviles)'!R1C8,1,0,
        COUNTA('RSSI>-80dBm 3G (moviles)'!C8),1),'RSSI>-80dBm 3G (moviles)'
        !R2C8:OFFSET('RSSI>-80dBm 3G (moviles)'
        !R1C8,1,0,COUNTA('RSSI>-80dBm 3G (moviles)'!C8),1)&""""))"
End Sub
```

Figura 77-Macro Móviles

En la siguiente Figura 78 se puede ver la tabla dinámica resumen que se ha comentado. En la parte superior se encuentran cuatro botones que permiten mostrar los resultados de cada una de las clasificaciones explicadas. En las columnas referentes a los meses se puede apreciar cuando se han visto esos SSID. Las líneas naranjas horizontales indican los totales por mes. En la columna de la derecha se encuentran los subtotales por potencia en el total de meses. El total global de veces que se ha visto ese dispositivo aparece en la columna de la derecha en naranja. En la parte inferior del libro se pueden apreciar las hojas de las que se compone.

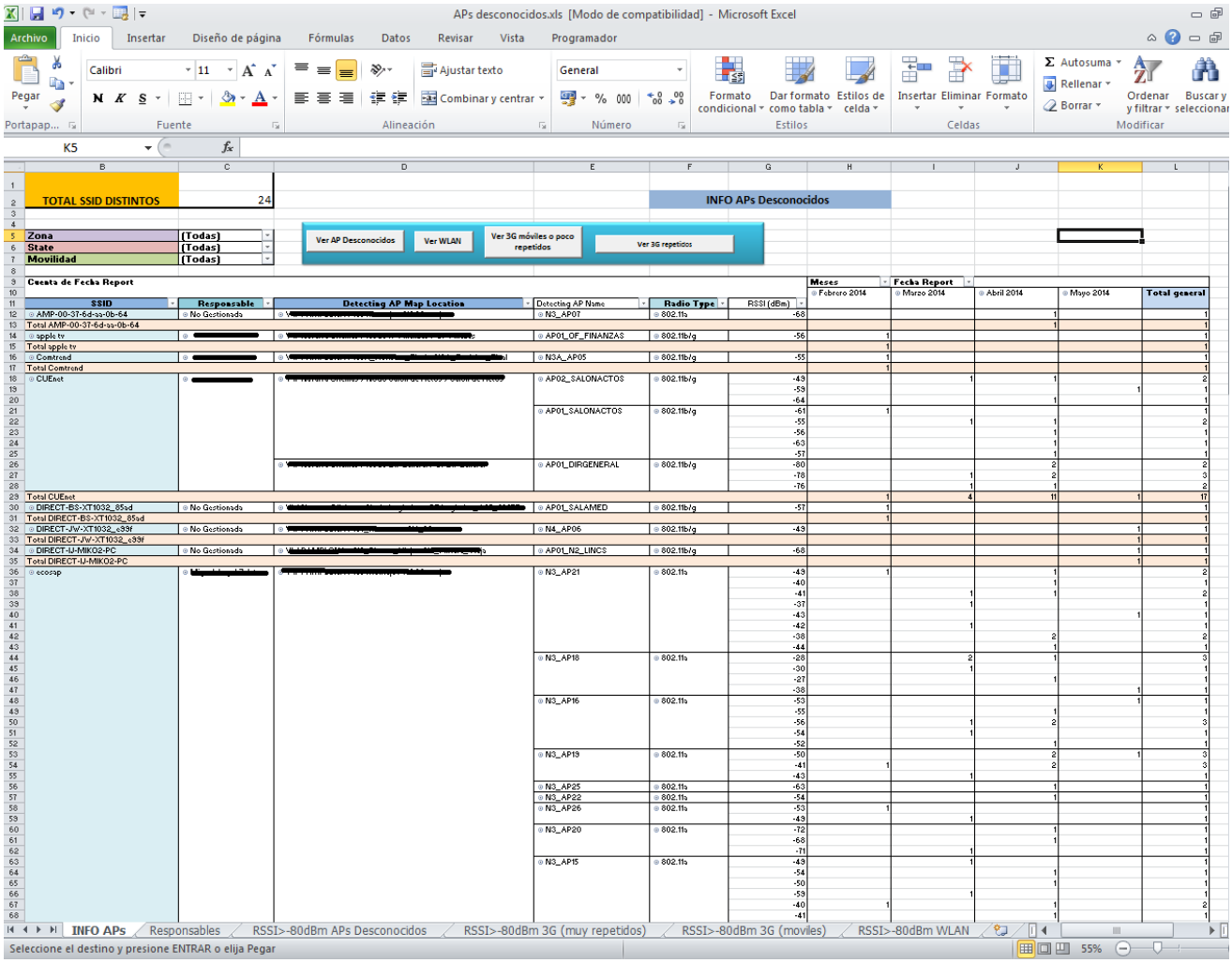


Figura 78- Tabla dinámica

Tras la obtención de los datos se realizó por una de las naves unas capturas mediante un software de Cisco (Spectrum) para ver los dispositivos Bluetooth y WIFI existentes en esa nave.

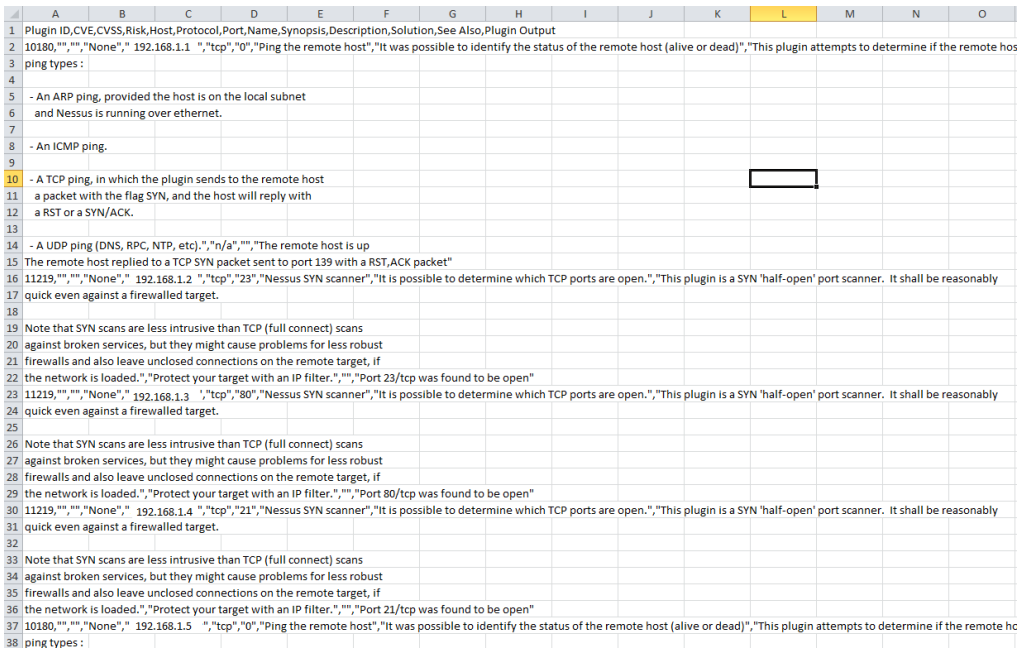
El siguiente paso consiste en localizar físicamente cada dispositivo y buscar el responsable del mismo.

5.2. Descubrimiento de red con NESSUS y reorganización de datos XML.

Tras el fin de soporte del sistema operativo Windows XP y su migración a Windows 7, fue necesario un análisis de las redes con el fin de obtener los posibles equipos con el sistema operativo antiguo.

Para la red corporativa se realizó el escáner mediante NESSUS, una herramienta de auditoría de seguridad que permite la detección de vulnerabilidades mediante la simulación de ataques a los equipos. Una de las posibilidades de este software es la detección del sistema operativo de cada equipo. Para no saturar la red se lanzaron los análisis a cada una de las VLANS que componen la red corporativa con espacios temporales de entre 10 y 30 minutos en varios días.

NESSUS permite exportar estos datos en diferentes formatos (HTML, PDF, CSV y XML) aunque sólo en HTML es capaz de permitir filtros de forma que sólo se muestren los datos necesarios de forma más clara. El formato exigido era CSV el cual no era legible de forma clara puesto que mostraba mucha información de forma desordenada. En este caso lo único que interesaba era obtener que sistema operativo tenía cada dirección IP, y mediante los reportes en CSV no se podía ver.



	A
1	Plugin ID,CVE,CVSS,Risk,Host,Protocol,Port,Name,Synopsis,Description,Solution,See Also,Plugin Output
2	10180,"","","None"," 192.168.1.1 ","tcp","0","Ping the remote host","It was possible to identify the status of the remote host (alive or dead)","This plugin attempts to determine if the remote hos
3	ping types :
4	
5	- An ARP ping, provided the host is on the local subnet
6	and Nessus is running over ethernet.
7	
8	- An ICMP ping.
9	
10	- A TCP ping, in which the plugin sends to the remote host
11	a packet with the flag SYN, and the host will reply with
12	a RST or a SYN/ACK.
13	
14	- A UDP ping (DNS, RPC, NTP, etc).","n/a","","The remote host is up
15	The remote host replied to a TCP SYN packet sent to port 139 with a RST,ACK packet"
16	11219,"","","None"," 192.168.1.2 ","tcp","23","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably
17	quick even against a firewalled target.
18	
19	Note that SYN scans are less intrusive than TCP (full connect) scans
20	against broken services, but they might cause problems for less robust
21	firewalls and also leave unclosed connections on the remote target, if
22	the network is loaded.","Protect your target with an IP filter.","","Port 23/tcp was found to be open"
23	11219,"","","None"," 192.168.1.3 ","tcp","80","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably
24	quick even against a firewalled target.
25	
26	Note that SYN scans are less intrusive than TCP (full connect) scans
27	against broken services, but they might cause problems for less robust
28	firewalls and also leave unclosed connections on the remote target, if
29	the network is loaded.","Protect your target with an IP filter.","","Port 80/tcp was found to be open"
30	11219,"","","None"," 192.168.1.4 ","tcp","21","Nessus SYN scanner","It is possible to determine which TCP ports are open.","This plugin is a SYN 'half-open' port scanner. It shall be reasonably
31	quick even against a firewalled target.
32	
33	Note that SYN scans are less intrusive than TCP (full connect) scans
34	against broken services, but they might cause problems for less robust
35	firewalls and also leave unclosed connections on the remote target, if
36	the network is loaded.","Protect your target with an IP filter.","","Port 21/tcp was found to be open"
37	10180,"","","None"," 192.168.1.5 ","tcp","0","Ping the remote host","It was possible to identify the status of the remote host (alive or dead)","This plugin attempts to determine if the remote hc
38	ping types :

Figura 79-Ejemplo reporte CSV

Como solución se obtuvieron los reportes en XML. Este documento XML se abrió con Excel mediante su opción para leer código XML. Esta opción muestra una tabla con las etiquetas que se encuentran en el código, y mediante un documento PDF proporcionado por la web del software, donde explicaba que era cada etiqueta del código XML y la estructura del mismo se consiguió aislar la dirección IP del dispositivo en una columna y la información del sistema operativo en la otra. Tras esto, el documento se podía guardar en formato CSV.

En el caso de la red industrial, la herramienta empleada fue NMAP. El resultado de los reportes proporcionados por esta herramienta eran XML por lo que el procedimiento para aislar la

información de los sistemas operativos fue el mismo que el utilizado con NESSUS, es decir, mediante Excel.

5.3. Reuniones con fabricantes.

Se ha asistido a una presentación de un comercial de la empresa RITTAL, la cual se encarga de aportar soluciones relacionadas con Racks, CPDs y equipamiento de red. La asistencia a esta presentación es de interés debido a que muestra un ámbito más comercial del sector de las telecomunicaciones y no uno técnico al que se está más acostumbrado. Además se ha aprendido de nuevas soluciones propuestas por el fabricante sobre todo en lo relacionado con CPDs, estructuras de pasillo en frío y armarios de comunicaciones.

Se ha asistido a una reunión con Schneider Electric los cuales han propuesto una solución para la construcción de un nuevo CPD (Centro de Procesado de Datos). En esta reunión se han podido ver aspectos más comerciales del ámbito de las telecomunicaciones, así como nuevas soluciones optimizadas en precio, sostenibilidad y ahorro energético para la construcción de centros de procesado de datos. Durante el transcurso de la reunión se han explicado los distintos tipos de CPDs existentes y temas referentes a la refrigeración y aislamiento de los mismos.

Se ha asistido a una reunión con los proveedores Phoenix Contact, encargados de la elaboración de soluciones de electrónica de red de la parte industrial. El idioma utilizado durante la presentación ha sido el inglés, y en la misma se han enseñado las propuestas del proveedor y se han aclarado las dudas sobre si los equipos del proveedor están dentro del libro de estándares de la empresa multinacional y por tanto si se pueden instalar dentro de la misma.

Otro de las reuniones ha sido con un representante de Cisco, en esta reunión se ha explicado el portfolio de Cisco con sus nuevos equipos y soluciones. Se ha explicado también parte del concepto NAC ofrecido por Cisco (Cisco ISE) el cual ya se ha comentado en este trabajo. Sobre el ámbito NAC, se afirmó que Cisco ISE busca ser una solución de gestión y control centralizada y se habló de la posibilidad de incorporar el sistema de monitorizado WIFI (Cisco Prime Infraestructure) con la posible futura implementación de Cisco ISE en la red cableada.

5.4. Mapas fibra óptica.

Una de las tareas realizadas ha sido la elaboración de dos diagramas de fibra óptica. El primero de ellos muestra de forma lógica las conexiones existentes entre las diferentes naves indicando el tipo de fibra en función del color y grosor de la línea. En cada una de estas uniones se especifica además el tipo de conector usado, el número de fibras libres y el número total de fibras de la tirada. El segundo diagrama añade además la separación de las fibras por capas de forma que se puedan mostrar aquellas que interesen. Se incorpora además una nueva capa con las futuras fibras a instalar tras la implantación de la fibra solicitada en la RFP. Este diagrama se ha realizado mediante el programa Microsoft Visio, el cual permite dibujar diagramas. En estos planos aparecen reflejados los dos LDR, así como todos los nodos de comunicación principales. También aparecen todos los armarios existentes distribuidos por la empresa, los cuales están unidos por fibra óptica formando el denominado backbone.

5.5. Conclusiones.

En este trabajo se pueden distinguir principalmente tres partes, la primera de ellas está dedicada a la descripción de la infraestructura de la red de datos de la empresa tanto física como lógicamente. Esta descripción está realizada con el fin de facilitar la comprensión de las siguientes partes que componen el trabajo, las cuales son el desarrollo del proyecto de cambio del backbone de fibra óptica, la implementación NAC y las tareas realizadas en la empresa.

En lo correspondiente al proyecto de fibra óptica se pueden apreciar los pasos a seguir para la elaboración del mismo así como las rectificaciones realizadas conforme se iba desarrollando el documento RFP. Cabe destacar que el objetivo inicial del proyecto era el cambio de la electrónica de red de la red corporativa y el backbone de fibra óptica dejando el cambio de la electrónica de red de la red industrial para otro proyecto futuro. La decisión final fue separar el Lote 1 referente a la renovación de la infraestructura de fibra óptica en una RFP y la electrónica de red de ambas redes (industrial y corporativa) en otro proyecto. Por cuestiones temporales no se ha podido realizar un seguimiento completo del proyecto de fibra óptica ni un análisis de las ofertas recibidas y la solución finalmente elegida, puesto que estos pasos se realizarán en fechas posteriores a la finalización de este trabajo de fin de grado.

Una de las partes de este trabajo es el NAC, un concepto de seguridad a nivel de puerto de usuario que pretende implementarse en la empresa para el cumplimiento de la normativa. Para ello es necesario introducir el estándar 802.1X que es el que la empresa debe de cumplir en su futura implementación de NAC. La empresa pretende separar la red corporativa en zonas protegidas por firewalls además de incorporar NAC en los switches de acceso. Se han explicado las dos soluciones NAC propietarias que la empresa admite (Cisco ISE y Enterasys NetSight) y las características de las mismas. Para entender mejor el concepto NAC y poder valorar estas soluciones se ha decidido implementar una maqueta mediante una solución OpenSource (PacketFence) gracias a ésta se ha podido comprobar cómo se configura y funciona un mecanismo NAC a grandes rasgos. Mediante esta implementación se han podido probar los dos modos de funcionamiento de las soluciones NAC (inline y out-of-band) viendo que el método out-of-band a pesar de necesitar una configuración más compleja y unos requisitos de compatibilidad con los switches o APs es una solución mucho más escalable, segura y viable que la solución inline. El mecanismo inline permite aislamiento a nivel 3, es decir, dos usuarios conectados a nivel 2 podrían verse puesto que no tienen que atravesar el servidor PacketFence que actúa como puerta de enlace y se encarga de ejercer las tareas de elemento de corte entre redes. En el método out-of-band el aislamiento es directamente a nivel 2, los usuarios no pueden verse a nivel 2 puesto que el puerto del switch no les permite enviarse tráfico hasta que el usuario esté autenticado obteniendo así una solución más segura y también escalable. Como líneas futuras se podría comprobar el funcionamiento del sistema NAC mediante el estándar 802.1X y el módulo FreeRadius que PacketFence tiene incorporado utilizando el suplicante 802.1X embebido de un host final y analizar si se encuentra alguna diferencia respecto de la solución implementada mediante SNMP.

La última parte está dedicada a describir algunas de las tareas realizadas durante las prácticas en empresa como por ejemplo el seguimiento de los puntos de acceso WIFI desconocidos y la

clasificación de los mismos, las diferentes reuniones con fabricantes o la elaboración de mapas de fibra óptica.

A lo largo del trabajo y las prácticas se han aprendido nuevos conceptos relacionados con las redes. Se ha podido ver una infraestructura de red real de una empresa y la distribución de la misma en sus tres capas lógicas (Core, Distribución y Acceso). Se ha podido ver la problemática que tiene la gestión de una red compleja y real y cómo es necesario tener un DRP (Disaster Recovery Plan) o plan de recuperación de desastres para solucionar caídas en la red de forma rápida para evitar así pérdidas en la producción de la empresa.

Se ha podido investigar sobre NAC y su funcionamiento así como tener una idea de un sistema real mediante las pruebas con la solución OpenSource. Este concepto de seguridad se está volviendo cada día más importante a nivel empresarial debido a que permite a los usuarios traer su propio dispositivo (BYOD) e incorporarlo a la red de forma segura facilitando la gestión a IT.

Se ha estado en contacto con el desarrollo de un proyecto real de cambio de una infraestructura de red, y se ha estado presente en reuniones y tomas de decisiones pudiendo apreciar así la complejidad del mismo, así como las dificultades que un proyecto tiene sobre todo en cuanto a objetivos de plazos temporales y coordinación.

En la parte relacionada a las prácticas se ha apreciado el funcionamiento de un equipo de trabajo dentro del área de las telecomunicaciones y concretamente en la relacionada a las redes. A parte de lo relacionado con el proyecto del cambio de la infraestructura de red se ha podido aprender el funcionamiento de la resolución de la problemática que causa una red de gran tamaño y el coste de trabajo del mantenimiento de la misma.

Anexos

Anexo 1. Documento de presupuesto estándar de la empresa

LOTE 1: RENOVACIÓN DE LA INFRAESTRUCTURA DE CABLEADO QUE COMPONE LA RED CORPORATIVA ANEXO VII - OFERTA ECONÓMICA

Empresa:	Por favor rellenar
Fecha y versión de la oferta:	
Fabricante fibra óptica:	
Descuento sobre PVP en fibra óptica para el proyecto:	

Concepto	Modo	Descripcion y codigo de producto del fabricante	Cantidad (Unidades)	COSTE UNITARIO (Euros / Unidad)	IMPORTE TOTAL	UNIDAD
FIBRA MONOMODO						
Manguera de 12 fibras monomodo OS2 (9/125µ)	Material		250		0,00	Euros / Metro
Instalación manguera de 12 fibras	Servicio		250		0,00	Euros / Metro
Manguera de 24 fibras monomodo OS2 (9/125µ)	Material		600		0,00	Euros / Metro
Instalación manguera de 24 fibras	Servicio		600		0,00	Euros / Metro
Manguera de 48 fibras monomodo OS2 (9/125µ)	Material		6726		0,00	Euros / Metro
Instalación manguera de 48 fibras	Servicio		6226		0,00	Euros / Metro
Manguera de 128 fibras monomodo OS2 (9/125µ)	Material		1750		0,00	Euros / Metro
Instalación manguera de 128 fibras	Servicio		1250		0,00	Euros / Metro
Patch pannels de 19" 1 UA (48 conectores)	Material		24		0,00	Euros / Patch Pannel
Cajas conexión LC para 24 fibras incl. Pigtails LC	Material		48		0,00	Euros /Caja
Fusiones	Servicio		1000		0,00	Euros / Fusion
Certificaciones	Servicio		500		0,00	Euros / Fibra
FIBRA MULTIMODO						
Manguera de 12 fibras multimodo OM3(4) (50/125µ)	Material		500		0,00 €	Euros / Metro
Instalación manguera de 12 fibras	Servicio		500		0,00 €	Euros / Metro
Manguera de 24 fibras multimodo OM3(4) (50/125µ)	Material		10903		0,00 €	Euros / Metro
Instalación manguera de 24 fibras	Servicio		10903		0,00 €	Euros / Metro
Patch pannels de 19" 1 UA (24 conectores)	Material		90		0,00 €	Euros / Patch Pannel
Cajas conexión LC para 24 fibras incl. Pigtails LC	Material		90		0,00 €	Euros /Caja
Fusiones	Servicio		2088		0,00 €	Euros / Fusion
Certificaciones	Servicio		1044		0,00 €	Euros / Fibra
CERTIFICACION DE FIBRA EXISTENTE (OPCIONAL)						
Auditoria y certificación fibra monomodo OS2	Servicio		300		0,00 €	Euros / Fibra
Auditoria y certificación fibra multimodo OM3	Servicio		300		0,00 €	Euros / Fibra
CANALIZACION ADICIONAL SEGÚN NECESIDAD						
Canal PUK de 300x100 sin tapa incluyendo soporteria	Material		1000		0,00 €	Euros / Metro
Instalación	Servicio		1000		0,00 €	Euros / Metro
ACTUACIONES ADICIONALES ARMARIOS (4.1.1.8)						
Armario de comunicaciones	Material	Incluir el importe total del material	1		0,00 €	Euros / Unidad
Instalación	Servicio		1		0,00 €	Euros / Unidad
Armario de comunicaciones en el LDR-B	Material	Incluir el importe total del material	1		0,00 €	Euros / Unidad
Instalación	Servicio		1		0,00 €	Euros / Unidad
Mantenimiento de tres armarios	Material	Incluir el importe total del material	1		0,00 €	Euros / Unidad
Instalación	Servicio		1		0,00 €	Euros / Unidad
RETIRADA DE FIBRA OBSOLETA (4.1.1.7)						
Análisis y retirada básica por fibra (cortar y marcar)	Servicio		64		0,00 €	Euros / Fibra
Metros fibra retirada fisicamente	Servicio		17297		0,00 €	Euros / Metro
					0,00 €	
LATIGUILLOS (OPCIONAL)						
Latiguillo bifibra monomodo OS2(9/125µ) LC - LC, 3m	Material		100		0,00 €	Euros / Unidad
Latiguillo bifibra monomodo OS2(9/125µ) LC - SC, 3m	Material		150		0,00 €	Euros / Unidad
Latiguillo bifibra multimodo OM 3 (4)(50/125µ) LC - LC, 3m	Material		600		0,00 €	Euros / Unidad
Latiguillo bifibra multimodo OM 3 (4) (50/125µ) LC - SC, 3m	Material		400		0,00 €	Euros / Unidad
GESTION DE PROYECTO						
Jefe de proyecto	Servicio				0,00 €	Euros / hora
OTROS ASPECTOS PRESENTADOS EN LA VALORACIÓN (Especificar uno por uno)					0,00 €	
		Importe Total Lote 1			0,00 €	Total

Anexo 2. Fichero de configuración de PacketFence switches.conf

```
#
# Copyright 2006-2008 Inverse inc.
#
# See the enclosed file COPYING for license information (GPL).
# If you did not receive this file, see
# http://www.fsf.org/licensing/licenses/gpl.html
[default]
description=Switches Default Values
vlans=1,2,3,4,5
normalVlan=1
registrationVlan=2
isolationVlan=3
macDetectionVlan=4
voiceVlan=5
inlineVlan=6
inlineTrigger=
normalRole=normal
registrationRole=registration
isolationRole=isolation
macDetectionRole=macDetection
voiceRole=voice
inlineRole=inline
VoIPEnabled=no
mode=testing
macSearchesMaxNb=30
macSearchesSleepInterval=2
uplink=dynamic
#
# Command Line Interface
#
# cliTransport could be: Telnet, SSH or Serial
cliTransport=Telnet
cliUser=
cliPwd=
cliEnablePwd=
#
# SNMP section
#
# PacketFence -> Switch
SNMPVersion=1
SNMPCommunityRead=public
SNMPCommunityWrite=private
```

```
#SNMPEngineID = 0000000000000
#SNMPUserNameRead = readUser
#SNMPAuthProtocolRead = MD5
#SNMPAuthPasswordRead = authpwdread
#SNMPPrivProtocolRead = DES
#SNMPPrivPasswordRead = privpwdread
#SNMPUserNameWrite = writeUser
#SNMPAuthProtocolWrite = MD5
#SNMPAuthPasswordWrite = authpwdwrite
#SNMPPrivProtocolWrite = DES
#SNMPPrivPasswordWrite = privpwdwrite
# Switch -> PacketFence
SNMPVersionTrap=1
SNMPCommunityTrap=public
#SNMPAuthProtocolTrap = MD5
#SNMPAuthPasswordTrap = authpwdread
#SNMPPrivProtocolTrap = DES
#SNMPPrivPasswordTrap = privpwdread
#
# Web Services Interface
#
# wsTransport could be: http or https
wsTransport=http
wsUser=
wsPwd=
#
# RADIUS NAS Client config
#
# RADIUS shared secret with switch
radiusSecret=

[192.168.0.1]
description=Test Switch
type=Cisco::Catalyst_2900XL
mode=production
uplink=23,24

[192.168.1.44]
mode=production
deauthMethod=SNMP
description=Cisco
type=Cisco::Catalyst_2950
VoIPEnabled=N
uplink=1,2
```

```
SNMPVersion=2c
vlans=1,4,100,200
isolationVlan=200
normalVlan=1
registrationVlan=100
defaultVlan=1
SNMPVersionTrap=2c
defaultRole=normail
#SNMPVersion = 3
#SNMPEngineID = 0000000000000
#SNMPUserNameRead = readUser
#SNMPAuthProtocolRead = MD5
#SNMPAuthPasswordRead = authpwdread
#SNMPPrivProtocolRead = DES
#SNMPPrivPasswordRead = privpwdread
#SNMPUserNameWrite = writeUser
#SNMPAuthProtocolWrite = MD5
#SNMPAuthPasswordWrite = authpwdwrite
#SNMPPrivProtocolWrite = DES
#SNMPPrivPasswordWrite = privpwdwrite
#SNMPVersionTrap = 3
#SNMPUserNameTrap = readUser
#SNMPAuthProtocolTrap = MD5
#SNMPAuthPasswordTrap = authpwdread
#SNMPPrivProtocolTrap = DES
#SNMPPrivPasswordTrap = privpwdread
```

Anexo 3. Fichero de configuración de PacketFence pf.conf

```
[general]
# general.domain
#
# Domain name of PacketFence system.
domain=pfserver.org
#
# general.hostname
#
# Hostname of PacketFence system.  This is concatenated with the domain in Apache rewriting rules and therefore must be resolvable by clients.
hostname=pf
# general.dhcpservers
#
# Comma-delimited list of DHCP servers.  Passthroughs are created to allow DHCP transactions from even "trapped" nodes.
```

```
dhcpservers=127.0.0.1,10.100.0.1,10.200.0.1,192.168.1.1

[trapping]
# trapping.range
# Comma-delimited list of address ranges/CIDR blocks that PacketFence will
monitor/detect/trap on.  Gateway, network, and
# broadcast addresses are ignored.
range=192.168.1.0/24

[alerting]
# alerting.emailaddr
# Email address to which notifications of rogue DHCP servers, violations with an action of
"email", or any other
# PacketFence-related message goes to.
emailaddr=////////////////////////////////////

[database]
# database.pass
# Password for the mysql database used by PacketFence.
pass=packetfence

[interface eth0.100]
ip=10.100.0.1
type=internal
mask=255.255.255.0
enforcement=vlan

[interface eth0.200]
enforcement=vlan
ip=10.200.0.1
type=internal
mask=255.255.255.0

[interface eth0]
ip=192.168.1.42
type=management
mask=255.255.255.0
```

Anexo 4. Fichero de configuración de PacketFence networks.conf

```
[10.200.0.0]
dns=10.200.0.1
dhcp_start=10.200.0.10
gateway=10.200.0.1
```

```
domain-name=vlan-isolation.pfserver.org
named=enabled
dhcp_max_lease_time=30
dhcpd=disabled
fake_mac_enabled=disabled
dhcp_end=10.200.0.246
type=vlan-isolation
netmask=255.255.255.0
dhcp_default_lease_time=30

[10.100.0.0]
dns=10.100.0.1
dhcp_start=10.100.0.10
gateway=10.100.0.1
domain-name=vlan-registration.pfserver.org
named=enabled
dhcp_max_lease_time=30
dhcpd=enabled
fake_mac_enabled=enabled
dhcp_end=10.100.0.246
type=vlan-registration
netmask=255.255.255.0
dhcp_default_lease_time=30
```

Anexo 5. Fichero de configuración de PacketFence authentication.conf

```
[local]
description=Local Users
type=SQL

[file1]
description=Legacy Source
path=/usr/local/pf/conf/admin.conf
type=Htpasswd

[file1 rule admins]
description=All admins
match=all
action0=set_role=default
action1=set_access_duration=12h

[sms]
description=SMS-based registration
```

sms_carriers=100056,100057,100061,100058,100059,100060,100062,100063,100071,100064,100116,100066,100117,100112,100067,100065,100068,100069,100070,100118,100115,100072,100073,100074,100075,100076,100077,100085,100086,100080,100079,100081,100083,100082,100084,100087,100088,100111,100089,100090,100091,100092,100093,100094,100095,100096,100098,100097,100099,100100,100101,100113,100102,100103,100104,100106,100105,100107,100108,100109,100114,100110,100078
type=SMS

[sms rule catchall]
description=
match=all
action0=set_role=guest
action1=set_access_duration=1D

[email]
description=Email-based registration
email_activation_timeout=10m
type=Email
allow_localdomain=yes

[email rule catchall]
description=
match=all
action0=set_role=guest
action1=set_access_duration=1D

[sponsor]
description=Sponsor-based registration
type=SponsorEmail
allow_localdomain=yes

[sponsor rule catchall]
description=
match=all
action0=set_role=guest
action1=set_access_duration=1D

[null]
description=Null Source
type=Null
email_required=no

Referencias

[1] Nortel Networks. Documentación sobre protocolos propietarios del fabricante Avaya: https://downloads.avaya.com/css/P8/documents/100101820 Fecha: 12-4-2010.

[2] Adolfo Aguayo Puerta. Información sobre MacroLAN de Telefónica. http://oa.upm.es/20935/1/PFC_ADOLFO_AGUAYO_PUERTA.pdf Fecha: Junio 2013.

[3] R. Hinden, Ed. RFC VRRP. http://tools.ietf.org/html/rfc3768 Fecha: 2004.

[4] Fotografía VRRP. http://rzbangka.files.wordpress.com/2010/06/vrrp1.jpg

[5] P. Congdon , B. Aboba , G. Zorn, A. Smith, J. Roese .RFC Norma 802.1X. http://tools.ietf.org/html/rfc3580 Fecha: 2003

[6] Imagen NAC http://en.wikipedia.org/wiki/File:802.1X_wired_protocols.png

[7] Peter J. Welcher. Información e imágenes sobre EAP y EAPOL http://www.netcraftsmen.net/resources/archived-articles/429-examining-8021x-and-eap.html Fecha: 04-06-2004

[8] Rajesh K. Información e imágenes sobre NAC. http://www.excitingip.com/758/ieee-802-1x-elements-protocols-advantages/ Fecha: 2010

[9] Rhys Haden. Tipos de EAP. http://www.rhyshaden.com/8021x.htm Fecha: 2007

[10] Información sobre certificados digitales http://portalae.sci.uma.es:8080/export/sites/default/uma/documentos/criptografia_certificado_digital_firma_digital.pdf

[11] Rhys Haden. Información sobre RADIUS. http://www.rhyshaden.com/8021x.htm. Fecha: 2007

[12]H3C Technologies Co. Información sobre RADIUS. www.h3c.com/portal/download.do?id=713325 Fecha:2003

[13] BradFord NetWorks. Información sobre NAC y 801.1X. Semejanzas y diferencias entre ellas. http://www.cadincweb.com/wp-content/uploads/2010/11/CAD_Bradford_Network_Access_Control_802.1X.pdf Fecha:2011

[14] Cisco. Documentación Cisco ISE At Glance. http://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-654884.pdf Fecha:2013.

[15] Cisco. Guía de usuario.
http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_overview.pdf
Fecha:2013.

[16] Cisco. Características Cisco ISE.
http://www.cisco.com/web/LA/assets/executives/pdf/Cisco_Bring_Your_Own_Device_-_Device_Freedom_without_Compromising_the_IT_Network_Whitepaper.pdf
Fecha:2013.

[17] Cisco. Catálogo Cisco At Glance.
http://www.cisco.com/c/dam/en/us/products/collateral/security/identity-services-engine/at_a_glance_c45-654884.pdf Fecha: 2013.

[18] Cisco. DataSheet Cisco ISE. Documentación técnica Cisco ISE.
http://www.digitalairwireless.com/files/Cisco-Identity-Services-Engine_1333230959.pdf Fecha:2012.

[19] Cisco. Tabla de protocolos de autenticación.
http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_man_id_stores.html Fecha:-

[20] Cisco. Información sobre los agentes ISE.
http://www.cisco.com/c/en/us/td/docs/security/nac/appliance/configuration_guide/49/cam/49cam-book/m_webagt.html Fecha:-

[21] Cisco. Resumen guía de usuario ISE.
http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_overview.html
Fecha:-

[22] Cisco. Guía de usuario Cisco ISE.
http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide.html Fecha:-

[23] Vmware. Máquina Virtual. http://www.vmware.com/

[24] Enterasys Networks. Protuctos para la gestión de acceso.
http://www.extremenetworks.com/product/network-access-control/

[25] Enterasys Networks. Netsight. http://www.extremenetworks.com/product/netsight/

[26] Enterasys. Networks. Datasheet de la solución NAC de Enterasys.
http://www.netsolutionstore.com/datasheets/software/nac-ds.pdf.

[27] Enterasys Networks. Manual de Enterasys NAC. Funcionamiento y componentes.
http://www.manualslib.com/manual/47699/Enterasys-Networks-9034385.html?page=5#manual

[28] PacketFence. Web del sistema NAC OpenSource. http://www.packetfence.org/.

[29] Opennac. Web del sistema NAC OpenSource.
http://www.opennac.org/opennac/en.html

[30]FreeNAC Web del sistema NAC OpenSource. http://freenac.net/es

[31]ChilliSpot. Web del portal cautivo Opensource. http://www.chillispot.info

[32] WifiDog. Web del portal cautivo Opensource. http://dev.wifidog.org

[33] PepperSpot. Web del portal cautivo Opensource. http://pepperspot.sourceforge.net

[34] PfSense. Solución Firewall OpenSource. https://www.pfsense.org/

[35] ZeroShell. Solución Firewall OpenSource. http://www.zeroshell.net/eng/

[36]VirtualBox. Web para descarga de VM. https://www.virtualbox.org/

[37]Snort. Web del programa. http://www.snort.org/

[38]Suricata. Web del programa. http://suricata-ids.org/

[39] Nessus. Web del software de análisis de vulnerabilidades. http://www.nessus.com/

[40] OpenVas. Web del software de análisis de vulnerabilidades. http://www.openvas.org/

[41]PacketFence. Listado de dispositivos soportados en Out-Of-Band
http://www.packetfence.org/about/supported_switches_and_aps.html

[42]PacketFence. Guía de configuración de PacketFence.
http://www.packetfence.org/downloads/PacketFence/doc/PacketFence_Network_Devices_Configuration_Guide-4.1.0.pdf Fecha:2013.

[43] PacketFence. Caracterísitcas.
http://www.packetfence.org/about/advanced_features.html

[44] PacketFence. Instalación del servidor en Ubuntu.
http://www.packetfence.org/support/faqs/article/how-to-install-packetfence-on-ubuntu.html

[45]PacketFence. Guia de configuración de los dispositivos.
http://www.packetfence.org/downloads/PacketFence/doc/PacketFence_Network_Devices_Configuration_Guide-4.1.0.pdf

[46] Movistar. Características del router ASL-26555
http://www.movistar.es/rpmm/estaticos/residencial/fijo/banda-ancha-adsl/manuales/modem-router-inalambricos-adsl/Manual-Usuario-Fabricante-Home-Station-Amper-ASL26555.pdf

[47]PacketFence. Guía de desarrollo. http://www.sogo.nu/files/downloads/PacketFence/doc/PacketFence_Developers_Guide-4.1.0.pdf

[48] Objeto MIB. http://www.alvestrand.no/objectid/1.3.6.1.2.1.1.3.html

[49]Objeto MIB. http://www.alvestrand.no/objectid/1.3.6.1.4.1.9.9.html

[50] Cisco. MIB de Cisco. Aplicación buscador de OID. http://tools.cisco.com/Support/SNMP/do/BrowseOID.do

[51] Cisco. Objetos MIB. http://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/45080-vlans.html

[52]Imagen Byod. http://www.thelearningplace.ph/wp-content/uploads/2013/05/BYOD2.jpg

[53] R. Hinden, Ed. RFC del protocol VRRP. http://www.ietf.org/rfc/rfc3768.txt Fecha: Abril 2004

[54]HLS. Programa de documentación y planos. http://www.weka-technology.com/maschinenbau/digitale-dokumentation/hallen-layout-system-hls/

[55] Imagen certificados. http://www.rinconastur.com/php/php21.php

[56] Imagen EAP. http://layer3.wordpress.com/2009/08/16/eap-authentication-protocols/ Fecha: Agosto 2009

- Además de todas estas referencias, para la elaboración del trabajo se ha empleado documentación interna de la empresa.