BOLETIN CIENTÍFICO IDEAS Y VOCES
ISSN 2960-8112

Optimización del tráfico de datos en redes educativas mediante RADIUS. Caso práctico en red de docentes Instituto Superior Tecnológico Tsa´chila.

Optimization of data traffic in educational networks through RADIUS: A practical case in the teachers' network of the Instituto Superior Tecnológico Tsa'chila.

Autores:

Mg. Freddy Patricio Núñez Núñez.[1] 0000-0001-8570-2471

Mg. Marco Alejandro Hinojosa Tonato.[2] 0009-0000-1060-4746

Tlga. Mishell Lisbeth Reino Vizuete.[2] 0009-0002-3124-836X

[1] *Instituto Superior Tecnológico Tsa'chila, Ecuador* freddynunez@tsachila.edu.ec

[2] *Instituto Superior Tecnológico Tsa'chila, Ecuador* marcohinojosa@tsachila.edu.ec

[3] *Independiente, Ecuador* mlrvaapc@outlook.com

Recepción: 17 de julio de 2025

Aceptación: 19 de julio de 2025

Publicación: 05 de agosto de 2025

Citación/como citar este artículo: Núñez, K., Hinojosa, M. & Reino, M. (2025). Optimización del tráfico de datos en redes educativas mediante RADIUS. Caso práctico en red de docentes Instituto Superior Tecnológico Tsa´chila. 5(2), Pág. 343-354.

Resumen

En el Instituto Superior Tecnológico Tsa`chila (ISTT) se ha reestructurado la red, implementando un sistema de gestión segmentado por IP con autenticación RADIUS en la nube a través de las direcciones MAC de los dispositivos finales. Inicialmente, se tenía una red con un solo segmento y se controlaba el acceso a internet por una tabla ARP y MAC-IP Binding donde se tenía 150 dispositivos conectados, incluyendo autorizados y no autorizados (tenían acceso a los recursos de red exceptuando la salida a internet), lo que generaba saturación y vulnerabilidad. Actualmente, existen 104 dispositivos autorizados, lo que representa un 69.33% del volumen histórico, distribuidos en 5 subredes activas, con una sexta reservada para un laboratorio en implementación. El servidor RADIUS está alojado en Google Cloud para reducir riesgos por fallas físicas y asegurando alta disponibilidad. El sistema utiliza un equipo MikroTik RB2011IL de forma local para asignar direccionamiento y está conectado al servidor Radius en la nube por IP pública. El sistema se encuentra en fase de prueba, con planes de aplicar encuestas de percepción y auditorías internas. Esta solución refleja un enfoque robusto y adaptable, alineado con los objetivos digitales institucionales y centrado en la seguridad, eficiencia y experiencia del usuario.

Palabras clave. Autenticación, Freeradius, Google Cloud, Segmentación IP, MAC Bypass.

Abstract

At the Tsa'chila Higher Technological Institute (ISTT), the network has been restructured by implementing an IP-segmented management system with RADIUS authentication in the cloud, using the MAC addresses of end devices. Initially, the network consisted of a single segment with internet access controlled through an ARP table and MAC-IP binding. A total of 150 devices were connected—both authorized and unauthorized. Although the unauthorized devices could access network resources, they were blocked from reaching the internet. This setup led to saturation and vulnerabilities. Currently, there are 104 authorized devices, representing 69.33% of the historical volume. These are distributed across five active subnets, with a sixth reserved for a laboratory that is still in development. To minimize physical failure risks and ensure high availability, the RADIUS server is hosted in Google Cloud. Locally, a MikroTik RB2011IL device manages IP assignments and connects to the cloud-based RADIUS server via a public IP. The system is in its testing phase, with plans to conduct user perception surveys and internal audits. This solution reflects a robust and adaptable approach that aligns with the institution's digital goals, focusing on security, efficiency, and user experience.

Keywords: Autenticación, Freeradius, Google Cloud, Segmentación IP, MAC Bypass.

Introducción

La transformación digital en instituciones de educación superior ha impulsado el uso de arquitecturas de red más seguras, escalables y gestionables, el protocolo RADIUS (Remote Authentication Dial-In User Service) ofrece una solución eficaz e innovadora para la gestión centralizada de autenticación, autorización y contabilidad (AAA) de usuarios en redes de datos empresariales (Al-Sarawi et al., 2022). Su integración con servicios como Hotspot, PPPoE, VPN, Wi-Fi y DHCP permite una administración minuciosa del acceso, mejorando la trazabilidad y reduciendo el riesgo de hackeo o intrusiones a la red.

A pesar de los avances tecnológicos en soluciones de conectividad, gran parte de las instituciones educativas ecuatorianas aún presentan deficiencias en la arquitectura física y lógica de sus redes, especialmente en lo referente a la segmentación interna de los dominios. La ausencia de mecanismos de segmentación como VLANs o control de acceso por listas genera dominios de difusión compartidos donde convergen usuarios, administradores, servidores institucionales, vídeovigilancia, equipos de red y dispositivos IoT, aumentando la vulnerabilidad frente a ciberataques (el mayor porcentaje de ciberataques se producen desde el interior de la infraestructura) y deteriorando el rendimiento de red en actividades académicas críticas (Guapulema Ocampo et al., 2024). Estas debilidades se ven agravadas por el uso de protocolos obsoletos como WPS o TKIP, que actualmente ya fueron reemplazados por por estándares seguros como WPA3. Si bien los informes oficiales sobre infraestructura digital (INEC, 2022) destacan avances en cobertura y acceso a Internet, se observa una carencia de indicadores técnicos sobre segmentación de redes y dominios, lo que limita el diseño de políticas de gestión de red adaptadas al ámbito educativo nacional.

La implementación de estas tecnologías y estándares seguros responde a los lineamientos de modernización educativa promovidos por organismos internacionales y nacionales que buscan

garantizar conectividad segura y equitativa en instituciones de formación técnica y tecnológica (Pino-Yancovic et al., 2024). Además, estudios recientes han demostrado que el uso de redes segmentadas y autenticación inteligente mejora la eficiencia operativa y la experiencia de usuario en campus de educación superior (Paspuel Fraga, 2014).

El servicio DHCP, cuando es gestionado por un servidor RADIUS, permite asignar direcciones IP estáticas o dinámicas de un segmento determinado, únicamente a dispositivos autenticados, fortaleciendo la segmentación de red y el control de tráfico (Khan et al., 2021). Esta combinación resulta especialmente útil en entornos educativos donde la diversidad de dispositivos y usuarios requiere políticas diferenciadas de acceso y priorización de ancho de banda.

Este artículo presenta la experiencia del Instituto Superior Tecnológico Tsa´chila (ISTT) en el cambio de una red basada en MAC Binding y ARP hacia una infraestructura que usa un servidor RADIUS virtualizado en Google Cloud, DHCP segmentado, y un dispositivo MikroTik RB2011iL. Se analizan los beneficios en seguridad, gestión de usuarios y rendimiento de red, proponiendo un modelo replicable para otras instituciones técnicas y tecnológicas del país.

Metodología

Esta propuesta siguió un enfoque cuantitativo descriptivo, orientado al análisis del comportamiento de conectividad antes y después de la implementación del sistema segmentado por IP y autenticación centralizada a través de RADIUS. El estudio empleó un método experimental aplicado, comparando métricas entre una red anterior con 150 dispositivos conectados (autorizados y no autorizados) y una red optimizada con 104 dispositivos verificados como autorizados. Según Jiménez Reyes (2012), la depuración de accesos mediante

RADIUS y listas blancas permite mayor control sobre el tráfico institucional y mejora la trazabilidad del comportamiento digital.

Para la gestión de acceso, se implementó el protocolo RADIUS mediante una instancia e2-micro de Google Cloud, para cumplir los principios AAA (autenticación, autorización, contabilidad), como señalan IBM (2024) y Roch (2024). La segmentación IP se desarrolló en el MikroTik RB2011iL, incorporando reglas de firewall y direccionamiento lógico por rol en varios segmentos. Para evitar incompatibilidad con 802.1X, se aplicó el esquema MAC Authentication Bypass (MAB), siguiendo las recomendaciones de Portnox (2023).

Durante la fase de implementación, se utilizó monitoreo con herramientas nativas de Winbox - MikroTik, análisis de logs y verificación manual de tráfico anómalo. Se proyectan auditorías internas y encuestas de percepción del servicio mientras el servicio vaya funcionando en el tiempo, buscando validar la experiencia de usuario y asegurar sostenibilidad. Este enfoque coincide con buenas prácticas de seguridad y escalabilidad en entornos cloud, como indica Google Cloud (2025).

Infraestructura física

La red institucional fue estructurada en torno al dispositivo central MikroTik RB2011iL, cuyo puerto ether1 se configuró como salida WAN hacia Internet. El puente interno comprendido entre ether2 y ether8 sirvió para enlazar distintos bloques de la institución que se encuentran físicamente separados mediante antenas Mikrotik SXT Lite5, las cuales extendieron la señal inalámbrica por radio enlaces PTP. En estos puntos se instalaron access points en modo transparente, entre ellos modelos hAP ax2 y otras marcas dual band, todos con el servidor DHCP desactivado para mantener el direccionamiento centralizado desde el RB2011iL. La tabla 1 presenta los componentes físicos usados.

Tabla 1. Componentes físicos de la red institucional

Componente	Modelo	Ubicación	Función principal
Router central	MikroTik RB2011iL	Bloque administrativo	Salida WAN y gestión de red interna
Antenas	SXT Lite5	Interbloques	Enlace inalámbrico entre bloques
Access Points	hAP ax2 / TP-Link	Salas docentes / aulas / laboratorios	Cobertura WiFi transparente

Nota: Esta tabla resume los elementos físicos instalados, destacando su rol en la conectividad y estructura base de la red.

Segmentación Broadcast y diseño de red

Para garantizar control y aislamiento del broadcast entre dispositivos, se definieron seis segmentos (ver tabla 2) IP en la red 172.16.0.0, cada uno asignado a una subred /24 según los roles académicos y operativos de los hosts. Esta segmentación permitió aislar dispositivos críticos como cámaras, alarmas, servidores y equipos de red, así como organizar el tráfico entre docentes y computadoras de laboratorios. La asignación de direcciones se realiza mediante DHCP estático gestionado desde el servidor RADIUS en función de la dirección MAC. los dispositivos deben haber sido previamente autorizados vía RADIUS.

Tabla 2. Segmentación IP implementada

Subred	Rango IP	Área funcional	Tipo de acceso	Gateway RB2011iL
1	172.16.15.0/24	Docentes C1	WiFi (MAC Bypass)	172.16.15.1
2	172.16.16.0/24	Laboratorio C1	WiFi (MAC Bypass) / Cableada	172.16.16.1
3	172.16.17.0/24	Docentes C2	WiFi (MAC Bypass)	172.16.17.1
4	172.16.18.0/24	Equipos de Red / IoT / Alarmas	WiFi (MAC Bypass)	172.16.18.1
5	172.16.19.0/24	Laboratorio C3	WiFi (MAC Bypass) / Cableada	172.16.19.1
6	172.16.20.0/24	Docentes C3	WiFi (MAC Bypass)	172.16.20.1

Nota: Esta tabla organiza los rangos IP definidos por segmento, mostrando cómo se aislaron los grupos

según la función. Los Gateway se configuraron en el bridge y son las puertas de enlace que permiten la salida a internet de cada segmento.

Además, se configuraron políticas de acceso basadas en MAC Bypass, donde la dirección MAC de cada dispositivo es registrada como credencial de acceso en la base de datos del servidor RADIUS, permitiendo una autenticación sin intervención directa del usuario.

Tabla 3. Protocolos de autenticación utilizados

Protocolo	Aplicación en red	Tipo de control	Observación
MAC Bypass	Acceso docente/laboratorio	Autenticación silenciosa	Registrado en base de datos
RADIUS	Gestión de acceso WiFi	Autenticación central	Verificación en la nube
DHCP	Asignación IP	Dinámico centralizado	Integrado a RB2011iL

Nota: Aquí se destacan los métodos de acceso configurados, con enfoque en la seguridad y centralización de credenciales.

Servidor RADIUS y autenticación en la nube

La autenticación se gestiona mediante una instancia e2-micro en Google Cloud, corriendo Debian 12, con 2 CPUs virtuales, 1 GB de RAM y 10 GB de almacenamiento. El motor de autenticación utilizado fue FreeRADIUS, integrado con una base de datos MySQL, donde se almacenan las direcciones MAC autorizadas, los rangos IP y las políticas de segmento (ancho de banda y asignación de IP según MAC). Todo el proceso de registro y consulta se realiza vía consola, lo que optimiza la seguridad y evita accesos no autorizados.

Resultados

La evaluación del rediseño se centró en tres dimensiones críticas: rendimiento, seguridad y estabilidad operativa. Se realizaron mediciones antes y después de la implementación, mediante herramientas nativas de MikroTik (Winbox, logs de RADIUS, firewall) y pruebas manuales (ping, navegación web), sobre una muestra representativa de dispositivos conectados en los bloques docentes.

Evaluación del rendimiento

Se compararon los tiempos de respuesta y el ancho de banda disponible en momentos de alta demanda, esto se observa en la tabla 4:

Tabla 4. Evaluación del rendimiento de la red, antes y después.

Métrica	Antes de la migración	Después de migración
Latencia servidor institucional	Hasta 104 ms	Estable en 12–15 ms
Ping a 8.8.8.8 desde hosts	Hasta 24 ms	4–12 ms promedio
Velocidad navegación	~9 Mbps (congestionado)	40–80 Mbps por segmento
Dispositivos simultáneos	>140 (todos en 172.16.20.0)	70 distribuidos en VLANs

Nota: La reorganización en segmentos redujo la saturación y estabilizó la conectividad incluso en horas pico.

Evaluación de seguridad

Se analizaron los intentos de acceso no autorizado y se verificaron los registros de autenticación, el resumen se observa en la tabla 5.

Tabla 5. Evaluación de la seguridad de la red.

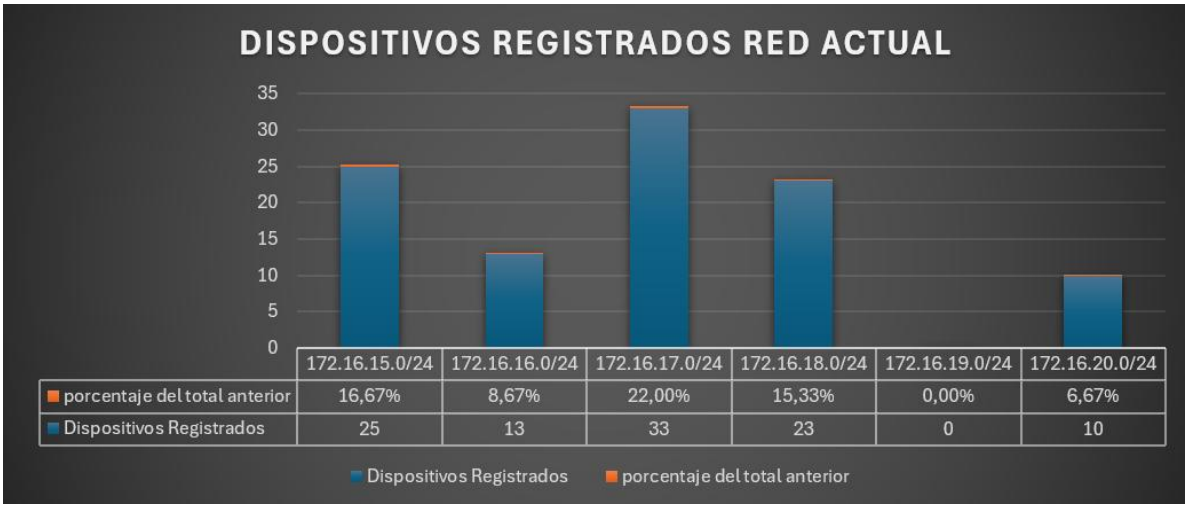
Criterio	Resultado posterior	Herramienta utilizada
Intentos de conexión no autorizada	No registrados	Log de RADIUS en MikroTik
Asignación de IP por MAC autorizada	IP fija según segmento	MYSQL + RADIUS
Visibilidad entre segmentos	Restringida por firewall	Reglas en MikroTik Firewall

Nota: existe riesgo de clonación de MAC, lo que sugiere implementar medidas complementarias.

La red actualmente tiene 104 dispositivos registrados, lo que representa un 69.33% del total anterior de 150. El segmento 172.16.17.0/24 mantiene el mayor peso con 22% del total anterior.

El segmento 172.16.19.0/24 está previsto para futuras implementaciones y puede destacarse como parte de la expansión del sistema.

Figura 1. Dispositivos registrados actualmente.

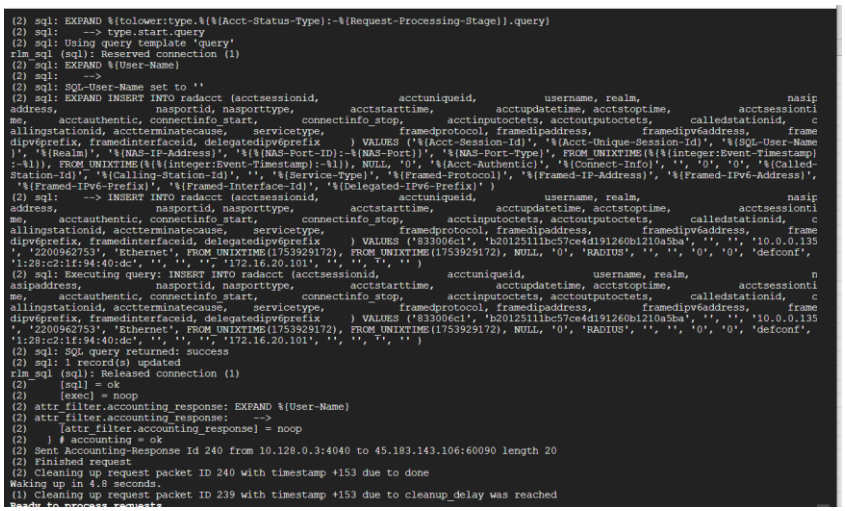


	172.16.15.0/24	172.16.16.0/24	172.16.17.0/24	172.16.18.0/24	172.16.19.0/24	172.16.20.0/24
porcentaje del total anterior	16,67%	8,67%	22,00%	15,33%	0,00%	6,67%
Dispositivos Registrados	25	13	33	23	0	10

Nota: El segmento 172.16.19.0 aún no tiene registrados ya que se asignará a un laboratorio en implementación.

Como parte de la auditoría y validación de accesos a la red institucional, se incluye en la figura 2, las respuestas del servidor RADIUS en modo debug donde se observa el estado actual de autenticaciones realizadas por los dispositivos registrados en los distintos segmentos IP configurados, esto respalda la implementación y funcionamiento adecuado de los protocolos de seguridad y control de identidad dentro del entorno educativo del ISTT.

Figura 2. Respuestas del Servidor RADIUS en modo debug.

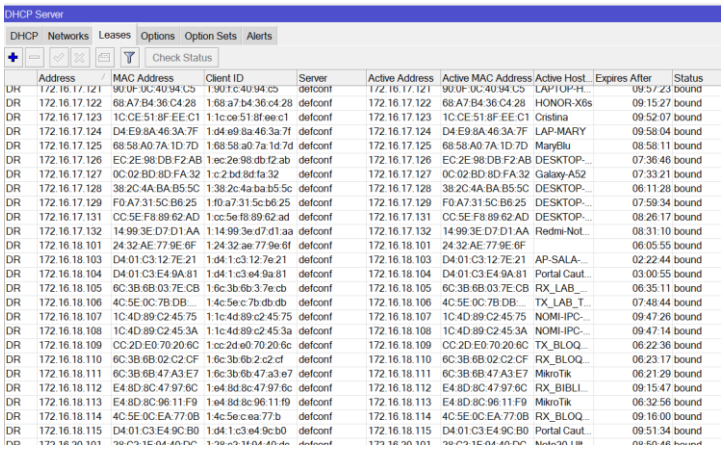


```
(2) sql: EXPAND %{tolower:type.%{%{Acct-Status-Type}:-%{Request-Processing-Stage}}.query}
(2) sql:     --> type.start.query
(2) sql: Using query template 'query'
rlm_sql (sql): Reserved connection (1)
(2) sql: EXPAND %{User-Name}
(2) sql:     -->
(2) sql: SQL-User-Name set to ''
(2) sql: EXPAND INSERT INTO radacct (acctsessionid,           acctuniqueid,          username, realm,                    nasip
address,          nasportid, nasporttype,        acctstarttime,        acctupdatetime, acctstoptime,          acctsessionti
me,     acctauthentic, connectinfo_start,      connectinfo_stop,      acctinputoctets, acctoutputoctets,     calledstationid,  c
allingstationid, acctterminatecause,    servicetype,          framedprotocol, framedipaddress,          framedipv6address,    frame
dipv6prefix, framedinterfaceid, delegatedipv6prefix     ) VALUES ('%{Acct-Session-Id}', '%{Acct-Unique-Session-Id}', '%{SQL-User-Name
}', '%{Realm}', '%{NAS-IP-Address}', '%{%{NAS-Port-ID}:-%{NAS-Port}}', '%{NAS-Port-Type}', FROM_UNIXTIME(%{%{integer:Event-Timestamp}
:-%1}), FROM_UNIXTIME(%{%{integer:Event-Timestamp}:-%1}), NULL, '0', '%{Acct-Authentic}', '%{Connect-Info}', '', '0', '0', '%{Called-
Station-Id}', '%{Calling-Station-Id}', '', '%{Service-Type}', '%{Framed-Protocol}', '%{Framed-IP-Address}', '%{Framed-IPv6-Address}',
 '%{Framed-IPv6-Prefix}', '%{Framed-Interface-Id}', '%{Delegated-IPv6-Prefix}' )
(2) sql:     --> INSERT INTO radacct (acctsessionid,           acctuniqueid,          username, realm,                    nasip
address,          nasportid, nasporttype,        acctstarttime,        acctupdatetime, acctstoptime,          acctsessionti
me,     acctauthentic, connectinfo_start,      connectinfo_stop,      acctinputoctets, acctoutputoctets,     calledstationid,  c
allingstationid, acctterminatecause,    servicetype,          framedprotocol, framedipaddress,          framedipv6address,    frame
dipv6prefix, framedinterfaceid, delegatedipv6prefix     ) VALUES ('833006c1', 'b20125111bc57ce4d191260b1210a5ba', '', '', '10.0.0.135
', '2200962753', 'Ethernet', FROM_UNIXTIME(1753929172), FROM_UNIXTIME(1753929172), NULL, '0', 'RADIUS', '', '', '0', '0', 'defconf',
'1:28:c2:1f:94:40:dc', '', '', '', '172.16.20.101', '', '', '', '' )
(2) sql: Executing query: INSERT INTO radacct (acctsessionid,           acctuniqueid,          username, realm,                    n
asipaddress,          nasportid, nasporttype,        acctstarttime,        acctupdatetime, acctstoptime,          acctsessionti
me,     acctauthentic, connectinfo_start,      connectinfo_stop,      acctinputoctets, acctoutputoctets,     calledstationid,  c
allingstationid, acctterminatecause,    servicetype,          framedprotocol, framedipaddress,          framedipv6address,    frame
dipv6prefix, framedinterfaceid, delegatedipv6prefix     ) VALUES ('833006c1', 'b20125111bc57ce4d191260b1210a5ba', '', '', '10.0.0.135
', '2200962753', 'Ethernet', FROM_UNIXTIME(1753929172), FROM_UNIXTIME(1753929172), NULL, '0', 'RADIUS', '', '', '0', '0', 'defconf',
'1:28:c2:1f:94:40:dc', '', '', '', '172.16.20.101', '', '', '', '' )
(2) sql: SQL query returned: success
(2) sql: 1 record(s) updated
rlm_sql (sql): Released connection (1)
(2)     [sql] = ok
(2)     [exec] = noop
(2) attr_filter.accounting_response: EXPAND %{User-Name}
(2) attr_filter.accounting_response:     -->
(2)     [attr_filter.accounting_response] = noop
(2)     } # accounting = ok
(2) Sent Accounting-Response Id 240 from 10.128.0.3:4040 to 45.183.143.106:60090 length 20
(2) Finished request
(2) Cleaning up request packet ID 240 with timestamp +153 due to done
Waking up in 4.8 seconds.
(1) Cleaning up request packet ID 239 with timestamp +153 due to cleanup_delay was reached
```

Nota: Se subió el tiempo de espera de respuesta del servidor en el router local debido a que este parámetro es variable y depende de la congestión en internet.

A continuación, en la figura 3, se presenta la lista de dispositivos actualmente conectados a la red, obtenido desde el panel de administración en la asignación DHCP. Este registro incluye direcciones MAC, IP asignadas, nombre de host y el tipo de conexión. Las siglas DR significa que la dirección fue asignada de manera dinámica mediante Radius.

Figura 3. Respuestas del Servidor RADIUS en modo debug.



Nota: La asignación del DHCP es estática y el servidor RADIUS es el que asigna IPs.

Discusión / Conclusiones

Actualmente, el sistema de gestión de red se encuentra en fase de prueba dentro del ISTT. Esta etapa permite validar los parámetros de configuración, el comportamiento de autenticación en el servidor RADIUS y la eficiencia de la segmentación IP. Si bien los resultados iniciales han sido favorables en términos de conectividad y control de acceso, es necesario avanzar hacia una evaluación integral del servicio más adelante. En futuras fases del proyecto se prevé la realización de una encuesta de percepción dirigida a los usuarios con el fin de medir los niveles de satisfacción, identificar experiencias de uso y recopilar sugerencias de mejora.

Así mismo, se han considerado posibles vulnerabilidades relacionadas con la autenticación, exposición de servicios, y gestión de dispositivos en red. Por ello, se recomienda una revisión

periódica de los logs del servidor RADIUS, análisis de tráfico, y auditorías internas que permitan mitigar riesgos y fortalecer la seguridad.

Cabe destacar que la evaluación del sistema se mantendrá activa en paralelo al crecimiento de la red, considerando que el número de dispositivos conectados se incrementará progresivamente a medida que se integren nuevos segmentos IP y se expandan los servicios digitales institucionales.

En conclusión, la implementación del sistema para optmizar el tráfico en el ISTT ha permitido establecer una estructura segmentada por IP y Autenticación RADIUS que optimiza la administración de dispositivos y fortalece el control de acceso mediante las direcciones MAC de los clientes. La evidencia recopilada hasta el momento muestra que la solución responde adecuadamente a los requerimientos técnicos institucionales, actualmente se registra un total de 104 dispositivos conectados, lo que representa un 69.33% del volumen histórico, con una configuración que permite escalabilidad y adaptación a futuras expansiones de la red. El sistema se encuentra en fase de prueba y su evaluación continuará mientras la red evoluciona. Se proyecta realizar una encuesta de percepción para valorar el servicio desde la experiencia del usuario, así como auditorías internas para detectar y corregir posibles vulnerabilidades. En conjunto, estos elementos reflejan un modelo de gestión de red robusto, adaptable y centrado en la mejora continua, alineado con las metas de transformación digital del Instituto.

Bibliografía

Al-Sarawi, S., Al-Roomi, M., & Al-Kuwari, H. (2022). Secure authentication mechanisms for educational networks using RADIUS protocol. International Journal of Computer Applications, 184(12), 15–22. https://doi.org/10.5120/ijca2022184123

Google Cloud. (2025). Métodos de autenticación en Google. https://cloud.google.com/docs/authentication?hl=es-419

Guapulema Ocampo, K. J., Alvarado Guapulema, P. A., Proaño del Castillo, M. G., & Peñaloza Camacho, K. I. (2024). La brecha digital en la educación ecuatoriana: Desafíos post pandemia. LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 5(5), 4038–4051. https://doi.org/10.56712/latam.v5i5.2907

IBM. (2024). Remote Authentication Dial In User Service (RADIUS) Overview. https://www.ibm.com/docs/es/i/7.5.0?topic=authentication-remote-dial-in-user-service-overview

Instituto Nacional de Estadística y Censos (INEC). (2022). Tecnologías de la Información y Comunicación – TIC 2022. Recuperado de ecuadorencifras.gob.ec

Jiménez Reyes, C. S. (2012). Implementación de un servidor RADIUS para apoyar la seguridad en una red de telecomunicaciones [Monografía de grado, Universidad Santo Tomás]. https://repository.usta.edu.co/bitstreams/5e98c0a8-7df4-411d-8110-875813419c98/download

Khan, M. A., Rehman, A., & Ullah, I. (2021). Dynamic IP allocation and access control using DHCP-RADIUS integration in campus networks. Journal of Network and Computer Applications, 178, 102999. https://doi.org/10.1016/j.jnca.2021.102999

Paspuel Fraga, D. F. (2014). Optimización del ancho de banda y control de tráfico en redes universitarias aplicando QoS. Universidad Técnica del Norte. Repositorio UTN

Pino-Yancovic, M., González, R., & Provan, K. (2024). El propósito y funcionamiento de las redes educativas en la nueva educación pública: logros y desafíos. Páginas de Educación, 17(1), 1–20. https://doi.org/10.22235/pe.v17i1.3735

Portnox. (2023). MAC Address Bypass: Navigating Network Security. https://www.portnox.com/cybersecurity-101/mac-address-bypass

Roch, R. (2024). Protocolo RADIUS: Guía completa sobre el RADIUS. LovTechnology. https://lovtechnology.com/protocolo-radius-guia-completa-sobre-el-radius/