Universidad Zaragoza
1542

Trabajo Fin de Grado

Diseño e implementación de una solución de seguridad en entorno local (LAN y WiFi) y remoto (VPN)

Design and implementation of a security solution in a local (LAN and WiFi) and remote (VPN)

Autor

Jorge Luis Olivera Pinies

Directores

Fernando Negré Ramos

Ignacio Martínez Ruiz

Ingeniería de Tecnologías y Servicios de Telecomunicación

instituto de investigación en ingeniería de Aragón
Universidad de Zaragoza

Escuela de Ingeniería y Arquitectura
Universidad Zaragoza

TRABAJOS DE FIN DE GRADO / FIN DE MÁSTER

Escuela de Ingeniería y Arquitectura Universidad Zaragoza

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD

(Este documento debe entregarse en la Secretaría de la EINA, dentro del plazo de depósito del TFG/TFM para su evaluación).

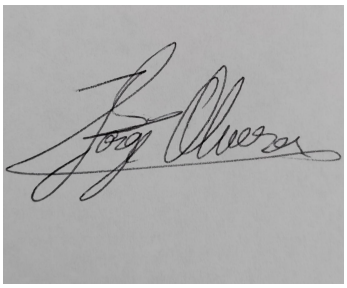
D./Dª. Jorge Luis Olivera Piniés ,en aplicación de lo dispuesto en el art. 14 (Derechos de autor) del Acuerdo de 11 de septiembre de 2014, del Consejo de Gobierno, por el que se aprueba el Reglamento de los TFG y TFM de la Universidad de Zaragoza, Declaro que el presente Trabajo de Fin de (Grado/Máster)

GRADO ING. TECNOG. Y SERV. TELECOMUNICACIÓN (Título del Trabajo)

DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE SEGURIDAD EN ENTORNO LOCAL (LAN Y WIFI) Y REMOTO (VPN)

es de mi autoría y es original, no habiéndose utilizado fuente sin ser citada debidamente.

Zaragoza, 15 DE ENERO DE 2021



Fdo: Jorge Luis Olivera Piniés

DEDICATORIAS Y AGRADECIMIENTOS

Quería agradecer en primer lugar a Instrumentación y Componentes SA por la oportunidad que me han ofrecido de poder desarrollar este Trabajo Fin de Grado con ellos, que marca el final de una etapa muy importante en mi vida.

En especial agradecer a Juan José Gil Morales, con quien más tiempo he pasado desarrollando el proyecto, por su dedicación, ganas de enseñarme y por poner a mi alcance todos los recursos que estaban a su disposición. También agradecer a Maite Oliván León por su colaboración, tiempo y el buen trato recibido. Además agradecer a todos los miembros de Inycom que me han hecho sentir como en casa y en especial a mi tutor Fernando Negré Ramos.

Igualmente quiero agradecer a mi tutor Ignacio Martínez Ruíz por las facilidades que me ha ofrecido durante el proyecto y su predisposición en todo momento.

RESUMEN DEL PROYECTO

"Diseño e Implementación de una solución de seguridad en entorno local (LAN y WiFi) y remoto (VPN)"

Realizado por: Jorge Luis Olivera Pinies

Director: Fernando Negré Ramos

Ponente: Ignacio Martínez Ruiz

El presente proyecto consiste en el diseño e implementación de soluciones de seguridad en un entorno local y remoto, gestionando y controlando el acceso a la red mediante el uso de las herramientas de seguridad existentes en el mercado y fomentadas por los grandes fabricantes de telecomunicaciones.

Para la elaboración de las soluciones empleamos como base aquellos equipos de comunicaciones que dispone y distribuye a sus clientes la empresa Inycom y las recomendaciones ofrecidas por el Centro Criptológico Nacional (CCN). En estas guías se difunden instrucciones para garantizar la seguridad de los sistemas de la información y las comunicaciones tanto en organizaciones de ámbito público y privado.

Para ello se ha hecho un estudio previo de las especificaciones de los equipos de comunicación, teniendo en cuenta el fabricante de cada dispositivo, las configuraciones óptimas de seguridad que deben tener a la hora de su puesta en marcha, los permisos y restricciones asignados a los usuarios que se conecten a la red en función de su rol dentro de la empresa, así como las interconexiones entre los demás dispositivos.

De este modo, se busca obtener una red de altas prestaciones cuyo acceso a través de diferentes infraestructuras cableada, inalámbrica y VPN se encuentra totalmente gestionado por la herramienta Network Access Control (NAC) ClearPass, la cual proporciona un seguimiento continuo de los usuarios y dispositivos conectados a la red.

El proceso de implementación de estas soluciones de seguridad lo ejecutamos sobre un laboratorio instalado en las oficinas de la empresa Inycom con los elementos de red proporcionados por la misma. Aquí simulamos la infraestructura de red que podría tener cualquier empresa, con diferentes arquitecturas de acceso a la red. En dichas pruebas de acceso utilizamos distintos dispositivos de usuario para acceder a la red, ordenadores, dispositivos móviles etc… verificando así que cada usuario entre con el rol correspondiente ya sea el administrador de la red, un empleado o un invitado cuyo acceso a los servicios de la empresa será limitado.

Finalmente con este proyecto queremos mostrar el proceso seguido para la implantación de una solución de seguridad basada en las recomendaciones del CCN en un entorno empresarial, así como un estudio de los componentes implicados en estas tecnologías.

Índice de contenidos

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ACRÓNIMOS

A
AAA: Authentication, Authorization and Accounting.
ACL: Access Control List.
AD: Active Directory.
AP: Access Point.
ARP: Address Resolution Protocol.

B
BBDD: Bases de datos.
BPDU: Bridge Protocol Data Unit.

C
CCN: Centro Criptológico Nacional.
CFI: Canonical Format Indicator.
CNI: Centro Nacional de Inteligencia.
COA: Change of authorization.
CSI: Crime Scene Investigation.

D
DHCP: Dynamic Host Configuration Protocol.

F
FBI: Federal Bureau of Investigation.
FCS: Frame Check Sequence.

H
HPE: Hewlett Packard Enterprise.
HTTP: Hypertext Transfer Protocol.
HTTPS: Hypertext Transfer Protocol Secure.

I
IEEE: Institute of Electrical and Electronics Engineers.
IP: Internet Protocol.
IPSEC: Internet Protocol Security.
ISE: Identity services engine.

L
LAN: Local Area Network.

M
MAC: Media Access Control.

N

NAC: Network Access Control.
NTP: Network time protocol.

O

OSI: Open System Interconnection.

P

POE: Power Over Ethernet.
PSA: Pulse Secure Access.

R

RFC: Request For Comments.
ROA: Real observatorio de la armada.
RSA: Rivest – Shamir – Adleman.
RSTP Rapid spanning tree protocol.

S

SA: Sociedad Anónima.
SFD: Start Frame Delimiter.
SFP: Small Form Factor Pluggable.
SNMP: Simple Network Management Protocol.
SSH: Secure Shell.
SSID: Service Set Identifier.
SSL: Secure Sockets Layer.
STIC: Seguridad de las Tecnologías de Información y Comunicaciones.
STP: Spanning tree protocol.

T

TCN Notificación de Cambio de Topología.
TIC: Tecnologías de la Información y la Comunicación.

U

UDP: User Datagram Protocol.
UPOE: Universal Power Over Ethernet.
URL: Uniform Resource Locator.

V

VID: VLAN Identifier.
VLAN: Virtual LAN.
VPN: Virtual Private Network.
VTY: Virtual Tele Type.

W

WIFI: Wireless Fidelity.
WLAN: Wireless Local Area Network.

1. INTRODUCCIÓN.

Conforme pasa el tiempo el número de empresas afectadas por los ciberataques va en aumento. Además, las nuevas tecnologías permiten que los usuarios puedan conectarse al trabajo desde cualquier lugar y que las organizaciones tengan oficinas distribuidas en distintas zonas geográficas. Todo ello acrecentado por la COVID-19 ha hecho que las necesidades del teletrabajo se implementen repentinamente y como consecuencia, los delincuentes aprovechen esto para robar información. [1]

Estos motivos hacen que las empresas vayan lentamente siendo más conscientes de las medidas que deben tomar para proteger sus activos. Esto obliga a desplegar soluciones de acceso a la red, configurarlas para que en todo momento sepan los dispositivos conectados y la formación de los empleados, para evitar riesgos por comportamientos no seguros. [2]

Permitir acceso a los recursos empresariales conlleva riesgos de seguridad, que deben ser prevenidos y mitigados por las soluciones que se implementen.

Existen varias preguntas que las empresas deben hacerse antes de plantear soluciones a los problemas de seguridad de la información. [3]

- ¿Qué controles se necesitan para determinar que una empresa se encuentre segura?
- ¿Los sistemas ya implementados tienen garantía a la hora de proteger la información de la empresa?
- ¿Qué personas de la organización tienen acceso a los datos que deben ser protegidos?

Los entornos locales, formados por conmutadores *Local Area Network* (LAN) y ethernet son fáciles de instalar y configurar, por ello es fácil olvidarse de las medidas de seguridad cuando las cosas parecen simples.

Existen múltiples vulnerabilidades en los conmutadores ethernet que debemos tener en cuenta. De lo contrario, si no está implementado de una manera óptima, un pirata informático puede acceder a los datos de la organización, rompiendo la confidencialidad o la integridad de este tráfico.

Además en los últimos años, numerosos estudios demuestran que los empleados no son entidades de confianza. La encuesta de seguridad y delitos informáticos del CSI/FBI 2006 informó que el 68% de las pérdidas de las organizaciones encuestadas fueron causadas por la mala actuación de los empleados internos como muestra en la Figura 1. [4], [5].

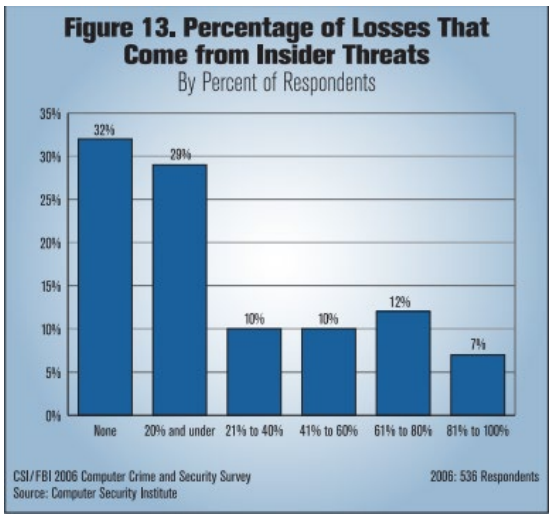


Figura 1: Percentage of Losses That Come from Insider Threats [5]

Reafirmando lo dicho anteriormente, los activos de una empresa forman su columna vertebral y las filtraciones de información pueden ser extremadamente perjudiciales. En algunos casos, la empresa puede perder clientes leales o incluso caer en la bancarrota.

Así, los controles de seguridad son las contramedidas impuestas por las empresas para:

- Proteger la confidencialidad, integridad y disponibilidad de la información que es procesada, almacenada y transmitida por esas organizaciones.
- Satisfacer un conjunto de requisitos de seguridad.

1.1 Antecedentes

El planteamiento de las soluciones de seguridad que se van a tratar vienen dadas por el CCN [6] . Esta organización ligada al Centro Nacional de Inteligencia (CNI) [7], colabora con todos los organismos públicos y diversas empresas en la detección, evaluación, respuesta y aprendizaje de incidentes de seguridad que pueden sufrir sus sistemas. Por ello la función del CCN es ofrecer apoyo a todas estas empresas y organizaciones, desarrollando procedimientos y estrategias para evitar o hacer frente a las amenazas y así contribuir a la mejora de la ciberseguridad.

Estas guías aportadas por el CCN denominadas Las Series CCN-STIC son desarrolladas con el fin de asegurar los sistemas y equipos de comunicación del sector TIC. [8], [9]

De todos los equipos y sistemas TIC de la actualidad, nos vamos a centrar en aquellos que emplean y son distribuidos por la empresa Inycom [10]. Esta ofrece servicios y soluciones para implementar y dar soporte a cualquier elemento o equipo de la infraestructura TIC. Además vamos a enfocarnos en la principal herramienta que ofrece Inycom a sus clientes para dar control de acceso y monitorizar los dispositivos conectados a la red.

La alternativa tecnológica NAC (*Network Access Control*) que se va a tratar es el ClearPass [11]. Proporciona control de acceso a la red en base a roles y dispositivos para todo tipo de empleados o visitantes, a través de cualquier infraestructura tanto local (cableada o inalámbrica), como remota.

Las redes de comunicación y los sistemas de información son un factor decisivo en la economía de cualquier institución. Debido a esto, garantizar la seguridad es una tarea de vital importancia.

Paralelamente al aumento del uso de la tecnología, también se ha incrementado el número de incidentes de seguridad. [12]

Además se nombrará a una de las personas más influyentes en este sector que ha sido Radia Perlman [13] y [14], figura de la informática moderna y creadora de uno de los protocolos de comunicación más utilizados del mundo, el *Spanning Tree Protocol* (STP) [15]. Gracias en parte a ella, las redes de las empresas son estables, seguras y funcionan correctamente, ya que permite la redundancia de caminos en las LAN.

Comprender, diseñar y construir una red informática sería una tarea demasiado difícil a menos que el problema se divida en varias subtareas más pequeñas. De aquí surge el modelo de referencia OSI (*Open System Interconnection*) [16], un modelo de referencia para los protocolo de red creado en 1980 por la Organización Internacional de Normalización. El objetivo de este estándar es interconectar diferentes sistemas para que estos puedan entenderse sin ningún problema debido a los protocolos con los que estos operen según su fabricante.

La Capa 2 denominada capa de enlace de datos: Se encarga del direccionamiento físico, del acceso al medio y existe como una capa de conexión entre los procesos de software de las capas por encima de ella y la capa física situada por debajo. Es decir, prepara los paquetes de capa de red para la transmisión a través de algún medio, ya sea cobre, fibra o entornos inalámbricos.

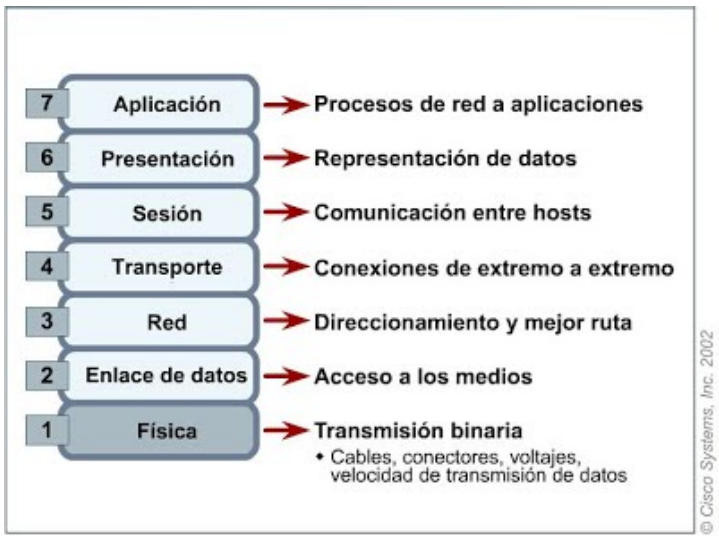


Figura 2: Modelo OSI [15]

Dada estas funciones el dispositivo que usa la capa de enlace es el switch. Encargado de la interconexión de equipos dentro de una red, junto al cableado, constituyen las redes LAN. Además se encargan de extenderla aportando altas velocidades de procesamiento y puertos donde conectar equipos finales o intermedios. [18]

Estas herramientas citadas anteriormente se desarrollarán a lo largo del trabajo, explicando al lector los conceptos básicos de su funcionamiento y su implementación.

En cuanto a la procedencia de este trabajo viene dada por las necesidades que tienen las empresas y que Inycom ha resuelto con sus proyectos. A continuación se detallará algún proyecto previo.

La implementación de soluciones LAN y *Wireless Local Area Network* (WLAN) en la Universidad de Mondragón [19], donde su red inalámbrica da cobertura a todo el campus universitario formado por varios edificios.

Otra empresa donde se han configurado equipos tratados en este proyecto es la empresa AMPO [20], una cooperativa que se dedica a la producción de válvulas, realizando todos los pasos de dicho proceso.

Por último otra organización donde han tratado dichos temas ha sido en el Parlamento de la rioja [21].

1.2 Motivación

La oportunidad de la realización de este Trabajo Fin de Grado viene dada por las prácticas extracurriculares que hice el verano de 2019 en la empresa Inycom (Instrumentación y Componentes SA).

Inycom es una compañía tecnológica, que lleva desde 1982 comercializando, asesorando y desarrollando soluciones avanzadas y servicios para sus clientes en diversos sectores TIC. Está formada por más de 750 profesionales, entre los cuáles se fomenta constantemente la formación. Además posee una extensa red internacional de *partners* estratégicos que les permiten desarrollar proyectos en distintas zonas geográficas.

Figura 3: Logo Inycom [10]

Actualmente la implantación de una solución de control de acceso es necesaria cuando se maneja información sensible (datos de personas, clientes, presupuestos etc…) de esa forma se garantiza que solo acceden a los recursos de la empresa los usuarios autorizados y que además solo acceden a los recursos asignados. Este control de acceso basado en la identidad, es el primer paso para poder desplegar una solución NAC más completa donde no solo se valida al usuario si no el estado del equipo (sistema operativo, parches, antivirus, protecciones instaladas en el mismo etc…) y en caso de que no se cumpla con los requerimientos asignados se apliquen de forma automática o manual las correcciones necesarias.

Nadie sabe en qué lugar va a quedar el "teletrabajo" después de la pandemia, pero a buen seguro que ha llegado para no irse y por lo tanto los potenciales riesgos aumentan, pues ya no solo habrá "trabajadores nómadas" (técnicos, comerciales que se desplacen a clientes), sino que además habrá "teletrabajadores" que estarán en sus casas y que en un momento dado acudirán a la oficina, por lo cual será si cabe más necesario controlar el estado de los equipos que acceden a la red corporativa, pues esos equipos pueden haber estado expuestos a riesgos que nadie conoce.

El aprendizaje durante este proyecto siempre ha seguido un marco práctico, donde gracias a los recursos que me han ofrecido, después de realizar el estudio teórico requerido, podía afianzar esos conocimientos mediante el desarrollo de una serie de tareas de índole práctico. Esto queda reflejado en la estructura del proyecto dónde primero se realiza una explicación teórica de los dispositivos y protocolos utilizados. Para más tarde en el laboratorio comprobar su funcionamiento y realizar pruebas de control de acceso.

Otros factores decisivos en la realización de este trabajo ha sido el poder trabajar con las herramientas de los grandes fabricantes del sector: Aruba, Cisco y Hewlett Packard Enterprise (HPE). También supone una excelente oportunidad para seguir desarrollándome como persona y seguir aprendiendo los conceptos relacionados con mis estudios, además de profundizar en las tecnologías empleadas actualmente por las empresas y conocer el funcionamiento de un proyecto dentro del ámbito laboral.

1.3 Objetivos

El objetivo principal de este trabajo es estudiar, diseñar e implantar soluciones de seguridad en entornos heterogéneos para distintos equipos y dispositivos de una red corporativa. Para ello se seguirán las recomendaciones aportadas por el CCN y se analizarán los diversos procedimientos que se requieren para trabajar en entornos seguros. Para ello se plantean los siguientes objetivos específicos:

- Analizar los dispositivos necesarios para el diseño y la implantación de soluciones de seguridad.
- Estudiar los aspectos conceptuales de los dispositivos empleados.
- Desarrollo de las soluciones siguiendo las recomendaciones de la CCN.
- Montaje del laboratorio en las oficinas de Inycom, para realizar las configuraciones y pruebas en un entorno aislado y seguro.
- Analizar las configuraciones y elementos más apropiados para cada empresa/situación/necesidad.
- Aumentar las capacidades de colaboración interpersonales dentro de un proyecto multidisciplinar.

1.4 Estructura de la memoria

La memoria de este proyecto se encuentra dividida en varios apartados, que sirven para entender los conceptos que se tratan a lo largo del Trabajo de Fin de Grado. Esta estructura sigue un hilo conductor donde primero se explican los conceptos y herramientas que se emplean, para posteriormente implementarlas.

En primer lugar, la introducción donde al estar realizada en una empresa se describen los antecedentes y la motivación para realizar dicho proyecto, además de los objetivos propuestos.

En segundo lugar titulado análisis y diseño, se va a tratar el marco tecnológico dando a conocer las tecnologías y herramientas empleadas, además de los conceptos de seguridad involucrados en ellos que posteriormente implementaremos en un entorno real.

En el tercer y cuarto capítulo, se explica brevemente la herramienta NAC empleada para controlar el acceso a las redes y el laboratorio instalado donde realizaremos las configuraciones y las implementaciones explicadas a lo largo del trabajo.

El quinto, sexto y séptimo capítulo, contiene las implementaciones de los conceptos tratados en el apartado dos, configuraciones adicionales y el desarrollo de la solución remota respectivamente.

El octavo capítulo, aborda la configuración de la solución NAC con la integración de los dispositivos de acceso a la red.

El noveno capítulo, muestra las pruebas de acceso realizadas y los resultados obtenidos por las implementaciones anteriores.

Finalmente las conclusiones y líneas de trabajo futuras están contenidas en el capítulo diez.

2. ANÁLISIS Y DISEÑO.

En este capítulo se analizan los equipos que forman una *Local Area Network* – Red de Área Local (LAN) y los sistemas de control de acceso que son tratados a lo largo del proyecto. También se presentan los conceptos básicos que hay que tener en cuenta en una infraestructura de red a la hora de implementar las soluciones y servicios de seguridad recomendadas por el CCN.

2.1 Infraestructura de un entorno de red local

Una LAN es una red que interconecta dispositivos cuyo alcance se limita a un espacio físico reducido, como una casa, oficinas, un edificio o un campus universitario.

Este tipo de redes son las usadas normalmente en las empresas, ya que pueden compartir recursos e información entre varios ordenadores y equipos informáticos, tales como impresoras, teléfonos IP (*Internet Protocol*), switches, *routers*, *access point* (AP) y servidores.

El medio de transmisión de una red LAN puede ser mediante cable o radiofrecuencia como se puede observar en la figura 4 (un ejemplo de infraestructura formada por dispositivos que se conectan a la red de diferente manera). Las redes cableadas son aquellas que se comunican a través de cables de datos, generalmente basadas en ethernet. Un estándar que controla los procesos de transmisión de datos a través de la LAN.

Por otro lado en la figura 4 también observamos las WLAN que son un conjunto de dispositivos comunicados a través de *Wireless Fidelity* (WiFi), un estándar de comunicación inalámbrico basado en la norma IEEE (*Institute of Electrical and Electronics Engineers*) 802.11. El AP es el centro de las comunicaciones de la mayoría de las WLAN, este puede actuar como medio de intercomunicación de todos los terminales inalámbricos y como puente de interconexión con la red fija e internet. [22]

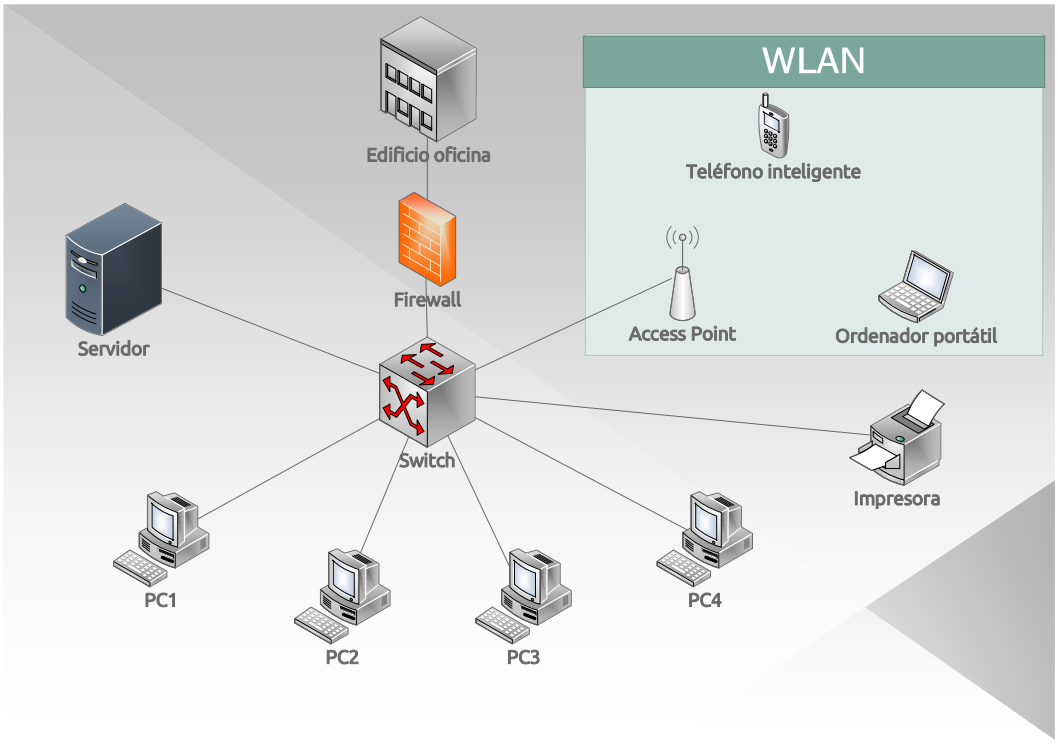


Figura 4: Infraestructura red LAN y WLAN

2.2 Elementos de red de acceso

En este apartado se va a hacer hincapié en los dispositivos que conforman la red de acceso. Son aquellos que establecen la comunicación directa con los dispositivos finales y les permiten dar conectividad de internet.

Entre sus funciones está el control de acceso, gestión de políticas, segmentación de dominios de colisión broadcast y la interconexión de dispositivos. A continuación veremos los elementos que proporcionan estas funciones.

2.2.1 Switch

En toda organización de tamaño considerable es esencial este dispositivo de nivel 2, el switch. Este es un conmutador de interconexión de red, que se encarga de enviar tramas de un equipo de red a otro. Para ello los switches procesan la información recibida pasando datos de un segmento a otro de la red, de acuerdo con la dirección MAC (*Media Access Control*) destino ubicada en la cabecera de la trama. En la figura 5 se muestra el formato comúnmente usado en la trama ethernet.

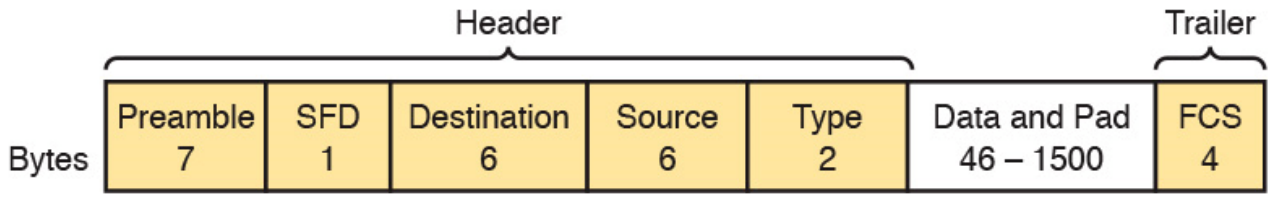


Figura 5: Formato trama Ethernet [23]

En la tabla 1, se adjunta una definición de cada campo de la trama Ethernet. Esta es la base de comunicación entre elementos dentro de una red LAN.

Tabla 1: IEEE 802.3 Campos y cabecera Ethernet

Field	***Bytes***	***Description***
Preamble	7	Sincronización
Start Frame Delimiter (SFD)	1	Significa que en el siguiente byte comienza el campo de dirección MAC de destino.
Destination MAC Address	6	Identifica el destinatario de esta trama.
Source MAC Address	6	Identifica el emisor de esta trama.
EtherType/length	2	Si el valor es ≥ 1536 → Identifica protocolo (0x0800) IPv4, (0x86DD) IPv6, (0x0806) ARP, etc. Si el valor es ≤ 1500 → Identifica la longitud del campo de datos.
*Data and Pad**	46-1500	Contiene datos de una capa superior, normalmente una L3PDU (paquete IPv4 o IPv6). El remitente agrega relleno para cumplir con el requisito de longitud mínima para este campo (46 bytes)
Frame Check Sequence (FCS)	4	Proporciona un método para determinar si la trama experimentó errores de transmisión.

Una característica básica de los switches son los puertos RJ45 que permiten la conexión de otros dispositivos. Los puertos RJ45 son aquellos donde se conectan los usuarios u otros switches. También pueden tener puertos especiales denominados puertos SFP, este puerto permite una conexión de fibra óptica, obteniendo una alta velocidad. Esto es muy útil para conectar servidores con gran demanda de tráfico ya que agiliza la transferencia de datos.

Figura 6: Puertos RJ45 y puertos SFP [24]

Power Over Ethernet

Otra característica que pueden tener los switches es el *Power Over Ethernet* (POE), es una tecnología que permite el envío de alimentación eléctrica junto con los datos en el cableado de una red ethernet, simplificando por tanto la infraestructura de cableado para su funcionamiento. Existen diferentes versiones Poe, Poe+ y UPOE (*Universal Power Over Ethernet*) cuyas diferencias se observan en la tabla 2.

Tabla 2: Tipos de POE

Propiedades	**PoE**	**PoE+**	**UPoE/PoE++**
Estándar	IEEE 802.3 af	IEEE 802.3 at	IEEE 802.3bt
Máxima Potencia del PSE	15.40 W	30 W	60 W
Tipo de cable utilizado	Categoría 3	Categoría 3	Categoría 5
Pares ethernet	2	2 o 4	4

2.2.2 AP

El *Access Point* es el dispositivo que crea una WLAN, normalmente en una oficina o un edificio de grandes dimensiones. Estos equipos proyectan una señal WiFi en un área designada y difunden un SSID (*Service Set Identifier*), que es el nombre que identifica la red al que se conectan los elementos inalámbricos.

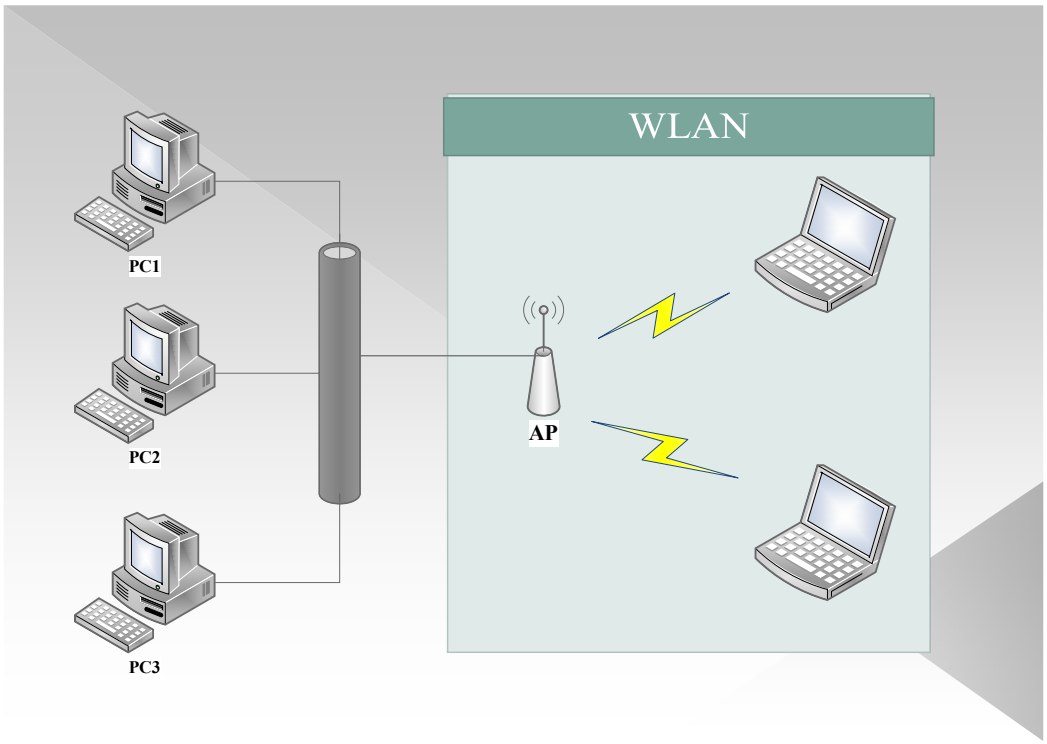


Figura 7: Diagrama modo infraestructura

Las redes más usuales que veremos con APs, son en modo infraestructura, es decir, los APs hacen de intermediarios o puentes entre los elementos WiFi y una red ethernet cableada. También se encargan de escalar a más usuarios según se necesite y podrá dotar de algunos elementos de seguridad.

Otras funciones que incluyen los APs son el Portal Cautivo, una página web que fuerza a los usuarios a registrarse para poder acceder a la red y las *Access Control List* (ACL) que son medidas de seguridad que limitan el acceso a los usuarios gestionando sus perfiles dentro de la red WiFi.

2.2.3 VPN

La VPN (*Virtual Private Network*) es una tecnología de red cada vez más conocida, ya que es la principal solución de acceso remoto para que los empleados puedan trabajar desde cualquier lugar. Los principales protocolos de seguridad empleados para garantizar la seguridad de las comunicaciones son IPsec [25] y SSL [26]. La VPN establece una conexión virtual segura, más conocida como "túnel", construida a través de una red física insegura (internet). [27]

Un túnel IPsec puede proporcionar las siguientes funciones de seguridad:

- Privacidad (mediante cifrado).
- Integridad del contenido (mediante autenticación de datos).
- Autenticación de remitente y -, si usa certificados, - no repudiación (mediante la autenticación de origen de datos).

Hay dos tipos de VPN:

- VPN *site-to-site*: Se emplea para conectar redes de oficinas secundarias con una sede central, mediante una conexión segura.
- VPN de acceso remoto tipo túnel: Se utiliza para que los clientes VPN se conecten de forma segura al servidor VPN situado en el interior de la empresa.

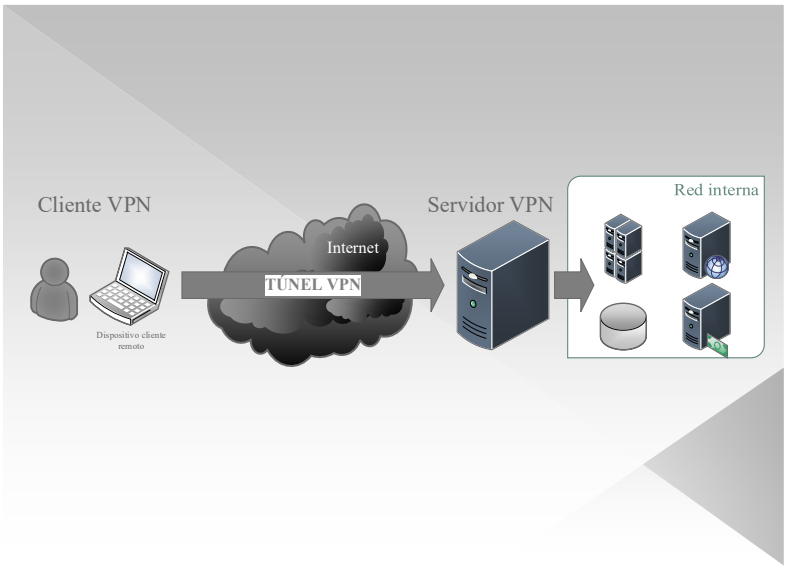


Figura 8: VPN de acceso remoto tipo túnel

Los beneficios que nos aporta una VPN son los siguientes:

- Seguridad: Las VPN incluyen protocolos de cifrado y autenticación avanzados que protegen los datos contra el acceso no autorizado.
- Escalabilidad: Las empresas pueden agregar nuevos usuarios sin necesidad de aumentar considerablemente la infraestructura.
- Ahorro de costos: Las VPN permiten que las organizaciones utilicen un transporte externo de internet de menor coste para conectar oficinas remotas y usuarios remotos al sitio principal, eliminando enlaces dedicados.

2.3 Conceptos de seguridad

La seguridad juega un papel predominante en las comunicaciones entre distintos dispositivos, debido a la cantidad de equipos interconectados y a la constante innovación. En este aspecto es esencial establecer cuál es la importancia que representan los datos, como se están enviando y que vulnerabilidades pueden surgir a la hora de enviarlos por la red de nuestra oficina. Pero antes de responder las cuestiones anteriores, se va a definir que es la seguridad en redes. Esta es mantener bajo protección los servicios y datos que componen la red, a través de herramientas y políticas de seguridad que nos permitan controlar la información que viaja a través de la red. [28]

Los elementos básicos que se demandan en una red para que la seguridad sea correcta se detalla a continuación: [4]

- Autenticación: Es el proceso de verificar a los usuarios antes de dejarlos entrar en el sistema, es decir, que ese usuario es quien dice ser.
- Confidencialidad: Protege los datos para que accedan solo aquellas personas que se encuentran autorizadas.
- Integridad: Garantiza que la información enviada no es modificada por personas no autorizadas.

Estos son los conceptos básicos para satisfacer el concepto de seguridad en redes, más adelante se focaliza en las herramientas que proporcionan estos mecanismos a la red.

2.3.1 Consejos previos a la configuración

El siguiente apartado pretende explicar los contenidos que se van a configurar en el Switch para proteger los entornos de sistemas de información y comunicaciones. Estos conceptos servirán para introducir protocolos, servicios de red ofrecidos por estos dispositivos, las herramientas que recomienda el CCN para el correcto funcionamiento de los Switches y que no existan brechas de seguridad.

2.3.2 Servicios de red para la gestión del switch

HTTP/HTTPS

Este servicio web con SSL nos permite acceder a él desde cualquier navegador, usando como *Uniform Resource Locator* (URL) la dirección IP o el nombre del equipo y en caso de definir un puerto diferente al por defecto, indicando dicho puerto.

Se basa en el protocolo *Hipertext Transfer Protocol* (HTTP) el cual nos permite realizar una petición de datos y recursos. Es la base de cualquier intercambio de datos en la web, y un protocolo de estructura cliente-servidor.

TELNET

Este es otro servicio que nos permite configurar el switch de forma remota. Es un protocolo de red que es utilizado desde 1969 con el que puedes acceder a otra máquina para manejarla remotamente como si estuvieras sentado frente a ella. Para poder establecer la conexión entre dos equipos, necesitaremos tener un cliente en nuestro terminal y un servidor en la máquina a la que nos queramos conectar.

SSH

SSH (*Secure Shell*) es el nombre de un protocolo y del programa que lo implementa. Su principal función es la conexión remota a un servidor por medio de un canal en el que toda la información intercambiada está cifrada.

Este protocolo es el usado principalmente para conectarse a servidores, la ventaja significativa que aporta este protocolo frente a otros es el uso del cifrado para asegurar la transferencia segura de información entre el host y el cliente.

SNMP

SNMP (*Simple Network Management Protocol*) es un protocolo que facilita el intercambio de datos entre dispositivos de red. Permite a los administradores de las redes supervisar el funcionamiento de la red de forma remota. En la actualidad todos los elementos de red de nivel profesional vienen con un agente SNMP. Estos agentes son los que permiten que los administradores de red se comuniquen con el dispositivo.

2.3.3 Seguridad basada en puertos

En este apartado veremos los conceptos que aplicaremos en los puertos, las ACLs. Esta solución nos permite seleccionar el tráfico al que queremos aplicarle algún tipo de restricción o atributo. Esto permite por ejemplo distribuir rutas por los puertos que el administrador elija. Las ACLs se evalúan de manera secuencial, es decir el equipo irá comparando cada paquete con cada una de las reglas de la ACL. En el momento en que un paquete coincida con una regla, ésta se ejecuta y no se sigue comparando. Por defecto se deniega todo el tráfico, por ello se recomienda siempre crear al final de la lista una declaración tipo *deny* para recordarlo. [29]

Existen dos tipos:

- ACL estándar: Filtran el acceso de los paquetes según la dirección IP de origen de un paquete.
- ACL extendida: Estas son más complejas ya que pueden filtrar los paquetes no sólo según la dirección IP de origen, sino también según la dirección IP de destino, el protocolo y puertos de origen y destino. Estas se utilizan más debido a que permiten un control más preciso.

Las ACLs una vez creadas hay que aplicarlas a un interfaz y especificar en qué sentido aplicarla, ya que las reglas solo se aplican a una parte de los paquetes, a los entrantes o a los salientes. Generalmente todos los interfaces soportan la aplicación de ACLs entrantes y salientes de forma simultánea.

2.3.4 VLANs

Virtual LAN (VLAN) es un método para crear redes lógicas independientes entre sí dentro de una red física. Cada VLAN creada corresponde a un dominio de difusión. Por lo tanto todos los miembros de un dominio reciben los paquetes broadcast de otros miembros de su VLAN pero no de los miembros de otras VLANs.

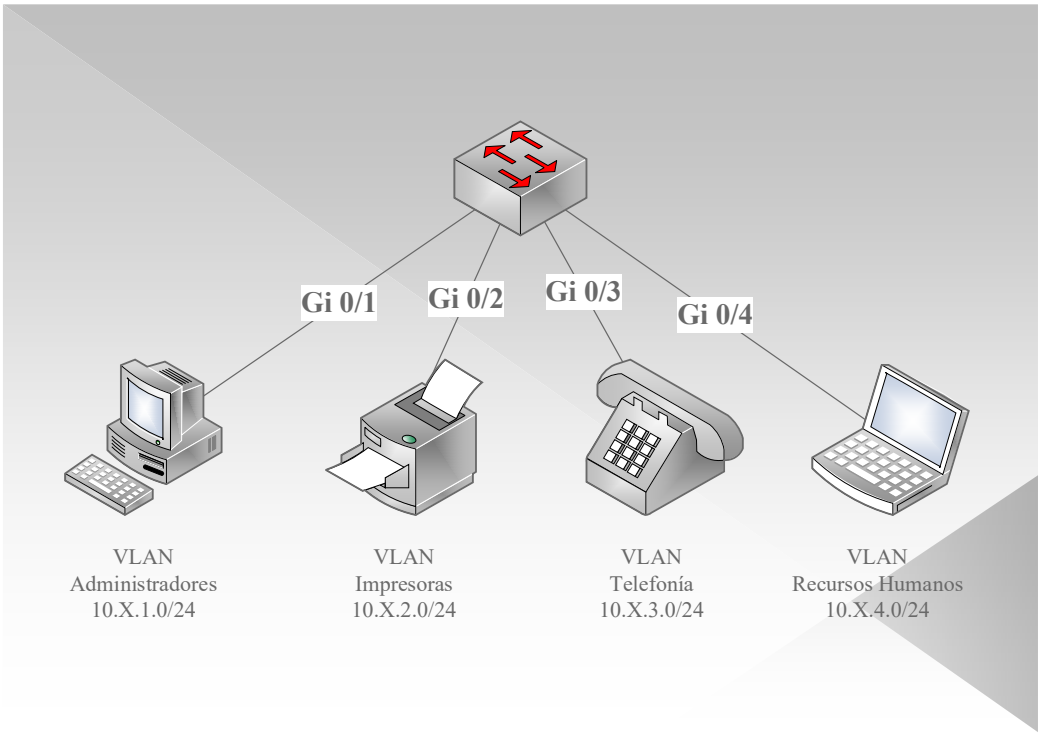


Figura 9: Ejemplo de configuración Switch VLAN

El principal beneficio de usar VLANs es que las agrupaciones de dispositivos y la creación de las subredes se implementan de forma lógica, y por lo tanto pertenecer a una VLAN no depende de la ubicación física de cada equipo. Esto reduce el dominio de difusión y ayuda en la administración de la red, separando los departamentos de la empresa y los segmentos de red que no deberían intercambiar datos. Como se observa en la figura 9 hay configuradas en el conmutador cuatro VLANs diferentes, cada una formando una subred lógica diferente, por ejemplo la VLAN “Telefonía”, estos dispositivos enviarían tráfico por esa VLAN, sin perjudicar el tráfico de las demás. Además a nivel de seguridad nos permite crear LANs que solo contengan ciertos equipos, como por ejemplo los equipos de administración, sin que estos tengan que estar físicamente juntos.

Formato de trama 802.1Q

Este protocolo IEEE 802.1Q es una mejora del estándar de Ethernet, en el que permite identificar a una trama proveniente de un equipo que se encuentra en una VLAN. Esto se identifica añadiendo 4 bytes a la trama ethernet. Como se observa en la Figura 10, el valor del campo *EtherType* se cambia a 0x8100 y se añade un nuevo campo denominado *Tag*.

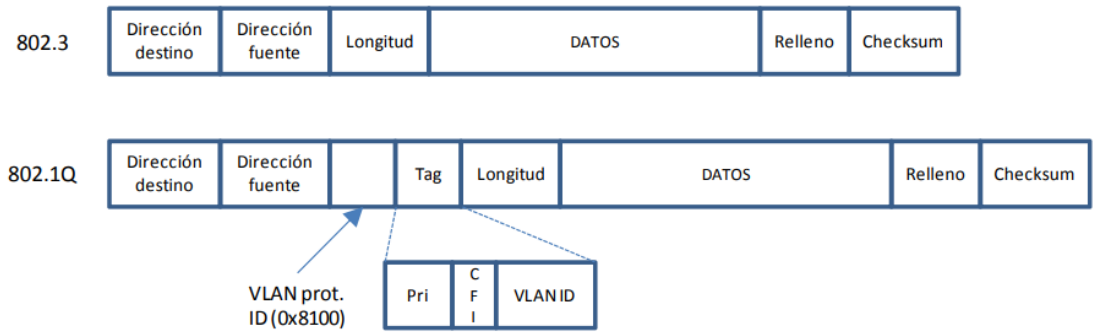


Figura 10: Formato de trama 802.1Q [30]

Este nuevo campo *Tag*, está formado por los siguientes apartados:

- ***User Priority Field***: Pueden ser usados para dar un nivel de prioridad a la trama.
- ***Canonical Format Indicator* (CFI)**: Identificador que indica si existen tramas *Token Ring*.
- ***VLAN Identifier* (VID)**: identifica a una única VLAN.

Tipos de puerto en los Switches respecto a las VLANs.

Los puertos de un Switch se pueden diferenciar respecto las características VLAN. Existen los puertos de acceso y los puertos *Trunk*.

- **Puertos de acceso:** Estos puertos solo pueden transportar tráfico que pertenezcan a la VLAN asignada a ese puerto.
- **Puertos *Trunk*:** Estos puertos transportan tráfico de varias VLANs, por ello las tramas deben ir etiquetadas con el formato de trama 802.1Q visto anteriormente.

2.3.5 STP

Spanning Tree Protocol (STP) es un algoritmo diseñado por Radia Perlman, cuya función es la de gestionar los bucles que pueden formarse en una red debido a la existencia de enlaces redundantes.

Este protocolo se gestiona a través del intercambio de mensajes BPDUs (*Bridge Protocol Data Unit*), para la elección del "*root bridge*" y para la detección de bucles.

De forma predeterminada, una BPDU se envía cada 2 segundos y generalmente se clasifican en dos tipos:

- **Configuración BPDU**: Se utiliza para calcular el STP.
- **TCN (Notificación de Cambio de Topología) BPDU**: Se utilizan para informar de cambios en la topología de red.

Cada switch envía BPDUs por cada puerto. La dirección de origen es la dirección MAC de ese puerto y la dirección de destino es la dirección de multidifusión (*multicast*).

Estos paquetes BPDU contienen información sobre puertos, direcciones, aseguran que los datos terminen donde estaban destinados y detectan bucles en la topología de red. [31]

Elección del *Root Bridge*

Los bucles se forman cuando existen rutas alternativas para llegar a un mismo destino. Estas rutas alternativas son fundamentales en redes profesionales, en caso de que un enlace falle.

Por ello, para evitar estos bucles, STP utiliza un punto de referencia: El *root bridge*. Este es el centro lógico de la topología del árbol que se crea y se elige atendiendo al *Bridge ID* del switch donde el valor más bajo es el preferido.

Sin este protocolo, una LAN con enlaces redundantes puede provocar que haya tramas ethernet que se repitan durante un tiempo ilimitado. Con STP habilitado, los conmutadores pueden bloquear determinados puertos para evitar el reenvío indefinido de tramas a través de estos.

STP previene tres problemas muy comunes en las LANs que pueden causar la caída de nuestras redes.

- Tormentas de Broadcast (*Broadcast Storms*): La acumulación de tráfico en una red, en la que se reenvían las mismas tramas por los mismos enlaces repetidamente. Consumiendo así la capacidad de los enlaces.
- MAC *table instability*: La actualización constante de la tabla de direcciones MAC de un switch con entradas incorrectas, lo que provoca que las tramas se envíen a ubicaciones incorrectas.
- *Multiple frame transmission*: Un efecto secundario del bucle de tramas, en el que se envían varias copias de una trama al *host* previsto, lo que confunde al *host*.

Por lo tanto STP previene de los bucles colocando cada puerto del switch en un estado de *forwarding* o *blocking*. Las interfaces que estén en el estado de *forwarding*, actúan enviando y recibiendo tramas. Por otro lado las interfaces en estado de *blocking*, no reenvían las tramas de usuario, no aprenden las direcciones MAC de las tramas de recepción y no procesan las tramas de usuario recibidas, pero sí procesan las tramas BPDUs. [32]

Como se muestra en la tabla 3, obtenemos una clasificación del estado en el que tienen que estar los puertos de un switch en función de la arquitectura en la red LAN.

Tabla 3: Estado STP de los puertos de un switch. [32]

Caracterización del Puerto	**Estado STP**	**Descripción**
Todos los puertos del switch raíz.	*Forwarding*	El switch raíz es siempre el conmutador designado en todos los segmentos conectados.
Cada puerto raíz, de los switches no definidos como *root* (raíz).	*Forwarding*	El puerto a través del cual el switch tiene el costo más bajo para llegar al switch raíz.
El puerto designado de cada LAN	*Forwarding*	El Switch con el costo más bajo hacia el raíz es el seleccionado para que en ese segmento de red tenga un puerto con estado *forwarding*.
Todos los demás puertos.	*Blocking*	El puerto no se utiliza para reenvío de tramas.

A lo largo de los años ha mejorado el protocolo y ha aparecido el RSTP (*Rapid Spanning Tree Protocol*) que reemplaza al STP original mientras conserva la compatibilidad con versiones anteriores.

La ventaja de RSTP reside en la velocidad de recalcular la topología de red cuando ocurre un cambio en ella. Un cambio en la topología RSTP provoca una transición en los estados de los puertos y estos estados RSTP corresponden a las siguientes operaciones básicas: descartar, aprender y reenviar. La tabla describe las características de los estados de los puertos RSTP. [33]

Tabla 4: Características de los estados de los puertos RSTP

Estado Puerto	**Descripción**
Descartar	Este estado se observa en una topología estable y durante los cambios de topología. Este estado evita el reenvío de tramas.
Aprender	Este estado se observa en una topología estable y durante los cambios de topología. Este estado acepta tramas de datos para llenar la tabla MAC en un esfuerzo por limitar la inundación de tramas *unicast* desconocidas.
Reenviar	Este estado solo se observa en topologías activas. Después de un cambio en la topología o durante la sincronización, permite el aprendizaje de direcciones MAC y el reenvío de tramas de datos.

Tras explicar el funcionamiento del STP y la evolución al RSTP, vemos que son herramientas muy importantes a la hora de configurar los switches en una arquitectura de red. Hay que conocer el diseño de cada red, para decidir cuál es el switch raíz de cada arquitectura, y los switches que van a depender de él, bien conectados directamente, bien indirectamente a través de otros. Además de la configuración del estado de cada puerto en función del diseño elegido. Estas decisiones se pondrán en práctica más adelante y se implementarán las configuraciones necesarias para ello.

2.3.6 Registros: Logs

El registro de *logging* es una herramienta que tienen los dispositivos de red para proporcionar información acerca de lo qué está ocurriendo en cada momento en el mismo. Supongamos que por algún motivo un enlace deja de estar operativo, si no averiguas el porqué de esa caída inmediatamente y no se soluciona, es posible que el administrador de la red pierda la oportunidad de mantenerla funcionando correctamente. Del mismo modo, puede recibir un mensaje de un problema dentro de la red y deba comenzar a solucionarlo. Por ello hay que aprovechar el sistema de *logging* para recopilar información. RFC 3164 [26].

Un registro configurado para que recoja demasiada información puede llegar a ser complejo y confuso, escondiendo información útil debajo de datos que no nos interesan. A su vez un registro demasiado sencillo, puede ser ineficaz para evaluar el estado de la red. Otro factor importante de los registros *logging* es su identificador temporal, de manera que esté bien configurado para que el administrador sepa exactamente en qué momento y en qué orden han ocurrido los eventos.

Por lo tanto estos mensajes que obtenemos por pantalla, se pueden recopilar y analizar para determinar qué sucedió, cuándo sucedió y qué tan grave fue el evento. Estos son los campos de un mensaje de log, generado por un switch Cisco Catalyst, empleado durante el desarrollo del proyecto.

- ***Timestamp*:** Fecha y hora del reloj interno del switch.
- ***Facility Code*:** Un identificador del sistema que categoriza el módulo o función del switch que ha generado el mensaje.
- ***Severity*:** Un número del 0 al 7 que indica que tan importante o grave es el evento.
- ***Mnemonic*:** Una cadena de texto corta que categoriza el evento ocurrido dentro del *Facility Code.*
- ***Message Text*:** Una descripción del evento.

La figura 11 indica los diferentes niveles de gravedad de cada mensaje, correspondiente al campo *severity*. Este campo del mensaje log ayuda a los administradores de la red a filtrar selectivamente y recibir rápidamente las notificaciones más importantes

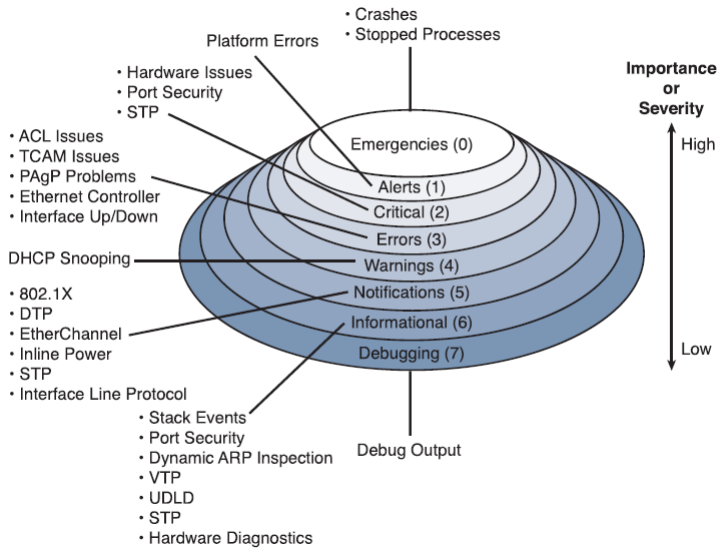


Figura 11: Niveles de gravedad, Logs [35]

2.3.7 Protocolo AAA

Existen diferentes mecanismos de autenticación y de creación de cuentas de forma centralizada. Esto nos permite que todos los equipos de red de acceso con los que se va a tratar en este proyecto, validen los datos de usuario y puedan modificarlos en un mismo equipo. A estos protocolos se les denomina triple AAA (*Authentication, Authorization and Accounting*).

- *Authentication*: Valida a los usuarios, ya sean remotos o locales antes de permitirles acceder a los recursos.
- *Authorizacion*: Regula el acceso a servicios del equipo dependiendo de los privilegios que tenga cada usuario. Esto lo veremos más adelante cuando creemos diferentes VLANs en nuestra red experimental y los usuarios que se conecten a dicha red, obtengan la VLAN que les corresponde dependiendo del grado de acceso.
- *Accounting*: Mide los recursos utilizados por un usuario durante el acceso.

El mecanismo de seguridad que nos va a permitir realizar esto se denomina RADIUS, un protocolo que administra las credenciales de acceso a un recurso de red.

RADIUS

Es un protocolo que define un sistema distribuido con topología cliente/servidor que protege del acceso de usuarios no autorizados. El cliente RADIUS se ejecuta en los equipos de red, los cuales envían peticiones de autenticación a un servidor central, que se encargará de verificar la autenticidad de la información y ser el encargado de determinar si el usuario accede o no a los servicios de red. Definido en el RFC 3576. [34]

Los pasos que suceden cuando un usuario quiere autenticarse son los siguientes:

- Se le pide al usuario que introduzca *login* y *password*.
- El *login* y *password* son enviados al servidor de RADIUS.
- El usuario recibe uno de los siguientes mensajes.
  - ***ACCEPT*:** El usuario ha sido autenticado con éxito y se permite su acceso a los servicios de red.
  - ***REJECT*:** El usuario no ha podido ser autenticado y, o bien se le solicita que introduzca sus datos de nuevo o se le niega el acceso.
  - ***CHALLENGE*:** Se le solicita más información al usuario.
  - ***CHALLENGE PASSWORD*:** Se le pide al usuario que introduzca un nuevo *password*. [29]

IEEE 802.1X

Es una norma del IEEE para el control de acceso a la red. Permite la autenticación de equipos y/o usuarios que desean acceder a la red a través de algún dispositivo de acceso (switches LAN, puntos de acceso WiFi, servidores VPN, etc…). Esta autenticación es realizada normalmente por un tercero, como por ejemplo un servidor RADIUS. Todos estos estándares y especificaciones son necesarios para que funcione un sistema de autenticación basado en puertos.

Ahora explicaremos los nombres propios que encontraremos al trabajar con estos estándares. Como se muestra en la figura 12 los componentes principales que forman un sistema de autenticación basado en puertos son el *supplicant*, *authenticator* y *authentication server*.

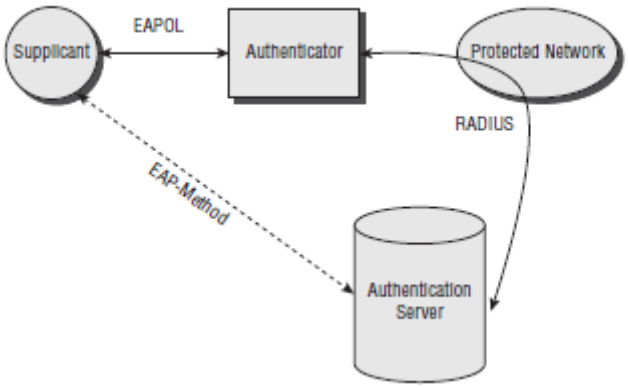


Figura 12: Componentes principales de un sistema de autenticación basado en puertos [36]

Supplicant

Es un dispositivo desconocido que debe autenticarse para poder tener acceso a la red. Su identidad está en duda hasta que sus credenciales son validadas por el servidor de autenticación.

Authenticator

Es un dispositivo de red que actúa como una puerta de seguridad entre el suplicante y la red de la empresa, permaneciendo cerrada hasta que el sistema verifica al suplicante y este es autorizado para acceder a la red. Además el autenticador se encarga de transmitir el flujo de tramas entre el suplicante y el servidor de autenticación.

Authentication Server

Dispositivo que realiza la autenticación, normalmente se emplea un servidor RADIUS.

3. CONTROL DE ACCESO

En este apartado vamos a tratar los diferentes métodos utilizados a lo largo del proyecto, para controlar el acceso a las redes. Tanto el protocolo que viene definido en los Switches mencionado en el apartado anterior, el RADIUS. Como otras tecnologías NAC (*Network Access Control*) que se encargan de autenticar a los usuarios, estableciendo políticas para cada usuario y dispositivo.

A lo largo del tiempo, los objetos de valor se han protegido estableciendo mecanismos de seguridad para controlar el acceso a los mismos: contraseñas, llaves etc…

En la época actual, la información contenida en los sistemas de información (servidores, bases de datos (BBDD), etc…) que dispone una organización, normalmente es accesible a través de redes de datos. Es por ello que se hace necesario controlar de forma rigurosa el acceso, tanto en las redes como a los recursos disponibles a través de estas.

Las áreas clave abordadas por el control de acceso son las siguientes. [37]

- Evitar el acceso no autorizado.
- Autenticar usuarios.
- Autorizar el acceso de todos los usuarios según el rol del usuario.
- Hacer cumplir las políticas de uso.
- Hacer cumplir los estándares de seguridad para diferentes dispositivos.
- Identificación y seguimiento del acceso de usuarios invitados.
- Monitoreo e informes sobre todos los accesos a la red.

Algunos de las amenazas más comunes que enfrentan las empresas en este ámbito son:

- **Detección de contraseñas:** La detección de contraseñas sin cifrar es una forma muy sencilla de obtener acceso a la red.
- **Craqueo de contraseñas:** Contraseña muy sencillas que no siguen reglas de complejidad, ya que palabras basadas en el diccionario son muy sencillas de que un atacante las adivine.
- **Hosts vulnerables:** Tener hosts vulnerables puede ocasionar que se utilicen para obtener acceso no autorizado a la red.
- **Ingeniería Social:** Una insuficiente formación y concienciación de los empleados respecto al manejo de las credenciales de usuario, puede conducir a ataques dirigidos a estos para engañarlos y que divulguen sus contraseñas.
- **Acceso de terceros:** El acceso de invitados es un riesgo sin dichas tecnologías NAC, ya que no se pueden diferenciar a los atacantes potenciales.

NAC (*Network Access Control*) es una solución que implementa políticas para controlar los dispositivos y el acceso de los usuarios a las redes.

Si bien en el mercado existen soluciones de distintos fabricantes (*Pulse Secure Access* –PSA- de *Pulse*, *Identity Services Engine* (ISE) de Cisco, etc…). La solución a utilizar en este trabajo/proyecto, es la desarrollada por el fabricante Aruba, denominada ClearPass.

Esta solución ha sido elegida por las posibilidades que existen a la hora de perfilar los dispositivos y políticas que se pueden aplicar sobre ellos. Además es una herramienta centralizada donde podemos controlar la gestión de todos los accesos a nuestra red y sigue la línea de trabajo de los proyectos realizados por Inycom.

ClearPass

Es una de las soluciones más reconocidas en este sector, diseñada por la empresa Aruba Networks, una compañía que pertenece a HP Enterprise.

Aparte de proporcionar control de acceso a la red en base a roles y a dispositivos. Está formada por varios módulos, que ofrecen otros tipos de servicio dentro del control de acceso, como acceso de invitados creando un portal cautivo o el aprovisionamiento de dispositivos. [38]

- ***Policy Manager*:** Es el módulo principal que realiza las labores de servidor AAA.
- ***OnGuard*:** Servicio de validación NAC y permite obtener información de los clientes conectados a la red.
- ***OnBoard*:** Este módulo proporciona servicio de gestión de dispositivos móviles.
- ***Guest*:** Este módulo permite aprovisionar a los invitados en una subred diferente.

Posteriormente a través de un laboratorio de pruebas creado en las oficinas de Inycom, se realizarán demostraciones del funcionamiento de esta herramienta NAC.

La diferencia de esta solución frente a otras es:

Ofrecer una amplia variedad de políticas y posibilidades aplicables al acceso de los dispositivos. Es decir puedes configurar el acceso según el rol que posea cada dispositivo, llegando hasta un nivel de análisis en el que por ejemplo puedas rechazar la conexión de aquellos equipos que no tienen el antivirus actualizado.

Soportar de forma centralizada equipos de diferentes fabricantes en distintas infraestructuras de red, ya sea inalámbrica, cableada o a través de una VPN como implementamos en el proyecto.

Integración de una amplia variedad de fuentes de autenticación/autorización dentro de los servicios.

Generación avanzada de reportes y alertas, dónde puedes obtener información de los datos de visitantes, dispositivos integrados etc…

La capacidad para administrar los dispositivos en función del rol asignado, permitiendo modificar privilegios de autorización fácilmente. [39]

4. DISEÑO LABORATORIO

Para poder trabajar con todos los conceptos desarrollados anteriormente hemos instalado un laboratorio en las oficinas de Inycom, con los dispositivos proporcionados por la empresa para poder configurarlos en base a las recomendaciones del CCN. Posteriormente hemos configurado el servidor ClearPass con los equipos de acceso, para realizar pruebas en un entorno seguro y totalmente controlado. Este laboratorio está configurado de tal forma que permita trabajar remotamente desde cualquier sitio, gracias a una VPN.

Esta infraestructura de red está formada por los siguientes equipos.

- 4 PCs.
- Switch Cisco C3560.
- Switch HPE HP5130.
- Switch Aruba AR2930.
- AP Cisco Meraki MR56.
- Teléfono IP Yealink T19P E2.
- Servidor NAC ClearPass 6.8 sobre VMWare ESXi 6.7.
- Servidor VPNs/ Firewall Cisco ASA 5506-X.

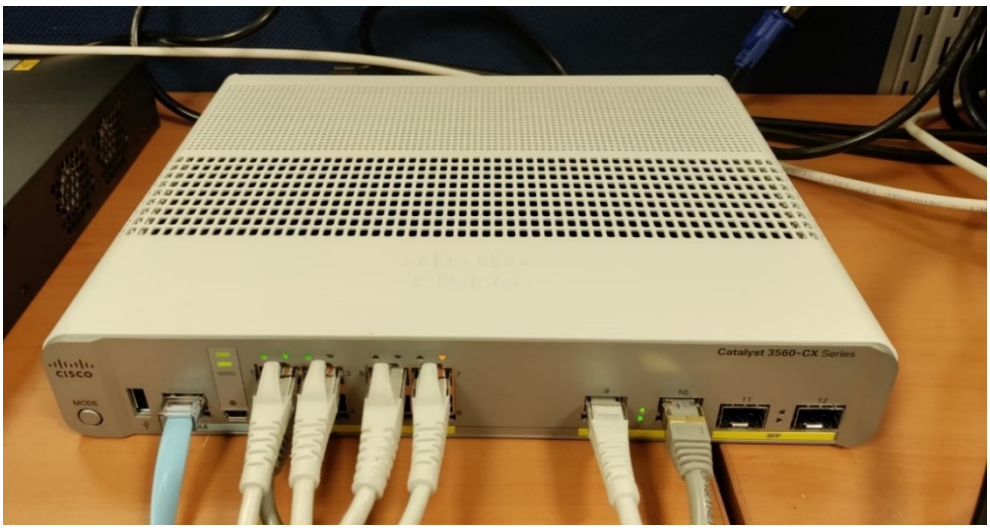


Figura 13: Switch Cisco C3560

Figura 14: Switch HPE HP5130

Figura 15: Switch Aruba AR2930

Figura 16: Cisco ASA5506

Figura 17: AP Meraki

Figura 18: Teléfono IP Yealink T19P E2

Empleamos un PC como centro de gestión, el cual está conectado a cada switch por el puerto consola. Por lo tanto tendremos acceso directo a la configuración de estos equipos. Además en este ordenador está habilitado el escritorio remoto para poder acceder desde cualquier sitio, una ventaja muy útil a la hora configurar los switches.

Los demás PCs se utilizan para realizar pruebas de acceso tanto a la red WiFi por el AP, como a la red Ethernet a través de los Switches.

También dispondremos de un teléfono IP de la marca Yealink, donde más adelante se verán las pautas necesarias para configurarlo de forma correcta y segura. Además a través del ClearPass mantendremos un control total de los dispositivos que se conecten a nuestra red del laboratorio.

El objetivo de este montaje es la simulación de una red empresarial, donde haya diferentes equipos de acceso a la red y de diferentes proveedores. Además de diseñar diferentes subredes lógicas a través de las VLANs, que nos permitan diferenciar los dispositivos conectados. Ya sea el administrador de la red que se conecte con su PC o el dispositivo móvil de un empleado. Todos ellos serán asignados a su VLAN correspondiente.

La figura 19 muestra el diseño del laboratorio con el que se harán las implementaciones de seguridad.

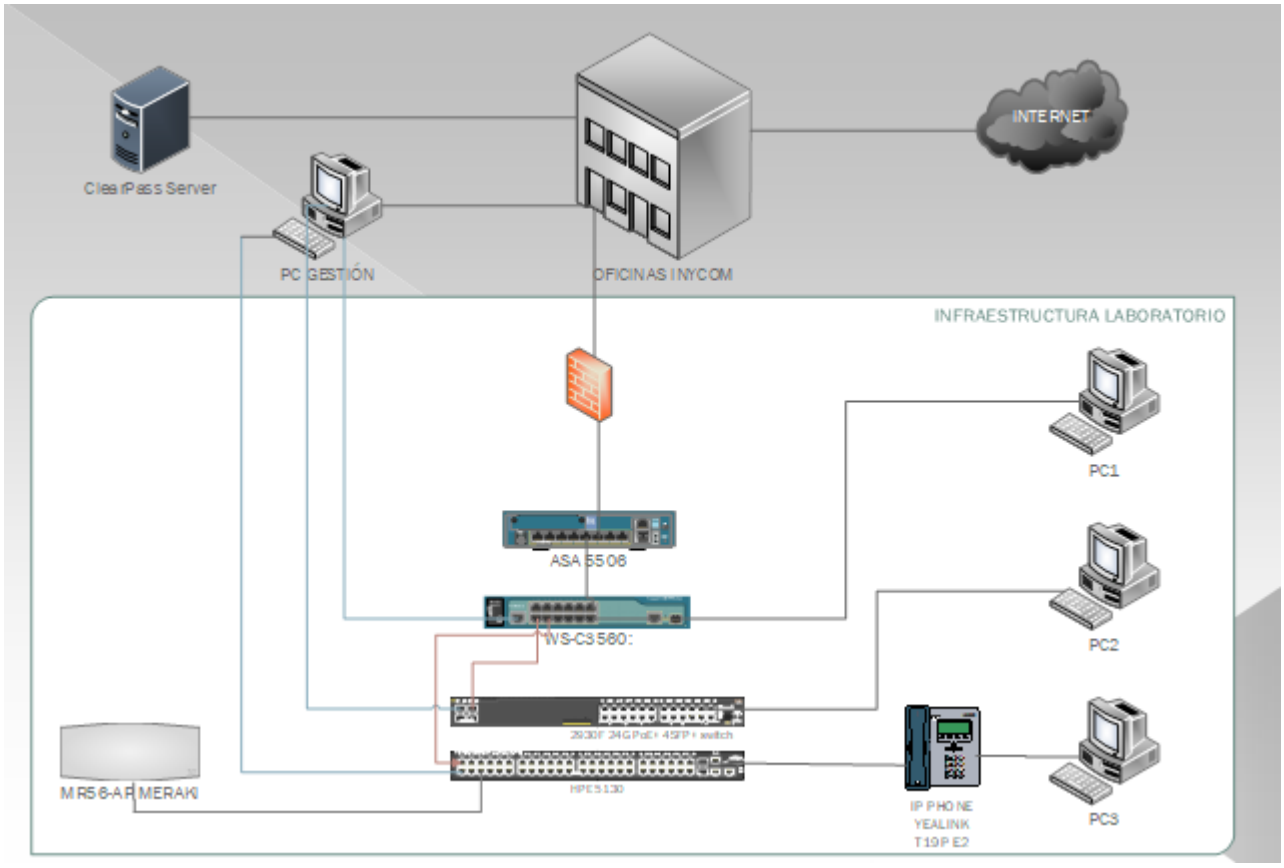


Figura 19: Infraestructura red del laboratorio

5. CONFIGURACIÓN SWITCHES

En este capítulo del proyecto analizaremos los mecanismos de seguridad comentados previamente y los implementaremos en los switches del laboratorio, siguiendo las guías ofrecidas por el CCN. La forma de configurar los tres switches y los conceptos a tener en cuenta son similares, solo varía brevemente la sintaxis utilizada. Por ello nos vamos a centrar en explicar paso a paso, lo realizado en el switch Cisco C3560.

Además en el Anexo 4 se incluye una breve metodología, plasmando los pasos a seguir que describe el CCN en las siguientes guías [29], [40] y [41].

Además una vez aplicados estos conceptos al switch del fabricante Cisco, podemos realizar una traducción de los comandos empleados a los demás switches Aruba y HPE, ya que los propios fabricantes ofrecen una traducción de los comandos empleados entre sus dispositivos. Esta información la encontramos en las siguientes referencias. [42], [43], [44].

La metodología empleada en este apartado y explicada en el anexo 4, se puede simplificar en los siguientes apartados.

- Consejos previos a la configuración.
- Servicios de red para la gestión del switch.
- Seguridad basada en puertos.
- VLANs.
- STP.
- Registros: Logs.
- Protocolo AAA.

5.1 Consejos previos a la configuración

En este dispositivo existen diferentes modos de línea de comando, donde cada uno permite realizar diferentes operaciones. Podemos configurar propiedades a nivel global que afecten a todas las interfaces del dispositivo, o cambiar las propiedades de un solo interfaz, por ello tenemos que tener claro que permite configurar cada uno de ellos. Estos modos de funcionamiento se desarrollan en el Anexo 1.

Además otra cosa a tener en cuenta es que los cambios que hagamos en la configuración del dispositivo, son guardados en una parte de la configuración denominada *running-config,* que se borrará cada vez que el equipo se reinicie. Por lo tanto, si queremos que los cambios se mantengan cada vez que arranque necesitamos guardar los cambios en la *startup-config* como se muestra en la figura 20.

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Switch#
```

Figura 20: Captura de switch Cisco, configuración guardada en fichero startup

Para empezar, creamos un mensaje informativo que aparecerá cuando se realicen conexiones al equipo. En caso de una demanda por el uso no autorizado del dispositivo, este aviso puede ser clave en procesos legales.

```
Switch# configure terminal

Switch# (config) # banner motd ^T AVISO: El uso de este dispositivo esta
restringido a los usuarios expresamente autorizados. Todos los usuarios estarán
monitorizados constantemente y podrán ser perseguidos en el caso de un uso
fraudulento de este dispositivo. ^T

Switch (config) # end

Switch# show running-config

Switch# copy running-config startup-config
```

La Figura 21 muestra el aviso que aparece cada vez que un usuario se conecte al dispositivo.

```
T Aviso: El uso de este dispositivo esta restringido a los usuarios expresamente autorizados. Todos los
 usuarios estaran monitorizados constantemente y podran ser perseguidos en el caso de un uso fraudulent
o de este dispositivo.
```

Figura 21: Captura de switch Cisco, mensaje banner

Las opciones existentes para evitar la conexión de intrusos son la configuración de usuarios y contraseñas con distintos privilegios. En este ejemplo configuramos el usuario JorgeInycom con la *password* Inycom2020TFG forzando a que se valide de forma local durante el proceso de *login* en la consola. En la figura 22 se muestra el usuario configurado.

```
Switch# configure terminal

Switch (config)# username JorgeInycom privilege 15 password Inycom2020TFG

Switch (config)# line console 0

Switch (config-line)# login local

Switch (config-line)# end
```

```
username JorgeInycom privilege 15 password 7 1067070006181F595C567A1F020F
```

Figura 22: Captura de switch Cisco, cuenta de usuario

Para finalizar los consejos previos, configuramos un *time-out period* para liberar conexiones que ya no se estén usando. Este valor lo fijamos en 8 minutos 59 segundos, como se muestra en la figura 23.

```
Switch# configure terminal

Switch(config)# line con 0

Switch(config-line)# exec-timeout 8 59

Switch(config-line)# end
```

```
!
line con 0
 exec-timeout 8 59
```

Figura 23: Captura de switch Cisco, time-out-period

5.2 Servicios de red para la gestión del switch

HTTP/HTTPS

Este servicio nos permite acceder al switch, usando como URL la dirección IP o nombre del equipo. En caso de no utilizar este tipo de conexión se recomienda deshabilitarlo, como observamos en la figura 24.

```
Switch# configure terminal
Switch (config)# no ip http server
Switch (config)# no ip http secure-server
Switch (config)# end
```

```
!
no ip http server
no ip http secure-server
```

Figura 24: Captura de switch Cisco, deshabilitar HTTP/HTTPS

TELNET

Este servicio de gestión también se recomienda deshabilitarlo, ya que al no tener cifrado podría ser una brecha de seguridad permitiendo ver la configuración. Para deshabilitarlo hay que configurar un método de acceso alternativo en todas las líneas *Virtual Tele Type* (VTY) empleadas para controlar las conexiones Telnet entrantes, en este caso el servicio SSH. Esta configuración se muestra en la figura 25.

```
Switch# configure terminal
Switch(config)# line vty 0 15
Switch(config-line)# transport input ssh
```

```
line vty 5 15
 no login
 transport input ssh
!
```

Figura 25: Captura de switch Cisco, deshabilitar Telnet

SSH

Este es el único método de gestión remoto recomendado plenamente por el CCN ya que garantiza seguridad. Para configurar este servicio, debemos seguir los siguientes pasos:

- Definir un nombre de switch.
- Definir un nombre de dominio en el switch.
- Generar una clave RSA.
- Configurar un *time-out* de SSH.
- Especificar el número de reintentos.

```
Switch# configure terminal
Switch(config)# hostname Switch-LabInycom
Switch(config)# ip domain-name Inycom.es
Switch(config)# crypto key generate rsa
Switch(config)# end
```

En la figura 26 y 27 se observa el nombre y dominio del switch configurado.

```
!
hostname Switch-LabInycom
!
```

Figura 26: Captura de switch Cisco, hostname

```
ip domain-name Inycom.es
!
```

Figura 27: Captura de switch Cisco, domain-name

Configuramos el servidor SHH, con un *timeout* de 90 segundos para la negociación con el cliente SSH y un máximo de intentos de conexión de dos, como se observa en la figura 28.

```
Switch(config)# ip ssh versión 2
Switch(config)# ip ssh time-out 90
Switch(config)# ip ssh authentication-retries 2
Switch(config)# end
```

```
ip ssh time-out 90
ip ssh authentication-retries 2
ip ssh version 2
!
```

Figura 28: Captura de switch Cisco, configuración servidor SSH

SNMP

En caso de utilizar el servicio SNMP es completamente necesario emplear la versión tres del protocolo, ya que es la única capaz de garantizar medidas de seguridad. Para comenzar creamos una *access list* que permita solo el acceso a los administradores. Después generamos un grupo para poder agrupar usuarios de SNMP y por último añadimos los usuarios que vayan a pertenecer al grupo.

```
Switch(config)# access-list 15 permit 192.168.64.2
Switch(config)# access-list 15 deny any log
```

```
access-list 15 permit 192.168.64.2
access-list 15 deny   any log
```

Figura 29: Captura de switch Cisco, accessl list - SNMP

```
Switch(config)# snmp-server group admin v3 auth read readview write writeview
Switch(config)# snmp-server user JorgeInycom admin v3 auth sha Cl@ve&secret@
access 15
```

Con el ejemplo ilustrado en la Figura 29 y 30, permitimos el acceso a la IP del administrador de la red. Para posteriormente crear el grupo llamado “admin” y con la última sentencia añadir al usuario “JorgeInycom” a dicho grupo.

```
snmp-server group admin v3 auth read readview write writeview
```

Figura 30: Captura de switch Cisco, grupo SNMP

De no aplicar este protocolo el CCN recomienda deshabilitarlo.

```
Switch# configure terminal
Switch(config)# no snmp-server community
Switch(config)# no snmp-server enable traps
Switch(config)# no snmp-server system-shutdown
Switch(config)# no snmp-server
Switch(config)# end
```

5.3 Seguridad basada en puertos

La primera medida a tomar a la hora de proteger los puertos del switch, es la de cerrar aquellos que no vayamos a utilizar.

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet0/6
Switch(config-if)# switchport block multicast
Switch(config-if)# switchport block unicast
Switch(config.if)# end
```

En la Figura 31 vemos la configuración aplicada al puerto seis, donde primero hemos bloqueado el tráfico al puerto y después lo hemos cerrado.

```
!
interface GigabitEthernet0/6
 switchport block unicast
 switchport block multicast
 shutdown
!
```

Figura 31: Captura de switch Cisco, bloqueo/cierre interfaz 6

Otra medida a tener en cuenta, es el control sobre paquetes que inundan la red. A veces existe un tráfico excesivo que disminuye la eficiencia de la red y esto puede ser causado por implementaciones erróneas o ataques de denegación de servicio. Por lo tanto se habilita el sistema "*Storm Control*".

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet0/7
Switch(config-if)# storm-control broadcast level 85.00 70.00
Switch(config-if)# storm-control multicast level 15.00
Switch(config-if)# storm-control unicast level 30.00
```

```
!
interface GigabitEthernet0/7
 storm-control broadcast level 85.00 70.00
 storm-control multicast level 15.00
 storm-control unicast level 30.00
end
```

Figura 32: Captura de switch Cisco, "Storm Control"

En la figura 32 se muestra la configuración del sistema *storm control* para el puerto 7. Cuyo tráfico será bloqueado cuando se alcance el 85% de tráfico *broadcast* en comparación con el tráfico total de ese puerto y también cuando el tráfico *multicast* supere el 15% o el tráfico *unicast* supere el 30%. Una vez bloqueado el tráfico *broadcast*, se volverá a reenviar cuando el valor de este índice baje a 70%.

ACLs

Existe otro método para asegurar la protección en los puertos, las ACLs. Estas se muestran en la Figura 33.

```
Switch(config)#access-list ?
  <1-99>            IP standard access list
  <100-199>         IP extended access list
```

Figura 33: Captura de switch Cisco, tipos ACLs

```
Switch# configure terminal
Switch(config)# Access-list 101 permit tcp host 10.1.1.2 any log
```

```
!
!
access-list 101 permit tcp host 10.1.1.2 any log
!
```

Figura 34: Captura de switch Cisco, ACL 101

La anterior ACL mostrada en la figura 34, está definida con el identificador 101 y permite el tráfico de la dirección IP 10.1.1.2 a cualquier dirección destino. Añadiendo el parámetro "log" se crea un informe cuando haya una coincidencia con la entrada de la ACL a la que se le haya aplicado este parámetro.

Ejemplo ACL

Una aplicación de ACL empleada en cualquier organización sería la siguiente, bloquear las conexiones SSH que se realizan desde la red, al firewall de la empresa. Para bloquear este intento de conexión creamos una ACL con el identificador 102 que descarta todos los paquetes provenientes de la red 192.168.65.0 con destino 192.168.64.1 la IP del firewall y puerto 22 correspondiente al servicio SSH. Como ilustra la figura 35.

```
Extended IP access list 102
    10 deny tcp 192.168.65.0 0.0.0.255 host 192.168.64.1 eq 22 log (1 match)
    20 permit ip any any
    30 deny ip any any
```

Figura 35: Captura de switch Cisco, ACL 102

La Figura 36 muestra la coincidencia de un paquete con la lista de acceso 102, resultado de intentar realizar una conexión SSH al Firewall.

```
Dec 15 12:30:58.712: %SEC-6-IPACCESSLOGP: list 102 denied tcp 192.168.65.1(58760) ->
 192.168.64.1(22), 1 packet
```

Figura 36: Captura de switch Cisco, mensaje de log ACL 102

5.4 VLANs

En los switches del fabricante Cisco nos encontramos con la VLAN 1 creada por defecto. La primera recomendación es crear una nueva VLAN que mantenga los puertos de configuración en una subred a la que solo puedan acceder los usuarios que administren los dispositivos. Esta VLAN la llamamos: "administradores" con el vlan-id 10. Además aquellos puertos que estén inactivos deberían estar en una VLAN diferente, aislados de todos los demás.

Después creamos diferentes VLANs para separar posibles departamentos y/o usuarios de la red, definiendo el vlan-id de cada una y su respectivo nombre como se muestra en la figura 37.

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# name administradores
```

Una vez creadas las VLANs correspondientes a nuestra organización, definimos aquellos puertos que sean *trunk* o *access* según la topología de red. Y añadimos cada puerto tipo *access* a su VLAN correspondiente de la siguiente forma.

```
Switch# configure terminal
Switch(config)# interface interface-id
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan vlan-id
Switch(config-if)# end
```

En nuestro caso definimos los puertos 1 y 9 como *trunk*, donde pasarán todas las VLANs, y los demás puertos configurados como *access* los asignamos a su grupo correspondiente, mostrado en la figura 37.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active
10   administradores                   active    Gi0/12
20   invitados                         active    Gi0/2
30   marketing                         active    Gi0/3
40   recursos-humanos                  active    Gi0/4
50   puertos-inactivos                 active    Gi0/5, Gi0/6, Gi0/7, Gi0/8
                                                 Gi0/10, Gi0/11
```

Figura 37: Captura de switch Cisco, VLANs asignadas a cada puerto

5.5 STP

Para evitar los bucles en la red se envían constantemente tramas definidas como BPDUs. Para ello configuramos los puertos de acceso destinados a los usuarios como *Port Fast*, donde el estado del puerto cambia a modo "*forwarding*" sin pasar por los estados previos de STP. Posteriormente añadimos el *BPDU Guard*. Esto implica asegurarnos de que no recibimos por esos enlaces información errónea la cual podría modificar la estructura que hemos predefinido al ejecutar STP entre los switches.

```
Switch# configure terminal
Switch(config)# interface interface-id
Switch(config-if)# spanning-tree portfast
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# end
```

En la Figura 38 mostramos está configuración para el puerto GigabitEthernet 0/3 del switch.

```
!
interface GigabitEthernet0/3
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast edge
 spanning-tree bpduguard enable
```

Figura 38: Captura de switch Cisco, STP en puerto usuario

Otra medida de seguridad ofrecida por este protocolo es la del uso de *Root Guard*. Esta opción nos permite bloquear a un switch que quiera hacer de *root*. En nuestro laboratorio tenemos configurado el switch Cisco con la prioridad más baja haciendo de *root* y conectado al switch HPE por el puerto 9. Por ello si activamos este servicio en dicho puerto nos aseguramos de que se bloquee si el switch HPE intenta actuar como *root*. Configuración mostrada en la figura 39.

```
Switch# configure terminal
Switch(config)# interface interface-id
Switch(config-if)# spanning-tree guard root
Switch(config-if)# end
```

```
!
interface GigabitEthernet0/9
 switchport mode trunk
 switchport nonegotiate
 spanning-tree guard root
 ip dhcp snooping trust
```

Figura 39: Captura de switch Cisco, STP - Root Guard

En la figura 40 se puede visualizar cómo actúa el puerto 7 dónde también se implementa este servicio. Este protege al *root* bloqueando el puerto (BKN) y poniéndolo en tipo *ROOT_Inc (*root inconsistent*).

```
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    1
              Address     68ca.e4b6.da80
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    1      (priority 0 sys-id-ext 1)
              Address     68ca.e4b6.da80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Gi0/1               Desg FWD 4         128.1    P2p
Gi0/2               Desg FWD 4         128.2    P2p Edge
Gi0/4               Desg FWD 4         128.4    P2p Edge
Gi0/7               Desg BKN*4         128.7    P2p *ROOT_Inc
Gi0/8               Desg FWD 4         128.8    P2p
Gi0/9               Desg FWD 4         128.9    P2p
Gi0/10              Desg FWD 4         128.10   P2p Edge
```

Figura 40: Captura de switch Cisco, ejemplo Root Guard

En la figura 41, se indica con dos mensajes log, que dicho puerto se queda en estado *uplink*, pero bloqueado y en estado *ROOT_Inc como hemos visto anteriormente en la figura 40.

```
Switch#
Jan 15 14:26:58.925: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port Gigab
itEthernet0/7 on VLAN0001.
Jan 15 14:27:00.878: %LINK-3-UPDOWN: Interface GigabitEthernet0/7, changed state
 to up
```

Figura 41: Captura de switch Cisco, ejemplo Root Guard – Logs

5.6 Registros: Logs

Los registros son fundamentales para saber que eventos suceden dentro de la red, para ello es importante saber cuándo ocurre cada evento. Esto se realiza configurando un servidor NTP (*Network Time Protocol*) para sincronizar el equipo de red con la hora real.

Para llevar a cabo esto al situarnos en España, utilizamos como servidor NTP la dirección IP 150.214.94.5 correspondiente al servidor hora.roa.es del Real Observatorio de la armada (ROA). Estos sistemas de la ROA, atienden las peticiones de sincronismo diarias de millones de dispositivos. [45]

La configuración NTP del switch se ilustra en la figura 42.

```
Switch# configure terminal

Switch(config) ntp server 150.214.94.5

Switch(config)# clock timezone GMT 1 0

Switch(config)# clock summer-time SPAIN recurring last Sun Mar 2:00 last Sun
Oct 3:00
```

```
clock timezone GMT 1 0
clock summer-time SPAIN recurring last Sun Mar 2:00 last Sun Oct 3:00
ntp server 150.214.94.5
!
```

Figura 42: Captura de switch Cisco, NTP

La figura 43 muestra el estado de la sincronización del dispositivo switch con el servidor NTP.

```
Switch-LabInycom#show ntp status
Clock is unsynchronized, stratum 2, reference is 150.214.94.5
nominal freq is 286.1023 Hz, actual freq is 286.1023 Hz, precision is 2**20
ntp uptime is 239399400 (1/100 of seconds), resolution is 3496
reference time is E385B00D.F0220055 (11:23:09.938 GMT Thu Dec 17 2020)
clock offset is 0.9795 msec, root delay is 38.04 msec
root dispersion is 7.19 msec, peer dispersion is 0.71 msec
loopfilter state is 'FREQ' (Drift being measured), drift is 0.000000000 s/s
system poll interval is 64, last update was 10 sec ago.
```

Figura 43: Captura de switch Cisco, estado servidor NTP

5.7 Protocolo AAA

En este caso vamos a utilizar el protocolo AAA, RADIUS. Para que el switch actúe como cliente RADIUS y pueda enviar peticiones de autenticación al servidor debemos identificar al servidor y otros datos de la conexión. En este caso identificamos el servidor ClearPass con la dirección 172.22.69.234 y los puertos UDP empleados para las peticiones de *authenticacion* (1812) y *accounting* (1813).

Además para que los equipos de acceso (*authenticator*) y el RADIUS (*authentication server*) mostrados en la figura 12 se validen entre ellos, debe configurarse entre ellos una clave secreta.

Siguiendo la guía del CCN de este dispositivo nos hemos dado cuenta que antes de realizar la identificación del servidor. [29] Debemos habilitar el triple A con el siguiente comando.

```
Switch# configure terminal
Switch(config)#  aaa new-model
```

Posteriormente definimos la dirección del servidor y sus puertos.

```
Switch(config)# radius server cpass
Switch(config-radius-server)# address ipv4 172.22.69.234 auth-port 1812 acct-port 1813
```

Una vez definido el servidor, especificamos como llevar a cabo el proceso de autenticación a través del estándar 802.1X, autorizamos las peticiones de servicios de red por parte del RADIUS y activamos el servicio de *accounting* para mantener un control sobre el consumo de recursos empleado por los usuarios.

```
Switch# configure terminal
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# aaa authorization network default group radius
Switch(config)# aaa accounting dot1x default start-stop group radius
```

La figura 44 muestra toda la configuración global realizada para vincular el switch con el servidor RADIUS.

```
aaa new-model
!
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
radius server cpass
 address ipv4 172.22.69.234 auth-port 1812 acct-port 1813
!
```

Figura 44: Captura de switch Cisco, RADIUS

Respecto a la guía del CCN vamos a añadir una configuración adicional para que el servidor RADIUS pueda emplear la función *Change of Authorization* (CoA) en el que permite cambiar dinámicamente las autorizaciones de sesión, se muestra en la figura 45.

```
Switch# configure terminal
Switch(config)#aaa server radius dynamic-author
Switch(config-locsvr-da-radius)# client 172.22.69.234 server-key secret-radius
Switch(config-locsvr-da-radius)# port 3799
Switch(config-locsvr-da-radius)# auth-type all
```

```
!
aaa server radius dynamic-author
 client 172.22.69.234 server-key 7 140417081E013E663629373C3700
 port 3799
 auth-type all
!
```

Figura 45: Captura de switch Cisco, RADIUS COA

6. CONFIGURACIONES ADICIONALES.

En este capítulo del trabajo vamos a añadir o a profundizar en importantes conceptos de seguridad que no hemos visto en los apartados anteriores, ya que en las guías del CCN no están contempladas o las nombran rápidamente.

Estas protecciones adicionales frente ataques las vamos a implementar sobre el switch Cisco C3560, podemos verlas en la figura 46.

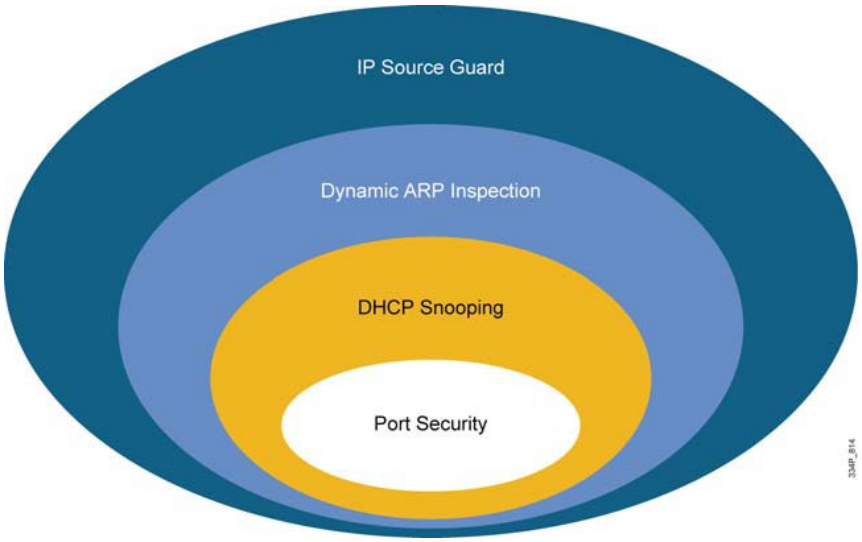


Figura 46: Cisco Catalyst características de seguridad [33]

- ***Port Security*** previene de los ataques de inundación de MAC.
- ***DHCP Snooping*** evita los ataques de los clientes al servidor DHCP y al conmutador.
- ***Dynamic ARP inspection*** agrega seguridad a *Address Resolution Protocol* (ARP) mediante el uso de la tabla de indagación DHCP para minimizar el impacto de los ataques de suplantación ARP.
- ***IP Source guard*** evita la suplantación de direcciones IP mediante el uso de la tabla DHCP *snooping*.

La figura 46, nos ofrece una representación de aquellas medidas de seguridad implantadas en el switch. El *Port Security* es una medida que ya hemos explicado anteriormente y se emplea para controlar que el flujo de tramas en un puerto no sea excesivo, por ello nos vamos a centrar en las demás medidas.

El siguiente punto en el que nos vamos a centrar es el *DHCP Snooping*.

DCHP Snooping

La protección *DHCP Snooping* es una solución frente a ataques de *DHCP Spoofing*. Esta es una técnica de engaño utilizada para asignar parámetros de configuración DHCP a los equipos que se encuentran dentro de una red LAN. [35]

Este protocolo DHCP se pone en funcionamiento cuando un equipo se conecta a una red de la que desconoce cualquier tipo de información. Por lo tanto la solución propuesta para evitar este ataque es la siguiente, a través del *DHCP Snooping*.

Se determina que puertos pueden responder a las solicitudes DHCP. Los puertos se identifican como *trust* o *untrusted*, siendo los *trust* aquellos donde se aloja un servidor DHCP o un enlace hacia el servidor. Y los puertos *untrusted* aquellos definidos para los clientes, donde solo pueden generar peticiones. En la figura 47 podemos observar un claro ejemplo de puertos *trust* y *untrusted*.

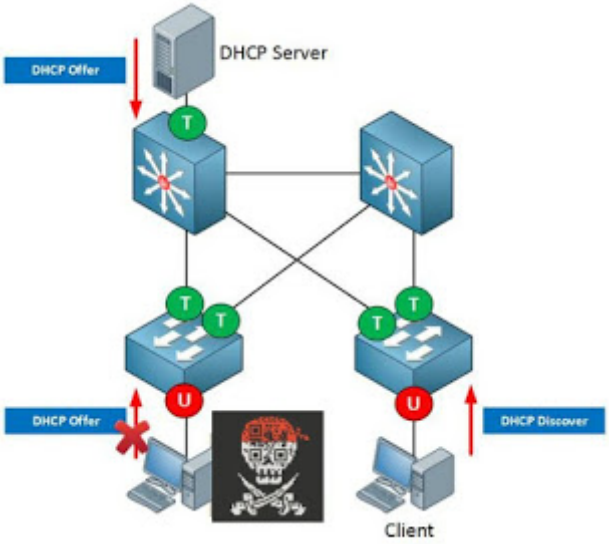


Figura 47: DHCP Snooping ejemplo de configuración de puertos [46]

Los pasos seguidos para habilitar esta solución son los siguientes:

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 1
```

La figura 48 muestra la configuración global necesaria para habilitar el *DHCP Snooping*.

```
!
ip dhcp snooping vlan 1
ip dhcp snooping database flash:dhcp-snooping.dat
ip dhcp snooping
```

Figura 48: Configuración DHCP Snooping global

```
Switch(config)# interface gigabitEthernet 0/8
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 3
```

La figura 49 muestra la configuracion a nivel de puerto para habilitar el *DHCP Snooping*.

```
!
interface GigabitEthernet0/8
 ip dhcp snooping limit rate 3
 ip dhcp snooping trust
!
```

Figura 49: Configuración DHCP Snooping puerto 8

La figura 50 ilustra el estado de configuración *DHCP Snooping* mostrado en cada interfaz.

```
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
GigabitEthernet0/8         yes        yes             3
Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
```

Figura 50: Estado configuración DHCP Snooping

Dynamic ARP inspection

Es una solución implantada contra el ataque *ARP Spoofing*. Donde el atacante suplanta la dirección MAC de un usuario y se coloca en la ruta de reenvío normal. [35]

Es muy similar al *DHCP Snooping*, donde todos los puertos del switch se clasifican como *trust* o *untrust*. El switch intercepta e inspecciona todos los paquetes ARP que llegan a un puerto *untrust*. Para ello configuro a nivel global el *ip arp inspection*, excepto aquellos puertos en los que haya algo estático definidos como *trust*.

Vamos a configurar como *trust* el puerto 8, donde está conectado el switch Aruba, esta configuración se observa en la figura 51.

```
Switch(config)# interface gigabitEthernet 0/8
Switch(config-if)# ip arp inspection trust
```

```
!
interface GigabitEthernet0/8
 description Switch Aruba
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 spanning-tree guard root
 ip dhcp snooping limit rate 3
 ip dhcp snooping trust
!
```

Figura 51: Configuración Dynamic ARP Inspection - Interfaz 8

IP Source Guard

Esta es una solución complementaria a las anteriores, que permite el tráfico IP solo cuando la dirección IP y MAC de los paquetes coinciden con una de las siguientes fuentes de enlace. [47]

- Entradas en la tabla de asociaciones *DHCP Snooping*.
- Entradas de origen IP estática.

El filtrado por enlaces de direcciones IP y MAC ayuda a prevenir ataques de suplantación de identidad, donde el atacante utiliza la dirección IP de un host válido para obtener acceso no autorizado a la red.

Observando el switch del laboratorio en la figura 52, se muestra la tabla de asociaciones *DHCP Snooping*. Si habilitamos esta herramienta en la interfaz GigabitEthernet 0/2 y el dispositivo recibe un paquete IP con una dirección 192.168.64.14, *IP Source Guard* solo reenvía el paquete si la dirección MAC del paquete es 00:11:6B:66:5E:29.

```
Switch-LabInycom#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:11:6B:66:5E:29   192.168.64.14    64          dhcp-snooping   1     GigabitEthernet0/2
Total number of bindings: 1
```

Figura 52: IP Source Guard, tabla de asociaciones DHCP Snooping

Para configurar esta solución en la interfaz GigabitEthernet 0/2 realizamos los siguientes pasos, ilustrados en la figura 53:

```
Switch# config
Switch(config)# interface gigabitEthernet 0/2
Switch(config-if)# ip verify source port-security
```

De esta forma se comprueba la dirección IP y MAC del tráfico que hay en ese puerto con lo aprendido en la tabla DHCP Snooping, mostrada en la figura 52.

```
interface GigabitEthernet0/2
 ip verify source port-security
!
```

Figura 53: IP Source Guard, configuración en interfaz 2

7. CONFIGURACION ASA-VPN

A través del firewall del laboratorio levantamos una VPN para que los usuarios remotos se conecten al ASA y reciban una dirección IP, lo que le permitirá el acceso a la red interna.

Para empezar, creamos en el ASA un grupo de servidores triple AAA donde añadimos el ClearPass, donde se realizará la posterior autenticación de los usuarios. Esto se observa en la figura 54.

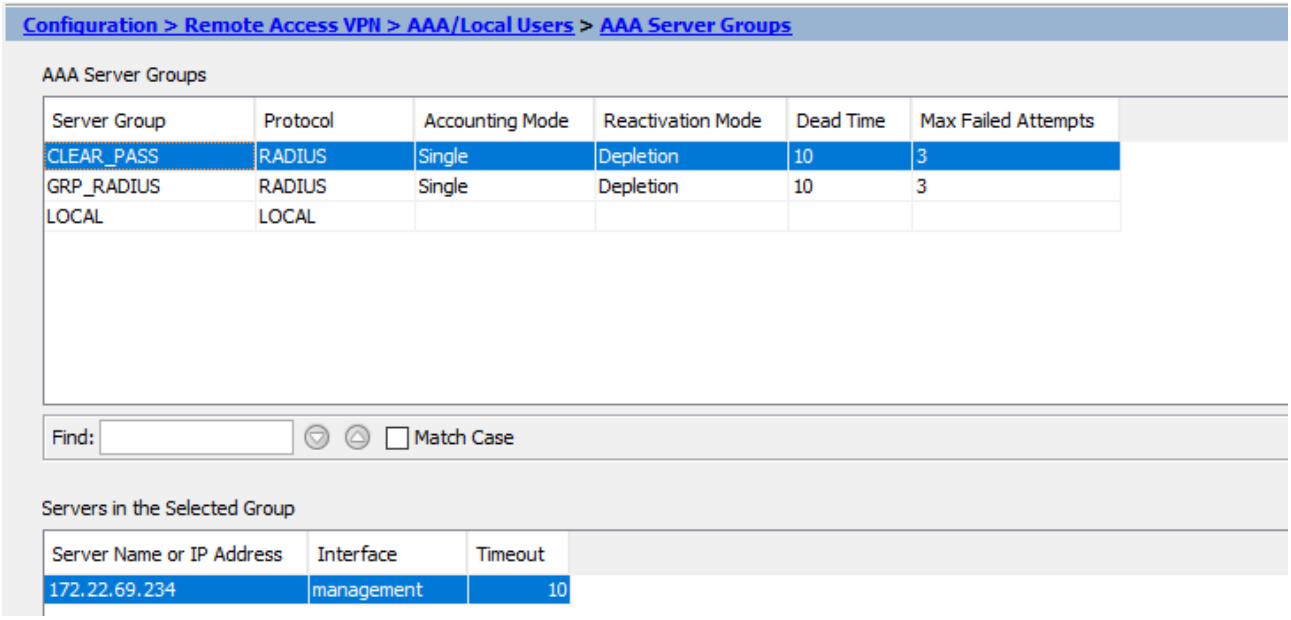


Figura 54: Firewall ASA, AAA servers groups

A continuación vamos a explicar las diferentes zonas que tenemos dentro del Firewall. Por un lado tenemos la zona exterior *outside* que corresponde a la red externa del laboratorio, es decir internet en la interfaz 8. Por otro lado tenemos la zona interior *inside* formada por la subred del laboratorio en la interfaz 1. Además existe un interfaz de *management* empleada por el administrador para la configuración del ASA. Mostrado en la figura 55.

Tener estos aspectos claros es esencial para poder formar reglas y limitar el acceso a los servicios de los clientes que se conecten. Esto se hace a partir de ACLs.

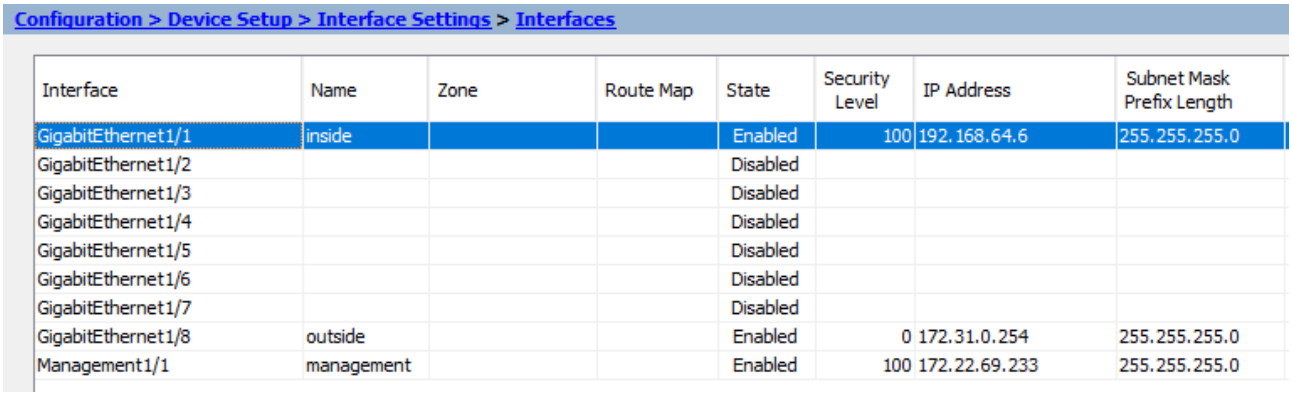


Figura 55: Interfaces Firewall ASA

Por último hemos creado estas ACLs. “A-ACL” actúa sobre direcciones origen de la 10.1.1.0/24, la “B-ACL” sobre direcciones de la 172.16.1.0/24 y la “C-ACL” sobre direcciones de la 192.168.1.0/24 que son las que asigna el ClearPass a los siguientes clientes: “wusr101”, “wusr102” y “wusr103” respectivamente. Mostrado en la figura 56.

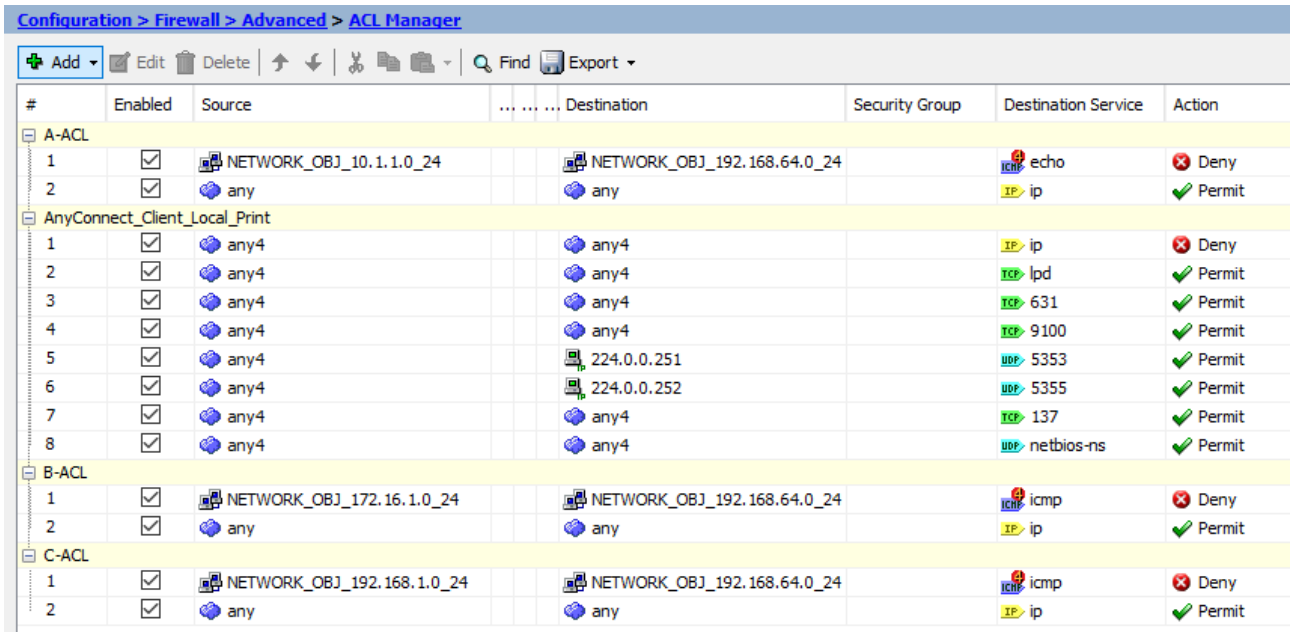


Figura 56: Firewall ASA, ACLs.,

El último aspecto a tener en cuenta en la configuración de la VPN es asignar las direcciones que va a tener cada cliente, figura 57. De esta forma puedes emplear un rango de direcciones para cada departamento de la empresa y después emplear ACLs que actúen sobre estas, para limitar lo que pueden hacer.

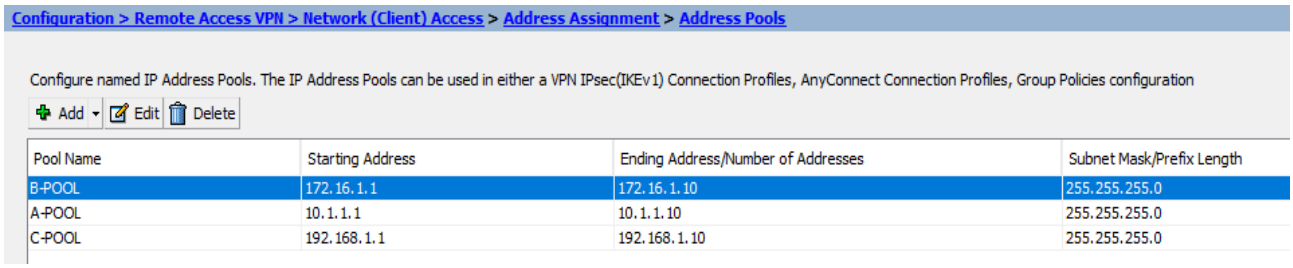


Figura 57: Firewall ASA, rango de direcciones

8. IMPLEMENTACIÓN CLEARPASS

8.1 Portal cautivo

A continuación vamos a explicar la solución de acceso diseñada en la red WiFi del laboratorio. Este servicio ofrecido por el ClearPass se denomina portal cautivo.

Es una página web que el invitado ve antes de acceder a la red inalámbrica. A través de esta página el usuario puede conectarse únicamente disponiendo de un usuario y contraseña o mediante un auto-registro donde el usuario obtiene las credenciales tras rellenar un formulario.

Además este servicio ofrece un control total sobre las entradas a la red, almacenando información de cada dispositivo y capaz de modificar la interfaz de usuario, para que la imagen de la página web sea afín a la imagen de la empresa.

8.2 Diseño Portal cautivo

El objetivo de este portal cautivo es dar acceso a los dispositivos inalámbricos de los empleados y a aquellas personas que acudan a la empresa como invitados. Los empleados deberán iniciar sesión con su nombre de usuario y contraseña, autenticándose contra el *Active Directory* (AD). Un servicio de varios servidores donde se encuentran los datos de los usuarios, con el objetivo de administrar los inicios de sesión. Por ello si el empleado se conecta con sus credenciales se le dará acceso a la red inalámbrica.

En la figura 58 se observa el diseño realizado del portal cautivo.

Figura 58: Portal cautivo - Inicio sesión

En caso de un invitado ajeno a la empresa es necesaria la aceptación por medio de un tercero, el flujo de eventos se muestra en la figura 59.

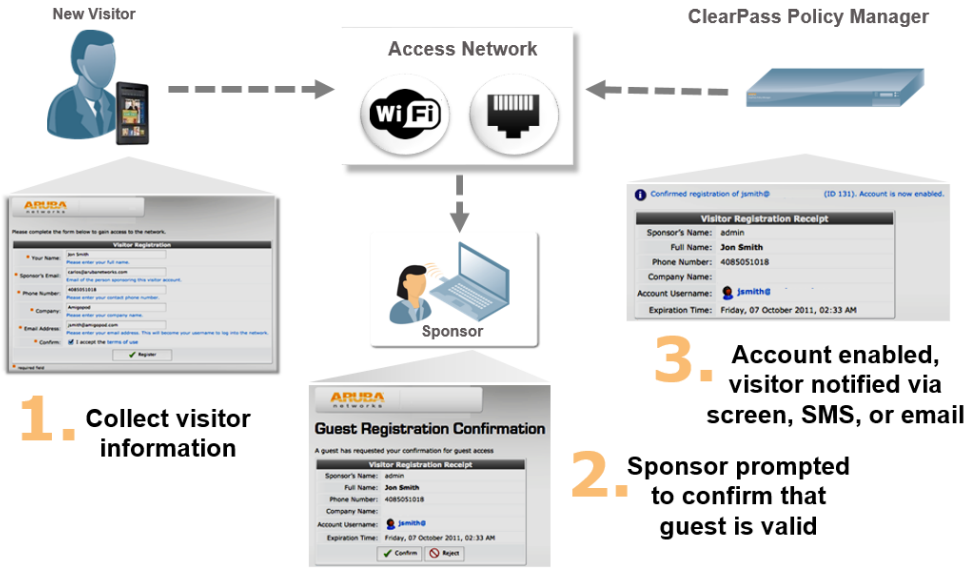


Figura 59: Flujo de aprobación [48]

El invitado rellenará el formulario y se notificará mediante correo electrónico al administrador de la red, que tras verificar la identidad del cliente, activará la cuenta. La figura 60 muestra el portal de auto registro para invitados.

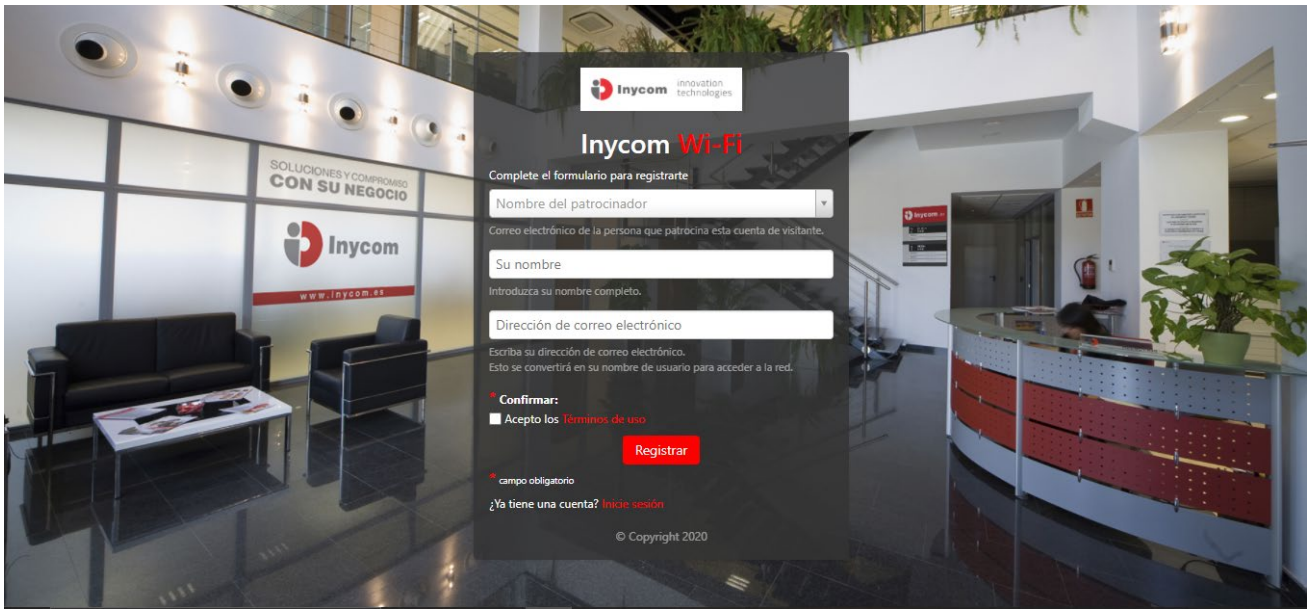


Figura 60: Portal cautivo - Auto Registro

8.3 Integración con AD

ClearPass soporta la integración con diferentes BBDD, siendo el AD el utilizado para la solución desarrollada, ya que hoy en día es una solución empleada por múltiples empresas. En esta se crean de forma centralizada todos los datos de acceso de los empleados. En la figura 61 se muestra la configuración del servidor AD.

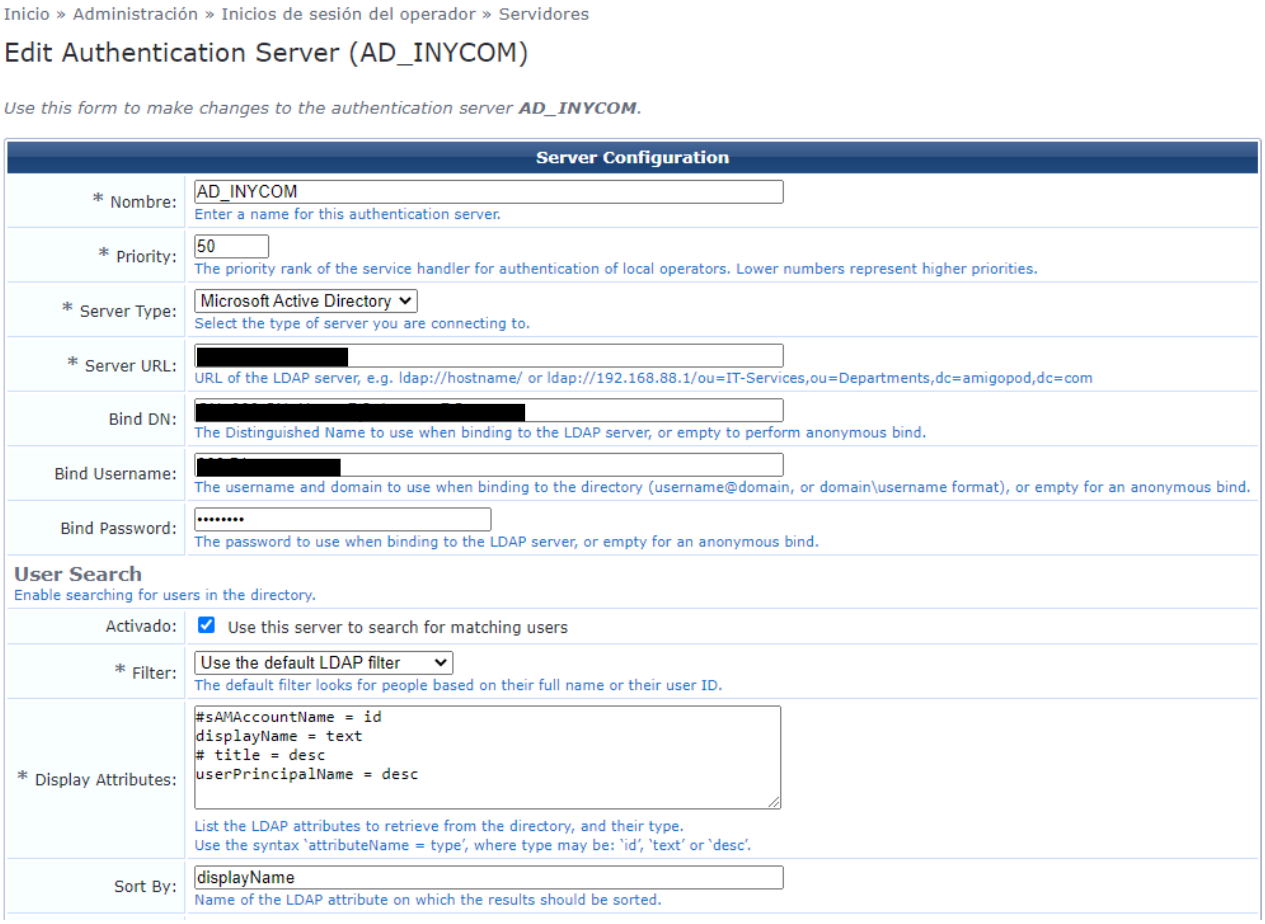


Figura 61: Integración con AD

8.4 Integración dispositivos

Posteriormente una vez definido el direccionamiento de cada dispositivo de acceso a la red, los incluimos en la base de datos del ClearPass para que se puedan conectar y validar gracias a la clave secreta compartida entre ellos. En la figura 62 se muestran todos los dispositivos que tenemos configurados en la arquitectura de acceso, con sus correspondientes direccionamientos.

Network Devices

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Filter: Name contains Go Clear Filter

#		Name ▲	IP or Subnet Address	Description
1.	☐	ap-meraki	192.168.64.5	Punto de acceso Cisco Meraki
2.	☐	switch-aruba	192.168.64.4	Switch Aruba 2930
3.	☐	switch-cisco	192.168.64.2	Switch cisco Catalyst 3560-CX
4.	☐	switch-hpe	192.168.64.3	Switch HPE 5130
5.	☐	vpn-asa	172.22.69.233	Cisco ASA / VPN

Figura 62: Dispositivos de red en ClearPass

8.5 Implementación servicio cableado (Ethernet)

Una vez vinculados los dispositivos de red, creamos un servicio cableado para los switches mostrado en la figura 63, que permita la autenticación IEEE 802.1X de todos aquellos usuarios que se conecten a la red. Configuramos este servicio para clientes que se conectan a través del grupo [777 – SWITCH INYCOM TFG], un grupo formado por los switches del laboratorio.

Services - [777 - INYCOM TFG]

Summary | Service | Authentication | Authorization | Roles | Enforcement

Service:

Name:	[777 - INYCOM TFG]
Description:	802.1X Wired Access Service
Type:	802.1X Wired
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Authorization

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Ethernet (15)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Connection	NAD-IP-Address	BELONGS_TO_GROUP	[777 - SWITCH INYCOM TFG]

Figura 63: Servicio cableado (Ethernet)

Posteriormente configuramos los métodos y fuentes de autenticación que tendrá el servicio, mostradas en la figura 64.

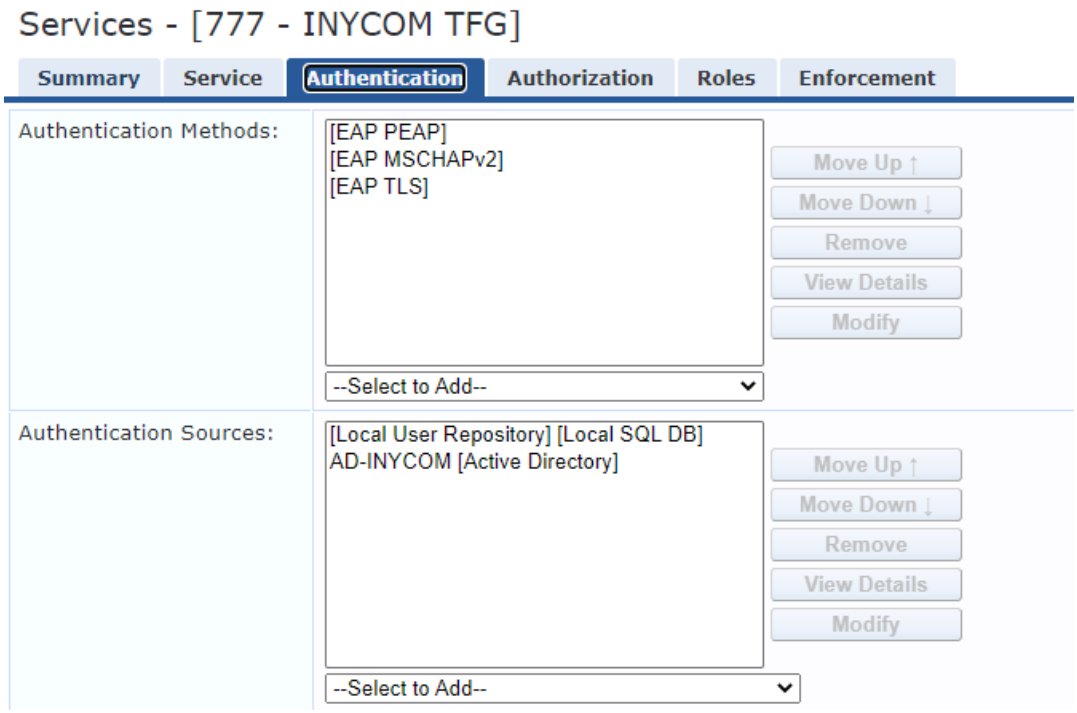


Figura 64: Servicio cableado (Ethernet), autenticación

Seguimos definiendo los métodos de autorización, ilustrados en la figura 65. Estos serán el AD de la empresa integrado anteriormente y una base de datos formados por usuarios locales cada uno con diferentes roles.

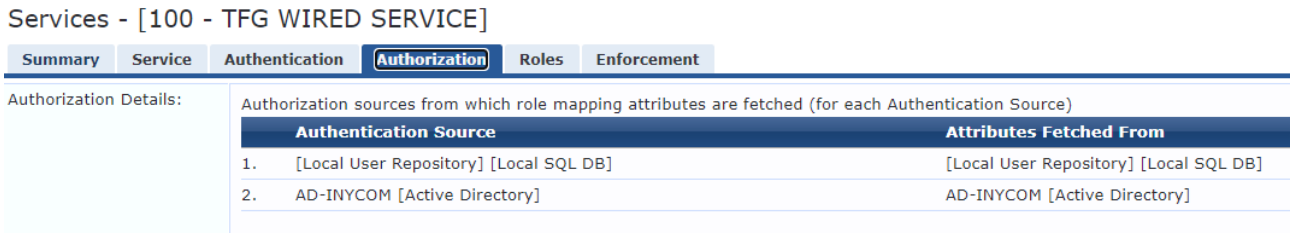


Figura 65: Servicio cableado (Ethernet), autorización

Después asignamos el *role mapping* [777 – INYCOM TFG ROLE MAPPING] al servicio, el cual asigna a la VLAN correspondiente el rol que tenga el usuario conectado. Por ejemplo en la figura 66, cuando se conecte un administrador de la red, el ClearPass le proporcionará acceso a la red en la VLAN 102.

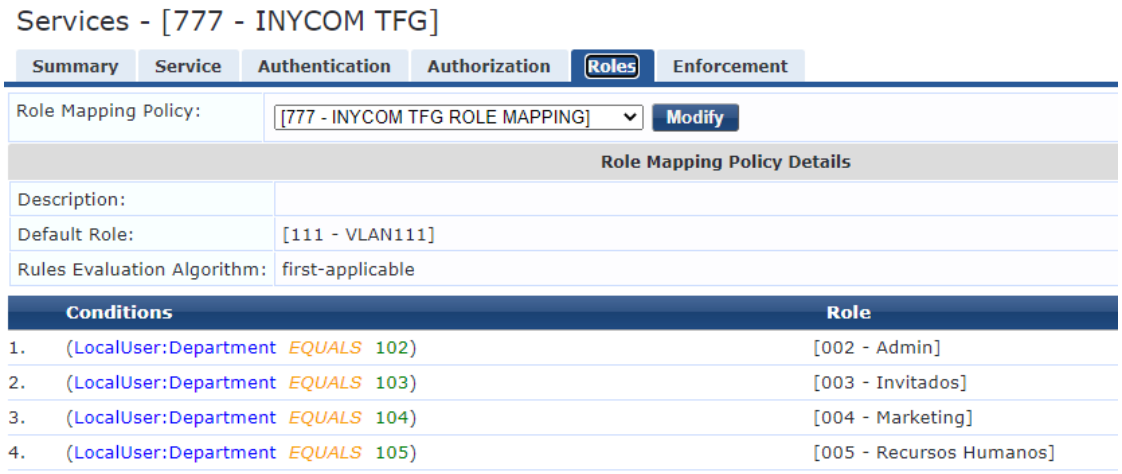


Figura 66: Servicio cableado (Ethernet), role mapping

Para finalizar el servicio ethernet, terminamos por definir el *enforcement*, cuya función es la de evaluar las condiciones mostradas en la figura 67 y aplicar el *profile* correspondiente. Este *enforcement profile* es el encargado de proporcionar los atributos del perfil al switch.

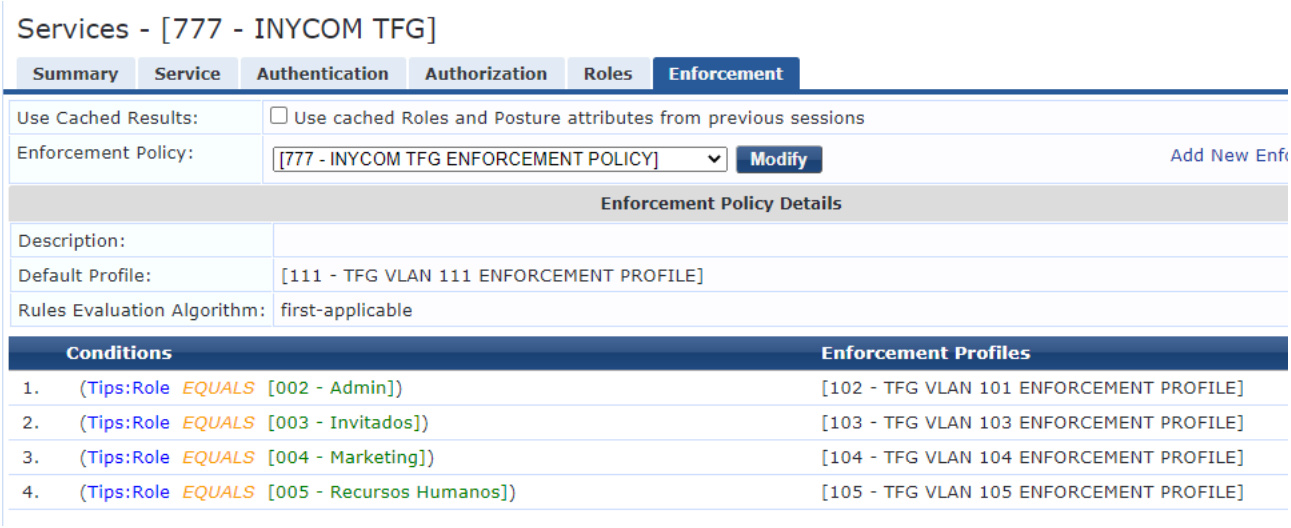


Figura 67: Servicio cableado (Ethernet), enforcement

De esta forma ya hemos configurado el servicio que da acceso a los usuarios de la red que se conectan a través de los switches. Más adelante observaremos el correcto funcionamiento del servicio conectándonos con diferentes usuarios de red.

8.6 Implementación servicio inalámbrico WiFi

A diferencia de lo visto en el apartado anterior, el servicio creado para la parte WiFi tiene significativas diferencias. La más importante son las condiciones aplicadas al crear el servicio, estas se muestran a continuación en la figura 68.

Donde el tipo de conexión en este caso será *Wireless-802.11*, a través del AP y evaluará todos aquellos usuarios conectados a la red WiFi del laboratorio, denominada "TFG-WIFI".

Services - [777 - WIFI INYCOM TFG]

Summary | Service | Authentication | Authorization | Roles | Enforcement

Service:

Name:	[777 - WIFI INYCOM TFG]
Description:	802.1X Wireless Access Service
Type:	802.1X Wireless
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Authorization

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Connection	SSID	EQUALS	TFG-WIFI

Figura 68: Servicio inalámbrico WiFi

8.7 Implementación servicio cableado VPN

Como hemos comentado anteriormente cada servicio de acceso tiene unos atributos que lo diferencian. Ya hemos visto la diferencia entre el servicio WiFi y el cableado (ethernet). Por lo tanto ahora veremos la implementación del servicio VPN en el ClearPass, mostrado en la figura 69.

Para este servicio como para los anteriores el atributo esencial a la hora de crear el servicio es: *NAS-Port-Type*. Este atributo indica el tipo de puerto físico del NAS que está autenticando al usuario. Cuyo valor es 5, indica que el estado del puerto es *Virtual*. [49]

Además también definimos el grupo de dispositivos por los que se recibe la petición de autenticación [777- VPN INYCOM TFG], donde se encuentra el firewall de Cisco.

Services - [777- TFG VPN SERVICE]

Summary | Service | Authentication | Authorization | Roles | Enforcement

Service:

Name:	[777- TFG VPN SERVICE]
Description:	TFG - VPN Access Service
Type:	802.1X Wired
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Authorization

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Virtual (5)
2.	Radius:IETF	NAS-IP-Address	BELONGS_TO_GROUP	[777 - VPN INYCOM TFG]

Figura 69: Servicio cableado VPN

9. RESULTADOS

En este apartado se describirán las pruebas realizadas en la herramienta ClearPass configurada, mostrando una serie de pruebas de acceso, tanto del usuario que se conecta a la red, como el administrador de esta. También diferenciaremos aquel acceso de red proporcionado por ethernet, inalámbricamente y aquel acceso remoto producido por VPN.

Estas pruebas son una valoración inicial de la solución implementada. Quedaría pendiente desarrollar más pruebas sistemáticas para garantizar el correcto funcionamiento del sistema.

9.1 Acceso WiFi

A continuación se describen las pruebas de usuario que se han realizado para garantizar el funcionamiento del sistema, además se incluyen capturas de pantalla que faciliten la comprensión del proceso seguido para el acceso inalámbrico

En primer lugar aparecerá un SSID llamado "TFG-WIFI" donde el usuario deberá conectarse, introduciendo su nombre y contraseña, representado en la figura 70.

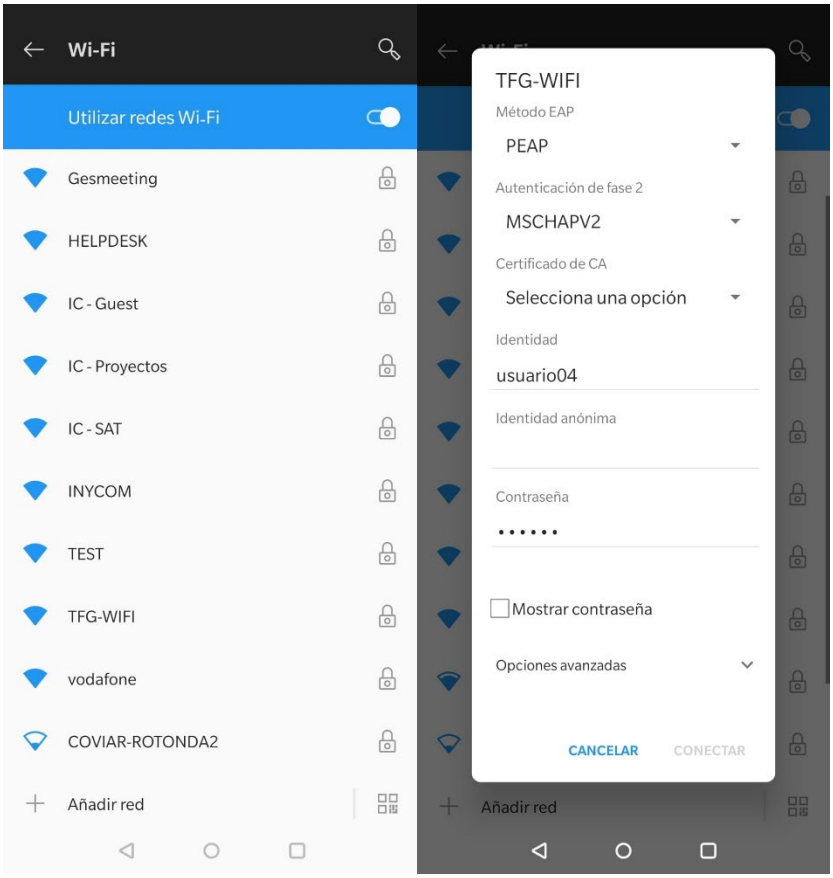


Figura 70: Acceso del usuario a la red WiFi

A continuación una vez introducido su usuario y contraseña correctamente. ClearPass realizará en este caso la autenticación contra el AD o contra la base de datos local, también es compatible con otras BBDD como LDAP. Una vez validadas estas credenciales se le asignará al empleado su VLAN correspondiente.

User ID ▲	Name	Role	Status
usuario01	usuario01	[002 - Admin]	Enabled
usuario02	usuario02	[002 - Admin]	Enabled
usuario03	usuario03	[003 - Invitados]	Enabled
usuario04	usuario04	[004 - Marketing]	Enabled
usuario05	usuario05	[005 - Recursos Humanos]	Enabled

Figura 71: Usuarios locales creados en el ClearPass

Para comprobar que asigna la VLAN correspondiente, vamos a comparar el acceso de dos usuarios. Por un lado tenemos el usuario04 del departamento de marketing y por otro lado el usuario02 que sería el administrador de la red. Ambos reciben una dirección IP acorde con su VLAN.

Tabla 5: Prueba de acceso WiFi

	Usuario02	**Usuario04**
Rol	Administrador	Departamento de marketing
VLAN	102	104
Dirección subred	192.168.66.0	192.168.68.0
Direccionamiento asignado	INFORMACIÓN DE LA RED Dirección MAC ea:1c:90:f2:01:34 Dirección IP 192.168.66.4 Puerta de enlace 192.168.66.2 Máscara de subred 255.255.255.0 DNS 1.1.1.1 8.8.8.8	INFORMACIÓN DE LA RED Dirección MAC ea:1c:90:f2:01:34 Dirección IP 192.168.68.4 Puerta de enlace 192.168.68.2 Máscara de subred 255.255.255.0 DNS 1.1.1.1 8.8.8.8

Como observamos en la tabla 5, las pruebas de acceso a través del WiFi se han realizado desde el mismo dispositivo. La primera vez hemos accedido con las credenciales del Usuario02 y hemos recibido una dirección IP de la subred 66. Por otro lado cuando nos hemos autenticado con el usuario04, hemos obtenido una IP de la subred 68.

Experiencia de administrador

A continuación se muestran los resultados que obtendrá el administrador tras realizar las pruebas de usuario vistas en el apartado anterior. Para ello el administrador accederá en su cuenta de ClearPass, y tendrá acceso al módulo *monitoring* que este ofrece, donde se visualiza toda la información de las distintas conexiones.

Para cualquier solicitud de acceso, el servidor NAC muestra el usuario, la fuente de autenticación, el servicio correspondiente al acceso, el estado de la conexión y la fecha y hora. Estos parámetros se muestran en la figura 72.

Server	Source	Username	Service	Login Status	Request Timestamp ▾
172.22.69.234	RADIUS	usuario04	[777 - WIFI INYCOM TFG]	ACCEPT	2020/12/29 12:40:56
172.22.69.234	RADIUS	usuario02	[777 - WIFI INYCOM TFG]	ACCEPT	2020/12/29 12:39:33

Figura 72: Monitorización de acceso

Además tambien podemos observar un resumen de los atributos de cada conexión, como la dirección MAC del dispositivo, la dirección IP del dispositivo que le ha dado acceso a la red. Y las políticas empleadas en la conexión, como se muestra en la figura 73.

Request Details

Summary | Input | Output

Login Status:	ACCEPT
Session Identifier:	R0000013c-01-5feb15c8
Date and Time:	Dec 29, 2020 12:40:56 CET
End-Host Identifier:	EA-1C-90-F2-01-34
Username:	usuario04
Access Device IP/Port:	192.168.64.5:1 (ap-meraki / Cisco)
Access Device Name:	1848d3183efd4e9a7476364ba1382a544a78cb6e4ba5b06a
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	[777 - WIFI INYCOM TFG]
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	Local:localhost
Authorization Source:	[Local User Repository], [Time Source]
Roles:	[004 - Marketing], [User Authenticated]
Enforcement Profiles:	[204 - TFG WIFI VLAN 104 ENFORCEMENT PROFILE]

◀◀ ◀ Showing 78 of 61-80 records ▶ ▶▶ | Change Status | Show Configuration | Export | Show Logs | Close

Figura 73: Resumen de los detalles de la conexión

9.2 Acceso Cableado (Ethernet)

A continuación, como hemos visto en el apartado de acceso inalámbrico, vamos a ver el procedimiento realizado para acceder a la red a través de un ordenador conectado al switch. Para ello habilitamos la autenticación IEEE 802.1X como se observa en la figura 74 e introducimos nombre y contraseña.

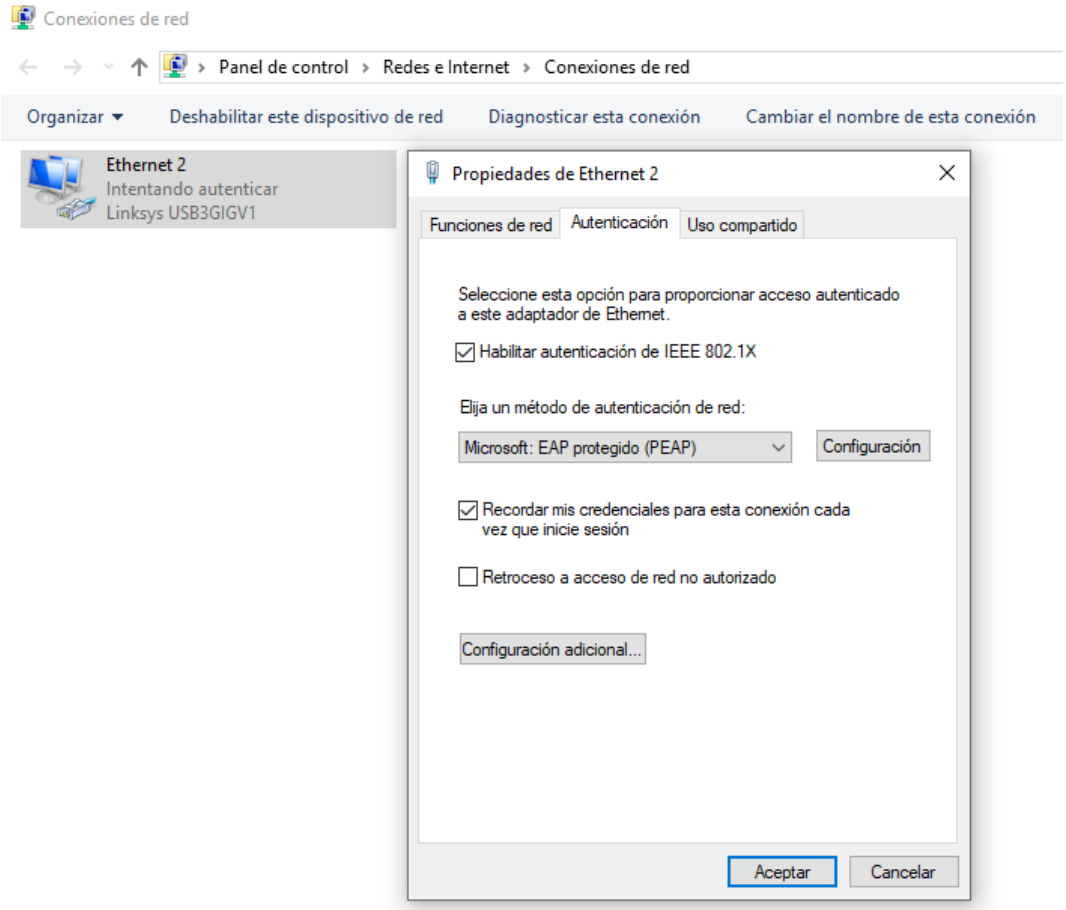


Figura 74: Configuración tarjeta de red PC

Una vez autenticado el usuario y con acceso a internet, observamos en el switch dos mensajes de log figura 75, que indican la conexión a red del dispositivo conectado al puerto 5.

```
Dec 29 12:03:03.365: %LINK-3-UPDOWN: Interface GigabitEthernet0/5, changed state to up
Dec 29 12:03:04.365: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/5, chang
state to up
Switch-LabInycom>
```

Figura 75: Log de conexión a la red

Como hemos verificado en el apartado anterior, el administrador tiene constancia del acceso de este dispositivo a través del ClearPass. Remarcando que el dispositivo conectado ha hecho coincidencia con el servicio [777 – INYCOM TFG] correspondiente al servicio cableado, ilustrado en la figura 76.

Server	Source	Username	Service	Login Status	Request Timestamp ▾
172.22.69.234	RADIUS	usuario04	[777 - INYCOM TFG]	ACCEPT	2020/12/29 13:06:50

Figura 76: Monitorización de conexión

9.3 Acceso VPN

En este apartado nos vamos a conectar a la red del laboratorio de forma remota a través de la VPN configurada.

Primero nos debemos descargar el cliente de la VPN, para ello abrimos cualquier navegador e ingresamos la dirección IP del ASA como URL. Para posteriormente autenticarse y descargar el cliente *Anyconnect* automáticamente.

Una vez hecho esto, al cliente le aparece en pantalla la siguiente figura 77. A continuación después de escribir la dirección IP del servidor VPN ya se puede iniciar la conexión remota.

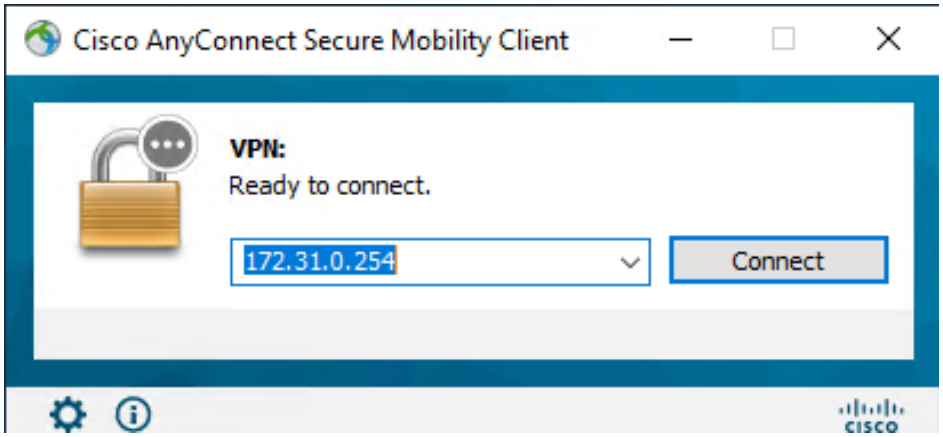


Figura 77: Conexión VPN

La figura 78 refleja la autenticación del usuario "wusr103" , este usuario recibirá una direccion IP correspondiente al rango ofrecido por la lista de acceso "C-ACL".

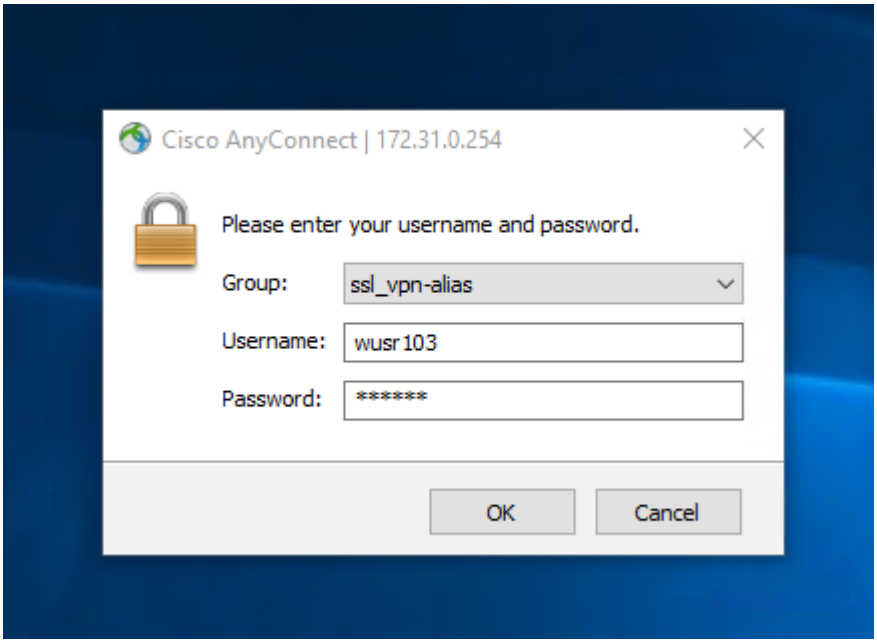


Figura 78: Autenticación VPN de usuario

Finalmente una vez realizada la conexión por parte del usuario, este puede visualizar los siguientes datos mostrados en la figura 79 donde se observa la dirección IP asignada la 192.168.1.1 que coincide con la *access list* "C-ACL" asignada para dicho usuario.

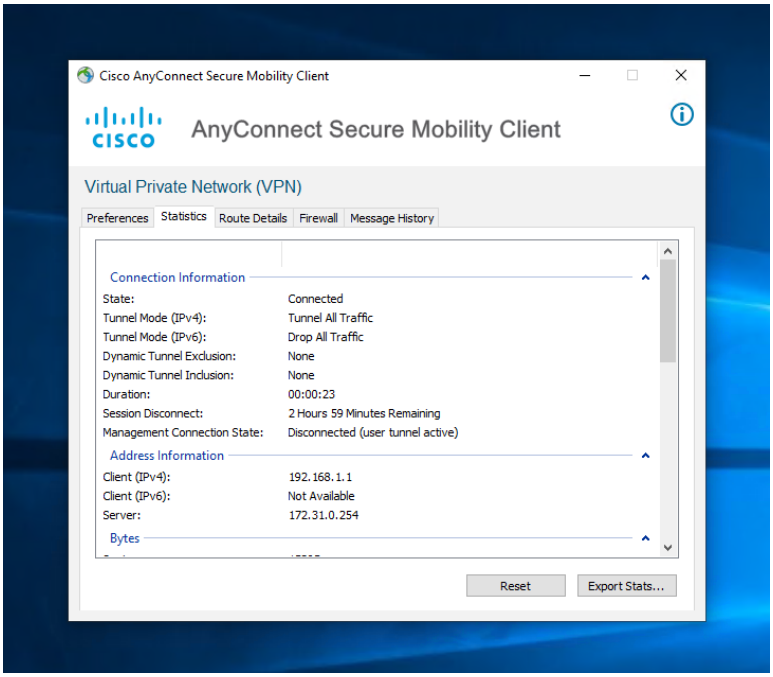


Figura 79: Información de conexión VPN – Vista Usuario

También podemos observar los datos de la conexión a través del ClearPass figura 80, es decir desde la perspectiva del administrador de la red. En este caso como en los intentos de conexión a través de WiFi y ethernet, podemos visualizar el servicio por el cual ha entrado en la red el cliente y las políticas usadas.

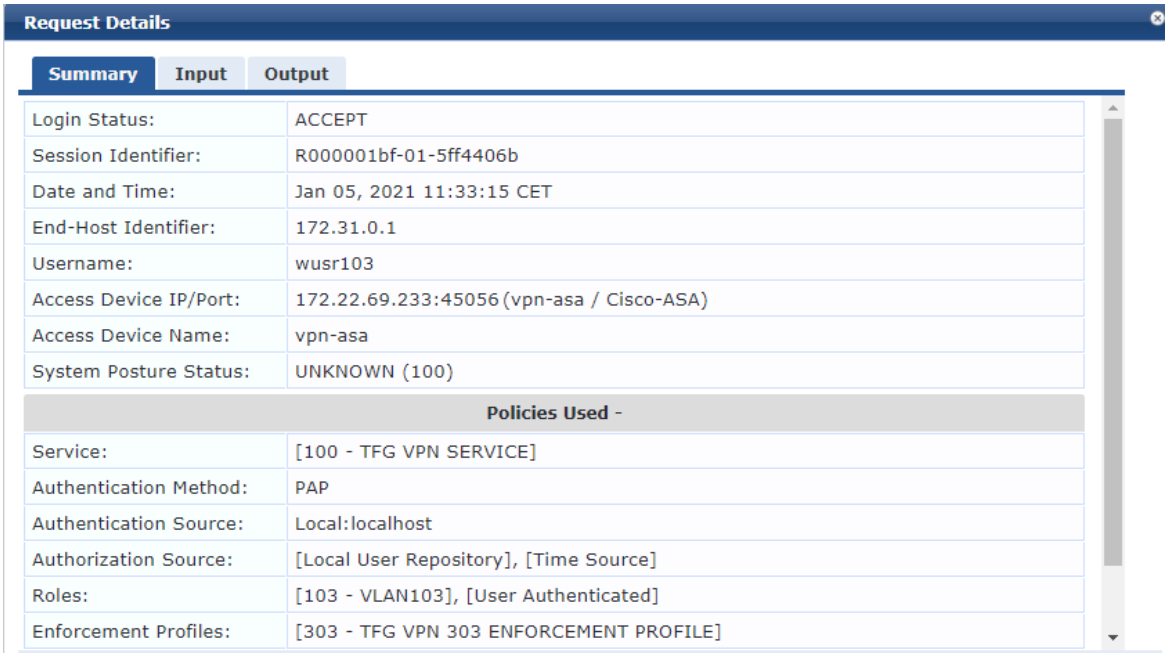


Figura 80: Información de conexión VPN – Vista Administrador

10. CONCLUSIONES Y LÍNEAS FUTRURAS.

10.1 Conclusiones

Este TFG está orientado a aquellas empresas que quieran seguir expandiendo su arquitectura de red o necesiten implementar nuevos equipos. Porque para ello es de vital importancia tener constancia de todos los aspectos de seguridad descritos en el proyecto, para posteriormente hacer una evaluación de la topología de red e implementar la seguridad a nivel de enlace. Por lo tanto todo este proyecto es una parte necesaria que todo administrador de red debe conocer. En este trabajo se ha puesto especial énfasis en la comprobación de las soluciones que propone el CCN en sus guías. Para ello hemos seguido una metodología explicada en el Anexo 4 y se ha instalado una infraestructura de red sobre la que trabajar de forma segura, completamente paralela a la red de Inycom. Siguiendo estas guías nos hemos dado cuenta de que había aspectos que estaban desfasados, por lo que nos hemos encargado de buscar información y completar la configuración de estos servicios.

También hemos comprobado que estas medidas de seguridad funcionen correctamente haciendo pruebas en el laboratorio y realizando ataques de denegación de servicios, para ver el funcionamiento de los equipos y los mensajes de depuración que aparecen en cada situación.

Durante el desarrollo del proyecto se han ampliado conocimientos vistos durante la carrera en lo referente a los servicios y protocolos de seguridad a nivel de enlace, y se han estudiado aspectos nuevos como las herramientas NAC que permiten el control de acceso a la red.

En cuanto a las herramientas empleadas me he dado cuenta de las posibilidades que existen a la hora de gestionar los dispositivos que se conectan a la red, tanto el ordenador de un empleado, su teléfono móvil, hasta una impresora. Si no se tiene constancia de todos estos equipos, cualquiera de ellos puede llegar a ser una brecha de seguridad. Además es vital tener una buena organización de todos los equipos para conocer a qué servicios puede acceder cada empleado.

A la vista del desarrollo del proyecto se puede decir que se han conseguido los objetivos marcados. Ya que he adquirido una experiencia considerable en el despliegue de sistemas de control de acceso en redes tanto en local como en remoto, y se ha comprobado que funciona correctamente en el laboratorio.

Como conclusión final, este trabajo puede ser una magnífica herramienta para aquellos estudiantes o personal con poca experiencia que le gustaría conocer el mundo de las redes, ya que en dicho proyecto se recogen técnicas y configuraciones empleadas en todas las redes del mundo.

10.2 Líneas futuras

Ya sea por falta de tiempo o de priorizar objetivos, han quedado varias cosas pendientes que se podrían tratar en el futuro. Una de ellas es poner en producción el portal cautivo diseñado para Inycom, donde aquellos invitados que acudan a la empresa y se conecten a la red, les aparecería dicha página web.

Por otra parte la herramienta ClearPass tiene muchas funciones que permiten la administración de los equipos y la monitorización de los mismos, y una parte muy interesante es la de *posture*. Este módulo permite inspeccionar los dispositivos que se conecten para permitir el acceso de los dispositivos en función del sistema operativo que posean o de si el antivirus está o no actualizado. Esta sería una forma de continuar con el proyecto añadiendo nuevas políticas que permitan un mayor control del acceso.

11. BIBLIOGRAFÍA.

[1] INTERPOL, Organización Internacional de Policía Criminal. *Cybercrime*: COVID-19 *Cybercrime Analysis Report*. (2020, Agosto). Recuperado de: https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

[2] Fundación Telefónica (2016). Ciberseguridad, la protección de la información en un mundo digital.Recuperado de: https://publiadmin.fundaciontelefonica.com/index.php/publicaciones/add_descargas?tipo_fichero=pdf&idioma_fichero=es_es&title=Ciberseguridad%2C+la+protecci%C3%B3n+de+la+informaci%C3%B3n+en+un+mundo+digital&code=531&lang=es&file=Ciberseguridad.pdf

[3] Barzanalla, Rafael. Gestión de la seguridad en Sistemas de Infromación. Recuperado de: https://www.um.es/docencia/barzana/GESESI/GESESI-Niveles-de-Gestion-de-la-Seguridad.pdf

[4] Vyncke E., Paggen C (2007). LAN *Switch Security what hackers know about your switches*.

[5] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson (2006). CSI/FBI *Computer Crime and Security Survey*. Recuperado de: http://pdf.textfiles.com/security/fbi2006.pdf

[6] CCN, Centro Criptológico Nacional. https://www.ccn-cert.cni.es/

[7] CNI, Centro Nacional de Inteligencia. https://www.cni.es/

[8] Listado de guías CCN-STIC, (2020, Diciembre). Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/1297-indice-series-ccn-stic/file.html

[9] Guías CCN-STIC, 1000 Procedimientos de empleo seguro. Recuperado de: https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/100-procedimientos-empleo-seguro.html

[10] Inycom, Instrumentación y Componentes SA. http://www.inycom.es/

[11] Aruba ClearPass. Recuperado de: https://www.arubanetworks.com/es/productos/seguridad/gestion-de-politicas/acceso-seguro/

[12] Gil Vera, Víctor Daniel, & Gil Vera, Juan Carlos (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*, 22(2) ,193-197. ISSN: 0122-1701. Recuperado de: https://www.redalyc.org/articulo.oa?id=84953103011

[13] Perlman, Radia (1992). *Interconnections: Bridges and Routers*.

[14] Perlman, Radia (1999). I*nterconnections: Bridges, Routers, Switches, and Internetworking Protocols* (2ª edición).

[15] STP, *Spanning Tree Protocol*. Recuperado de: https://es.wikipedia.org/wiki/Spanning_tree

[16] Modelo OSI, Modelo de interconexión de sistemas abiertos. Recuperado de: https://es.wikipedia.org/wiki/Modelo_OSI

[17] Redesbasico150, ¿Qué es el modelo OSI? Recuperado de: https://sites.google.com/site/redesbasico150/protocolos-de-red/-que-es-el-modelo-osi

[18] Redes Telemáticas. El Switch: cómo funciona y sus principales características (2013). Recuperado de: http://redestelematicas.com/EL-SWITCH-COMO-FUNCIONA-Y-SUS-PRINCIPALES-CARACTERISTICAS/

[19] Universidad de Mondragón. https://www.mondragon.edu/ES/ESCUELA-POLITECNICA-SUPERIOR

[20] AMPO. https://www.ampo.com/es/

[21] Parlamento de la Rioja. https://www.parlamento-larioja.org/

[22] Yunquera Torres, Juan José. Diseño de una red WiFi para la E.S.I: Capítulo 3: El estándar IEEE 802-11. Recuperado de: http://bibing.us.es/proyectos/abreproy/11138/fichero/memoria%252FCap%C3%ADtulo+3.pdf+

[23] Wendell Odom. (2016) CCENT/CCNA ICND1 100-105 *Official Cert Guide*.

[24] FS Comunidad, Switch Gigabit: Puerto SFP vs Puerto RJ45 vs Puerto GBIC. Recuperado de: https://community.fs.com/es/blog/gigabit-switch-sfp-port-vs-rj45-port-vs-gbic-port.html

[25] RFC6071, *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap (Informational)*. Recuperado de: https://tools.ietf.org/html/rfc6071

[26] RFC4251, *The Secure Shell (SSH) Protocol Architecture (Proposed Standard)*. Recuperado de: https://tools.ietf.org/html/rfc4251

[27] Informe CCN-PYTEC nº6, Arquitecturas de Acceso Remoto Seguro. Recuperado de: https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/boletines-pytec/335-pildorapytec-31ago2020-arquitecturas-de-acceso-remoto-seguro/file

[28] ComDatosGrupo4, Capítulo 6. Principios de Seguridad en Redes. Recuperado de: https://sites.google.com/site/comdatosgrupo4/contenidos/cap6_princ-seg-redes#TOC-Aspectos-de-Seguridad-en-Redes

[29] CCN (2007, Diciembre). Instrucción Técnica de Seguridad de las TIC (CCN-STIC-644), Seguridad en EQ. Comunicaciones Switches Cisco.

[30] Capella Hernández, Juan Vicente. Universidad Politécnica de Valencia. Características y configuración básica de VLANs. Recuperado de: https://riunet.upv.es/bitstream/handle/10251/16310/Art%C3%ADculo%20docente%20configuraci%C3%B3n%20b%C3%A1sica%20VLANs.pdf

[31] RFC7727, *Spanning Tree Protocol* (STP) *Application of the Inter-Chassis Communication Protocol* (ICCP). Recuperado de: https://tools.ietf.org/html/rfc7727#SECTION-1.2

[32] Wendell Odom, CCNA *Routing and Switching* 200-125 *Official Cert Guid. Chapter 2 Spanning Tree Protocol Concepts*.

[33] David Hucaby, Cisco CCNP Switch 642-813 *Student Guide Volume 1*.

[34] RFC3579, RADIUS (*Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol* (EAP). Recuperado de: https://tools.ietf.org/html/rfc3579

[35] David Hucaby. (2014) CCNP *Routing and Switching* SWITCH 300-115 *Official Cert Guide*.

[36] Jim Geler. (2008) *Implementing* 802.1X *Security Solutions for Wired and Wireless Networks*.

[37] Chris Jackson. (2010) *Network Security Auditing. The complete guide to auditing network security, measuring risk, and promoting compliance*.

[38] Rubén Martínez. (2018) ClearPass: la herramienta de control de acceso a la red. Recuperado de: https://www.sothis.tech/CLEARPASS-LA-HERRAMIENTA-DE-CONTROL-DE-ACCESO-A-LA-RED/

[39] *Aruba a Hewlett Packard Enterprise Company*, hoja de datos Aruba ClearPass *Policy Manager*. Recuperado de: https://www.arubanetworks.com/assets/_es/ds/DS_ClearPass_PolicyManager.pdf

[40] CCN (2016, Enero). Guía/norma de seguridad de las TIC (CCN-STIC-647), Seguridad en Switches HP *Comware*. Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1303-647-seguridad-en-switches-hpcomware/file.html

[41] CCN (2019, Mayo). Guía de Seguridad de las TIC CCN.STIC 647C, Seguridad en conmutadores HPE Aruba. Recuperado de: https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/600-guias-de-otros-entornos/3695-ccn-stic-647c-seguridad-en-conmutadores-hpe-aruba/file.html

[42] *Aruba a Hewlett Packard Enterprise Company*. (2019, Enero) *ArubaOS-Switch and Cisco IOS CLI Reference Guide*. Recuperado de: https://oss.arubase.club/wp-content/uploads/2019/05/ArubaOS-Switch_and_Cisco_IOS_CLI_Reference_Guide.pdf

[43] *Hewlett Packard Enterprise. HPE Solutions Series, Aruba HPE Networking and Cisco CLI Reference Guide versión 3.2*. Recuperado de: https://www.catelsys.eu/images/Catelsys/images/2017/04/0-Notices-HPE_Aruba_and_Cisco_CLI_Ref_Guide.pdf

[44] *Hewlett Packard Enterprise*. (2015, Noviembre) *HP Networking and Cisco CLI Reference* Guide, HPE Partner Ready Certification and Learning.

[45] Real Observatorio de la Armada Española. https://armada.defensa.gob.es/ArmadaPortal/page/Portal/ArmadaEspannola/cienciaobservatorio/prefLang-es/06Hora--01QueHoraEs

[46] CCNP Switch. (2017) *DHCP Snooping*. Recuperado de: http://ccnp300-115.blogspot.com/2016/08/dhcp-snooping.html

[47] *Configuring IP Source Guard*. Recuperado de: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x_chapter_01110.pdf

[48] *Community Aruba Networks. Guest; Captive Portal; sponsor approval architecture*. Recuperado de: https://community.arubanetworks.com/community-home/digestviewer/viewthread?MID=14397

[49] *Radius Attribute – NAS Port – Type*. Recuperado de: https://www.dialogic.com/webhelp/BorderNet2020/2.2.0/WebHelp/radatt_nas_port_type.htm

12. APÉNDICES.

Anexo 1 Modos de línea de comando del switch Cisco

Tabla 6: Modos de línea de comando del switch Cisco[27]

Modo	**Método de acceso**	**Prompt**	**Salir o pasar al siguiente modo**
User EXEC	Este es el primer nivel de configuración. Permite cambiar propiedades del terminal, realizar funciones básicas y mostrar información del sistema.	Switch>	Introducir el comando *logout*. Para pasar al modo *privileged* EXEC introducir el comando *enable*.
Privileged EXEC	Desde el modo *User EXEC* introducir el comando *enable*.	Switch#	Para salir al modo *User EXEC* introducir el comando *disable*. Para pasar al modo global de configuración usar el comando configure.
Configuración global	Desde el modo *privileged EXEC* introducir el comando configure	Switch(config)#	Para pasar al modo *privileged* EXEC introducir los comandos *end* o *exit*, o pulsar Ctrl-z.
Configuración de interfaz	Desde el modo de configuración global introducir el comando interface seguido de un identificador de interfaz	Switch(config-if)#	Para pasar al modo *privileged* EXEC introducir el comando *end* o pulsar Ctrl.z. Para pasar al modo de configuración global introducir el comando *exit*.
Config-vlan	Desde el modo de configuración global introducir el comando vlan seguido de un identificador de vlan	Switch(config-vlan)#	Para pasar al modo *privileged* EXEC introducir el comando *end* o pulsar Ctrl-z. Para pasar al modo de configuración global introducir el comando *exit*.
Configuración de VLANs	Desde el modo *privileged* EXEC introducir el comando vlan database	Switch(vlan)#	Para pasar al modo *privileged* EXEC introducir el comando *exit*.
Line configuration	Desde el modo de configuración global especificamos una “línea” usando el comando line	Switch(config-line)#	Para pasar al modo *privileged* EXEC introducir el comando *end* o pulsar Ctrl-z. Para pasar al modo de configuración global introducir el comando *exit*.

Anexo 2 Configuración teléfono IP

En este anexo se va a explicar la configuración necesaria sobre los equipos de comunicación, para la integración y funcionamiento seguro de un teléfono IP y otro dispositivo, normalmente un PC.

Estos tipos de teléfono admiten la conexión de un dispositivo conectado en cascada. Por este motivo la interfaz del switch puede llevar una mezcla de tráfico de datos y voz.

La siguiente figura 81, muestra la configuración realizada para la correcta autenticación del Teléfono IP y del ordenador.

```
!
interface GigabitEthernet0/5
 switchport mode access
 switchport nonegotiate
 authentication event fail action authorize vlan 69
 authentication event no-response action authorize vlan 69
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
 spanning-tree portfast edge
!
```

Figura 81: Configuración interfaz teléfono y pc

Este puerto del switch está configurado de tal forma, que los dispositivos de acceso tienen que autenticarse a través del protocolo 802.1X. En este caso si los datos de usuario son introducidos incorrectamente o el método de autenticación no responde, el switch directamente coloca a este usuario que está intentando acceder a la red, a una VLAN restringida. En este caso la VLAN 69, denominada puertos_inactivos, como se muestra en la figura 82.

```
COM3 - PuTTY
face Gi0/5 AuditSessionID C0A840020000008A28394E9A
Switch-LabInycom#
Dec 30 09:11:20.091: %DOT1X-5-RESULT_OVERRIDE: Authentication result overridden for client (80
5e.c0e1.67c8) on Interface Gi0/5 AuditSessionID C0A840020000008A28394E9A
Switch-LabInycom#sh vla
Switch-LabInycom#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                                                Gi0/6, Gi0/8, Gi0/10, Gi0/11
                                                Gi0/12
65   Administradores                  active
66   Invitados                        active
67   Marketing                        active
68   Recursos_humanos                 active
69   puertos_inactivos                active    Gi0/5
```

Figura 82: Fallo de autenticación VLAN 69

Una vez confirmada la autenticación del teléfono IP, este es colocado directamente en la VLAN de voz correspondiente. Pero otro factor a tener en cuenta es, que por defecto la configuración del puerto solo permite una dirección MAC. Por lo tanto cuando intentemos conectar un ordenador en cascada con el teléfono, el puerto se deshabilitará y no tendremos acceso. Esto se muestra en la figura 83, donde el estado del puerto GigabitEthernet0/5 pasa a *err-disabled*.

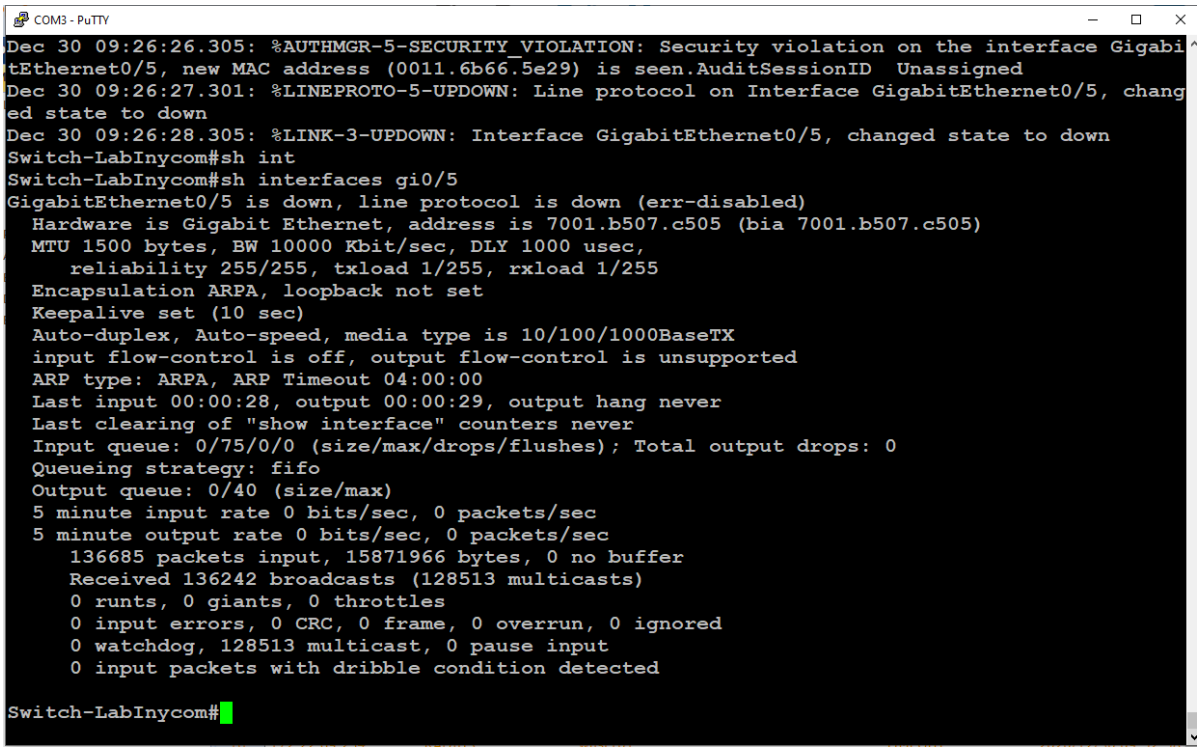


Figura 83: Múltiples dispositivos sin autorización

Para solucionar esto es imprescindible el siguiente comando observado anteriormente en la figura 80.

authentication host-mode multi-auth

Esta instrucción permite autenticar varios hosts en un solo puerto, pudiendo estos utilizar diferentes métodos. Cada host se autentica individualmente antes de que pueda acceder a los recursos de la red y permite un cliente en la VLAN de voz y varios clientes en la VLAN de datos.

En la imagen 84 se observa como una vez finalizada la autenticación de los dos dispositivos, cada uno accede a una VLAN distinta, a la VLAN 102 el ordenador y a la Voice_VLAN el teléfono IP.

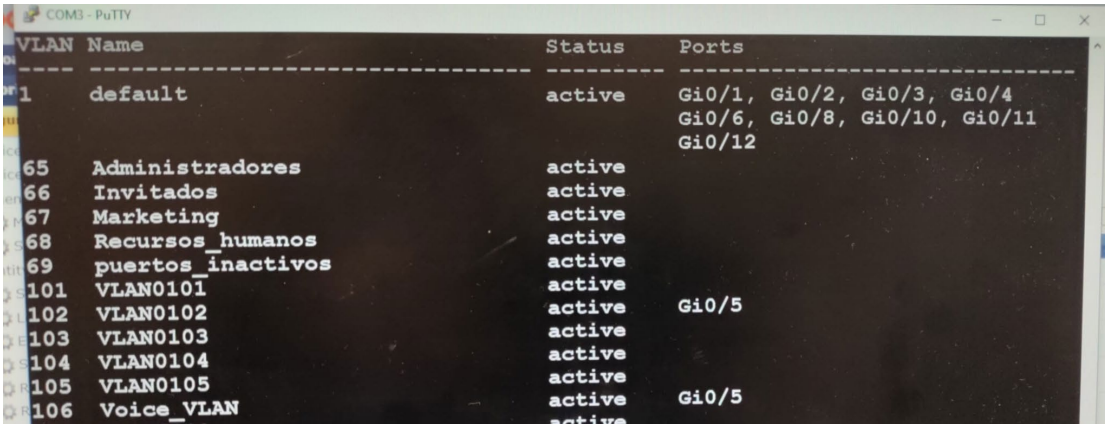


Figura 84: Interfaces con sus respectivas VLANs

Anexo 3 Distintas configuraciones de seguridad 802.1X

En este apartado vamos a explicar las posibles configuraciones que podemos utilizar para la autenticación IEEE 802.1X.

Como hemos comentado durante el trabajo, esta medida de seguridad se configura en puertos donde se vayan a conectar usuarios finales y queremos evitar que dispositivos no autorizados obtengan acceso a la red.

Configuración estándar 802.1X

```
switchport mode access
switchport nonegotiate
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
spanning-tree portfast
```

Configuración fallo autenticación 802.1X

```
switchport mode access
switchport nonegotiate
authentication event fail action authorize vlan 10
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
spanning-tree portfast
```

Configuración sin suplicante 802.1X

```
switchport mode access
switchport nonegotiate
authentication event no-response action authorize vlan 1
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
spanning-tree portfas
```

Anexo 4 Pasos a seguir en configuración de switch

1. Consejos previos a la configuración

- Configurar nombre de equipo.
- Definir política de contraseñas.
- Creación de cuentas con privilegios de usuario y administrador.
- Configurar tiempo de inactividad.
- Añadir mensaje de banner.

2. Servicios de red para la gestión del switch

- Deshabilitar HTTP/HTTPS.
- Deshabilitar TELNET.
- Configurar SNMPv3 si es necesario.

3. Seguridad basada en puertos

- Deshabilitar puertos inactivos.
- Limitar mensajes que llegan a los puertos, *Storm Control*.
- Definición de MAC seguras.
- Limitar número de MACs.
- Creación de ACLs.

4. VLANs

- VLAN diferente para enlaces inactivos.
- Cambiar todos los puertos que no sean de gestión a una VLAN diferente a la nativa.

5. STP

- Configurar puertos de acceso como *Port Fast*.
- Habilitar *BPDU Guard*.
- Uso de *Root Guard*.

6. Registros: Logs

- Configurar registros y depuración de mensajes.
- Configurar servidor NTP.

7. Protocolo AAA

- Configuración de un servicio de acceso a los servidores de seguridad.