|Jurnal Jaringan Komputer dan Keamanan |JJKK|Vol. 6| No. 3|Oct|Year 2025|
This is an Open Access article, published by Institute of Information Technology and Social Science (IITSS), Indonesia

Implementation of Radius Server–Based User Management on the WLAN Network of Dinas PUBMTR South Sumatra Province Using RADIUSdesk

Rizky Widiansyah[1*]

Abstract

Wireless Local Area Network (WLAN) technology is widely utilized across government offices, private companies, schools, and healthcare institutions. The Dinas Pekerjaan Umum, Bina Marga, dan Tata Ruang (PUBMTR; Office of Public Works, Highways, and Spatial Planning) of South Sumatra Province is one of the government institutions relying on WLAN technology to support operational activities and internet-based services. However, the agency frequently encounters challenges in managing and authenticating WLAN users, resulting in the absence of differentiation between employee and non-employee access. This condition causes network instability, bandwidth degradation, and operational disruptions during peak usage. This study proposes the implementation of a Radius Server–based user-management system to provide differentiated authentication for employees and ensure more secure, stable WLAN operations. The research methodology includes problem analysis, system design, Radius Server implementation using RADIUSdesk, and WLAN testing. The results indicate that the deployment of Radius Server–based user management using RADIUSdesk successfully improves WLAN management efficiency, simplifies user administration, and enhances network security.

Keywords

Radius Server, WLAN Network, RADIUSdesk, User Management

Article History
Received 24 July 2025
Accepted 30 October 2025

How to Cite
Widiansyah, R. (2025). Implementation of Radius Server–Based User Management on the WLAN Network of Dinas PUBMTR South Sumatra Province Using RADIUSdesk. ***Jurnal Jaringan Komputer dan Keamanan,*** *6*(3), 106-114.

[1*] Universitas Bina Darma, Indonesia, Corresponding email: 211220021@student.binadarma.ac.id

Introduction

The Office of Public Works, Highways, and Spatial Planning (Dinas Pekerjaan Umum, Bina Marga, dan Tata Ruang—PUBMTR) of South Sumatra Province carries out strategic responsibilities in supporting regional development, particularly in infrastructure management such as roads, bridges, irrigation systems, and spatial planning. These diverse and complex duties require fast, precise, and well-coordinated workflows. To achieve this, the agency relies heavily on information and communication technology (ICT), including internet access, file-sharing services, email communication, Google Drive, online meeting platforms, e-catalogue access, and office productivity applications (Fachry Altarik & Putra, 2023). This reliance highlights the critical importance of network quality and secure access in ensuring operational efficiency.

Among the essential components of the agency's ICT infrastructure is the Wireless Local Area Network (WLAN), a wireless network that enables computers, laptops, smartphones, and tablets to connect through access points (Rohmah & Alexander, 2019; Cipta et al., 2020). WLAN technology offers advantages such as mobility, flexibility, ease of deployment, and adaptability to dynamic organizational needs (Hafiz & Kurnia, 2021). As such, WLAN has become indispensable for modern office environments where mobility and collaboration among employees are vital.

However, the existing WLAN system at the PUBMTR office currently lacks user authentication mechanisms. Any device within the network's coverage can connect freely without verification, including guests, vendors, and non-staff members. During meetings, public events, or official gatherings, a large number of visitors often connect simultaneously, resulting in network congestion, bandwidth depletion, and overall performance degradation. Such issues negatively affect employee productivity, especially when daily tasks rely on stable and high-speed internet connectivity (Dasmen, Putra, & Ibadi, 2021).

To address these challenges, implementing a user management and authentication system is essential. User management ensures that WLAN access is restricted exclusively to authorized personnel, separates employee traffic from visitor traffic, and improves overall network stability (Khamdani et al., 2020; Permadi, 2019). A structured authentication framework enables network administrators to control user access more effectively and monitor activity across the network in real-time (Alfaridzi, Irawan, & Orisa, 2022). This is crucial for safeguarding organizational resources and maintaining consistent performance.

One of the most reliable technologies for centralized authentication and user authorization in WLAN environments is the Radius Server, which provides Authentication, Authorization, and Accounting (AAA) functionalities (Tenggario & Lukas, 2011; Ferdiansyah & Satria, 2022). Radius allows administrators to verify user credentials securely, manage access policies from a centralized interface, and enforce consistent authentication standards across the network. According to Hadi et al. (2022), Radius enables complete and centralized user control, including bandwidth limitations, session duration restrictions, and network profile configurations.

A commonly adopted open-source Radius implementation is RADIUSdesk, which runs on the Linux Ubuntu operating system and provides features such as account creation, access profile configuration, usage tracking, and real-time activity monitoring (Budiman &

Suharyanto, 2021). Through RADIUSdesk, PUBMTR can implement structured user-access policies, restrict unauthorized connections, and enhance network management efficiency. By integrating a Radius-based authentication system, the agency can improve network stability, ensure that only verified staff can access internal resources, and strengthen the security and reliability of its ICT services (Samudro & Rizqi, 2019; Zulkarnaen, 2021).

Methodology

This study applies an experimental research method (Zulkarnaen, 2021), conducted systematically to ensure consistent outcomes in accordance with the identified WLAN issues. The research consists of four stages:

Analysis

Examination of the PUBMTR WLAN topology and existing issues, including the absence of user authentication and network instability.

Design

Development of a new network topology employing Radius authentication, configured through RADIUSdesk.

Implementation

Installation and configuration of Radius Server, user registration, bandwidth limitation, and WLAN authentication integration.

Analysis of WLAN Topology

The researchers analyzed the existing WLAN topology using Cisco Packet Tracer (Figure: Page 2, Image 2). The WLAN operated using a star topology but lacked authentication procedures. This resulted in unrestricted access, bandwidth instability, and the absence of a structured user-management system.

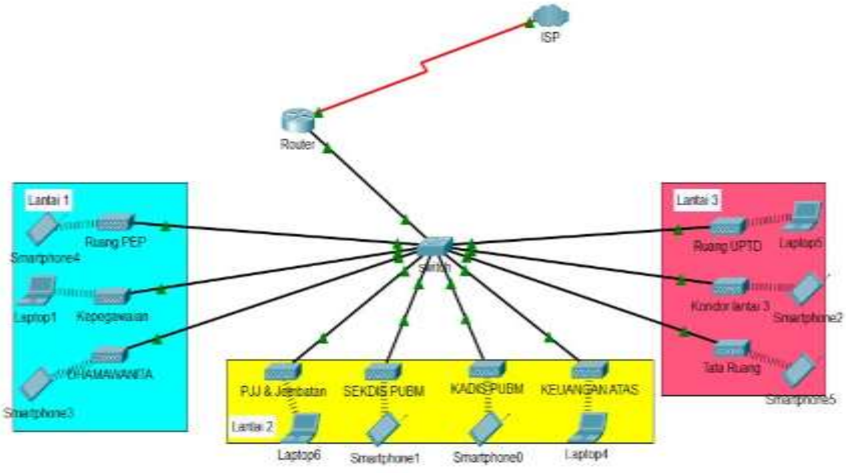


Figure 1. Network Topology at the PUBMTR Service

Design of Radius-Based Topology

A Radius-integrated WLAN topology was designed (Figure: Page 3, Image 3). The design included:

- A dedicated Radius Server
- Access Point configuration
- User-profile allocation
- Access-control rules
- Bandwidth-limitation strategy

This design ensures secure and centralized user authentication.

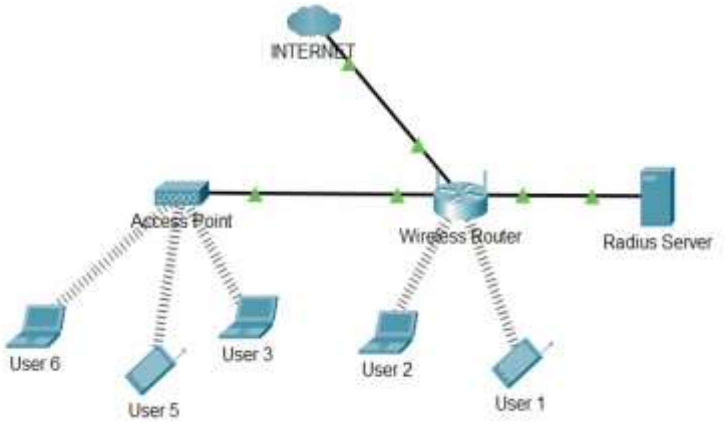


Figure 2. Radius Topology Design

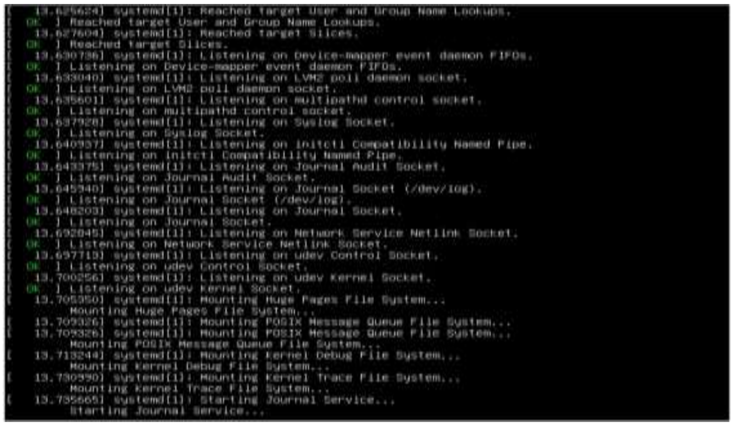
Implementation

Implementation included:

- Installing RADIUSdesk on a dedicated Ubuntu-based server (Page 4, Figure 4)
- Running RADIUSdesk services (Page 4, Figure 5)
- Logging into RADIUSdesk terminal using system credentials (Page 4, Figure 6)

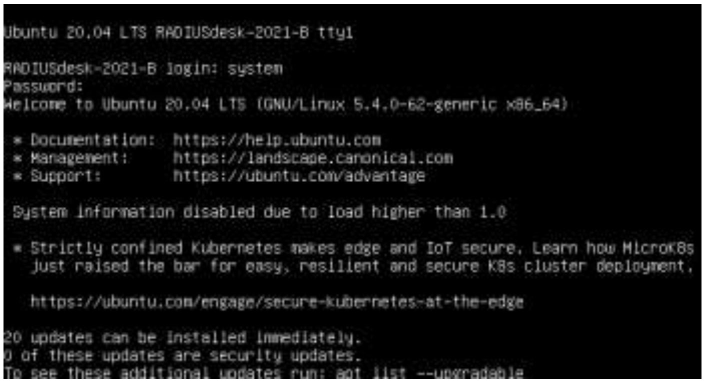
```
                    GNU GRUB  version 2.04

 *Ubuntu
  Advanced options for Ubuntu




     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```

Figure 4. Radiusdesk Installation Process



```
[   13.625624] systemd[1]: Reached target User and Group Name Lookups.
[  OK  ] Reached target User and Group Name Lookups.
[   13.627604] systemd[1]: Reached target Slices.
[  OK  ] Reached target Slices.
[   13.630736] systemd[1]: Listening on Device-mapper event daemon FIFOs.
[  OK  ] Listening on Device-mapper event daemon FIFOs.
[   13.633040] systemd[1]: Listening on LVM2 poll daemon socket.
[  OK  ] Listening on LVM2 poll daemon socket.
[   13.635601] systemd[1]: Listening on multipathd control socket.
[  OK  ] Listening on multipathd control socket.
[   13.637928] systemd[1]: Listening on Syslog Socket.
[  OK  ] Listening on Syslog Socket.
[   13.640937] systemd[1]: Listening on initctl Compatibility Named Pipe.
[  OK  ] Listening on initctl Compatibility Named Pipe.
[   13.643375] systemd[1]: Listening on Journal Audit Socket.
[  OK  ] Listening on Journal Audit Socket.
[   13.645340] systemd[1]: Listening on Journal Socket (/dev/log).
[  OK  ] Listening on Journal Socket (/dev/log).
[   13.648203] systemd[1]: Listening on Journal Socket.
[  OK  ] Listening on Journal Socket.
[   13.692045] systemd[1]: Listening on Network Service Netlink Socket.
[  OK  ] Listening on Network Service Netlink Socket.
[   13.697713] systemd[1]: Listening on udev Control Socket.
[  OK  ] Listening on udev Control Socket.
[   13.700256] systemd[1]: Listening on udev Kernel Socket.
[  OK  ] Listening on udev Kernel Socket.
[   13.705350] systemd[1]: Mounting Huge Pages File System...
         Mounting Huge Pages File System...
[   13.709326] systemd[1]: Mounting POSIX Message Queue File System...
[   13.709326] systemd[1]: Mounting POSIX Message Queue File System...
         Mounting POSIX Message Queue File System...
[   13.713244] systemd[1]: Mounting Kernel Debug File System...
         Mounting Kernel Debug File System...
[   13.730990] systemd[1]: Mounting Kernel Trace File System...
         Mounting Kernel Trace File System...
[   13.735665] systemd[1]: Starting Journal Service...
         Starting Journal Service...
```

Figure 5. RADIUSdesk Running Process.



```
Ubuntu 20.04 LTS RADIUSdesk-2021-B tty1

RADIUSdesk-2021-B login: system
Password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

 System information disabled due to load higher than 1.0

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

20 updates can be installed immediately.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable
```

Figure 6. RADIUSdesk Terminal View.

Bandwidth Configuration

Bandwidth limitation was configured by:

- Creating a new profile ("5 Mbps") under the Profiles tab (Page 5, Figure 7)
- Editing Profile Components with Vendor WISPr attributes:
  WISPr-Bandwidth-Max-Up
  WISPr-Bandwidth-Max-Down

Value set to 5,120,000 bits (equivalent to 5 Mbps) (Page 5, Figure 8)

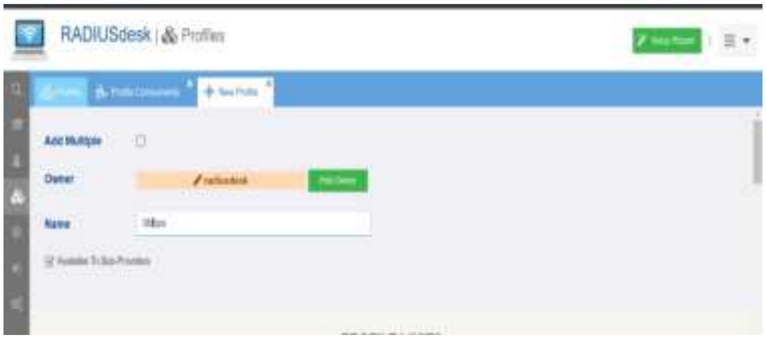
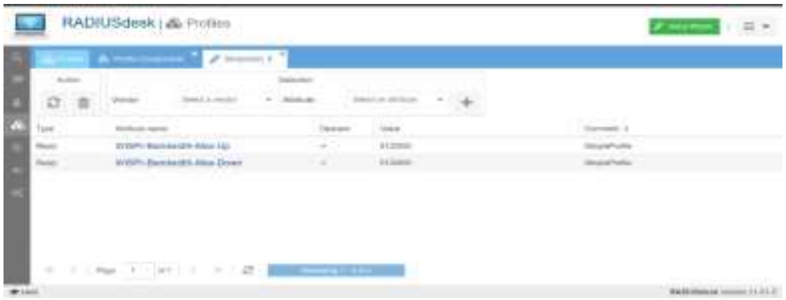


Figure 7. Bandwidth configuration.



Type	Attribute name	Operator	Value	Comment
Reply	WISPr-Bandwidth-Max-Up	:=	512000	SimpleProfile
Reply	WISPr-Bandwidth-Max-Down	:=	512000	SimpleProfile

Figure 8. Bandwidth limitation.

User-Management Configuration

User accounts were created through the Permanent Users tab (Page 6, Figures 9–10) by defining: Owner, Username, Password, Realm, Assigned profile.

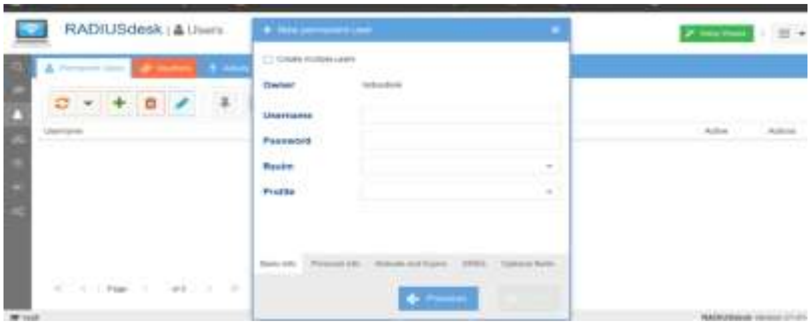
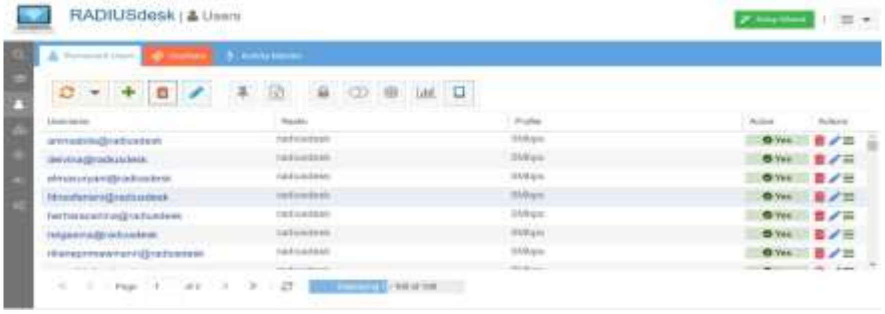


Figure 9. User registration process.



Username	Realm	Profile	Active	Actions
[illegible]@radiusdesk	radiusdesk	5Mbps	Yes	
devina@radiusdesk	radiusdesk	5Mbps	Yes	
[illegible]@radiusdesk	radiusdesk	5Mbps	Yes	
[illegible]@radiusdesk	radiusdesk	5Mbps	Yes	
[illegible]@radiusdesk	radiusdesk	5Mbps	Yes	
[illegible]@radiusdesk	radiusdesk	5Mbps	Yes	
[illegible]@radiusdesk	radiusdesk	5Mbps	Yes	

Figure 10. Results on the user manager.

Testing

Testing consisted of:

1. Login Interface
   The login page was evaluated for accessibility and proper function (Page 6, Figure 11).
2. Authentication TestingAuthorized users successfully logged into the WLAN (Page 7, Figure 12)Unauthorized users were rejected by RADIUSdesk (Page 7, Figure 13)
3. Bandwidth TestingTesting was conducted between 11:00–12:00 WIB, during peak network usage (Page 7, Figure 14). Results confirmed: Bandwidth was successfully limited to 5 Mbps per userBandwidth usage stabilized No significant degradation occurred after policy implementation

Results

The implementation of Radius Server–based user management successfully: Ensured only authorized users could access the network Applied consistent bandwidth allocation Improved overall WLAN stability Enabled centralized user monitoring Reduced network congestion during peak usage The system demonstrated effective authentication and reliable enforcement of access policies.

Discussion

The introduction of centralized user authentication through Radius Server significantly improved WLAN security and performance. Prior to implementation, unrestricted access resulted in uncontrolled bandwidth consumption and operational inefficiencies. With RADIUSdesk:

- Authentication became mandatory
- Unauthorized access was eliminated
- Bandwidth distribution became fair and consistent
- WLAN congestion was reduced during agency events

These results align with findings by Tenggario & Lukas (2011), Satria (2022), and Budiman & Suharyanto (2021), who reported that Radius Server implementations enhance network reliability, security, and administrative control.

Conclusion and Recommendations

The study concludes that Radius Server–based user management implemented using RADIUSdesk successfully enhances the WLAN system at Dinas PUBMTR South Sumatra Province. The solution ensures:

- Successful authentication of legitimate users
- Rejection of unauthorized access attempts
- Stable and controlled bandwidth distributionImproved operational continuity for employees

Thus, the user-management system contributes to better WLAN performance, improved security, and enhanced administrative efficiency.

Disclosure Statement

The authors declare no conflict of interest related to this research.

Acknowledgments

The authors express their gratitude to Dinas Pekerjaan Umum, Bina Marga, dan Tata Ruang (PUBMTR) Provinsi Sumatera Selatan and Universitas Bina Darma for providing support and infrastructure required to conduct this study.

References

Alfaridzi, F., Irawan, J. D., & Orisa, M. (2022). Design of a web-based hotspot user-management system using the MikroTik API. https://bit.ly/jurnalresistor

Budiman, M., & Suharyanto, C. E. (2021). Design of user management for hotspots using RADIUSdesk.

Cipta, D., Gunawan, T., & Kurniawan, D. F. (2020). Development of a Wireless Local Area Network (WLAN) using static-routing methods at SMPN 7 Pesawaran.

Dasmen, R. N., Putra, A., & Ibadi, T. (2021). Online training in implementing Radius technology at PT Taspen (Persero) Palembang. Abdi, 2(1). https://doi.org/10.29408/ab.v2i1.3581

Fachry Altarik, M., & Putra, A. D. (2023). Design of hotspot-authentication security using MikroTik routers at PT Nusindo Rekatama Semesta.

Ferdiansyah, P., & Satria, D. A. (2022). Hotspot management using FreeRadius and monitoring systems. *Jurnal Sistem Komputer*, 5, 153–160. https://ojs.trigunadharma.ac.id/index.php/jsk/index

Hadi, H. A., Dwilestari, G., Faqih, A., & Dienwati Nuris, N. (2022). User authentication management using the Radius Server method at RS Jantung Hasna Medika. KOPERTIP: Jurnal Ilmiah Manajemen Informatika dan Komputer.

Hafiz, A., & Kurnia, I. (2021). Development of WLAN and hotspot systems at AMIK Dian Cipta Cendikia using MikroTik routers. Jurnal Informatika Software dan Network, 2(1), 15–22.

Khamdani, W., Putra, I., Prismana, E., Prapanca, A., & Dermawan, D. A. (2020). Implementation of WPA2 Enterprise–based attendance-authentication systems. Journal of Informatics and Computer Science, 2.

Permadi, F. A. (2019). Optimization of internet hotspots through user-management systems at the Indonesian Insurance HR Development Center.

Rohmah, A. N., & Alexander, G. (2019). User management in hotspot networks at PT Inti Bharu Mas Bandar Lampung.

Samudro, W. A., & Rizqi, S. K. (2019). User management and bandwidth allocation on hotspot networks using MikroTik routers.

Tenggario, R. P., & Lukas, J. (2011). Wireless-network management using Radius Server.

Wahyudi, D., Nalendra, A. K., Wahyudi, M. I., & Lestari, H. P. (2022). Voucher-based authentication systems for RT/RW-Net using Mikhmon. JAMI, 3(1), 51–60. https://doi.org/10.46510/jami.v3i1.95

Zulkarnaen. (2021). Implementation of UserManager as Radius Server on MikroTik RB750GR3 routers. https://doi.org/10.46764/teknimedia.v2i2.43

Biographical Notes

RIZKY WIDIANSYAH is a student in the Computer Engineering Program at Universitas Bina Darma with interests in network security, WLAN infrastructures, and authentication systems.