Implementación de un Sistema de Control de Acceso a la Red Cableada del metro de Medellín mediante Cloudpath

David Alexander Sánchez García

Informe de práctica presentado como requisito parcial para optar al título de Ingeniero de Telecomunicaciones

Modalidad de Práctica

Semestre de Industria o Práctica Empresarial

Asesor

Prof. Sergio Armando Gutiérrez, Ph.D.

Universidad de Antioquia

Facultad de Ingeniería

Ingeniería de Telecomunicaciones

Medellín, Antioquia, Colombia

2024

Cita	Sánchez García [1]
Referencia Estilo IEEE (2020)	[1] Sánchez García, “Implementación de un sistema de control de acceso a la red cableada del metro de Medellín, mediante Cloupadth” Informe de práctica, Ingeniería de Telecomunicaciones, Universidad de Antioquia Medellín, Antioquia, Colombia, 2025.

Dedicatoria

A mi mamá ,familia y amigos por ser el motor para cumplir este sueño.

TABLA DE CONTENIDO

LISTA DE FIGURAS

SIGLAS, ACRÓNIMOS Y ABREVIATURAS

IEEE Institute of Electrical and Electronics Engineers

Vlan Virtual Local Area Networks

LAN Local Area Network

NAC Network Access Control

RFC Request for Comments

API Application Programming Interface

DA Active Directory

DPSKs Dynamic pre-shared keys

MAC Media Access Control

RESUMEN

En varios procesos que se tenían asignados en la compañía, como el apoyo en tareas relacionadas con el sistema de control de acceso, soporte de la red LAN y red inalámbrica, identifiqué un gran interés por el control de acceso en la red LAN, un área llena de desafíos y retos. Inicialmente, esta red carecía de controles de acceso, permitiendo que cualquier persona pudiera conectarse a la red, lo que representaba un riesgo significativo para la seguridad de la organización.

Por ello, se desarrolló un proyecto conjunto con el Metro de Medellín, la empresa Ticline y Ruckus, para implementar una solución que garantizara que solo usuarios autorizados pudieran acceder a la red cableada. Este proyecto se aprovechó de la experiencia previa de dichas compañías en la gestión de la red inalámbrica (Control de acceso a la red Inalámbrica mediante Cloupath), enfrentando el desafío de integrar una solución similar en la red cableada (LAN). Esta red Inalámbrica cuenta con un portal de Cloudpath donde se integra las redes WLAN Metro (Conectividad para equipos de propiedad Metro de Medellín), Gente Metro (Conectividad para Equipos de colaboradores) e Invitado Metro (Conectividad para contratistas y visitantes).

Palabras clave — Cloudpath**,** Mac, Control de acceso, Sistema, Protocolo.

ABSTRACT

In various processes within the company, such as supporting tasks related to the access control system, LAN support and wireless network, I identified a strong interest in access control on the LAN, an area full of challenges and challenges. Initially, this network was unrestricted, allowing anyone to connect to the network, which represented a significant security risk for the organization.

Therefore, a joint project was developed with Metro de Medellín, Ticline and Ruckus to implement a solution that would ensure that only authorized users could access the wired network. This project took advantage of the previous experience of these companies in the management of the wireless network (access control to the wireless network through Cloupath), facing the challenge of integrating a similar solution in the wired network (LAN). This wireless network has a Cloudpath portal where the Metro WLAN (connectivity for Metro de Medellin property equipment), Gente Metro (connectivity for collaborators' equipment) and Invitado Metro (connectivity for contractors and visitors) are integrated

Keywords— Cloudpath,Mac, Control de acceso, Sistema,Protocolo.

INTRODUCCIÓN

El problema central que se abordó en este proyecto de semestre de industria es la mitigación a la falta de controles de acceso efectivos en las redes corporativas cableadas, lo que permite que cualquier dispositivo o usuario se conecte sin las restricciones de seguridad necesarias. Esta falta de controles introduce una vulnerabilidad que pone en riesgo la red, exponiéndose a accesos no autorizados y posibles amenazas a los datos y servicios críticos.

Para abordar este problema, se realizó la implementación del Cloudpath (Network Access Control, NAC), una herramienta integral que gestiona el acceso seguro de usuarios y dispositivos, mediante mecanismos avanzados tales como el uso de certificados digitales y autenticación por medio de credenciales. Esta solución centraliza el control de acceso a través de la aplicación de políticas de seguridad estrictas para el acceso, asegurando que solo usuarios y dispositivos verificados puedan acceder a los recursos de la red.

Con el despliegue de una herramienta como Cloudpath se busca fortalecer significativamente la seguridad de la red cableada, garantizando un acceso controlado y gestionado de manera efectiva. El principal desafío en la red cableada es integrar sistemas con infraestructura y configuraciones heterogéneas. Esta heterogeneidad requiere un enfoque específico para garantizar la interoperabilidad entre los elementos de infraestructura, asegurando que funcionen de manera coordinada. La clave está en implementar una solución que permita la interacción eficiente de los distintos sistemas, tales como directorio activo y servidores, sin afectar la estabilidad ni la seguridad de la red. Se realizó el despliegue y ajuste de la plataforma de control de acceso, procurando la interoperabilidad y minimizando los tiempos de configuración y posibles fallos durante la integración, para lograr una operación fluida y segura.

1. OBJETIVOS

1.1 Objetivo general

Fortalecer la seguridad de la red cableada corporativa mediante la implementación de un sistema robusto de autenticación y control de acceso, que garantice que solo usuarios y dispositivos autorizados puedan conectarse a la red, para proteger y garantizar de manera efectiva la integridad, confidencialidad y disponibilidad de los datos corporativos.

1.2 Objetivos específicos

- Desarrollar e implementar la separación del tráfico en la red mediante la creación de Vlans específicas para controlar el acceso de los usuarios además de un protocolo de autenticación con el fin de mejorar la seguridad y la eficiencia operativa.
- Desplegar una plataforma de control de acceso para gestionar de manera segura la conexión a la red corporativa mediante acceso cableado, con el fin de garantizar que solo usuarios y dispositivos autorizados puedan acceder a los recursos.
- Diseñar e implementar un mecanismo de monitoreo y evaluación continua para verificar la correcta integración y funcionamiento del sistema de control de acceso.
- Desarrollar un proceso integral de revisión y ajuste continuo del sistema de autenticación y control de acceso, con el fin de garantizar la seguridad y estabilidad de la red cableada a largo plazo.

2. MARCO TEÓRICO

La base teórica de este proyecto se fundamenta en los principios esenciales de seguridad de redes y en el control de acceso implementado mediante el despliegue de una plataforma de control de acceso a la red (Network Access Control, NAC por su acrónimo en inglés) [1]. Este enfoque es

crucial para la gestión del acceso a la red cableada, asegurando que solo los usuarios y dispositivos autorizados puedan conectarse a los recursos de la red corporativa.

2.1 Separación de la Red Mediante VLAN Específicas

Una VLAN (Red de Área Local Virtual) es una agrupación lógica de recursos de red conectados a puertos definidos administrativamente en un switch. Esta práctica limita la exposición de la red y asegura que cada dispositivo solo tenga acceso a los recursos que le corresponden. De esta manera, se segmenta la red, garantizando que cada equipo esté en la VLAN correspondiente al área. La integración de Cloudpath con VLAN mejora el control y la visibilidad sobre el tráfico de red. Esto se logra mediante la asignación automática de VLANs basada en la autenticación y validación de los dispositivos o usuarios [2].

Es por esta razón que lo primero que se realiza es un laboratorio de pruebas, donde se puede segmentar la red sin afectar los servicios en producción. Este laboratorio se divide en dos partes: en la primera etapa, se utiliza un switch Ruckus ICX 7150-24P [3] para llevar a cabo la configuración siguiendo las instrucciones detalladas en la guía técnica de Ruckus [4]. Una vez configurado y validado el primer laboratorio, se procede con la segunda etapa, en la que se emplea un switch de pruebas Alcatel-Lucent OS6560-P24Z8 [5]. Este último se conecta a la red LAN para homologar los comandos de manera correcta y preparar el despliegue sectorizado.

2.2 Control de Acceso a la Red (NAC)

Esta es una de las tantas soluciones que existen en seguridad de las redes, ya que permite a las organizaciones implementar políticas de control de acceso a la red. Este sistema utiliza una combinación de políticas y protocolos para autenticar y autorizar tanto a dispositivos como a usuarios antes de permitirles el acceso a los recursos de la red.

Los sistemas NAC son capaces de denegar el acceso a dispositivos no conformes, que son aquellos equipos que no cumplen con las políticas de seguridad previamente establecidas por la organización. En estos casos, el NAC puede colocar dichos dispositivos en áreas de cuarentena o concederles acceso restringido. Este enfoque es fundamental para prevenir que dispositivos inseguros comprometan la integridad y seguridad de la red. Se logra evidenciar que un gran número de personas (Contratistas y visitantes) acceden a la red y que no cuentan con permisos

para ello.Este tipo de problemas son los que se abordan mediante soluciones como cloudpath, cuyo funcionamiento se explica a continuación.[6].

2.2.1 Funcionamiento Cloudpath

La función principal del sistema es restringir el acceso a la red, permitiendo la conexión únicamente a dispositivos autorizados mediante certificados digitales o autenticación basada en direcciones MAC (Media Access Control). La autenticación mediante certificados digitales se implementa principalmente para eliminar el uso de contraseñas compartidas, mejorando así la seguridad de la red. Cada usuario o dispositivo cuenta con un certificado único que actúa como su identificación. Para dispositivos estáticos, como impresoras, sistemas de aire acondicionado y otros equipos sin capacidad de autenticación avanzada, se utiliza la autenticación mediante dirección MAC.

La información de autenticación es gestionada y validada a través del Directorio Activo (Active Directory, AD por su sigla en inglés) y un servidor RADIUS, que se encargan de verificar las credenciales y otorgar el acceso a la red. En este proceso, Cloudpath se integra con el servidor RADIUS, facilitando la validación y el control de acceso. Aquellos dispositivos que no cumplen con la autenticación inicial son redirigidos a un portal cautivo (https://cloudpath.metrodemedellin.gov.co/enroll/MetrodeMedellin/DPSK_Produccion/process), donde los usuarios deben iniciar sesión con sus credenciales. Una vez autenticados, se descarga un certificado digital que contiene la clave necesaria para conectar de forma segura el dispositivo a la red.

2.2.2 Protocolo 802.1x

El protocolo 802.1X, conocido también como dot1x (forma abreviada para referirse al acrónimo de 802.1X, que describe su especificación técnica), es un estándar de seguridad que pertenece a la familia IEEE 802. Su principal objetivo es proporcionar un control de acceso robusto tanto para redes cableadas como inalámbricas, mediante un modelo de autenticación que verifica la identidad de los usuarios o dispositivos antes de otorgarles acceso a la red [7]. Este protocolo opera asegurando que cada dispositivo conectado sea autenticado correctamente a través de sistemas como RADIUS y métodos de autenticación avanzados, como EAP-TLS con certificados digitales.

En el caso de redes cableadas, como en la infraestructura considerada en este proyecto, 802.1X se emplea para garantizar la autenticación segura a nivel de puerto en los switches. Este protocolo evita accesos no autorizados y asegura que únicamente los dispositivos y usuarios verificados puedan interactuar con los recursos de la red.

2.2.3 Componentes Protocolo 802.1x

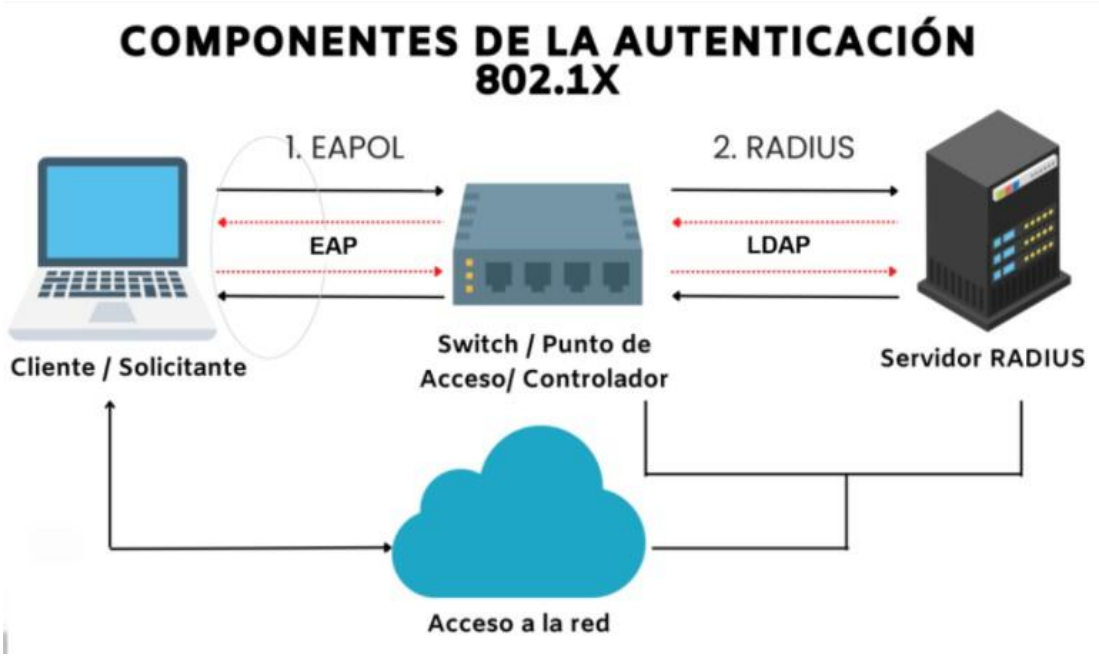

Fig. 1. Comunicación y componentes de protocolo 802.1x.

Este protocolo está diseñado para trabajar en conjunto con diferentes mecanismos de autenticación como lo son los servidores RADIUS (Remote Authentication Dial-In User Service) [8] .

Los componentes principales del protocolo 802.1X son tres. El primero es el solicitante, que corresponde al dispositivo que necesita acceder a la red, como una computadora, teléfono u otro equipo. Este dispositivo envía sus credenciales de autenticación al siguiente componente, el autenticador. En nuestro caso, el autenticador es el switch donde se integró Cloudpath para gestionar el proceso de control de acceso. Estos switches, configurados para soportar 802.1X, actúan como intermediarios entre el solicitante y el servidor de autenticación. Por último, el tercer componente es el servidor de autenticación RADIUS, encargado de validar las credenciales enviadas por el solicitante.

La comunicación entre el cliente (solicitante), el autenticador (switch) y el servidor RADIUS se realiza mediante el protocolo EAP (Extensible Authentication Protocol), que soporta múltiples métodos de autenticación. Asimismo, la validación de las credenciales con el Directorio Activo utiliza el protocolo LDAP (Lightweight Directory Access Protocol), que facilita el acceso y la verificación en servicios de directorio centralizados.

2.2.4 Protocolo EAP

El protocolo EAP (Extensible Authentication Protocol) está definido en el RFC 3748 [9]. Es un estándar de autenticación que habilita una amplia gama de tecnologías, como el acceso mediante IEEE 802.1X en redes cableadas. EAP permite tanto al solicitante como al autenticador utilizar diferentes métodos de autenticación ajustados a las necesidades específicas del sistema.

EAP encapsula diversos mecanismos de autenticación dentro de su marco, lo que le da flexibilidad para soportar métodos basados en contraseñas, tokens, certificados digitales y criptografía de clave pública. Su diseño altamente extensible permite que se integre con tecnologías de autenticación emergentes, garantizando su relevancia en entornos de seguridad modernos.

El funcionamiento del protocolo se basa en un intercambio de mensajes entre el cliente (solicitante) y el servidor (autenticador), donde se negocia y establece el método de autenticación a utilizar. Una vez seleccionado, EAP facilita el proceso de autenticación, asegurándose de que las credenciales del cliente sean verificadas correctamente antes de otorgar acceso a la red.

2.2.5 Protocolo LDAP

LDAP (Lightweight Directory Access Protocol) o también conocido como «Protocolo Ligero de Acceso a Directorios» Hace parte del conjunto de protocolos TCP/IP que permite el acceso a un servicio de directorio ordenado y distribuido, para buscar cualquier información en un entorno de red. LDAP permite acceder a los recursos de la red local en este caso del Directorio Activo, donde puede realizar tareas de autenticación y autorización [10]. Este protocolo tiene la arquitectura Cliente – Servidor, donde se establece una conexión e intercambian datos.

2.2.6 Servidor RADIUS

El servidor RADIUS (Remote Authentication Dial-In User Service) es un sistema esencial para la seguridad en redes corporativas, diseñado para cumplir con tres funciones principales: autenticación, autorización y contabilidad (Authentication, Authorization, and Accounting - AAA). A través de la autenticación, valida las credenciales enviadas por el solicitante (usuario) mediante el autenticador, asegurando que solo usuarios autorizados puedan acceder a la red. Posteriormente, en la etapa de autorización, asigna permisos específicos que determinan los recursos y servicios a los que puede acceder el usuario, en función de las políticas de la organización. Finalmente, con la función de contabilidad, registra y monitorea las actividades del usuario, como la duración de la conexión y los recursos utilizados, proporcionando una trazabilidad completa para auditorías y control[11]. a través de políticas de
seguridad estrictas para el accesoEstas características convierten al servidor RADIUS en un componente clave para gestionar el acceso, garantizar la seguridad y mantener el control de la red.

RADIUS también permite monitorear, controlar y registrar las actividades de acceso a la red, facilitando la administración de usuarios y dispositivos. Es compatible con diversos protocolos y puede integrarse con sistemas de autenticación basados en LDAP, lo que lo convierte en una herramienta versátil para gestionar el acceso a redes corporativas de manera segura y eficiente.

2.3 Cloudpath y su función en la seguridad de redes

La seguridad de las redes corporativas es un desafío crítico en la actualidad, dado el crecimiento de las amenazas y la complejidad de las infraestructuras tecnológicas. En este contexto, Cloudpath emerge como una solución avanzada de NAC, diseñada para gestionar y proteger el acceso tanto a redes cableadas como inalámbricas [12].

2.3.1 Seguridad Continua

Cloudpath proporciona un control centralizado y robusto del acceso a la red mediante autenticación basada en certificados digitales y la integración con protocolos como 802.1X. Esta autenticación garantiza que sólo los dispositivos y usuarios autorizados puedan conectarse, reduciendo significativamente las vulnerabilidades asociadas con contraseñas compartidas.

Además, Cloudpath es compatible con la infraestructura existente de cualquier proveedor, lo que facilita su implementación en redes heterogéneas [13].

2.3.1 Interoperabilidad y flexibilidad

Una de las características más relevantes de Cloudpath es su interoperabilidad y flexibilidad, que le permite integrarse de manera eficiente con productos de terceros a través de APIs [14]. Esta capacidad de integración amplía las funcionalidades de seguridad y mejora la experiencia del usuario, permitiendo que Cloudpath se adapte fácilmente a infraestructuras tecnológicas preexistentes en diversas organizaciones. La flexibilidad del sistema facilita la implementación de controles de acceso personalizados, ajustados a las necesidades específicas de cada entorno, lo que resulta en una solución de seguridad más robusta y escalable. Además, esta interoperabilidad permite la implementación de políticas de acceso más estrictas, garantizando que cada dispositivo y usuario se autentique de acuerdo con los requisitos de seguridad, sin comprometer la eficiencia operativa ni la facilidad de gestión.

2.4 Despliegue flexible y Multi-tenancy

Cloudpath ofrece opciones de despliegue tanto en la nube como en instalaciones locales, lo que proporciona flexibilidad a las organizaciones para elegir la solución que mejor se adapte a su infraestructura y políticas de seguridad. Además, su arquitectura Multi-tenancy [15] integrada permite gestionar múltiples redes o segmentos desde una plataforma centralizada, optimizando la administración de recursos. Esto trae consigo beneficios clave como el licenciamiento rentable por cada usuario, su facilidad de uso, ya que la plataforma se destaca por su interfaz intuitiva, lo que facilita la gestión y el monitoreo de los accesos a la red.

2.5 Integración con Infraestructura Actual

El control de acceso en redes es fundamental para garantizar la seguridad y el correcto funcionamiento de los sistemas de información en una organización incluso en entornos donde no sea tan fácil su adecuación. Este mecanismo permite establecer políticas claras sobre quiénes pueden ingresar a la red, bajo qué condiciones y qué recursos pueden utilizar, limitando así las acciones de usuarios no autorizados que podrían comprometer la integridad y la confidencialidad de los datos sensibles. Además, es esencial para prevenir diversos tipos de ciberataques.

Así mismo, el control de acceso facilita la auditoría y el monitoreo continuo de las actividades de los usuarios dentro de la red, permitiendo detectar y responder a posibles vulnerabilidades o incidentes de seguridad de manera oportuna. De esta forma, las organizaciones pueden no solo proteger sus activos digitales, sino también cumplir con normativas y estándares internacionales de seguridad. Este enfoque holístico fortalece la confianza en la infraestructura tecnológica y asegura que los datos estén disponibles sólo para aquellos con los permisos adecuados, maximizando la protección contra amenazas externas e internas.

3. METODOLOGÍA

Este proyecto siguió un enfoque mixto, dividiéndose en varias etapas clave: evaluación inicial de la red, implementación del Cloudpath, pruebas y validación, monitoreo continuo.

En la primera etapa se analizó la infraestructura existente, realizando reuniones periódicas con personal de nivel 2 para la validación de activación de protocolos como 802.1x masivamente e identificando los dispositivos conectados. En estas reuniones se habló del impacto del proyecto además de los requerimientos que podían salir de él. También se abordaron elementos claves a tener en cuenta en toda la ejecución del proyecto. En esta primera etapa se llevaron las actividades de:

- Creación de una guía para la habilitación del protocolo 802.1x.
- Descarga del certificado del Cloudpath en los servidores de dominio de la organización.

La segunda etapa del proyecto se desarrolló en dos laboratorios de pruebas con el objetivo de garantizar la integración y compatibilidad entre diferentes equipos en la infraestructura de la organización. En el primer laboratorio, se utilizó un switch Ruckus ICX 7150-24P, siguiendo los pasos detallados en la guía de configuración de Cloudpath para validar su correcto funcionamiento. Este equipo fue elegido por su compatibilidad directa con Cloudpath, lo que permitió realizar pruebas sin inconvenientes gracias a las instrucciones claras proporcionadas en la documentación técnica [3]. Posteriormente, se realizó el segundo laboratorio con un switch Alcatel-Lucent OS6560-P24Z8, parte de la infraestructura actual de la organización. Durante esta fase, se trabajó con el contratista encargado de los equipos Alcatel-Lucent para adaptar y alinear

los comandos de configuración, asegurando que el switch Alcatel pudiera operar de forma equivalente al switch Ruckus. Este proceso garantiza la compatibilidad y coherencia entre ambos dispositivos, permitiendo una integración eficiente con Cloudpath y el correcto funcionamiento de la infraestructura de red.

Estas pruebas se realizaron de la siguiente manera:

- Las pruebas por parte del contratista de los Switch Alcatel se llevaron a cabo durante dos semanas, donde se realizó homologación de comandos y un estudio de la expansión en toda la red.
- Creación de Script donde se encuentra registrada toda la homologación de comandos y su correcto funcionamiento.
- Manual de guía para las diferentes versiones de software de los switches Alcatel Lucent.

En esta última etapa, se realiza un monitoreo continuo utilizando una plataforma de gestión, donde se puede observar qué usuarios están conectados a la red. Una vez que un dispositivo ha instalado el certificado, es posible verificar el estado de conexión, así como los equipos registrados para cada usuario. Esta herramienta permite gestionar y auditar los accesos, facilitando la administración de dispositivos y usuarios dentro de la red.

4. ANÁLISIS DE RESULTADOS

En esta sección se presentarán los resultados obtenidos durante el proceso de implementación del Cloudpath, sus problemas y soluciones hasta llegar a la correcta implementación.

4.1 Resultados del laboratorio de pruebas número 1

En este laboratorio se crea una imagen muy global del segmento de red donde se proceden a realizar las primeras pruebas de este proyecto.

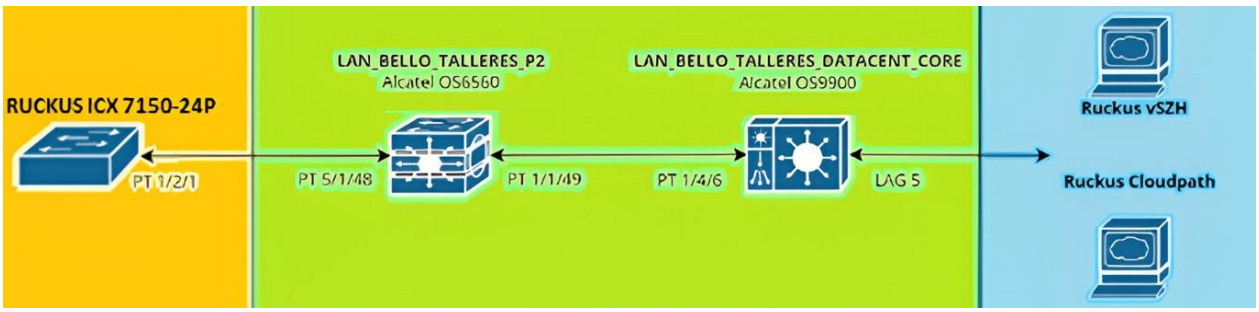

Fig. 2. Montaje Laboratorio Pruebas con Switch Ruckus.

El primer paso consiste en integrar el switch Ruckus ICX 7150 a la infraestructura existente, conectándose a través de los switches Alcatel-Lucent, que actúan como intermediarios para facilitar la comunicación hasta el sistema Cloudpath. Tal como se muestra en la figura. Este diseño garantiza una conectividad estable y segura, permitiendo la integración fluida entre la infraestructura de red y los sistemas de control de acceso, optimizando tanto la gestión de tráfico como la seguridad de la red.

Esta evaluación permitirá obtener una visión integral de la red, identificando los primeros equipos que se verán impactados por la implementación, asegurando una transición fluida y sin interrupciones en el servicio.

A continuación, se procede a diseñar la separación del tráfico mediante la creación de VLANs específicas, que permiten controlar el acceso de los usuarios, mejorando la seguridad y maximizando el rendimiento operativo de la red. Esta estrategia de segmentación es esencial para aislar diferentes tipos de tráfico, asignando cada dispositivo autenticado a una subred controlada según su perfil de acceso. Sin embargo, una incorrecta definición de los segmentos de red puede generar conflictos dentro de la infraestructura, afectando negativamente el desempeño y la estabilidad. Por ello, es fundamental realizar una planificación adecuada que garantice una segmentación eficiente y alineada con los objetivos operativos y de seguridad de la organización.

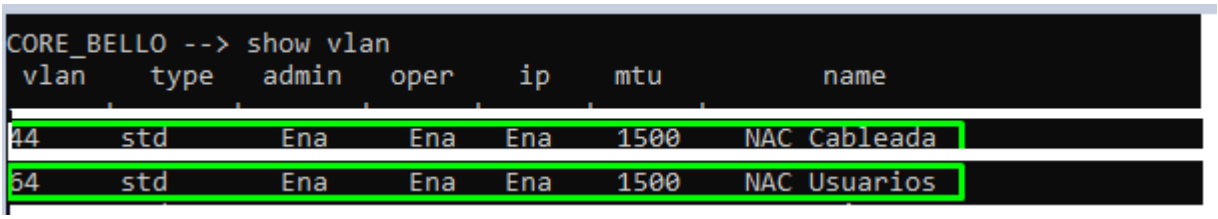

Fig. 3. Creación de las Vlan para la separación del Tráfico desde el Core.

Las VLAN 64 y VLAN 44 han sido configuradas en el Core de la red para gestionar el tráfico de autenticación y acceso mediante Cloudpath. La VLAN 44 se encarga de la comunicación entre los switches y el servidor Cloudpath, permitiendo el intercambio seguro de información de autenticación. Por otro lado, la VLAN 64 actúa como una zona restringida, donde los usuarios sin certificados válidos acceden al portal cautivo para completar el proceso de autenticación y descarga de certificados digitales.

El enlace Linkagg 5, visible en la parte derecha de la Figura 1, está diseñado para gestionar la comunicación directa con el servidor Cloudpath, garantizando un tránsito seguro entre los dispositivos y el servidor. En cuanto a la infraestructura de conexión, el switch del piso 2 de los talleres se enlaza con el Core, y a través de este, se establece una conexión segura con el switch Ruckus, lo que asegura una comunicación fluida entre los distintos segmentos de la red. Este diseño asegura una correcta segmentación de la red y gestiona la autenticación de dispositivos y usuarios de manera adecuada a través de Cloudpath, mejorando el control de acceso y la seguridad de los recursos de la red. Las VLANs adicionales, como las de invitados y las de áreas específicas de acceso tradicional ya existentes, se mantendrán en funcionamiento, garantizando una segmentación adecuada del tráfico en toda la red.

A continuación se procede con la configuración del Switch de Ruckus con la ayuda de la guía [3], se implementan los comandos con resultados positivos.

4.2 Resultados del laboratorio de pruebas número 2

Al igual que en el laboratorio 1, se mantiene la misma topología de red, con la única diferencia de que el switch Ruckus es reemplazado por el Alcatel. Se llevó a cabo la homologación de comandos 1:1, proceso que se realiza mediante consultas y datasheets, en los cuales se especifica qué se desea ejecutar en cada línea de código, para luego implementarlo. No obstante, se observó que la creación del portal cautivo presenta diferencias significativas, especialmente en lo relacionado con el redireccionamiento hacia la red del portal, lo que llevó consultas y aplicaciones de lo encontrado.

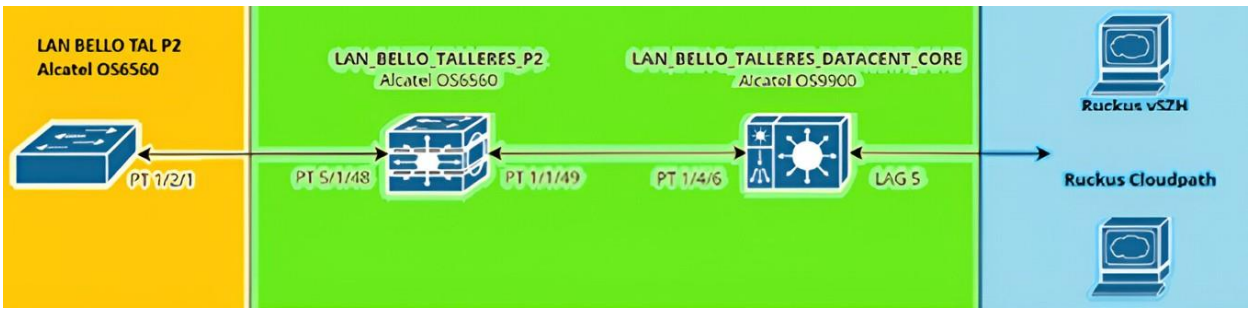

Fig. 4. Montaje Laboratorio Pruebas con Switch Alcatel.

4.3 Redireccionamiento al Portal Cautivo

En esta sección se detallan el funcionamiento del portal cautivo y el proceso por el cual los usuarios son redirigidos al portal al conectarse a un puerto del switch. Se observa que, en esta red sin acceso a internet, es necesario seleccionar la red WLAN Metro para autenticarse con las credenciales corporativas, lo que permite al usuario ser enrutado a la red correspondiente a su dependencia. Además, se asignan direccionamiento en una VLAN específica junto con los parámetros de red necesarios para su acceso.

En este portal cautivo se va a redireccionar a cualquier persona que intente conectarse a la red y solo si tiene credenciales válidas puede loguearse y acceder a la red. Toda esta sección es autogestionable por cada usuario y así poder facilitar tiempos de instalación y ejecución.

Fig.5. Portal Cautivo de acceso a la red.

4.4 Registro con credenciales correctas

Una vez seleccionamos la red Wlan Metro, se tiene una interfaz de Login, donde solo personas registradas en el DA con credenciales válidas pueden descargar el certificado del Cloudpath. Estas credenciales son las más recientes, debido a que por políticas del DA se están actualizando constantemente.

4.5 Descarga Certificado

Si se tienen credenciales válidas, se accede a la descarga del certificado del Cloudpath. Este certificado tiene vigencia de un año, tiene un algoritmo hash de firma sha256, con una clave pública RSA (2048 Bits), además de estar ligado a la dependencia en la que se encuentra.

Fig. 6. Descarga del Certificado.

4.6 Instalación Certificado y conexión

Una vez descargado el certificado, se procede a su instalación, la cual se observa en la Figura 8. También se obtiene una IP válida de la dependencia en la que se encuentra el usuario, de manera que pueda acceder a los servicios de red. Todo este proceso anterior dura alrededor de 5 minutos y es auto gestionable por cada usuario permitiendo un acceso seguro, solo por medio de las credenciales.

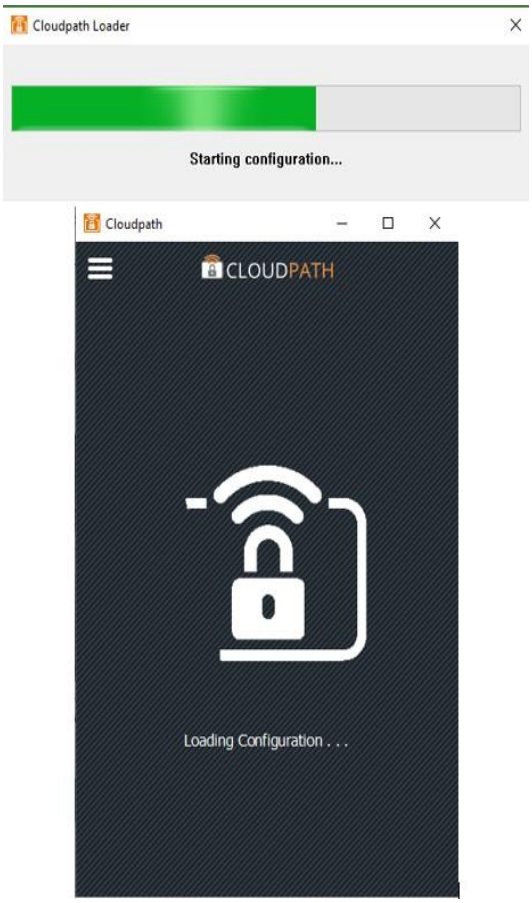

Fig. 7. Instalación del Certificado.

4.7 Plataforma Cloudpath

En esta sección, se presenta la plataforma Cloudpath, una solución de Multi-Tenancy descrita en la sección 2.4 del marco teórico. Al acceder a la plataforma, el sistema muestra una interfaz de bienvenida que incluye una imagen representativa del flujo de trabajo, como se observa en la Figura 10. Esta plataforma es clave para la gestión continua de las conexiones, ya que implementa un mecanismo de monitoreo y evaluación que permite realizar un seguimiento constante del sistema de autenticación. A través de este proceso, Cloudpath lleva a cabo una revisión integral y ajustes periódicos al sistema, garantizando una gestión efectiva y segura del acceso a la red.

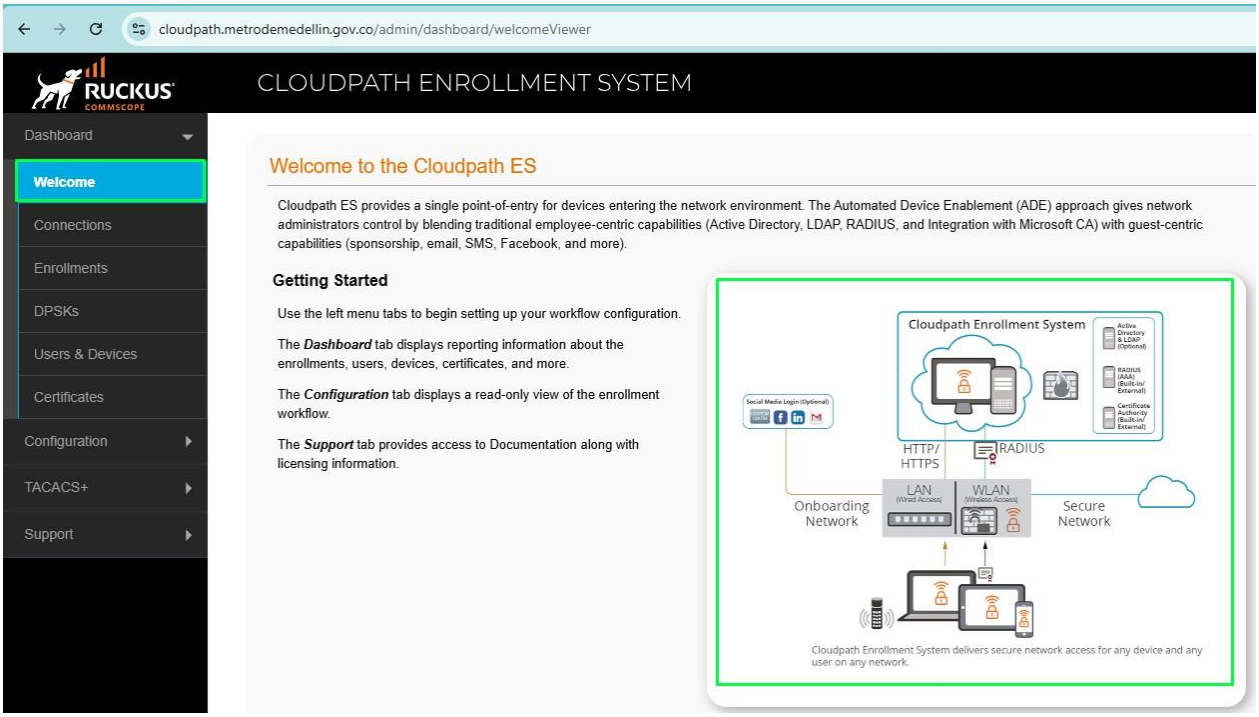

Fig. 8. Plataforma Cloudpath.

A continuación, se pueden visualizar todas las conexiones a la red, donde se proporciona información detallada, como la IP asignada, la dirección MAC del dispositivo, el nombre del certificado y la duración de la conexión. Además, se muestra el estado de las inscripciones a la red, incluyendo el estado del certificado, el nombre del usuario, el nombre del dispositivo conectado y su sistema operativo. También se incluye el nombre común del dispositivo, que varía según el área a la que pertenece (por ejemplo, @Administrativa, @Financiera, @Tecnología, etc.), así como la fecha de vencimiento del certificado.

En la sección de Dynamic pre-shared keys por sus siglas DPSKs (Figura [10]), se puede observar el estado de los certificados, mostrando los activos, revocados y expirados, además de las dependencias organizacionales y estadísticas sobre los días con mayores conexiones. El sistema DPSKs mejora la seguridad al proporcionar claves únicas y temporales para cada usuario o dispositivo, facilitando así la gestión y garantizando un acceso más seguro.

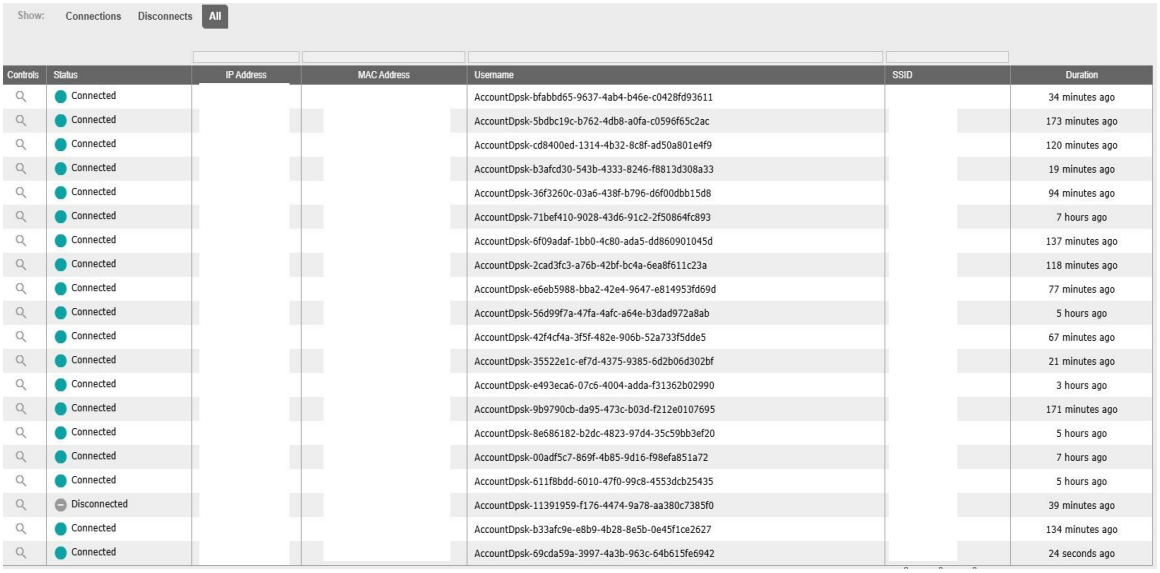

Fig. 9. Sección DPSKs.

Esta Figura 10 se observa como la plataforma muestra las conexiones durante un año, donde el eje Y representa la cantidad de certificados en el eje X los meses del año. A través de esta interfaz se obtiene información de los certificados activos, con el fin de dar un monitoreo constante, en cuanto van creciendo las áreas y las proyecciones en un futuro.

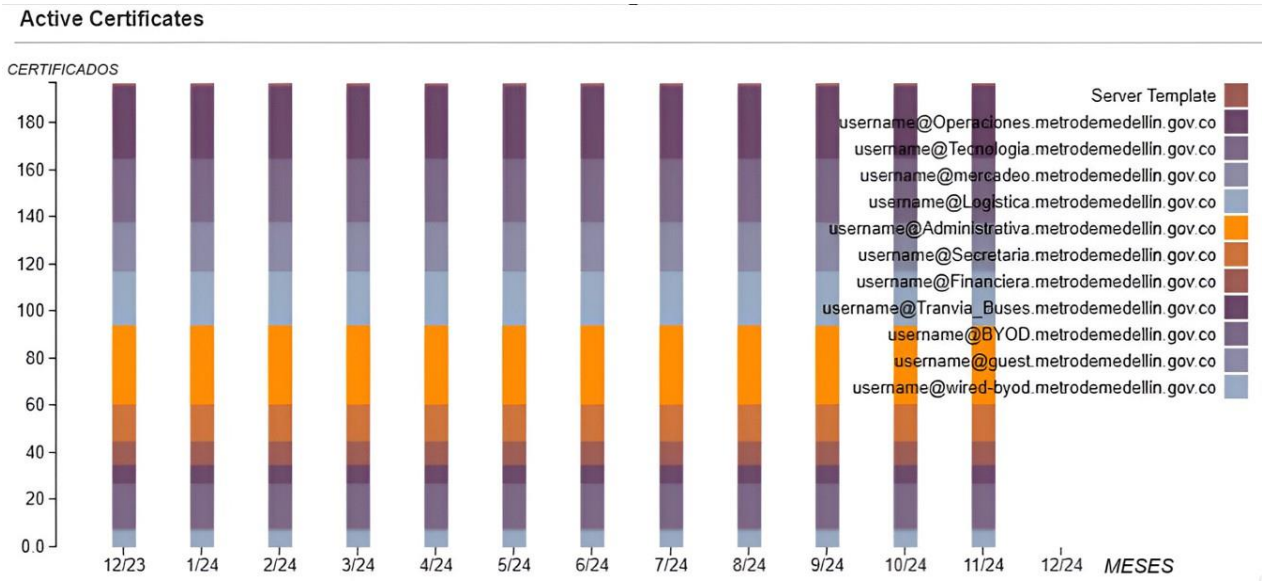

Fig. 10. Certificados Activos y Proyección Futura.

La sección de Users y Devices presenta información de los usuarios como su nombre de usuario, su área corporativa a la cual fue redireccionado, y el tipo de autenticación. En la sección de certificados se tiene el nombre común del certificado, su tiempo de inspiración, nombre del certificado y la política empleada por el servidor Radius que hace referencia al área donde pertenece el usuario.

VI.CONCLUSIONES Y RECOMENDACIONES

La implementación de Cloudpath ha sido un éxito rotundo, cumpliendo con los objetivos planteados y generando múltiples beneficios para la organización. Los principales logros alcanzados incluyen:

- Impacto en la seguridad: La implementación de Cloudpath ha fortalecido significativamente la seguridad de la red al reducir drásticamente los puntos de acceso no autorizados. La autenticación basada en certificados digitales ha minimizado el riesgo de intrusiones y ha garantizado que solo usuarios y dispositivos verificados puedan acceder a los recursos de la red.
- Mejora en la gestión: La plataforma Cloudpath ha simplificado considerablemente la gestión del acceso a la red, proporcionando una visibilidad completa de los dispositivos conectados y las actividades de los usuarios. Esto ha agilizado los procesos de administración y ha facilitado la detección y resolución de incidentes de seguridad.
- Automatización: La automatización de tareas como la asignación de VLANs y la generación de certificados ha reducido significativamente el tiempo dedicado a tareas manuales que se realizaban anteriormente. Como resultado cada dependencia y sus usuarios correspondientes realizan la autogestión de la red.
- Conformidad normativa: La implementación de Cloudpath ha contribuido a cumplir con los requisitos de seguridad establecidos en las normas y regulaciones aplicables, mejorando la postura de seguridad de la organización y reduciendo el riesgo de sanciones.
- Lecciones aprendidas: Durante la implementación del proyecto, se identificó la importancia de una adecuada capacitación del personal para garantizar la adopción exitosa de la nueva solución. Además, se evidenció la necesidad de contar con una documentación detallada de los procesos y configuraciones para facilitar el mantenimiento y la resolución de problemas.

Departamento de Ingeniería Electrónica y de Telecomunicaciones

Implementación de un Sistema de Control de Acceso a la Red Cableada del metro de Medellín mediante Cloudpath

UNIVERSIDAD DE ANTIOQUIA
Facultad de Ingeniería

PRACTICANTE: David Alexander Sánchez García
ASESORES: Sergio Armando Gutierrez Betancur, Vladimir Londoño Lozano
PROGRAMA: Ingeniería de Telecomunicaciones
Semestre de la práctica: 2024-2

Introducción

El proyecto abordó la falta de controles de acceso en redes corporativas cableadas, un problema que permitía conexiones no autorizadas y exponía los recursos críticos de la organización a vulnerabilidades y amenazas de seguridad.

Para resolver esta situación, se implementó Cloudpath, una herramienta NAC (Network Access Control) que gestiona el acceso seguro mediante certificados digitales y autenticación con credenciales.

Este sistema centraliza el control de acceso, aplicando políticas de seguridad estrictas que garantizan conexiones exclusivamente para usuarios y dispositivos verificados.

Un desafío clave fue la integración de sistemas con infraestructuras y configuraciones heterogéneas, como directorios activos y servidores. Se logró una interoperabilidad eficiente a través del despliegue y ajuste de la plataforma, minimizando tiempos de configuración y posibles errores, y asegurando un funcionamiento coordinado, estable y seguro de la red cableada.

Objetivos

- Desarrollar e implementar la separación del tráfico en la red mediante la creación de Vlans específicas para controlar el acceso de los usuarios además de un protocolo de autenticación con el fin de mejorar la seguridad y la eficiencia operativa.
- Desplegar una plataforma de control de acceso para gestionar de manera segura la conexión a la red corporativa mediante acceso cableado, con el fin de garantizar que solo usuarios y dispositivos autorizados puedan acceder a los recursos.
- Diseñar e implementar un mecanismo de monitoreo y evaluación continua para verificar la correcta integración y funcionamiento del sistema de control de acceso.
- Desarrollar un proceso integral de revisión y ajuste continuo del sistema de autenticación y control de acceso, con el fin de garantizar la seguridad y estabilidad de la red cableada a largo plazo.

Metodología

Evaluación Inicial de la red → Implementación del Cloudpath → Pruebas y Validación → Monitoreo Continuo

Resultados

Conclusiones

- Impacto en la seguridad: La implementación de Cloudpath mejoró la seguridad al reducir accesos no autorizados y riesgos de intrusión, garantizando que solo usuarios y dispositivos verificados accedan a los recursos de la red mediante autenticación con certificados digitales.
- Mejora en la gestión: Cloudpath simplificó la gestión del acceso, brindando visibilidad total de los dispositivos conectados y facilitando la administración, detección y resolución de incidentes de seguridad.
- Automatización: Automatizó tareas como la asignación de VLANs y la generación de certificados, reduciendo tiempo en procesos manuales y permitiendo la autogestión de usuarios en la red.
- Lecciones aprendidas: Resaltó la importancia de capacitar al personal y contar con documentación detallada para garantizar una implementación exitosa y facilitar el mantenimiento.

DATOS DE CONTACTO DEL AUTOR:
+57 3054070255 +57 3054070255 dasanchezg@udea.edu.co http://ca.linkedin.com/in/david-garcia-5168062a9

REFERENCIAS

[1] R. Wireless, «Cloudpath Deployment Guide (Supporting Software Release 5.2),» 7 Ruckus Wireless, September 2017. [En línea]. Available: https://xpc.cloudpath.net/documents/ES_QuickStartGuide.pdf. [Último acceso: 10 October 2024].

[2] I. Corporation, «Redes de área local virtuales (VLAN),» Copyright IBM Corporation , 2020. [En línea]. Available: https://www.ibm.com/docs/es/aix/7.2?topic=cards-virtual-local-area-networks. [Último acceso: 10 10 2024].

[3] CommScope, «RUCKUS® ICX 7150 Enterprise-class stackable access switch,» 22 8 2022. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://es.ruckusnetworks.com/global assets/digizuite/61729-ds-icx-7150.pdf. [Último acceso: 10 10 2024].

[4] A. E. LLC, «Ruckus ICX Flexible Authentication with,» 05 02 2019. [En línea]. Available: file:///C:/Users/dasanchez/Downloads/NAC/ruckus-icx-flexible-auth-cloudpath-52-dp.pdf. [Último acceso: 01 10 2024].

[5] Alcatel-Lucent, «Alcatel-Lucent OmniSwitch 6560/E,» 11 2024. [En línea]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.al-enterprise.com/-/media/assets/internet/documents/omniswitch-6560-6560e-datasheet-en.pdf. [Último acceso: 01 10 2024].

[6] J. G. H. Alexa M Ramires, «Guía metodológica para la implementación de,» REVISTA COLOMBIANA DE COMPUTACIÓN, Bucaramanga, 2017.

[7] M. Seaman, «802.1X: Port-Based Network Access Control,» 2010. [En línea]. Available: https://1.ieee802.org/security/802-1x/. [Último acceso: 04 11 2024].

[8] Servidores, «Descubre para qué sirve un servidor RADIUS y su funcionamiento,» 15 05 2024. [En línea]. Available: https://www.redeszone.net/tutoriales/servidores/que-es-servidor-radius-funcionamiento/. [Último acceso: 04 11 2024].

[9] «Protocolo de autenticación extensible (EAP) para acceso a redes,» 28 06 2024. [En línea]. Available: https://learn.microsoft.com/es-es/windows-server/networking/technologies/extensible-authentication-protocol/network-access?tabs=eap-tls%2Cserveruserprompt-eap-tls%2Ceap-sim. [Último acceso: 15 10 2024].

[10] C. I. Corporation, «LDAP (Lightweight Directory Access Protocol),» 29 07 2024. [En línea]. Available: https://www.ibm.com/docs/es/ibm-http-server/8.5.5?topic=systems-lightweight-directory-access-protocol. [Último acceso: 15 10 2024].

[11] IBM, «Visión general de RADIUS (Remote Authentication Dial In User Service),» 07 10 2024. [En línea]. Available: https://www.ibm.com/docs/es/i/7.5?topic=authentication-remote-dial-in-user-service-overview. [Último acceso: 20 11 2024].

[12] R. Cloudpath, «DATA SHEET RUCKUS Cloudpath Enrollment System,» COMMSCOPE, 22 03 2022. [En línea]. Available: https://www.commscope.com/globalassets/digizuite/61721-ds-cloudpath.pdf. [Último acceso: 05 11 2024].

[13] A. International, «Sistema de gestión de red,» Alcatel-Lucent, 11 2023. [En línea]. Available: https://www.al-enterprise.com/-/media/assets/internet/documents/omnivista-2500-nms-datasheet-es.pdf. [Último acceso: 15 11 2024].

[14] COMMSCOPE, «Cloudpath Security and Management Platform,» 07 07 2021. [En línea]. Available: https://docs.commscope.com/bundle/cloudpath-511-deployment-admin-guide/page/GUID-6EEFD797-348C-42F5-8381-82A322B42DC5.html. [Último acceso: 15 11 2024].

[15] Cloudflare, «What is multitenancy? | Multitenant architecture,» Cloudflare, Inc, 2024. [En línea]. Available: https://www.cloudflare.com/learning/cloud/what-is-multitenancy/. [Último acceso: 15 11 2024].