

Kajian Implementasi, Kinerja, dan Keamanan Asterisk untuk VoIP

Wahab Sukoraharjo

Program Studi Sistem Informasi, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Gunadarma, Indonesia

Article History

Received : 2026-03-07

Revised : 2026-04-23

Accepted : 2026-05-29

Published : 2026-08-10

Corresponding author*:

joned@staff.gunadarma.ac.id

Cite This Article: Wahab Sukoraharjo. (2026). Kajian Implementasi, Kinerja, dan Keamanan Asterisk untuk VoIP. Jurnal Teknik Dan Science, 5(2), 157–165.

DOI:

<https://doi.org/10.56127/jts.v5i2.3044>

Abstract: This review analyses Asterisk implementation, performance, and security as an open-source VoIP platform. Eight provided sources were selected: one technical book and seven empirical studies. Data were extracted into a matrix and synthesised into implementation, Quality of Service, VPN security, and research limitations. Asterisk was deployed on Linux servers, FreePBX or Trixbox distributions, OpenWRT routers, powerline networks, wired and wireless environments, and processing clusters. Performance was assessed mainly through delay, jitter, packet loss, throughput, and Mean Opinion Score. Controlled small networks generally produced acceptable quality, while restricted bandwidth, UDP load, unstable media, and inconsistent configurations reduced performance. VPN improved confidentiality, but its impact on QoS varied across studies. Firmware cloning succeeded on identical routers and failed across different devices. Future studies should use current Asterisk versions, modern security protocols, larger call loads, multiple codecs, and standardised test procedures.

Keywords: Asterisk, VoIP, Quality of Service, VPN, literature review.

PENDAHULUAN

Voice over Internet Protocol (VoIP) mengubah suara menjadi paket digital yang dikirim melalui jaringan berbasis Internet Protocol. Pendekatan ini memungkinkan komunikasi suara memanfaatkan infrastruktur data yang telah tersedia dan membuka peluang integrasi layanan telepon dengan aplikasi jaringan. Dalam arsitektur tersebut, Asterisk berperan sebagai perangkat lunak telephony sumber terbuka yang dapat menjalankan fungsi Private Branch Exchange, menangani registrasi dan sesi panggilan, mengelola dialplan, serta berinteraksi dengan protokol dan perangkat telekomunikasi. Fleksibilitas Asterisk juga diperluas melalui Asterisk Gateway Interface, Asterisk Manager Interface, integrasi basis data, dan dukungan terhadap protokol VoIP seperti Session Initiation Protocol dan Inter-Asterisk eXchange (Van Meggelen et al., 2007).

Asterisk tidak hanya digunakan pada server Linux konvensional. Sumber-sumber yang dikaji memperlihatkan implementasi pada router berbasis OpenWRT, distribusi FreePBX dan Trixbox, jaringan Powerline Communication, jaringan kabel dan nirkabel, serta cluster berbasis parallel processing. Keragaman tersebut menunjukkan bahwa Asterisk dapat ditempatkan sebagai inti sistem telephony, sedangkan FreePBX atau Trixbox menyediakan lingkungan pengelolaan yang mempermudah konfigurasi dan administrasi. Namun, fleksibilitas platform tidak otomatis menjamin kualitas panggilan. Layanan suara waktu nyata sangat sensitif terhadap delay, jitter, packet loss, keterbatasan bandwidth, beban trafik, dan stabilitas media transmisi (Sadiq, 2017; Siboro & Affandi, 2010).

Aspek keamanan menjadi persoalan lain karena trafik VoIP berada pada jaringan paket yang dapat dipantau atau disadap apabila tidak dilindungi. Buku teknis Asterisk

menekankan pentingnya pemisahan jaringan suara dan data, penggunaan firewall atau Virtual Local Area Network, penempatan sistem pada zona yang sesuai, hardening server, menjalankan Asterisk sebagai pengguna non-root, serta penggunaan Virtual Private Network untuk melindungi trafik antarlokasi. Perlindungan tersebut mempunyai biaya performa karena proses enkripsi, dekripsi, dan enkapsulasi menambah pekerjaan sistem dan jaringan (Van Meggelen et al., 2007). Studi-studi eksperimental yang diunggah juga menunjukkan hasil yang belum konsisten mengenai dampak VPN terhadap Quality of Service. Sebagian memperoleh kenaikan jitter atau packet loss, sedangkan penelitian lain melaporkan hasil yang lebih baik pada skenario VPN (Putro & Widiyastuti, 2022; Rawadi et al., 2025).

Bukti penelitian mengenai Asterisk masih tersebar pada tema portabilitas, pengukuran performa, media transmisi, pembebanan server, dan keamanan. Perbedaan topologi, perangkat, jumlah klien, parameter, satuan, serta standar penilaian menyulitkan pembaca menarik kesimpulan umum dari satu studi saja. Oleh karena itu, artikel ini menyusun kajian literatur terstruktur terhadap delapan sumber relevan yang diberikan, terdiri atas satu buku teknis dan tujuh penelitian empiris. Kajian diarahkan untuk menjawab empat pertanyaan: (1) bagaimana Asterisk diimplementasikan pada berbagai perangkat dan infrastruktur; (2) parameter apa yang digunakan untuk menilai kinerja; (3) bagaimana bandwidth, beban, media transmisi, dan VPN memengaruhi hasil; dan (4) apa keterbatasan serta peluang penelitian berikutnya.

LITERATURE REVIEW

VoIP menggunakan jaringan paket untuk membawa komunikasi suara secara real-time. Dalam implementasi yang dikaji, SIP banyak digunakan untuk registrasi dan pengendalian sesi, sedangkan RTP membawa media suara. Karena paket suara harus tiba secara berurutan dan tepat waktu, penilaian performa umumnya menggunakan delay, jitter, packet loss, dan throughput. Beberapa penelitian menambahkan Mean Opinion Score atau R-Factor untuk menerjemahkan gangguan jaringan menjadi estimasi kualitas suara yang dirasakan pengguna (Sadiq, 2017; Siboro & Affandi, 2010). Meskipun parameter tersebut muncul berulang, prosedur pengukuran dan standar interpretasinya tidak seragam sehingga angka antarpenelitian tidak dapat dibandingkan secara langsung tanpa memperhatikan konteks pengujian.

Asterisk merupakan platform inti telephony yang dapat dikonfigurasi langsung melalui berkas konfigurasi dan command line. FreePBX, pada sumber yang dikaji, diposisikan sebagai antarmuka berbasis web untuk mengontrol dan mengelola Asterisk, sedangkan Trixbox merupakan distribusi yang menggabungkan sistem operasi, Asterisk, dan antarmuka administrasi. Dengan demikian, perbandingan Asterisk dan FreePBX perlu dibaca secara hati-hati. Keduanya bukan selalu dua mesin telephony yang independen, melainkan dapat mewakili perbedaan cara instalasi dan pengelolaan sistem berbasis Asterisk (Sadiq, 2017; Siboro & Affandi, 2010).

Portabilitas dalam kajian ini merujuk pada kemampuan membawa atau menggandakan fungsi server VoIP ke perangkat lain. Prasetyo (2014) menerapkan Asterisk sebagai paket OpenWRT pada router Huawei HG553 dan TP-Link MR3020. Pendekatan embedded mengurangi kebutuhan komputer khusus, tetapi kompatibilitas firmware menjadi batas utama. Di sisi lain, implementasi Powerline Communication menggunakan jaringan listrik sebagai media pembawa data agar layanan VoIP dapat menjangkau ruangan tanpa penarikan kabel jaringan baru (Farhandika & Christianto, 2024). Kedua pendekatan

menegaskan bahwa konteks perangkat dan media transmisi merupakan bagian penting dari desain Asterisk.

Keamanan VoIP pada sumber-sumber empiris terutama dibahas melalui VPN dan pengujian penyadapan. (Rohman dan Cahyanto, 2021) menggunakan VPN PPTP serta serangan Man in the Middle, sedangkan (Putro dan Widiyastuti, 2022) menggunakan OpenVPN pada Linux Asterisk. VPN membangun jalur privat di atas jaringan publik sehingga paket suara tidak mudah dibaca oleh pihak yang tidak berwenang. Akan tetapi, keamanan yang meningkat harus dianalisis bersama kualitas layanan karena enkripsi dan enkapsulasi dapat menambah overhead. Oleh sebab itu, evaluasi Asterisk yang memadai perlu menempatkan implementasi, performa, dan keamanan sebagai tiga dimensi yang saling berkaitan.

METODE PENELITIAN

Penelitian ini menggunakan kajian literatur terstruktur dengan sintesis naratif dan tematik. Bahan kajian dibatasi pada dokumen yang diberikan dalam percakapan ini. Tahap identifikasi menemukan sembilan dokumen. Kriteria inklusi mencakup: membahas Asterisk atau distribusi yang menggunakan Asterisk sebagai inti layanan VoIP; memuat aspek implementasi, performa, atau keamanan; dan menyediakan teks lengkap yang dapat diekstraksi. Setelah penyaringan, delapan sumber dianalisis.

Setiap sumber diekstraksi ke dalam matriks yang memuat identitas, jenis dokumen, tujuan, platform, topologi atau skenario, parameter, temuan, keterbatasan, serta kontribusi terhadap pertanyaan kajian. Sumber kemudian diberi kode S01 sampai S08. Pengodean tematik menghasilkan empat kelompok utama, yaitu implementasi dan portabilitas; kinerja dan Quality of Service; keamanan dan VPN; serta keterbatasan dan peluang penelitian. Angka kuantitatif dipertahankan sesuai laporan sumber. Apabila terdapat inkonsistensi satuan atau kondisi eksperimen yang tidak terkontrol, hal tersebut dicatat sebagai keterbatasan dan tidak diperbaiki secara diam-diam.

Kajian ini tidak melakukan meta-analisis karena topologi, jumlah klien, codec, jenis jaringan, metode pengukuran, dan standar penilaian antarstudi terlalu heterogen. Buku Asterisk digunakan sebagai landasan konseptual, sedangkan tujuh penelitian empiris menjadi dasar sintesis implementasi dan hasil pengujian.

HASIL DAN PEMBAHASAN

1. Profil dan Karakteristik Sumber

Delapan sumber memperlihatkan rentang bentuk publikasi dan konteks implementasi yang luas. S01 merupakan buku teknis yang menjelaskan fondasi Asterisk, sedangkan S02-S08 merupakan penelitian implementatif atau eksperimental. Lima penelitian menggunakan Wireshark sebagai alat utama untuk menangkap trafik dan menghitung parameter QoS. Distribusi FreePBX atau Trixbox muncul pada empat studi, sementara Asterisk dipasang langsung pada Linux atau OpenWRT pada studi lainnya. Tabel 1 merangkum karakteristik utama sumber.

Tabel 1. Karakteristik delapan sumber kajian

Kode	Sumber/tahun	Platform utama	Fokus	Metode atau skenario
S01	Van Meggelen et al. (2007)	Asterisk 1.4 pada Linux	Konsep, konfigurasi, protokol, keamanan	Buku teknis dan dokumentasi konseptual
S02	Prasetyo (2014)	Asterisk-OpenWRT pada HG553 dan MR3020	Portabilitas server embedded	Backup-restore LuCI, sysupgrade, dan mtd write
S03	Sadiq (2017)	FreePBX Asterisk, SIP, G.711	QoS dan MOS E-Model	Limitasi 512, 384, 256, dan 128 Kbps
S04	Rohman & Cahyanto (2021)	Trixbox dan VPN PPTP	QoS dan keamanan MITM	Panggilan 1-6 menit; dua skenario VPN
S05	Rawadi et al. (2025)	Asterisk Linux dan VPN	Perbandingan QoS VPN/non-VPN	Delapan skenario perangkat dan operator
S06	Farhandika & Christianto (2024)	Trixbox pada jaringan PLC	QoS media listrik	Perbandingan tegangan 110 V dan 220 V
S07	Putro & Widiasari (2022)	Ubuntu, Asterisk, OpenVPN	Keamanan dan QoS	Wired/wireless, variasi jarak dan enam hari
S08	Siboro & Affandi (2010)	Asterisk dan FreePBX pada cluster	Beban dan parallel processing	Beban TCP/UDP 10, 20, dan 30 Mbyte

2. Implementasi dan Portabilitas Asterisk

Sintesis menunjukkan bahwa Asterisk dapat ditempatkan pada spektrum perangkat yang lebar. Buku teknis S01 menjelaskan Asterisk sebagai platform yang dapat menghubungkan telepon IP, jaringan PSTN, perangkat analog, dan aplikasi eksternal. Implementasi pada studi empiris kemudian mengoperasionalkan fleksibilitas tersebut pada server Linux, distribusi berbasis antarmuka web, router embedded, PLC, dan cluster. Keragaman ini menjadi keunggulan karena organisasi dapat memilih arsitektur sesuai biaya, kebutuhan administrasi, dan kapasitas sistem.

S02 memberikan bukti paling langsung mengenai portabilitas embedded. Duplikasi firmware dan konfigurasi berhasil pada dua belas skenario yang menggunakan perangkat dengan spesifikasi sama, baik dengan maupun tanpa exroot. Sebaliknya, ketiga metode restore lintas perangkat gagal karena image tidak sesuai, pemeriksaan image gagal, atau header tidak diterima. Temuan ini menunjukkan bahwa portabilitas konfigurasi tidak identik dengan portabilitas image firmware. Agar dapat dipindahkan lintas perangkat, konfigurasi Asterisk sebaiknya dipisahkan dari komponen firmware dan dependensi khusus perangkat, kemudian dipasang ulang melalui prosedur yang kompatibel dengan arsitektur tujuan (Prasetyo, 2014).

Pada S06, Trixbox digunakan sebagai server dan PLC sebagai media transmisi antarruang. Pendekatan tersebut mengurangi kebutuhan penarikan kabel data baru karena adaptor PLC memanfaatkan aliran listrik yang telah ada. Implementasi berhasil menghubungkan perangkat guru pada ruangan berbeda melalui Zoiper. Namun, PLC hanya diuji pada satu lokasi, satu model adaptor, dan aliran satu fasa sehingga generalisasi terhadap bangunan lain masih terbatas (Farhandika & Christianto, 2024).

S08 menggunakan cluster server dan node dengan tujuan meningkatkan kapasitas melalui parallel processing. Meskipun penelitian menyimpulkan parallel processing dapat meningkatkan performa server, laporan tidak memberikan ukuran kapasitas maksimum atau perbandingan terkontrol sebelum dan sesudah clustering. Nilai penting studi tersebut justru terletak pada pengaruh pembebanan jaringan dan kemudahan administrasi. FreePBX dinilai lebih mudah digunakan karena penambahan extension dapat dilakukan melalui antarmuka web, sedangkan konfigurasi Asterisk langsung membutuhkan pemahaman console dan berkas konfigurasi (Siboro & Affandi, 2010).

3. Kinerja dan Quality of Service

Delay, jitter, packet loss, dan throughput merupakan parameter yang paling konsisten digunakan. Dua studi menambahkan MOS sebagai indikator kualitas suara. Secara umum, jaringan kecil yang terkontrol menghasilkan kualitas yang dapat diterima, tetapi performa menurun ketika bandwidth dipersempit, beban UDP ditingkatkan, media transmisi kurang stabil, atau VPN menambah overhead. Ringkasan hasil kuantitatif disajikan pada Tabel 2.

S03 menunjukkan hubungan yang jelas antara bandwidth dan kualitas suara. FreePBX Asterisk menggunakan SIP dan codec G.711 A-law serta mu-law memperoleh MOS 4,3 pada kondisi tanpa queue, 512 Kbps, dan 384 Kbps. Pada 256 Kbps, MOS turun menjadi 4,1-4,2, sedangkan pada 128 Kbps turun menjadi 3,8-3,9. Penelitian menyimpulkan 384 Kbps sebagai datarate minimum untuk empat klien pada topologi yang diuji. Kesimpulan ini tidak dapat langsung diterapkan pada jumlah klien atau codec lain karena G.711 mempunyai karakteristik bandwidth berbeda dari codec terkompresi (Sadiq, 2017).

S08 memperlihatkan bahwa beban jaringan memperbesar delay, jitter, dan packet loss dibandingkan kondisi tanpa beban. Pengaruh beban UDP lebih jelas daripada TCP karena media VoIP dibawa melalui RTP di atas UDP dan UDP tidak melakukan mekanisme retransmisi seperti TCP. Studi tersebut melaporkan delay Asterisk dan FreePBX sama dan masih berada di bawah batas standar yang digunakan, sedangkan MOS FreePBX sedikit lebih tinggi. Karena FreePBX mengelola Asterisk, perbedaan MOS sebaiknya tidak ditafsirkan sebagai bukti dua mesin media yang sepenuhnya berbeda tanpa informasi konfigurasi yang lebih rinci (Siboro & Affandi, 2010).

Media transmisi juga memengaruhi hasil. Pada S06, throughput berada sekitar 175-180 Kbps, packet loss seluruh skenario 0%, dan delay serta jitter sekitar 9,4-9,6 ms. Tegangan 220 V sedikit lebih baik daripada 110 V, tetapi selisihnya kecil dan tidak mengganggu percakapan. S07 justru melaporkan nilai yang jauh lebih ekstrem, termasuk packet loss rata-rata 24% tanpa VPN dan 0,8% dengan VPN serta delay dalam satuan detik. Karena pengujian S07 mengubah jarak, media wired/wireless, kualitas kabel, dan kondisi cuaca, hasilnya menunjukkan kuatnya pengaruh konteks jaringan sekaligus membatasi perbandingan kausal VPN dan non-VPN (Putro & Wideasari, 2022).

Tabel 2. Ringkasan temuan kuantitatif penelitian performa

Kode	Skenario	Temuan utama	Interpretasi kajian
S03	G.711 dengan limitasi bandwidth	MOS 4,3 pada tanpa limitasi, 512 dan 384 Kbps; 3,8-3,9 pada 128 Kbps	Bandwidth rendah menurunkan kualitas; hasil khusus untuk empat klien dan G.711
S04	Trixbbox dengan VPN PPTP	Delay 7,758 dan 7,657 ms; packet loss 0%; throughput 299 dan 210 bps	QoS baik pada jaringan uji; satuan throughput perlu dibaca sesuai laporan sumber
S05	Asterisk VPN dan non-VPN	Delay sekitar 20 ms; jitter VPN rata-rata 9,332 ms; packet loss VPN rata-rata 2,375%; throughput tabel 80-85 Kbps	VPN menambah overhead pada sebagian skenario; terdapat inkonsistensi satuan dalam naskah
S06	PLC 110 V dan 220 V	Throughput 175-180 Kbps; packet loss 0%; delay/jitter sekitar 9,4-9,6 ms	220 V sedikit lebih baik, tetapi seluruh panggilan tetap berjalan baik
S07	Asterisk dengan dan tanpa OpenVPN	Packet loss 24% vs 0,8%; jitter 95,7 vs 94,8 ms; delay 5,3 vs 3,5 detik	Hasil dipengaruhi banyak faktor pengganggu dan tidak dapat digeneralisasi langsung
S08	Beban TCP/UDP hingga 30 Mbyte	Beban meningkatkan delay, jitter, packet loss; UDP berdampak lebih besar; MOS FreePBX sedikit lebih tinggi	Kapasitas jaringan dan jenis trafik penting bagi kualitas panggilan

4. Keamanan dan Dampak VPN

Keamanan pada sumber-sumber kajian berfokus pada kerahasiaan percakapan dan ketahanan terhadap penyadapan. S01 merekomendasikan pendekatan berlapis, meliputi pembatasan akses ke jaringan suara, pemisahan trafik suara dan data, penggunaan firewall atau VLAN, hardening server, menjalankan Asterisk sebagai non-root, keamanan fisik, serta VPN untuk trafik antarlokasi. VPN dipandang efektif, tetapi biaya performanya harus dipertimbangkan (Van Meggelen et al., 2007).

S04 memberikan bukti bahwa cakupan perlindungan endpoint menentukan hasil. Ketika kedua klien terhubung ke VPN, penyerang masih dapat memindai IP dan MAC address, tetapi tidak dapat merekam atau mendengarkan percakapan. Ketika hanya satu klien terhubung ke VPN, penyerang dapat melakukan ARP spoofing dan memperoleh rekaman singkat. Dengan demikian, perlindungan parsial meninggalkan segmen komunikasi yang tidak terlindungi dan dapat menjadi titik lemah (Rohman & Cahyanto, n.d.).

S05 dan S07 menghasilkan kesimpulan performa yang berbeda. S05 menemukan bahwa VPN menaikkan packet loss atau jitter pada sebagian skenario akibat overhead enkapsulasi dan enkripsi, walaupun delay tetap berada pada kategori baik. S07 melaporkan packet loss dan delay lebih rendah dengan OpenVPN serta menyatakan isi komunikasi tidak dapat diambil melalui Wireshark. Perbedaan tersebut tidak harus dianggap

bertentangan secara mutlak karena kedua penelitian memakai topologi, kondisi jaringan, media, dan prosedur pengujian berbeda. Sintesis yang lebih aman adalah bahwa VPN meningkatkan kerahasiaan, sedangkan dampak QoS bersifat kontekstual dan harus diuji pada lingkungan implementasi yang sebenarnya.

Penelitian yang tersedia belum membandingkan VPN modern, enkripsi media langsung, autentikasi kuat, hardening konfigurasi SIP, atau ketahanan terhadap serangan selain MITM dan sniffing. Selain itu, penggunaan PPTP pada salah satu studi mencerminkan teknologi yang lebih lama. Kajian keamanan berikutnya perlu menggunakan versi Asterisk dan protokol keamanan terkini, mendefinisikan model ancaman, memisahkan variabel keamanan dari kualitas jaringan, serta mencatat konfigurasi kriptografi secara rinci.

5. Sintesis Lintas Studi dan Kesenjangan Penelitian

Tiga pola utama muncul dari delapan sumber. Pertama, Asterisk mempunyai fleksibilitas implementasi tinggi, tetapi kompatibilitas perangkat dan dependensi sistem menentukan keberhasilan. Kedua, kualitas panggilan lebih dipengaruhi oleh kondisi jaringan dan konfigurasi daripada nama antarmuka pengelola. Ketiga, keamanan tidak dapat dipisahkan dari performa karena perlindungan tambahan dapat mengubah ukuran paket, jalur, dan beban pemrosesan.

Keterbatasan metodologis yang berulang adalah jumlah klien kecil, durasi pengujian terbatas, penggunaan satu codec, kurangnya replikasi, dan tidak adanya pengendalian faktor pengganggu. Sejumlah studi juga menggunakan perangkat atau versi perangkat lunak yang sudah lama. Selain itu, terdapat ketidakkonsistenan pelaporan satuan dan istilah. Pada S05, tabel throughput menggunakan Kbps, sementara abstrak atau kesimpulan menyebut Mbps. Pada S07, delay dilaporkan dalam detik, jauh di atas studi lain, tanpa desain yang memungkinkan isolasi penyebab. Ketidakkonsistenan tersebut perlu dipertahankan sebagai catatan kritis agar sintesis tidak memberikan kepastian yang lebih tinggi daripada bukti sumber.

Arah penelitian berikutnya meliputi pengujian versi Asterisk terkini pada perangkat modern; perbandingan codec dan protokol dengan beban panggilan yang meningkat; evaluasi konsumsi CPU, memori, energi, dan kapasitas panggilan simultan; portabilitas konfigurasi berbasis container atau otomasi alih-alih cloning firmware; serta pengujian keamanan menggunakan enkripsi dan model ancaman modern. Protokol pengujian perlu menetapkan topologi, bandwidth, jumlah klien, codec, durasi, alat ukur, standar penilaian, dan ulangan secara konsisten. Tabel 3 merangkum implikasi utama dan kesenjangan yang ditemukan.

Tabel 3. Sintesis tema, implikasi, dan peluang penelitian

Tema	Bukti utama	Implikasi	Peluang penelitian
Implementasi	Linux, FreePBX/Trixbox, OpenWRT, PLC, dan cluster	Asterisk fleksibel, tetapi bergantung pada kompatibilitas dan administrasi	Versi terkini, container, otomasi konfigurasi, dan kapasitas skala besar
Kinerja	Bandwidth, beban UDP, media, dan stabilitas jaringan memengaruhi QoS	Hasil suatu topologi tidak dapat digeneralisasi tanpa konteks	Protokol uji seragam, multi-codec, banyak klien, dan ulangan statistik

Tema	Bukti utama	Implikasi	Peluang penelitian
Keamanan	VPN mencegah pembacaan isi trafik pada beberapa skenario	Perlindungan harus end-to-end dan diuji bersama overhead	VPN modern, enkripsi media, autentikasi, dan model ancaman lebih luas
Pelaporan	Satuan dan kondisi eksperimen tidak selalu konsisten	Sintesis harus mempertahankan ketidakpastian dan keterbatasan	Dataset, konfigurasi, dan skrip uji terbuka untuk replikasi

KESIMPULAN

Kajian terhadap delapan sumber menunjukkan bahwa Asterisk merupakan platform VoIP sumber terbuka yang dapat diimplementasikan pada server Linux, distribusi FreePBX atau Trixbox, router OpenWRT, Powerline Communication, jaringan wired/wireless, dan cluster. Fleksibilitas tersebut mendukung penggunaan pada berbagai skala dan keterbatasan perangkat. Akan tetapi, portabilitas tidak selalu berlaku lintas perangkat. Duplikasi firmware berhasil pada perangkat yang sama, tetapi gagal ketika image diterapkan pada router berbeda.

Kinerja Asterisk umumnya dinilai melalui delay, jitter, packet loss, throughput, dan MOS. Hasil pada jaringan kecil relatif baik, tetapi bandwidth yang terlalu rendah, beban UDP, kualitas media transmisi, dan kondisi jaringan dapat menurunkan kualitas. VPN memberikan manfaat yang lebih konsisten pada aspek kerahasiaan daripada pada aspek performa. Beberapa penelitian menemukan tambahan overhead, sedangkan penelitian lain melaporkan QoS lebih baik dengan VPN karena perbedaan konteks dan faktor pengganggu.

Berdasarkan sintesis, pengembangan Asterisk sebaiknya menggunakan desain keamanan end-to-end, pengujian QoS pada kondisi nyata, dokumentasi konfigurasi, dan protokol eksperimen yang konsisten. Penelitian lanjutan perlu menguji versi Asterisk serta protokol keamanan modern, jumlah panggilan lebih besar, beberapa codec, dan metrik sumber daya server. Dengan pendekatan tersebut, fleksibilitas Asterisk dapat dimanfaatkan tanpa mengabaikan kualitas layanan dan perlindungan komunikasi.

REFERENCES

- Farhandika, M. K. R., & Christianto, E. (2024). Analisa Quality of Service (QoS) Voice over Internet Protocol (VoIP) pada Powerline Communication (PLC) di aliran listrik 110 volt dan 220 volt. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, 9(4), 1936-1947. <https://doi.org/10.29100/jipi.v9i4.5606>
- Prasetyo, A. B. (2014). Implementasi portabilitas VoIP menggunakan Asterisk pada OpenWRT. *Teknik Informatika, Universitas Dian Nuswantoro*.
- Putro, R. E., & Widiyari, I. R. (2022). Analisis keamanan komunikasi VoIP server portable dilengkapi OpenVPN menggunakan Linux Asterisk. *Jurnal Media Informatika Budidarma*, 6(2), 943-951. <https://doi.org/10.30865/mib.v6i2.3884>
- Rawadi, B. R., Kurniawan, W. N., Maulana, R. B., Wulandari, A., & Herfiah, S. (2025). Analisa QoS pada jaringan VoIP menggunakan Asterisk dengan VPN. *Seminar Nasional Inovasi Vokasi*, 4(1), 1081-1089.
- Rohman, M. F., & Cahyanto, T. A. (2021). Analisis QoS (Quality of Service) pada jaringan VoIP dengan menggunakan protokol VPN sebagai keamanan jaringan. *Program Studi Teknik Informatika, Universitas Muhammadiyah Jember*.

- Sadiq, A. R. (2017). Analisis kinerja VoIP open source FreePBX Asterisk menggunakan metode MOS E-Model (ITU-T G.107). Jurusan Teknik Informatika, Universitas Muhammadiyah Jember.
- Siboro, J., & Affandi, A. (2010). Analisis perbandingan performansi server VoIP antara Asterisk dengan FreePBX berbasis parallel processing. Proceeding Seminar Tugas Akhir Jurusan Teknik Elektro FTI-ITS, 1-5.
- Van Meggelen, J., Madsen, L., & Smith, J. (2007). Asterisk: The future of telephony (2nd ed.). O'Reilly Media.