https://doi.org/10.22201/dgtic.ctud.2024.2.3.66

Vol. 2, Núm. 3. julio-septiembre 2024, págs. 8 - 15

Red inalámbrica con asignación de VLAN dinámica

Información del reporte:

Para citar este reporte técnico:

Mares Mendoza, E. (2024). Red inalámbrica con asignación de VLAN dinámica. Cuadernos Técnicos Universitarios de la DGTIC, *2* (3) páginas(8 - 15).

https://doi.org/10.22201/dgtic.ctud.2024.2.3.66

Enrique Mares Mendoza

Dirección General de Cómputo y de Tecnologías de Información y Comunicación

Universidad Nacional Autónoma de México

enrique.mares@unam.mx

ORCID: 0009-0008-5529-0080

Resumen

El estudio examinó la necesidad de modernizar la infraestructura tecnológica de una dependencia incorporada a la UNAM, debido al aumento en el uso de dispositivos móviles y la demanda de acceso a Internet desde lugares remotos. Se propuso diseñar una red inalámbrica con un único SSID para gestionar múltiples VLAN, abordando así las limitaciones de las redes Wi-Fi existentes. La solución recomendada incluyó la asignación dinámica de VLAN mediante un servidor de autenticación RADIUS. La implementación se logró configurando cuidadosamente componentes como el controlador de LAN inalámbrica (WLC), puntos de acceso, servidor NPS, Active Directory, DHCP, IEEE 802.1X y EAP. Los resultados mostraron una correcta asignación de VLAN, mejorando la flexibilidad y la seguridad de la red, lo cual se confirmó mediante pruebas de acceso. Se enfatizó la importancia de implementar políticas de seguridad para limitar el acceso; en general, esta solución no solo mejoró la experiencia del usuario al admitir la conectividad y la movilidad de la red, sino que también proporcionó a los administradores un control de acceso más seguro y eficiente mediante una combinación de protocolos de autenticación y seguridad.

Palabras clave:

Servicios de red, políticas de acceso, acceso a información.

https://doi.org/10.22201/dgtic.ctud.2024.2.3.66 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 9 - 15

1. INTRODUCCIÓN

Durante los últimos años ha sido notorio el incremento en el uso de dispositivos móviles en la vida diaria. Esta creciente adopción de la tecnología móvil demanda una actualización en la manera en que se accede a Internet. El concepto de movilidad se refiere a las ventajas que brindan los dispositivos inalámbricos, los cuales permiten la interacción con diferentes áreas de trabajo y acceder a información en tiempo real desde cualquier ubicación.

En una dependencia perteneciente a la UNAM, se han instalado dispositivos de Wi-Fi para proporcionar la conectividad necesaria que permita el acceso a los diferentes servicios informáticos; sin embargo, las redes Wi-Fi implementadas tienen limitaciones en el acceso a la información ya que los usuarios que utilizan la red inalámbrica pertenecen a distintas áreas o son externos a la dependencia, por lo que, para acceder a cierta información específica, es necesario hacer una conexión cableada.

Cada área de la dependencia tiene necesidades específicas para el uso de la red de datos, por lo que ésta se divide en VLAN: "una red de área local virtual (Virtual Local Area Network o VLAN) es un segmento lógico más pequeño dentro de una gran red física cableada" (IONOS, 2019).

En los últimos años, ha habido un gran aumento de solicitudes de servicio por parte de personal de la dependencia, lo que ha generado la necesidad de escalabilidad en los nodos de red; no obstante, factores económicos y de infraestructura física limitan el crecimiento de la red cableada.

1.1 ANTECEDENTES

En las redes inalámbricas implementadas en las áreas de la dependencia, se aplica una política estática a todos los clientes asociados a un identificador de conjunto de servicios (SSID). Aunque efectivo, este método tiene limitaciones, ya que requiere que los clientes se asocien con diferentes SSID para heredar distintas políticas de calidad de servicio (QoS) y seguridad.

1.2 PROBLEMÁTICA

El problema surge de un mal funcionamiento del controlador de Wi-Fi, que complicó la administración de los dispositivos. Como solución temporal, se implementó el uso de Puntos de Acceso (AP) autónomos que se administraban de forma independiente, esto redujo las capacidades de los AP y provocó que las redes inalámbricas se restringieran a 3 SSID con autenticación a través de WPA2 y sin una asignación por área, lo que limitó el acceso a la información. "La utilización del protocolo WPA2, también conocido como Wi-Fi Protected Access 2, utiliza el protocolo de autenticación 802.1X, que proporciona una autenticación más segura que la de WPA, y el cifrado Advanced Encryption Standard (AES)" (Salazar Herrera et al., 2023).

Lo anterior resultaba poco óptimo: no era posible entregar las claves de conexión al usuario y mantener el control de los dispositivos en la red. El objetivo de lo presentado en este reporte es brindar movilidad y oportunidad de acceso desde cualquier sitio de la dependencia, segmentando el tráfico y tomando en cuenta la seguridad en función de las necesidades del usuario que se autentique a través de una red inalámbrica con un único SSID que gestione múltiples VLAN.

https://doi.org/10.22201/dgtic.ctud.2024.2.3.66 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 10 - 15

2. DESARROLLO TÉCNICO

2.1 PROPUESTA DE SOLUCIÓN

Al actualizar físicamente el hardware del firewall, se incorporó la característica de administración mediante un controlador de Wi-Fi que admitía mayores funcionalidades para la gestión de las redes inalámbricas. Una de estas funcionalidades era la capacidad de utilizar el protocolo WPA2-Enterprise, lo que permitía el uso de un servidor RADIUS y el empleo de credenciales exclusivas en lugar de una única contraseña universal.

Con base en lo anterior, se propuso la implementación de una red inalámbrica que con un único SSID gestione múltiples VLAN y permita segmentar el tráfico del usuario que se autentique en la red. Esto representa un paso crucial en la modernización y optimización de la infraestructura tecnológica de la dependencia. Al abordar esta iniciativa, se busca no solo mejorar la accesibilidad a los servicios digitales, sino también aumentar la flexibilidad y la productividad del personal al eliminar las limitaciones físicas impuestas por las conexiones cableadas tradicionales. En este contexto, la planificación detallada, la selección adecuada de equipos y la implementación de medidas de seguridad robustas, son elementos clave para garantizar y satisfacer las necesidades actuales y futuras de la dependencia.

2.2 METODOLOGÍA

Se llevó a cabo un análisis de requisitos para desplegar una infraestructura de acceso inalámbrico mediante la configuración de VLAN dinámicas. Este análisis abordó diversas consideraciones técnicas que implicaban los siguientes componentes:

AD (Active Directory): Esta herramienta proporciona un servicio ubicado en uno o varios servidores, capaz de crear objetos como usuarios, equipos o grupos para la gestión de credenciales durante el inicio de sesión. El AD está implementado en la dependencia para la autenticación del dominio y facilita la asignación de permisos de acceso a los usuarios registrados por la dependencia. Para la configuración se crearon los grupos correspondientes a las áreas y se asignaron dichos grupos a los usuarios respectivos.

NPS (Network Policy Server): Este servidor de directivas de red de Windows permite la creación y aplicación de directivas de acceso a la red en toda la organización, para autenticar y autorizar solicitudes de conexión. En el entorno que actualmente se encuentra en producción para el soporte de la VPN, será empleado como un servidor RADIUS, al configurar el WLC como un cliente RADIUS en el NPS. Este servidor se configuró para utilizar el AD como fuente de autenticación y políticas de red, dependiendo del grupo creado para la asignación de las VLAN donde se asignaron los atributos del usuario de RADIUS que se utilizan para la asignación del ID de VLAN:

- Tipo de túnel: Definición de la VLAN.
- Tipo de túnel medio: Definición del protocolo 802.IX.
- Túnel Pvt Grupo ID: Definición del ID de VLAN.

WLC (Wireless LAN Controller): El Controlador de LAN inalámbrica gestiona los puntos de acceso a la red inalámbrica, el cual permite la conexión de dispositivos inalámbricos a la red de una forma centralizada. Esta característica está integrada en el firewall, lo que facilita la administración de los puntos de acceso. Se

https://doi.org/10.22201/dgtic.ctud.2024.2.3.66 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 11 - 15

establecieron los parámetros de autenticación 802.1X al WLC para que coincidieran con la configuración en NPS como cliente RADIUS, y posteriormente se configuró el AP para enviar las solicitudes de autenticación de tipo WPA2-Enterprise.

AP (Access Point): Los puntos de acceso se utilizaron para establecer conexiones inalámbricas entre equipos, lo que posibilita la creación de redes inalámbricas y contribuye a la reducción de las conexiones cableadas. Se configuró el puerto del AP como un puerto Troncal para que permita múltiples VLAN y se trasmitan a través de un único SSID.

DHCP (Dynamic Host Configuration Protocol): Este protocolo, que opera bajo una arquitectura cliente-servidor, se encarga de asignar direcciones IP de manera dinámica y automática. Dado que este protocolo ya está implementado en la dependencia, será utilizado para asignar las direcciones IP correspondientes a cada área, según las reglas establecidas por el NPS. En el DHCP se asignaron los parámetros de red apropiados, incluidas las direcciones IP, máscaras de subred, puertas de enlace predeterminadas y servidores DNS para cada VLAN configurada para acceso inalámbrico.

Estándar IEEE 802.1X: "Es un estándar para el control de acceso basado en puertos que ofrece un marco para una autenticación basada en usuario y contraseña o certificados digitales y distribución de claves de cifrado" (González Paz et al., 2016). El control de acceso que se eligió fue basado en credenciales de autenticación validadas por un servidor RADIUS, las credenciales de los usuarios serán las mismas que ocupan para ingresar a su sesión de dominio en el equipo.

EAP (Extensible Authentication Protocol): "Es un marco de autenticación que permite el uso de diferentes métodos de autenticación para tecnologías de acceso a redes seguras" (Microsoft, 2023). El tipo de EAP que se utilizó fue PEAP, ya que permite la autenticación por medio de usuario y contraseña y es compatible con NPS de Microsoft.

2.3 RESULTADOS

Al implementar una infraestructura inalámbrica utilizando una solución de seguridad basada en WPA2-Enterprise, al emplear 802.1x y EAP-PEAP se obtuvo un SSID con múltiples VLAN, que permitió reducir las redes inalámbricas administradas.

Posteriormente se llevaron a cabo pruebas de acceso con el fin de validar la capacidad de los usuarios para ingresar a la red y garantizar que, al conectarse, cada usuario recibiera una dirección IP correspondiente a su área respectiva, para esto fue fundamental implementar políticas de seguridad a través del NPS, con el propósito de asegurar el cumplimiento por parte de cada usuario de las políticas establecidas, así como restringir el número de conexiones. Dichas medidas garantizan que cada VLAN contenga únicamente a los usuarios pertinentes a su área designada. Por ejemplo, se restringen los usuarios a la conexión de dos dispositivos en la red usando las credenciales asignadas para evitar la pérdida de control administrativo sobre la misma y tener accesos no deseados a la VLAN que corresponde.

Se observó que la conexión a la red inalámbrica fue más sencilla para los usuarios ya que no necesitan una clave o el apoyo del área de infraestructura.

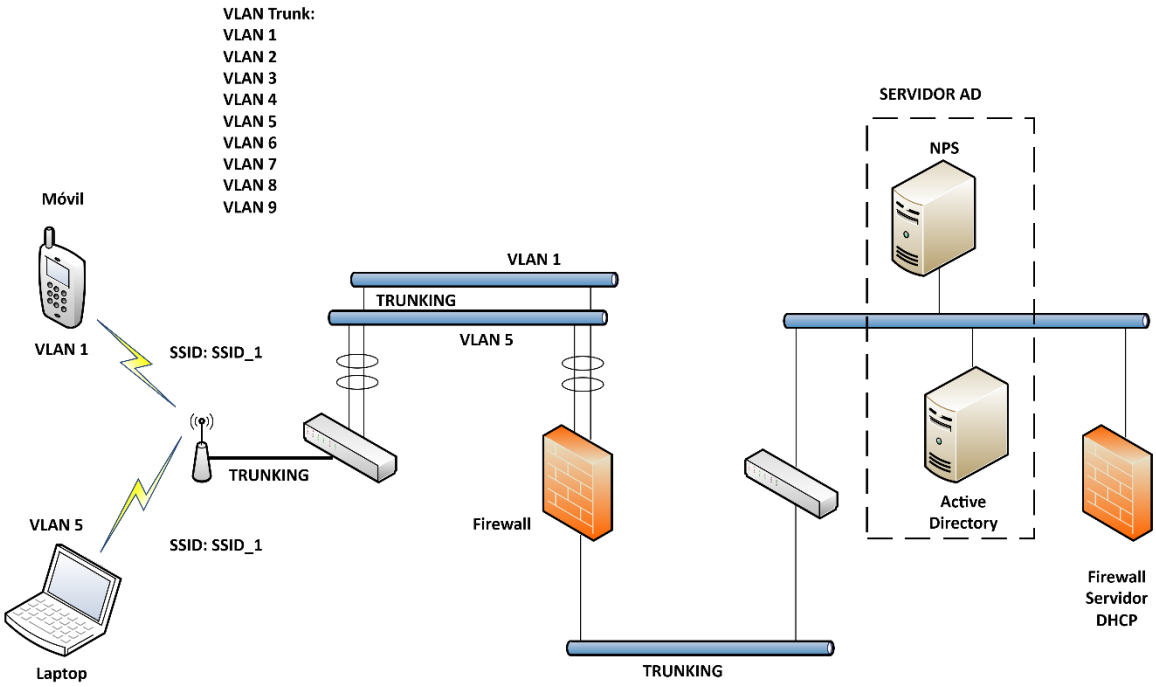
Las pruebas que se realizaron en esta red también arrojaron resultados no deseados, por ejemplo, la existencia de dispositivos que no son compatibles con el protocolo WPA2-Enterprise, ya que son dispositivos desactualizados, lo que evita la conexión a esta red.

https://doi.org/10.22201/dgtic.ctud.2024.2.3.66 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 12 - 15

Gracias a ello se identificó que la infraestructura de la red inalámbrica con asignación de VLAN dinámica implementada resuelve el problema del acceso a la información que necesitan los usuarios al conectarse por Wi-Fi, pero aún existen áreas de oportunidad que son necesarias para la seguridad de la red, tales como la distinción de dispositivos al tener una asignación en una VLAN o la actualización de dispositivos para implementar conexiones seguras con distintos protocolos. La figura 1 muestra la arquitectura de la red inalámbrica implementada.

Figura 1

Proceso de conexión de un dispositivo a la red inalámbrica con VLANs dinámicas



3. CONCLUSIONES

Las redes inalámbricas se han convertido en un recurso importante para facilitar la movilidad y tener acceso a recursos necesarios cuando no hay forma de conectar un cable al equipo, por ello, es necesario tener en cuenta la seguridad del medio por el cual viaja la información.

Esta implementación permitió observar la ventaja significativa en la facilidad de conexión para los usuarios, ya que se utilizan las mismas credenciales que emplean para acceder a sus equipos en el dominio, lo que les concede conectarse a la red con la asignación de la VLAN correspondiente, sin necesidad de cableado; de igual manera, facilitó la gestión de accesos al medio inalámbrico para el administrador de la red, lo que le permite mejorar el control de quien se encuentra conectado a la red inalámbrica.

Implementar una red inalámbrica con asignación dinámica de VLAN no resuelve por completo el problema del acceso a la información, ya que hay dispositivos que por su antigüedad no son compatibles

https://doi.org/10.22201/dgtic.ctud.2024.2.3.66 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 13 - 15

con algunos métodos de seguridad o no hay distinción en los dispositivos que acceden a la red como los teléfonos móviles, los cuales no deberían ser asignados a una VLAN que tenga información de la dependencia. Por ello, es fundamental identificar los requisitos de seguridad que se desean lograr y, a partir de ellos, combinar los protocolos según las necesidades específicas e identificando las áreas de oportunidad para mejorar el acceso a la información.

REFERENCIAS

González Paz, Alex, Beltrán Casanova, David, & Fuentes Gari, Ernesto Roberto. (2016). Propuesta de Protocolos de Seguridad para la Red Inalámbrica Local de la Universidad de Cienfuegos. Revista Universidad y Sociedad, 8(4), 130-137. Recuperado de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202016000400017&lng=es&tlng=es.

Intel. (2021). Legacy Intel® Wireless Products. Recuperado de https://www.intel.la/content/www/xl/es/support/articles/000006999/wireless/legacy-intel-wireless-products.html

IONOS. (2019.). ¿Qué es una VLAN? Concepto, ventajas y aplicaciones. IONOS. https://www.ionos.es/digitalguide/servidores/know-how/vlan/

Microsoft. (2023). Protocolo de autenticación extensible (EAP). Recuperado de https://learn.microsoft.com/es-es/windows-server/networking/technologies/extensible-authentication-protocol/network-access?tabs=eap-tls%2Cserveruserprompt-eap-tls

Salazar Herrera, A. F., Barahona Cuji, D. A., Delgado Delgado, J. V., & Suárez León, J. C. (2023). Seguridad en redes WIFI (Tesis de maestría en Ciberseguridad). Universidad Internacional del Ecuador. Recuperado de https://repositorio.uide.edu.ec/handle/37000/6106

https://doi.org/10.22201/dgtic.ctud.2024.2.3.66 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 14 - 15

ANEXO A.

CARACTERÍSTICAS DE IEEE 802.1X

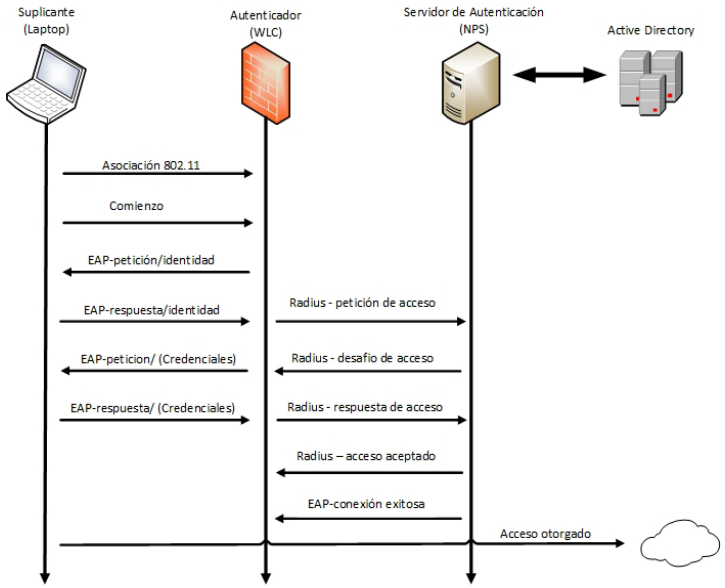
Es un estándar de control de acceso basado en puertos protegidos por autenticación. Al autenticarse a través de 802.1X para acceder a una red, se genera un puerto virtual en el punto de acceso para permitir la comunicación. Si la autorización no se realiza correctamente, no se creará el puerto virtual y se bloqueará la comunicación.

La autenticación 802.1X consiste en tres elementos fundamentales: el solicitante, que es el dispositivo que busca acceder a la red; el autenticador, que es el dispositivo que facilita la comunicación con el medio de conexión; y el servidor de autenticación, que es la base de datos que guarda las credenciales de autorización para el acceso al medio. Para que cada elemento se comunique entre sí, se requiere el uso de un protocolo de autenticación extensible. "El tipo de EAP en realidad maneja y define la autenticación. El punto de acceso que actúa como autenticador es solo un proxy que permite la comunicación entre el solicitante y el servidor de autenticación" (Intel, 2021).

Este sistema opera cuando el usuario de un dispositivo (solicitante) busca acceder a la red. En este proceso, el WLC actúa como autenticador, al solicitar las credenciales del usuario del dispositivo. Posteriormente, el usuario envía sus credenciales al WLC, el cual las redirige al servidor NPS para su autenticación. Una vez que las credenciales son comparadas con los datos almacenados en la base de datos del servidor, si son válidas, el servidor otorga al WLC la autorización para el acceso a la red al dispositivo, como se muestra en la figura 2.

Figura 2

Proceso que realiza el protocolo EAP basada en una autenticación tipo PEAP



https://doi.org/10.22201/dgtic.ctud.2024.2.3.66 Vol. 2, Núm. 3. julio-septiembre 2024, págs. 15 - 15

El protocolo EAP es capaz de manejar distintos tipos de autenticación para satisfacer las necesidades y entornos de seguridad. Estos métodos proporcionan a la organización diversos mecanismos de autenticación para acceder a la red. Algunos de los métodos más habituales incluyen:

EAP-TLS es una forma de autenticación que se apoya en el uso de certificados digitales para verificar la identidad tanto del cliente como del servidor. Este enfoque se emplea en situaciones que demandan un alto nivel de seguridad, ya que proporciona un cifrado sólido para la comunicación segura.

EAP-TTLS con este método hace más accesible al método EAP-TLS ya que crea un túnel mediante TLS, por medio del cual se pueden realizar otros métodos de autenticación adicionales. Por este método, sólo el servidor debe autenticarse con un certificado digital, mientras que del lado del cliente puede usar métodos más sencillos como contraseñas.

PEAP es un método que crea un túnel TLS seguro para proteger el proceso de autenticación. Esto se logra mediante la autenticación del servidor con un certificado digital, y las credenciales del cliente se transmiten de foma cifrada a través del túnel para garantizar una mayor seguridad.

EAP-FAST es un método que crea un túnel sin necesidad de un certificado digital, sino que en su lugar se autentifica mediante un PAC (credencial de acceso protegido) que el servidor de autentificación crea directamente.

EAP-SIM es un método que emplea autenticación a través de una tarjeta SIM. Dicha tarjeta utiliza una clave WEB basada en sesiones dinámicas, y se necesita introducir un código de verificación o PIN para acceder.

LEAP es un método que utiliza un cifrado de transmisión de datos mediante claves WEB dinámicas.