https://jurnal.pustakagalerimandiri.co.id/index.php/pustakadata
DOI: https://doi.org/10.55382/jurnalpustakadata.v6i3.2080

Jurnal Pustaka Data

Pusat Akses Kajian Database, Analisa Teknologi, dan Arsitektur Komputer

Vol. 6 No. 3 (2026) 420 – 426

E ISSN: 2809-7483

Perancangan Keamanan Jaringan WLAN WPA2 *Enterprise* di Puskesmas Kederasan Panjang

Rolly Gios Sholid[1], Alegriya Windi Septiana [2]
[1,2]Tekno*log*i Informasi, Fakultas Saintek, Universitas Merangin
[1]rgsholid123@gmail.com [2]alegriyawindiseptiana@gmail.com

Abstract

The development of Wireless networks in healthcare facilities, such as Puskesmas Kederasan Panjang, creates significant security risks to patient medical records. The objective of this study is to develop a robust, centralized security system for Wireless networks using WPA2-Enterprise encryption techniques. The research applies an engineering approach through simulation using Cisco Packet Tracer. version 8.2.1 without direct implementation in the real environment. The simulated network architecture consists of a RADIUS Server as the authentication center, a WRT300N Wireless router, a Cisco 2960 switch, and several Client devices representing health center staff. The authentication process implements the IEEE 802.1X standard and the Protected Extensible Authentication Protocol (PEAP) to replace the less secure Pre-Shared Key (PSK) method. Simulation results show that only Clients with valid credentials registered in the RADIUS database can access the internal network, while unauthorized users are automatically denied access. The proposed system successfully enhances Wireless network security by reducing the risks of unauthorized access, data interception, rogue devices, and credential theft. Therefore, WPA2-Enterprise can be considered an effective solution for securing Wireless networks in healthcare environments.

Keywords: Wireless Security, WPA2 Enterprise, RADIUS Server, Cisco Packet Tracer., Puskesmas Kederasan Panjang.

Abstrak

Perkembangan jaringan nirkabel pada fasilitas kesehatan seperti Puskesmas Kederasan Panjang membawa kerentanan keamanan yang besar terhadap data rekam medis pasien. Penelitian ini memiliki tujuan untuk mengembangkan sebuah sistem keamanan untuk jaringan nirkabel yang kokoh dan terpusat dengan memanfaatkan teknik enkripsi *WPA2-Enterprise*. Karena adanya keterbatasan, penelitian ini menggunakan pendekatan rekayasa dengan metode simulasi melalui perangkat lunak *Cisco Packet Tracer.* versi 8.2.1 tanpa melakukan pengujian langsung di lapangan. Arsitektur yang disimulasikan meliputi *Server RADIUS* sebagai pusat otoritas autentikasi, *Wireless router* WRT300N, *switch* 2960, serta beberapa perangkat klien yang merepresentasikan staf Puskesmas. Proses autentikasi menerapkan standar IEEE 802.1X dan protokol PEAP untuk menggantikan metode *Pre-Shared Key* (PSK) yang rentan. Hasil simulasi menunjukkan bahwa sistem berhasil menerapkan lingkungan jaringan berkonsep *zero-trust*, di mana hanya klien dengan kredensial valid yang terdaftar pada *database RADIUS* yang dapat terhubung ke jaringan *internal*. Klien dengan kredensial tidak valid secara otomatis ditolak, sehingga mampu mengurangi risiko penyadapan data, masuknya perangkat asing, dan pencurian akun di lingkungan puskesmas.

Kata kunci: Keamanan Nirkabel, *WPA2 Enterprise*, *Server RADIUS*, *Cisco Packet Tracer.*, Puskesmas Kederasan Panjang.

Submitted : 12-06-2026 | Reviewed : 01-07-2026 | Accepted : 04-07-2026

1. Pendahuluan

Kemajuan dalam tekno*log*i komunikasi yang tidak menggunakan kabel telah memberikan dampak yang besar terhadap kemudahan mendapatkan akses dan bergerak di dalam sistem rangkaian komputer. Di institusi pelayanan publik seperti Puskesmas Kederasan Panjang, penggunaan jaringan nirkabel sangat penting untuk membantu para petugas medis dalam menginput data pasien, memeriksa kekosongan stok obat, serta mengakses sistem informasi manajemen puskesmas. Namun, penggunaan jaringan tanpa kabel yang semakin meningkat juga menyebabkan berbagai tantangan di bidang keamanan, karena cara data disampaikan mudah disadap, diubah, dan diserang oleh berbagai jenis ancaman *cyber* lainnya. Kebocoran data pada fasilitas kesehatan dapat melanggar privasi pasien dan menurunkan kredibilitas instansi.

Oleh karena itu, merancang sistem keamanan yang kuat untuk jaringan nirkabel sangat penting agar dapat memastikan integritas, kerahasiaan, dan ketersediaan data dalam jaringan area lokal nirkabel di Puskesmas Kederasan Panjang. Salah satu standar keamanan yang umum digunakan untuk jaringan *Wi-Fi* adalah *Wi-Fi Protected Access* versi 2, yang dikenal sebagai WPA2. Secara khusus, varian *Enterprise* dari WPA2 ini mengandalkan protokol 802.1X dan *RADIUS* (*Remote Authentication Dial-In User Service*) untuk melakukan proses autentikasi berdasarkan identitas masing-masing pengguna secara terpisah. Berbeda dengan WPA2 *Personal* yang menggunakan metode Kunci Bersama (PSK) dengan satu kunci yang sama untuk semua pengguna, WPA2 *Enterprise* menyediakan metode autentikasi yang lebih aman dan lebih fleksibel. Ini dilakukan dengan menggunakan protokol EAP (*Extensible Authentication Protocol*) yang bisa mendukung beberapa metode autentikasi, seperti PEAP (*Protected EAP*) dan MSCHAPv2.

Protokol keamanan pertama untuk jaringan nirkabel, yang dikenal sebagai *Wired Equivalent Privacy* (WEP), ternyata memiliki banyak kelemahan yang serius, sehingga akhirnya digantikan oleh *Wi-Fi Protected Access* (WPA) dan versi yang lebih aman lagi, yaitu WPA2 (Fairlie, 2025). *WPA2-Enterprise* dirancang khusus untuk jaringan perusahaan. Ini memberikan perlindungan yang lebih kuat dengan menerapkan protokol IEEE 802.1X dan *server RADIUS* untuk mengelola data pengguna. Namun, meskipun *WPA2-Enterprise* dianggap lebih aman, berbagai penelitian dan laporan terbaru menunjukkan bahwa protokol ini tidak sepenuhnya bebas dari serangan siber. Salah satunya adalah serangan *Key Reinstallation Attacks* (*KRACK*) yang mengeksploitasi kelemahan dalam proses *handshake* WPA2 (Vanhoef & Piessens, 2017). Oleh karena itu, dalam merancang sistem keamanan untuk jaringan nirkabel yang menggunakan *WPA2-Enterprise*, diperlukan pendekatan yang tepat dalam penerapan serta pengujian keamanan secara menyeluruh agar dapat meminimalkan risiko yang mungkin timbul.

Beberapa penelitian sebelumnya telah membahas implementasi *WPA2-Enterprise* pada lingkungan pendidikan, perkantoran, dan sistem kehadiran berbasis jaringan nirkabel. Penelitian tersebut menunjukkan bahwa penggunaan *server RADIUS* dan protokol IEEE 802.1X mampu meningkatkan keamanan akses jaringan dibandingkan metode *WPA2-Personal.* Namun, masih sedikit penelitian yang secara khusus membahas perancangan keamanan jaringan nirkabel pada fasilitas kesehatan tingkat pertama, khususnya Puskesmas, menggunakan pendekatan simulasi *Cisco Packet Tracer.*. Selain itu, kebutuhan keamanan data rekam medis yang bersifat sensitif menuntut adanya sistem autentikasi yang lebih terpusat dan terkontrol. Oleh karena itu, penelitian ini menawarkan rancangan keamanan jaringan nirkabel berbasis *WPA2-Enterprise* dengan *server RADIUS* pada studi kasus Puskesmas Kederasan Panjang sebagai upaya meningkatkan keamanan akses jaringan dan perlindungan data pasien.

Berdasarkan penjelasan tersebut, penelitian ini bertujuan untuk membuat dan menguji sistem keamanan jaringan tanpa kabel yang menggunakan *WPA2-Enterprise* dengan bantuan *server RADIUS* di Puskesmas Kederasan Panjang. Simulasi dilakukan menggunakan *Cisco Packet Tracer.* untuk menguji mekanisme autentikasi pengguna, pembatasan akses jaringan, serta kemampuan sistem dalam mencegah akses tidak sah. Hasil penelitian diharapkan dapat menjadi acuan dalam penerapan keamanan jaringan nirkabel yang lebih baik pada fasilitas pelayanan kesehatan.

2. Metode Penelitian

Penelitian ini adalah jenis penelitian teknik yang bertujuan untuk merancang dan menerapkan sistem keamanan jaringan tanpa kabel yang menggunakan protokol WPA2 *Enterprise* sebagai dasarnya. Tujuannya adalah membuat sistem jaringan tanpa kabel yang lebih aman dengan cara mengenali pengguna melalui *server RADIUS*. Tujuan ini adalah untuk mencegah akses yang tidak sah dan

Submitted : 12-06-2026 | Reviewed : 01-07-2026 | Accepted : 04-07-2026

memperkuat pengendalian keamanan jaringan. Seluruh proses dilakukan dengan simulasi menggunakan perangkat lunak *Cisco Packet Tracer.* untuk menguji jaringan dan mengatur perangkat.

Setelah itu, dilakukan evaluasi perbandingan dengan cara mengukur seberapa efektif sistem *WPA2-Enterprise* yang memanfaatkan *RADIUS* dibandingkan dengan metode lainnya seperti *WPA2-Personal.* Hal ini terutama terlihat dari aspek pembatasan akses serta perlindungan terhadap perangkat yang tidak dikenal. Selanjutnya, kami akan mengevaluasi kinerja jaringan dan seberapa mudah sistem keamanan yang sudah diterapkan dengan metode ini akan diintegrasikan. Pastikan jaringan nirkabel tetap aman dengan menggunakan otentikasi yang terpusat, membatasi akses yang tidak diizinkan, dan melindungi dari berbagai bahaya keamanan.

Tujuan penelitian ini adalah membuat simulasi sistem keamanan jaringan nirkabel yang mengandalkan standar *WPA2-Enterprise*. Sistem ini bisa memeriksa pengguna satu persatu dengan cara memverifikasi identitas mereka. Dalam penelitian ini, kami menggunakan beberapa perangkat jaringan virtual dari *Cisco Packet Tracer.* untuk melakukan simulasi. Perangkat yang digunakan mencakup *router* nirkabel (WRT300N), *switch* (2960-24TT), *server RADIUS*, serta perangkat petugas seperti komputer, laptop, dan ponsel yang digunakan dalam simulasi jaringan nirkabel.

2.1. Langkah-Langkah Perancangan Simulasi

Adapun Langkah-langkah perancangan simulasi yang digunakan adalah sebagai berikut:

1. Merancang struktur jaringan dengan menggunakan perangkat lunak *Cisco Packet Tracer.*
2. Mengatur *server RADIUS* dengan IP tetap dan konfigurasi layanan autentikasi AAA.
3. Menghubungkan *router* WRT300N ke *server RADIUS* menggunakan *switch* 2960-24TT.
4. Mengonfigurasi parameter *WPA2 Enterprise* dan *Shared Key* pada *router* WRT300N.
5. Mengatur akun *Username* dan *Password* khusus untuk staf di *database server RADIUS*.
6. Mengecek koneksi dan proses verifikasi dari sisi pengguna ke jaringan internet tanpa kabel.
7. Menganalisis konektivitas dan hasil autentikasi.

2.2. Data Dan Instrumen

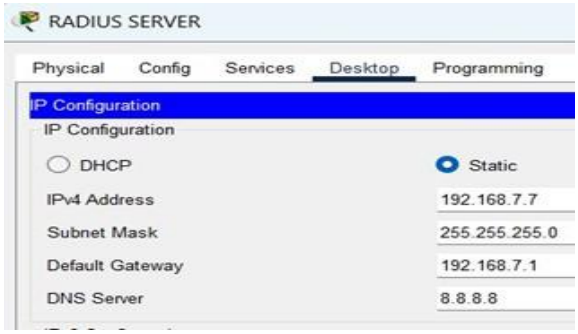
Data yang dikumpulkan mencakup hasil tes koneksi, catatan *log* autentikasi yang berhasil atau gagal dari *server RADIUS*, serta kondisi koneksi perangkat petugas puskesmas. Alat yang digunakan dalam penelitian ini meliputi perangkat lunak *Cisco Packet Tracer.* versi 8.2.1, dokumentasi mengenai konfigurasi IP, serta *output log* dari *server* AAA.Teknik pengumpulan data dilakukan dengan mengamati langsung jalannya proses simulasi, mengambil tangkapan layar *(screensh-ot)* konfigurasi, dan mencatat respon konektivitas dari *log server.*

2.3. Teknik Analisa Data

Data dianalisis menggunakan pendekatan kualitatif deskriptif, yaitu dengan membandingkan hasil pengujian dengan tujuan yang sudah ditentukan dalam desain sistem keamanan WPA2-*Enterprise*. Analisis dilakukan dengan memperhatikan tingkat keberhasilan koneksi, ketepatan konfigurasi, dan kemampuan perangkat untuk melakukan autentikasi dengan *server RADIUS*, serta kemampuan sistem dalam menolak perangkat yang tidak terdaftar.

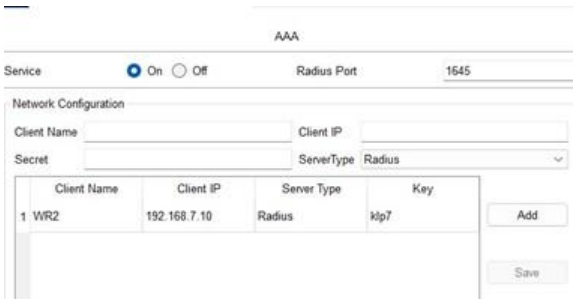
2.4. Tahapan Rancangan

Pertama, lakukan pengaturan pada *server* dengan memberikan alamat IP kepada *server* tersebut,



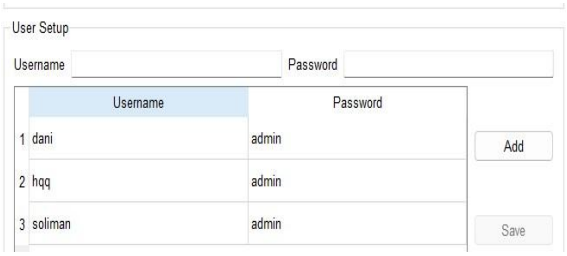
Gambar 1. Konfigurasi IP Server

Masih di *Server*, langkah berikutnya adalah melakukan Konfigurasi *RADIUS-Server*. Ini bisa ditemukan pada menu Service dengan mengaktifkan fitur AAA. Selanjutnya, buat konfigurasi *server RADIUS* dengan mengisi nama petugas, alamat IP klien, jenis *server RADIUS*, dan kunci yang digunakan. Setelah itu, klik *Add* dan simpan.



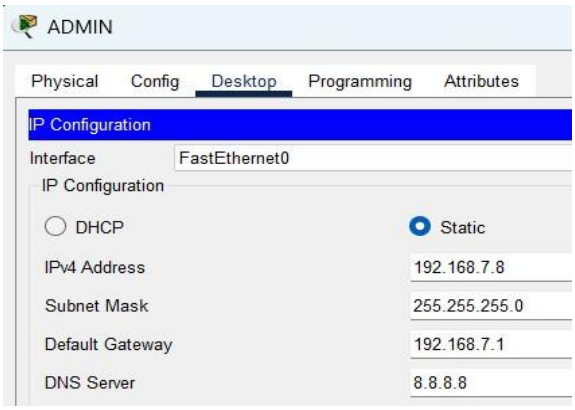
Gambar 2. Konfigurasi *RADIUS Server*

Di dalam menu Service *Server* AAA, tambahkan daftar klien dengan memberikan *Username* dan *Password* sebagai cara autentikasi.



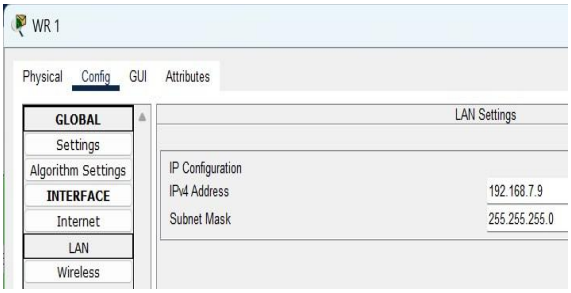
Gambar 3. Menambah Daftar *Client*

Beralih pada perangkat Laptop *Admin*, kemudian berikan *IP*



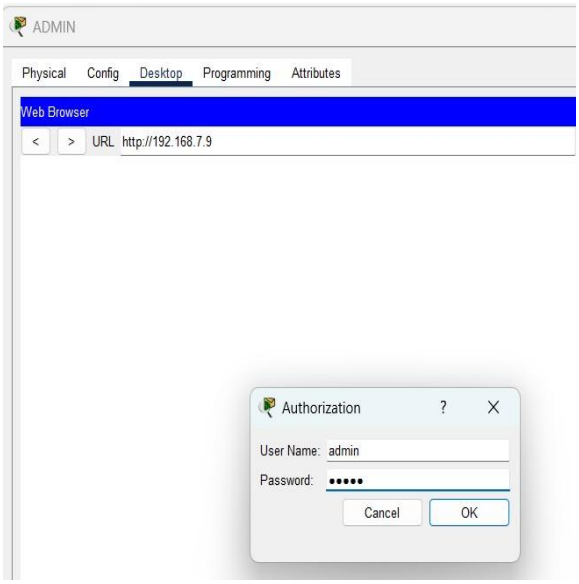
Gambar 4. Menambah Daftar *Client*

Lanjutkan pada Perangkat *Wireless router*/WR1 pada topo*log*i, dan berikan *IP*



Gambar 5. *Setting IP Addr*ess *Wireless router*

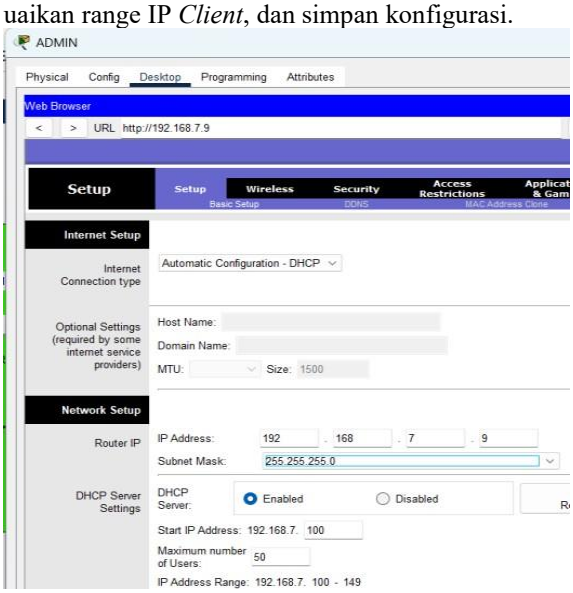
Kembali ke Laptop *Admin* untuk mengatur konfigurasi WPA *Enterprise*s di WR1 melalui Laptop *Admin*.



Gambar 6. Konfigurasi WPA *Enterprise*s

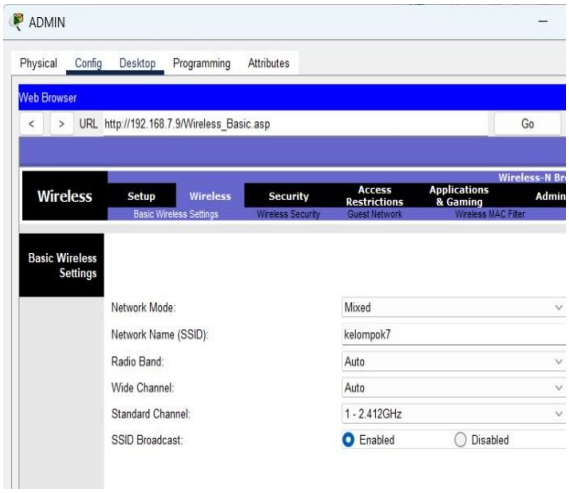
Masuk pada menu *Web Browser* dan pada kolom URL ketikkan IP WR1 dan *enter*. Maka akan muncul menu autorisasi. Masukkan nam a pengguna dan kata sandi *default*, "*Admin*", di sana.

Lanjutkan ke menu Konfigurasi, aktifkan DHCP, ses uaikan range IP *Client*, dan simpan konfigurasi.



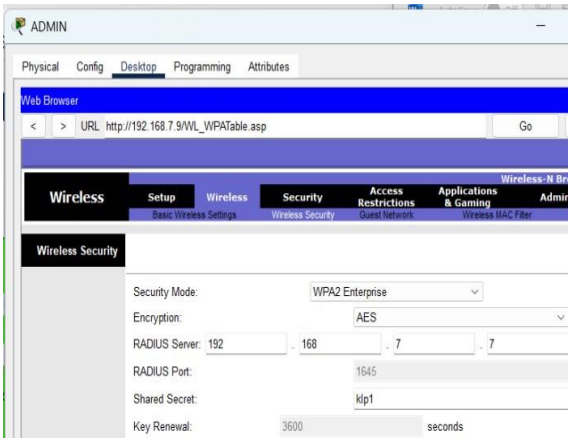
Gambar 7. *Setting* DHCP

Beralih ke tab perangkat nirkabel, masukkan nama network yang akan digunakan dan simpan pengaturan.



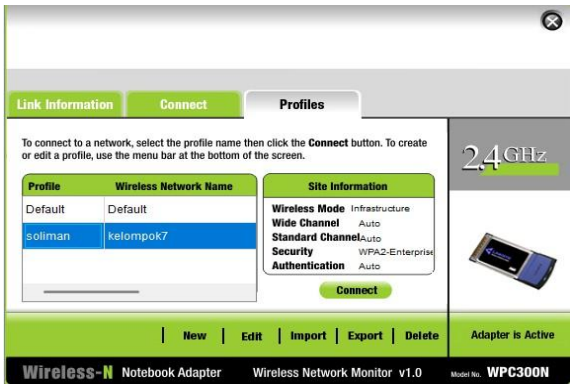
Gambar 8. Memberi SSID

Selanjutnya, pada *tab* Keamanan Nirkabel, pilih *mode* keamanan *WPA2-Enterprise*, pilih enkripsi AES, pilih *server RADIUS* IP, dan masukkan kunci bersama yang sesuai *server*. Lalu simpan *setting*.



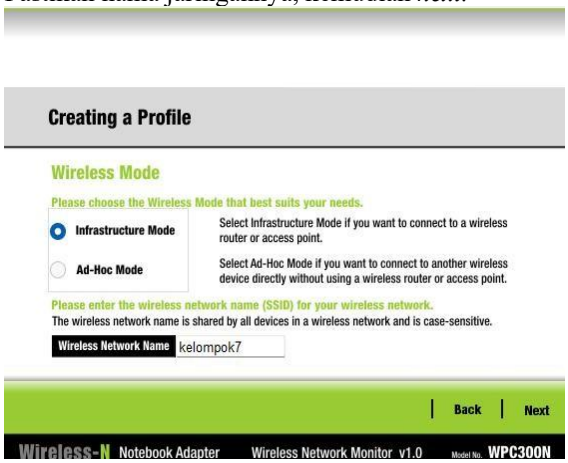
Gambar 9. Shared Key

Selanjutnya, klien harus dihubungkan ke jaringan yang sudah diatur. Pilih menu PC *Wireless* di klien. Kemudian, pilih tab Profiles.Kemudian, pilih jaringan yang anda inginkan, pilih *new*, dan pilih *Advanced Setup*.



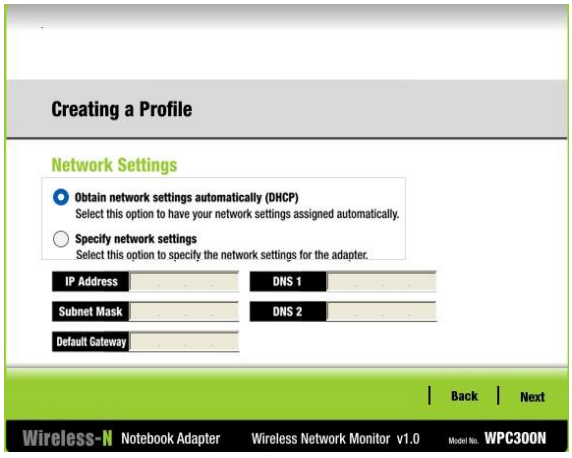
Gambar10. Menghubungkan *Client* kedalam jaringan

Pastikan nama jaringannya, kemudian *next.*



Gambar 11. Verifikasi Nama SSID

Pilih *Obtain DHCP* dan *Next*

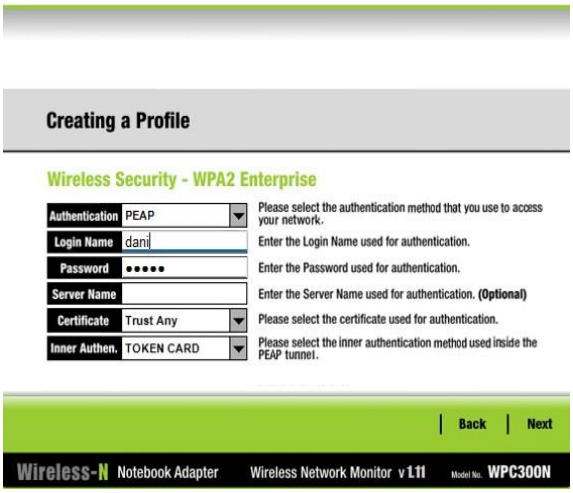


Gambar 12. Konfigurasi DHCP *Client*

Keamanan memilih WPA2-*Enterprise*s sesuai dengan sistem perlindungan jaringan dan berikutnya.

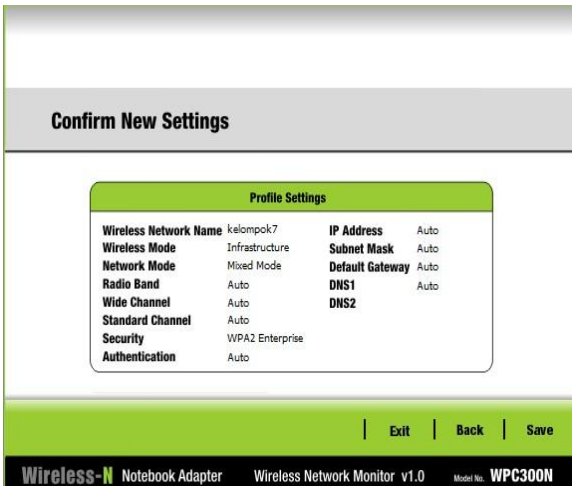
Gambar 13. *Pemilihan WPA2 Enterprise*

Masukkan nama *log* masuk dan *Password* dengan menggunakan salah satu *Username* yang telah terdaftar pada *server*



Gambar 14. Input Kredensial Pengguna

Simpan *Setting.*



Gambar 15. Penyimpanan Profil Jaringan

Selesaikan, lalu pilih "Sambungkan ke Jaringan".

Gambar 16. Koneksi ke Jaringan WLAN

3. Hasil Dan Pembahasan

Sistem perlindungan untuk jaringan tanpa kabel menggunakan WPA2-*Enterprise* pada kasus Puskesmas Kederasan Panjang telah berhasil dikembangkan dan diuji. Melalui arsitektur ini, protokol *PEAP* dengan otentikasi EAP 802.1x mampu berjalan optimal dalam memisahkan hak akses. Implementasi ini sangat krusial bagi Puskesmas Kederasan Panjang untuk melindungi *database* lokal rekam medis pasien dari upaya intercept (penyadapan) oleh pengguna umum atau pasien di ruang tunggu yang menggunakan segmen jaringan nirkabel yang sama.

Berdasarkan hasil pengujian pada *model* simulasi, ketika tiga perangkat klien (*Client* 1, *Client* 2, *Client* 3) mencoba melakukan asosiasi ke SSID "Staf_Puskesmas_KederasanPanjang", *server RADIUS* secara aktif melakukan *lookup* terhadap *database* AAA. Perangkat klien yang memasukkan kombinasi *Username* dan *Password* staf dengan benar langsung diberikan akses penuh ke jaringan lokal puskesmas. Sebaliknya, ketika dilakukan pengujian menggunakan akun tiruan (akun tidak valid/penyusup), *server* secara otomatis mengirimkan instruksi penolakan akses (*Access-Reject*), sehingga perangkat asing tersebut sama sekali tidak bisa terhubung maupun mengendus paket data di dalam jaringan.

Penggunaan enkripsi *AES* yang dikombinasikan dengan autentikasi per-*user* ini terbukti memberikan keamanan yang jauh lebih tinggi daripada model WPA2 *Personal* (PSK) yang umumnya dipakai. Dengan sistem terpusat ini, manajemen Puskesmas Kederasan Panjang dapat dengan mudah menambah atau mencabut hak akses komunikasi staf tanpa mengganggu aktivitas konektivitas staf lainnya. Secara keseluruhan, sistem ini telah memenuhi prinsip dasar *zero-trust network architecture* yang sangat direkomendasikan untuk menjaga kerahasiaan data pada sektor fasilitas kesehatan.

4. Kesimpulan

Menurut hasil dari rencana dan pemodelan, sistem perlindungan untuk jaringan tanpa kabel yang memakai *WPA2-Enterprise* dengan menggunakan *server RADIUS* di Puskesmas Kederasan Panjang telah berhasil diterapkan dengan efektif menggunakan *Cisco Packet Tracer.* Mekanisme autentikasi berbasis IEEE 802.1X dan PEAP memungkinkan setiap pengguna melakukan akses jaringan menggunakan kredensial yang terdaftar pada *server RADIUS*, sehingga hanya pengguna yang berwenang yang dapat terhubung ke jaringan *internal*.

Keputusan dari ujian menunjukkan bahwa sistem boleh memberikan akses kepada pengguna yang mempunyai bukti sah dan menolak pengguna yang tidak berdaftar. Oleh karena itu, penggunaan *WPA2-Enterprise* bisa memperkuat keamanan jaringan tanpa kabel dan mengurangi kemungkinan akses yang tidak diizinkan, pencurian informasi, serta penyalahgunaan pengguna.

Untuk pengembangan selanjutnya, sistem dapat diimplementasikan pada lingkungan nyata dan dikombinasikan dengan teknologi VLAN untuk memisahkan jaringan staf dan jaringan publik sehingga tingkat keamanan jaringan dapat lebih ditingkatkan.

Daftar Rujukan

[1] Adiguna, M. A., & Widagdo, B. W. (2022). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : *Router* Tp-Link Mercusys Mw302r). *Jurnal SISKOM-KB (Sistem Komputer Dan Kecerdasan Buatan)*, *5*(2), 1–8. https://doi.org/10.47970/siskom-kb.v5i2.268

[2] Fairlie, M. (2025). *With WPA3-Enterprise, Companies Find Wireless Security*. Business.Com. https://www.business.com/articles/deploying-*WPA2-Enterprise*-encryption/

[3] Koutto. (2024). *07. WPA/WPA2 Enterprise (MGT).https://github.com/koutto/pi-pwnboxrogueap/wiki/07*.-WPA-*WPA2-Enterprise*-(MGT)

[4] Prismana, I. P. E., Permadi, G. S., & Khamdani, W. (2020). Implementasi *WPA2 Enterprise* dan LDAP Dalam Membangun Sistem Informasi Kehadiran Karyawan. *Jurnal Sistem Informasi Bisnis*, *10*(2), 195–202. https://doi.org/10.21456/vol10iss2pp195-202

[5] Vanhoef, M., & Piessens, F. (2017). Key reinstallation attacks: Forcing nonce Reuse in WPA2. *Proceedings of the ACM Conference on Computer and Communications Security*, 1313–1328. https://doi.org/10.1145/3133956.3134027

[6] Saskara, G. A. J., Indrawan, I. P. O., & Putra, P. M. (2019). Keamanan Jaringan Komputer Nirkabel dengan *Captive Portal* dan WPA/WPA2 di Politeknik Ganesha Guru. *Jurnal Pendidikan Teknologi dan Kejuruan*, 16(2), 236-247.https://doi.org/10.23887/jptk-undiksha.v16i2.18559

[7] Wibowo, S. H., Andesti, C. L., Suleman, Hendarsyah, D., Santoso, N. A., Dewantara, R., Wahidin, A. J., Santoso, L. W., Sihombing, F. A., & Saputra, H. (2022). *Teknologi Jaringan Nirkabel*. Padang: PT Global Eksekutif Tekno*log*i. *http://repository.stmiktegal.ac.id/id/eprint/33/1/BUKU%20TEKNOLOGI%20JARINGAN%20NIRKABEL.pdf*

[8] Rinaldi, R., & Sadikin, M. (2019). Analisa dan Pengujian Serangan Evil Twin pada Jaringan berbasis *Wireless* dengan Keamanan WPA2-PSK. *Ph. D. diss.*

[9] Und*IP* E-Journal. (2022). Implementasi *WPA2 Enterprise* dan LDAP Dalam Membangun Sistem Absensi Berbasis Jaringan WiFi. [Daring]. https://ejournal.und*IP*.ac.id/index.php/jsinbis/article/download/32570/pdf

[10] Mentang, R., Sinsuw, A. A. E., & Najoan, X. B. N. (2020). Perancangan Dan Analisis Keamanan Jaringan Nirkabel Menggunakan *Wireless* Intrusion Detection System. *Jurnal Elektronika dan Komunikasi, Universitas Sam Ratulangi*. *https://ejournal.unsrat.ac.id/index.php/elekdankom/article/view/10592*

Submitted : 12-06-2026 | Reviewed : 01-07-2026 | Accepted : 04-07-2026