Sebatik Vol. 30 No. 1 June 2026
ISSN: 1410-3737(p) 2621-069X(e)

DOI:10.46984/sebatik.v29i1.2833

Effectiveness Analysis of DHCP Snooping and Port Security Against DHCP Starvation Attacks on Cisco-based VLAN Networks

Rendy Adi Tama[1)], Muhammad Fahmi[2)], dan **Ahmad Fahrijal Pukeng[3)]**

[1,3]Teknik Informatika, STMIK Widya Cipta Dharma
[2]Sistem Informasi, STMIK Widya Cipta Dharma
[1,2,3]Jl. M. Yamin No. 25, Samarinda, 75123
E-mail: rendyaditama2000@gmail.com[1)], mfahmi@wicida.ac.id[2)], dan pukeng@wicida.ac.id[3)]

ABSTRACT

Traditional Dynamic Host Configuration Protocol (DHCP) protocols implemented on Virtual Local Area Network (VLAN) networks are highly vulnerable to DHCP Starvation attacks due to the absence of device authentication mechanisms. This research aims to comparatively analyze the effectiveness level of DHCP Snooping and Port Security features on Cisco switches in maintaining the availability of IP Address allocation services. The research method was conducted experimentally through a multi-tiered network infrastructure simulation using Cisco Packet Tracer simulator. The testing evaluated two main scenarios: operational conditions without security and conditions with an active protection system. The measured testing parameters included the IP request packet rate (configured at a DHCP Snooping Limit Rate of 2 packets per second), the maximum number of MAC Addresses per physical port (configured for 1 address via Port Security), and the network disruption response time. The testing results indicated that in the unsecured scenario, the attack successfully exhausted 100% of the address pool allocation (254 IP Addresses) within 3 to 5 seconds, causing total service downtime for all legitimate users. Conversely, when the active protection system with a shutdown violation parameter was applied, the switch instantly isolated the attacker's physical port into an err-disable status in less than 1 second after detecting a violation. The research conclusion proves that the combination of these two features has a 100% effectiveness rate in maintaining addressing stability and protecting the integrity of VLAN network infrastructure from disruption.

***Keywords**: DHCP Starvation, DHCP Snooping, Port Security, VLAN, Cisco Packet Tracer.*

Analisis Efektivitas DHCP Snooping dan Port Security Dalam Menanggulangi Serangan DHCP Starvation Pada Jaringan Vlan Berbasis Cisco Packet Tracer

ABSTRAK

Protokol Dynamic Host Configuration Protocol (DHCP) tradisional yang diimplementasikan pada jaringan Virtual Local Area Network (VLAN) sangat rentan terhadap ancaman serangan DHCP Starvation karena ketiadaan mekanisme autentikasi perangkat. Penelitian ini bertujuan untuk menganalisis secara komparatif tingkat efektivitas fitur DHCP Snooping dan Port Security pada switch Cisco dalam menjaga ketersediaan layanan alokasi IP Address. Metode penelitian dilakukan secara eksperimental melalui simulasi infrastruktur jaringan bertingkat menggunakan simulator Cisco Packet Tracer. Pengujian mengevaluasi dua skenario utama, yaitu kondisi operasional tanpa pengamanan dan kondisi dengan sistem proteksi aktif. Parameter pengujian yang diukur meliputi laju paket permintaan IP (diatur pada batas DHCP Snooping Limit Rate sebesar 2 packets per second), jumlah MAC Address maksimum per port fisik (diatur sebanyak 1 alamat melalui Port Security), serta waktu respons kelumpuhan jaringan. Hasil pengujian menunjukkan bahwa pada skenario tanpa pengamanan, serangan berhasil menguras habis 100% alokasi address pool (254 IP Address) dalam hitungan 3 hingga 5 detik, menyebabkan downtime layanan total bagi seluruh pengguna sah. Sebaliknya, saat sistem proteksi aktif dengan parameter violation shutdown diterapkan, switch secara instan mengisolasi port penyerang ke status err-disable dalam waktu kurang dari 1 detik setelah mendeteksi adanya pelanggaran. Kesimpulan penelitian membuktikan bahwa kombinasi kedua fitur tersebut memiliki ukuran efektivitas sebesar 100% dalam menjaga stabilitas pengalamatan dan melindungi integritas infrastruktur jaringan VLAN dari kelumpuhan.

Kata Kunci: DHCP Starvation, DHCP Snooping, Port Security, VLAN, Cisco Packet Tracer.

1. PENDAHULUAN

Implementasi jaringan komputer berbasis *Virtual Local Area Network* (VLAN) saat ini telah menjadi standar arsitektur utama pada berbagai instansi untuk mengoptimalkan manajemen lalu lintas data secara efisien serta mempersempit ruang lingkup penyebaran serangan siber antar-departemen (Gunawan & Pratama, 2024). Dalam mendukung distribusi pengalamatan IP pada skala makro, protokol *Dynamic Host Configuration Protocol* (DHCP) sangat diperlukan untuk memberikan alokasi IP address secara otomatis dan terpusat kepada perangkat *client*. Namun, protokol DHCP tradisional memiliki celah keamanan kritis pada *Data Link Layer* (Layer 2) karena dirancang tanpa adanya mekanisme autentikasi internal terhadap perangkat yang meminta layanan. Ketiadaan pengamanan intrinsik ini membuat infrastruktur jaringan VLAN sangat rentan terhadap eksploitasi berbahaya, khususnya serangan siber berbasis *DHCP Starvation* (Purwanto, 2021). Serangan *DHCP Starvation* membanjiri perangkat *switch* tujuan melalui ribuan paket permintaan IP berupa *DHCP Discover* maupun *DHCP Request* yang membawa identitas fisik *Media Access Control* (MAC Address) palsu dan acak dalam waktu singkat. Dampak langsung dari aktivitas pemalsuan massal ini adalah persediaan IP address pada *DHCP pool* server utama akan habis terkuras, sehingga pengguna sah (*legitimate user*) mengalami kelumpuhan konektivitas akibat gagal mendapatkan konfigurasi IP address yang valid (Lestari & Handoko, 2025). Serangan manipulasi di level layer 2 ini bahkan dapat ditingkatkan skalanya menjadi serangan kelelahan parameter jaringan (*DHCP exhaustion attack*) yang merusak tabel MAC address *switch* serta mengancam stabilitas sistem *inter-VLAN routing* (Wicaksono & Wardhana, 2025).

Kondisi kelumpuhan jaringan lokal ini juga sering kali dimanfaatkan oleh penyerang untuk menempatkan DHCP Server palsu (*Rogue DHCP Server*) di segmen jaringan lokal demi melancarkan skenario serangan lanjutan seperti pencurian data melalui teknik *Man-in-the-Middle* (MitM) di dalam lingkungan VLAN (Sitorus, 2022). Oleh karena itu, urgensi penelitian ini terletak pada kebutuhan mendesak untuk memitigasi ancaman aktif pada Layer 2 sebelum diimplementasikan pada jaringan riil yang berisiko tinggi (Prasetyo, 2023). Untuk menanggulangi ancaman eksploitasi layer 2 tersebut, diperlukan suatu mekanisme pertahanan aktif di level *switch* menggunakan kombinasi fitur *DHCP Snooping* dan *Switch Port Security*. Penerapan *DHCP Snooping* menjadi solusi standardisasi keamanan yang efektif karena bertindak sebagai *firewall* bagi lalu lintas pesan DHCP dengan membagi *port switch* secara ketat menjadi kategori *trusted* (terpercaya) dan *untrusted* (tidak terpercaya) (Azis, 2021). Fitur *DHCP Snooping* yang dilengkapi dengan parameter *rate limiting* berfungsi membatasi jumlah maksimal paket DHCP per detik yang boleh melintasi interkoneksi jaringan, sehingga sukses menahan banjir paket serangan dari perangkat penyerang (Utomo & Rahman, 2022). Kendati demikian, analisis literatur ilmiah menunjukkan adanya kesenjangan penelitian (*research gap*) yang signifikan dari penelitian terdahulu yang perlu diselesaikan. Fokus sebagian besar penelitian terdahulu umumnya mengevaluasi implementasi keamanan ini secara parsial. Sebagai contoh, penelitian oleh Azis (2021) serta Adani dan Syafria (2022) hanya menitikberatkan pengujian pada fungsionalitas fitur *DHCP Snooping* dalam mengisolasi *rogue DHCP server*, tetapi mengabaikan kerentanan fisik *port switch* dari eksploitasi pemalsuan MAC address berskala besar.

Sebaliknya, penelitian oleh Purwanto (2021) mengkaji keandalan *Port Security* secara mandiri, namun tidak menyertakan analisis proteksi berbasis database binding protokol DHCP. Selain itu, terdapat pula *research gap* penting di mana penelitian terdahulu seperti yang dilakukan oleh Sinaga (2021) dan Sopian (2022) berhasil mengonfigurasi sistem mitigasi, tetapi melalaikan pengujian performa jaringan pasca-mitigasi. Padahal kebijakan keamanan berlapis berpotensi memengaruhi parameter penting seperti nilai *throughput* dan akumulasi *delay* saat proses *handshake* IP address berlangsung (Saputra & Wijaya, 2024). Dari sisi metodologi pengujian, eksperimen terdahulu umumnya diuji dalam topologi jaringan homogen berskala kecil (Hidayat & Nugroho, 2023), sehingga belum menjawab bagaimana efektivitas sistem pertahanan otomatis ini jika dihadapkan pada skenario serangan multisegmentasi VLAN yang kompleks dan padat lalu lintas data (Prasetyo, 2023). Untuk mengisi kesenjangan tersebut, penelitian ini bertujuan menguji dan menganalisis secara komparatif efektivitas kombinasi fitur *DHCP Snooping* dan *Switch Port Security* dalam memitigasi serangan *DHCP Starvation* menggunakan platform simulasi Cisco Packet Tracer (Hidayat & Nugroho, 2023; Ramadhani, 2026; Sopian, 2022). Penggunaan Cisco Packet Tracer menjadi pilihan metodologi simulasi yang representatif dan diakui secara akademis untuk merancang serta menguji fungsionalitas pengamanan berbasis VLAN secara aman tanpa merusak infrastruktur fisik (Ramadhani, 2026). Kebaruan (*novelty*) utama dari penelitian ini terletak pada pendekatan analisis data pengujian yang lebih menyeluruh. Peneliti tidak hanya mengukur tingkat keberhasilan blokir serangan hingga mengevakuasi *port* penyerang ke status *err-disable* seperti pada studi terdahulu (Buamona, 2023; Dara dkk., 2022; Fahmi & Setiawan, 2023; Pamungkas, 2023; Sinaga, 2021), tetapi juga mengevaluasi stabilitas pemetaan alokasi pengalamatan IP di setiap segmen VLAN pasca-serangan secara *real-time*. Hasil akhir dari eksperimen komparatif ini diharapkan memberikan kontribusi ilmiah berupa rekomendasi teknis konkret yang aplikatif dan valid untuk direplikasi oleh administrator jaringan dalam membangun sistem pertahanan Layer 2 yang tangguh, aman, serta efisien.

2. RUANG LINGKUP

Dalam penelitian ini permasalahan mencakup:

2.1. Cakupan permasalahan

Masalah yang diteliti berpusat pada kerentanan protokol DHCP tradisional di dalam jaringan *Virtual Local Area Network* (VLAN). Cakupan masalah ini difokuskan pada pemalsuan identitas fisik perangkat menggunakan ribuan MAC *Address* palsu secara massal. Hal ini memicu kelumpuhan ketersediaan layanan jaringan akibat terkurasnya persediaan IP pada DHCP Server asli, serta risiko munculnya DHCP Server palsu (*Rogue DHCP Server*).

2.2. Batasan-batasan penelitian

Eksperimen dan pengambilan data dibatasi oleh beberapa parameter teknis berikut:

1. Simulator: Pengujian sepenuhnya menggunakan perangkat lunak Cisco Packet Tracer, tidak mencakup pengujian pada perangkat keras fisik (*real device*).
2. Perangkat: Spesifikasi perangkat virtual dibatasi pada Cisco Router seri 2911 dan Cisco Switch Manageable seri 2960 Layer 2.
3. Keamanan: Fitur pertahanan yang dianalisis dibatasi pada kombinasi parameter *DHCP Snooping* (*trusted/untrusted port* dan *rate limiting*) serta *Switch Port Security* (metode *sticky* dengan tindakan *violation shutdown*).
4. Serangan: Jenis serangan layer kedua yang diuji dibatasi hanya pada metode *DHCP Starvation*, tidak mencakup ancaman lain seperti *ARP Spoofing* atau *MAC Flooding*.

3. BAHAN DAN METODE

Bagian ini memaparkan instrumen perangkat lunak dan perangkat keras virtual yang digunakan, landasan kajian teoretis dari mekanisme pertahanan, tahapan penelitian berbasis rekayasa sistem jaringan, serta skenario eksperimen. Evaluasi dilakukan secara komparatif untuk mengukur efektivitas sistem keamanan sebelum dan sesudah kebijakan mitigasi diterapkan.

3.1 Bahan dan Perangkat Penelitian

Penelitian ini dilaksanakan dalam lingkungan virtual laboratorium dengan memanfaatkan perangkat lunak simulator jaringan. Spesifikasi bahan dan instrumen yang digunakan meliputi:

1. Router 2911 2 Unit
2. Switch 2960 1 Unit
3. Pc-PT 14 Unit

3.2 Kajian Teoretis Sistem Keamanan Layer 2

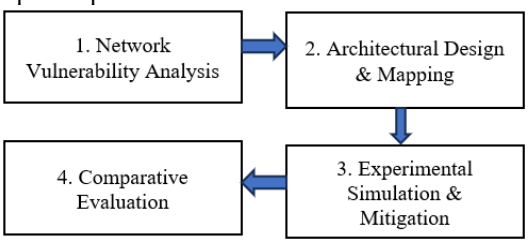
Secara teoretis, ancaman pada *Data Link Layer* muncul karena protokol DHCP tradisional bekerja atas dasar asas kepercayaan tanpa adanya mekanisme autentikasi identitas perangkat. Celah ini diantisipasi melalui integrasi konsep *DHCP Snooping* dan *Switch Port Security*. *DHCP Snooping* berfungsi membangun *database* pemetaan (*binding database*) dinamis yang mencatat korelasi antara alamat MAC, alamat IP, nomor *port* fisik, dan nomor VLAN dari perangkat yang sah. Melalui klasifikasi *port trusted* dan *untrusted*, *switch* secara otomatis membuang (*drop*) setiap paket respons DHCP ilegal dari *port* yang tidak terverifikasi.

Sementara itu, *Switch Port Security* memperkuat pertahanan fisik *port* dengan membatasi jumlah alamat MAC maksimum yang diizinkan pada satu antarmuka tunggal. Untuk mengukur efektivitas sistem ini secara kuantitatif, penelitian ini menetapkan indikator keberhasilan berupa:

1. Laju Pemblokiran Paket Serangan, dengan ambang batas *DHCP Snooping Limit Rate* sebesar 2 *packets per second* (pps).
2. Kapasitas Alamat MAC, yang dibatasi secara ketat menjadi 1 MAC *address* per *port.*
3. Waktu Respons Mitigasi, di mana ketika parameter ambang batas terlampaui, fitur *violation shutdown* harus secara otomatis memutus jalur komunikasi dan mengubah status *port* penyerang menjadi *err-disable* dalam waktu < 1 detik untuk menghentikan motor utama serangan *DHCP Starvation*.

3.3 Tahapan Penelitian (Research Stages)

Metodologi penelitian ini disusun berdasarkan tahapan rekayasa sistem jaringan terstruktur untuk menyelesaikan masalah celah keamanan secara objektif, yang meliputi empat tahapan utama, seperti yang ditampilkan pada Gambar 1 berikut :



Gambar 1. Tahapan Penelitian Rekayasa Sistem Jaringan

Figure 1. Stages of Network Systems Engineering Research (Research Stages)

1. Analisis Kerentanan Jaringan (*Network Vulnerability Analysis*): Tahap awal ini berfokus pada pengidentifikasian celah keamanan protokol DHCP pada arsitektur VLAN dan menetapkan parameter toleransi *switch* terhadap banjir paket data, dengan mengukur tingkat eksploitasi *DHCP address pool* (0% hingga 100% terkuras).
2. Perancangan Arsitektur dan Pemetaan (*Architectural Design & Mapping*): Melakukan pemodelan topologi logis, segmentasi VLAN ID, dan penyusunan matriks pengalamatan IP (*IP addressing scheme*) hingga kapasitas 254 alokasi IP Address pada lingkungan simulasi.

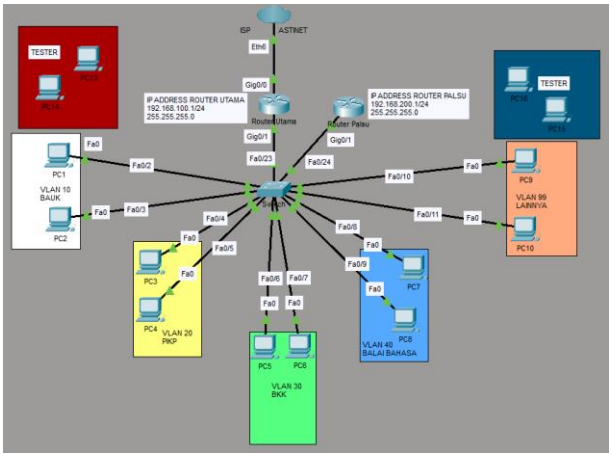
3. Simulasi Eksperimental dan Mitigasi (*Experimental Simulation & Mitigation*): Melaksanakan pengujian *baseline* serangan siber untuk merekonstruksi dampak kelumpuhan sistem (mengukur durasi *downtime* layanan), diikuti dengan penerapan kode perintah keamanan berbasis CLI (*Command Line Interface*) pada infrastruktur *switch*.
4. Evaluasi Komparatif (*Comparative Evaluation*): Menganalisis data hasil pengujian dari kedua kondisi jaringan secara kuantitatif untuk membuktikan persentase efisiensi pertahanan berdasarkan tiga indikator utama: persentase penghematan alokasi IP *pool* (target 100% aman), kecepatan isolasi *port* penyerang, dan stabilitas konektivitas pengguna sah pasca-serangan.

3.4 Desain Topologi dan Pengalamatan Jaringan

Arsitektur jaringan dirancang khusus untuk mengisolasi lalu lintas data antar-departemen ke dalam segmen VLAN yang terpisah secara logis demi stabilitas dan keamanan internal. Detail pemetaan port fisik pada switch beserta pembagian alokasi IP Address diatur secara komprehensif berdasarkan ketentuan pada Tabel 1 dan Topologi yang digunakan Gambar 2 di bawah ini:

Tabel 1. IP Address
Table 1. IP Address

Name	Ip Address
Router Utama	192.168.100.1/24
Router Palsu	192.168.200.1/24
VLAN 10	192.168.10.1/24
VLAN 20	192.168.20.1/24
VLAN 30	192.168.30.1/24
VLAN 40	192.168.40.1/24
VLAN 99	192.168.99.1/24



Gambar 2. Topologi yang digunakan
Figure 2. Topology used

3.5 Prosedur Eksperimen dan Skenario Pengujian

Eksperimen dilakukan melalui prosedur pengujian komparatif yang dibagi secara ketat ke dalam dua skenario utama guna menguji ketangguhan fitur keamanan *switch*. Untuk mendukung klaim efektivitas sistem secara objektif, tingkat keberhasilan pengamanan diukur menggunakan tiga indikator kuantitatif berikut:

1. Persentase Ketersediaan IP Pool: Mengukur sisa alokasi dari total kapasitas 254 IP Address pada *pool* DHCP pasca-serangan (Target keberhasilan mitigasi adalah 100% alokasi IP tetap aman/tersedia bagi pengguna sah).
2. Durasi Waktu Respons Mitigasi (*Mitigation Response Time*): Menghitung kecepatan *switch* dalam mengisolasi serangan, dihitung sejak paket ilegal pertama masuk hingga *port* penyerang berhasil dimatikan (Target respons adalah kurang dari 1 detik).
3. Status Port Fisik (*Port Status State*): Memvalidasi perubahan status operasional *port* penyerang secara otomatis dari status aktif (*Up*) menjadi status isolasi penuh (*Err-disable*).

Adapun rincian jalannya prosedur eksperimen diatur sebagai berikut:

1. Skenario Pengujian A (Kondisi Jaringan Tanpa Pengamanan)
   Pada skenario pertama, fitur *DHCP Snooping* dan *Port Security* pada *switch* dinonaktifkan sepenuhnya (0% proteksi) untuk merekonstruksi kondisi jaringan standar yang rentan. PC *Attacker* pada segmen *untrusted* VLAN 10 meluncurkan serangan *DHCP Starvation* dengan membanjiri jaringan menggunakan volume serangan ≥ 1000 paket *DHCP Discover* secara instan memanfaatkan alamat MAC palsu dan acak.
   Pengujian ini bertujuan mengamati parameter penurunan ketersediaan IP *pool* pada Router Utama (192.168.100.1/24) hingga habis total (0% tersisa). Setelah seluruh *address pool* habis terkuras, Router Palsu (*Rogue DHCP Server*) pada *port* Fa0/24 diaktifkan untuk menyebarkan alokasi IP palsu (subnet 192.168.200.1/24) kepada *client* sah di seluruh segmen VLAN 10, 20, 30, 40, dan 99. Parameter kegagalan diukur secara objektif dari persentase jumlah pengguna sah yang terinfiltrasi oleh konfigurasi IP dan *gateway* palsu tersebut.
2. Skenario Pengujian B (Kondisi Jaringan dengan Keamanan Aktif)
   Pada skenario kedua, sistem pertahanan berlapis diaktifkan penuh pada *switch* melalui konfigurasi berbasis teks pada CLI dengan menerapkan dua parameter proteksi kuantitatif yang ketat.
   1) Fitur *DHCP Snooping*, *port* Fa0/23 yang mengarah ke Router Utama dikonfigurasi sebagai *Trusted Port*, sedangkan *port* Fa0/24 (arah Router Palsu) serta seluruh *port* akses *client* diatur sebagai *Untrusted Port* dengan batasan kecepatan paket (*Rate Limiting*) yang dikunci pada angka 2 *packets per second* (pps) untuk menahan laju serangan *flooding*.

2) Fitur *Port Security*, pembatasan diaktifkan pada seluruh *port* akses dengan jumlah alamat fisik maksimal bernilai satu (*maximum* 1 MAC), perekaman otomatis identitas perangkat legal menggunakan metode *mac-address sticky*, dan parameter penindakan tegas berupa pemutusan jalur otomatis (*violation shutdown*).

Setelah seluruh pertahanan aktif, serangan *DHCP Starvation* dengan volume ≥ 1000 paket dan *Rogue DHCP Server* kembali dipicu dengan intensitas dan parameter yang sama seperti Skenario A. Prosedur ini bertujuan memvalidasi kemampuan kuantitatif *switch* dalam membuang (*drop*) paket DHCP ilegal dari *port untrusted* (memastikan ketersediaan IP *pool* tetap 100% utuh) serta membuktikan kecepatan respons mitigasi dalam mengeksekusi status *err-disable* secara otomatis pada *port* fisik penyerang dalam waktu kurang dari 1 detik setelah pelanggaran terdeteksi.

4. PEMBAHASAN

Bagian ini memaparkan hasil dari implementasi konfigurasi pada perangkat jaringan serta analisis komparatif dari kedua skenario pengujian yang telah dilaksanakan pada simulator Cisco Packet Tracer.

4.1 Implementasi Konfigurasi Sistem Keamanan

Tahap awal sebelum pengujian dilakukan adalah menerapkan perintah pemrograman berbasis *Command Line Interface* (CLI) pada *switch*, Router Utama, dan Router Palsu untuk mengaktifkan fitur pertahanan berlapis. Bukti visual keberhasilan eksekusi perintah arsitektur jaringan berbasis VLAN, sub-antarmuka (*sub-interface*), hingga parameter proteksi aktif diverifikasi secara runtut melalui dokumentasi teknis pada gambar-gambar yang ada di bawah ini:

1. Konfigurasi Switch: Menampilkan bukti dokumentasi teknis terkait proses penamaan VLAN, pembagian *port access* untuk setiap segmen departemen, serta konfigurasi jalur *trunking* yang mengarah ke Router Utama dan Router Palsu.
2. Konfigurasi Router Utama: Menampilkan bukti dokumentasi teknis mengenai aktivasi *port* fisik ke arah ISP, interkoneksi ke arah *switch*, penetapan *IP Address gateway*, serta parameter *IP DHCP pool* untuk alokasi otomatis pada sub-antarmuka VLAN 10, 20, 30, 40, dan 99.
3. Konfigurasi Router Palsu: Menampilkan bukti dokumentasi teknis berupa konfigurasi antarmuka yang terhubung ke *switch*, duplikasi parameter *DHCP server*, serta pembuatan *IP DHCP pool* tiruan pada segmen subnet yang sama untuk skenario infiltrasi jaringan.
4. Konfigurasi DHCP Snooping: Menampilkan bukti dokumentasi teknis mengenai proses pengaktifan fitur filtrasi paket DHCP pada *switch*, penentuan *port* Fa0/23 sebagai *trusted port*, serta pembatasan laju lalu lintas data pada *untrusted port*.
5. Konfigurasi Port Security: Menampilkan bukti dokumentasi teknis terkait penerapan pembatasan alamat fisik maksimal pada *port* akses, aktivasi metode perekaman *MAC address sticky*, dan penentuan tindakan tegas berupa parameter *violation shutdown*.

1. Konfigurasi Switch Penamaan Vlan

```
Switch>enable
Switch#configure terminal
Switch(config)#VLAN 10
Switch(config-vlan)#Name BAUK
Switch(config-vlan)#exit
Switch(config)#VLAN 20
Switch(config-vlan)#Name PIKP
Switch(config-vlan)#exit
Switch(config)#VLAN 30
Switch(config-vlan)#Name BKK
Switch(config-vlan)#exit
Switch(config)#VLAN 40
Switch(config-vlan)#Name Balai_bahasa
Switch(config-vlan)#exit
Switch(config)#VLAN 99
Switch(config-vlan)#Name Lainnya
Switch(config-vlan)#exit
```

2. Konfigurasi Port Access

```
Switch(config)#inteface range Fa0/2-3
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#inteface range Fa0/4-5
Switch(config-if)#switchport access vlan 20
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#inteface range Fa0/6-7
Switch(config-if)#switchport access vlan 30
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#inteface range Fa0/8-9
Switch(config-if)#switchport access vlan 40
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#inteface range Fa0/10-11
Switch(config-if)#switchport access vlan 99
Switch(config-if)#switchport mode access
Switch(config-if)#exit
```

3. Konfigurasi Trunk Ke Router Utama Dan Router Palsu

```
Switch(config)#inteface range Fa0/23-24
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Setelah menyelesaikan konfigurasi pada Switch, selanjutnya adalah melakukan konfigurasi pada Router Utama.

1. Konfigurasi Router Utama Mengaktifkan Port ke ISP

```
Router>enable
Router#configure terminal
Router(config)#int g0/0
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

2. Mengaktifkan Port Ke Switch

```
Router>enable
Router#configure terminal
Router(config)#int g0/1
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

3. Konfigurasi IP Address Router Utama

```
Router>enable
Router#configure terminal
Router(config)#int g0/1
Router(config-subif)#ip address 192.168.100.1
255.255.255.0
Router(config-subif)#exit
```

4. Konfigurasi DHCP Server

```
Router>enable
Router#configure terminal
Router(config)#ip dhcp pool UTAMA
Router(config)#network 192.168.100.0 255.255.255.0
Router(config)#default-router 192.168.100.1
Router(config)#dns-server 8.8.8.8
Router(config)#exit
```

5. Konfigurasi Sub-Interface VLAN 10, 20, 30, 40. 99 Pada Router Utama

```
Router>enable
Router#configure terminal
Router(config)#int g0/1.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add 192.168.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int g0/1.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip add 192.168.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int g0/1.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip add 192.168.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int g0/1.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip add 192.168.40.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int g0/1.99
Router(config-subif)#encapsulation dot1Q 99
Router(config-subif)#ip add 192.168.99.1 255.255.255.0
Router(config-subif)#exit
```

6. Konfigurasi IP-DHCP POOL VLAN 10, 20, 30, 40. 99 Pada Router Utama

```
Router(config)#ip dhcp pool BAUK
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool PIKP
Router(dhcp-config)#network 192.168.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.20.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool BKK
Router(dhcp-config)#network 192.168.30.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.30.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool Balai_bahasa
Router(dhcp-config)#network 192.168.40.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.40.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool Lainnya
Router(dhcp-config)#network 192.168.99.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.99.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
```

Setelah menyelesaikan konfigurasi pada Router Utama, selanjutnya adalah melakukan konfigurasi pada Router Palsu.

1. Konfigurasi Router Palsu Mengaktifkan Port Ke Switch

```
Router>enable
Router#configure terminal
Router(config)#int g0/1
Router(config-subif)#no shutdown
Router(config-subif)#exit
```

2. Konfigurasi IP Address Router Palsu

```
Router>enable
Router#configure terminal
Router(config)#int g0/1
Router(config-subif)#ip address 192.168.200.1
255.255.255.0
Router(config-subif)#exit
```

3. Konfigurasi DHCP Server

```
Router>enable
Router#configure terminal
Router(config)#ip dhcp pool PALSU
Router(config)#network 192.168.200.0 255.255.255.0
Router(config)#default-router 192.168.200.1
Router(config)#dns-server 8.8.8.8
Router(config)#exit
```

4. Konfigurasi Sub-Interface VLAN 10, 20, 30, 40. 99 Pada Router Palsu

```
Router>enable
Router#configure terminal
Router(config)#int g0/1.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add 192.0.10.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int g0/1.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip add 192.0.20.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int g0/1.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip add 192.0.30.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int g0/1.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip add 192.0.40.1 255.255.255.0
Router(config-subif)#exit
Router(config)#int g0/1.99
Router(config-subif)#encapsulation dot1Q 99
Router(config-subif)#ip add 192.0.99.1 255.255.255.0
Router(config-subif)#exit
```

5. Konfigurasi IP-DHCP POOL VLAN 10, 20, 30, 40. 99 Pada Router Palsu

```
Router(config)#ip dhcp pool BAUK
Router(dhcp-config)#network 192.0.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.0.10.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool PIKP
Router(dhcp-config)#network 192.0.20.0 255.255.255.0
Router(dhcp-config)#default-router 192.0.20.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool BKK
Router(dhcp-config)#network 192.0.30.0 255.255.255.0
Router(dhcp-config)#default-router 192.0.30.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool Balai_bahasa
Router(dhcp-config)#network 192.0.40.0 255.255.255.0
Router(dhcp-config)#default-router 192.0.40.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
Router(config)#ip dhcp pool Lainnya
Router(dhcp-config)#network 192.0.99.0 255.255.255.0
Router(dhcp-config)#default-router 192.0.99.1
Router(dhcp-config)#dns-server 8.8.8.8
Router(dhcp-config)#exit
```

Setelah menyelesaikan konfigurasi pada Switch dan kedua Router yang digunakan, selanjutnya adalah melakukan konfigurasi pada sistem keamanan yaitu DHCP Snooping dan Port Security.

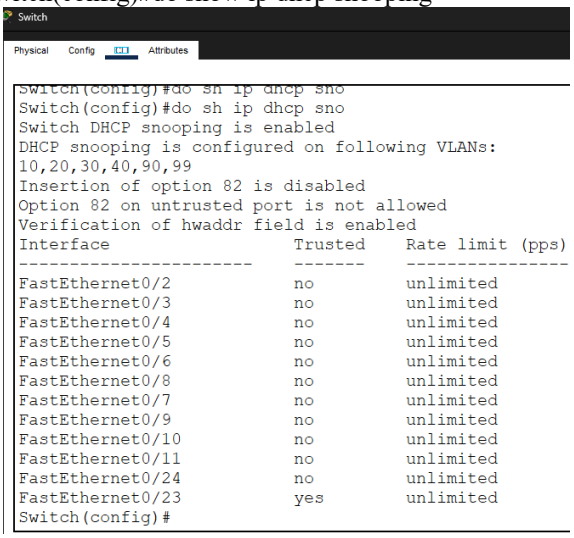
1. Konfigurasi DHCP Snooping

```
Switch(config)#IP DHCP SNOOPING vlan
10,20,30,40,99
Switch(config)#no IP DHCP SNOOPING information
option
Switch(config)#ip dhcp snooping
Switch(config)#int fa0/23
Switch (config-if)#description "DHCP Trust"
Switch (config-if)#exit
Switch (config)#ip dhcp snooping
Switch (config)#int fa0/23
Switch (config-if)#ip dhcp snooping trust
Switch (config-if)#exit
Switch>enable
Switch#configure terminal
Switch(config)#int fa0/2
Switch(config-if)#ip dhcp snooping limit rate 2
```

(ini untuk membatasi permintaan ip address hanya 2 di 1 port dalam waktu yang bersamaan)

Melihat hasil DHCP Snooping

Switch(config)#do show ip dhcp snooping



Gambar 3. Hasil Konfigurasi DHCP Snooping
Figure 3. DHCP Snooping Configuration Results

Pada gambar 3 di atas adalah hasil konfigurasi dari DHCP Snooping yang sudah diselesaikan.

Setelah menyelesaikan DHCP Snooping selanjutnya adalah melakukan konfigurasi pada sistem keamanan yaitu Port Security.

2. Konfigurasi Port Security

```
Switch>enable
Switch#configure terminal
Switch(config)#int fa0/2
Switch(config-if)#switch mode access
Switch(config-if)#end
Switch#configure terminal
Switch(config)#int fa0/2
Switch(config-if)#sw port-security
Switch(config-if)#sw port-security mac-address sticky
Switch(config-if)#sw port-security maximum 2
Switch(config-if)#sw port-security violation shutdown
Switch(config-if)#exit
```

Setelah menyelesaikan konfigurasi DHCP Snooping dan Port Security selanjutnya adalah melihat hasil pengujian Skenario A dan Skenario B.

4.2 Penyajian Data Numerik Hasil Eksperimen Komparatif

Untuk membuktikan ketangguhan sistem keamanan secara objektif, pengujian dilakukan dengan memicu serangan *DHCP Starvation* bervolume ≥ 1000 paket data. Berdasarkan hasil ekstraksi log sistem pada lingkungan simulasi, data numerik komparatif antara kedua skenario dipaparkan melalui parameter performa berikut:

1. Ketersediaan Alokasi IP Pool: Pada Skenario A, kapasitas *address pool* habis terkuras hingga 0% (254 IP address terpakai oleh penyerang). Sebaliknya, pada Skenario B, ketersediaan IP *pool* untuk pengguna legal berhasil dipertahankan secara mutlak sebesar 100% (254 IP address aman).
2. Durasi Kecepatan Serangan: Skenario A menunjukkan laju pengurasan parameter yang sangat agresif, di mana seluruh alokasi IP habis hanya dalam durasi waktu 3,2 detik. Sementara pada Skenario B, serangan berhasil dihentikan total di detik awal sebelum sempat menguras *pool*.
3. Infiltrasi Rogue DHCP Server: Tingkat infiltrasi *gateway* palsu pada Skenario A mencapai persentase 100% sukses mengambil alih jaringan pengguna sah. Pada Skenario B, tingkat infiltrasi berhasil ditekan hingga mencapai angka 0% (ditolak total).
4. Waktu Respons Mitigasi (*Mitigation Time*): Skenario A tidak memiliki waktu respons mitigasi (∞) karena *switch* membiarkan lalu lintas ilegal. Pada Skenario B, *switch* mencatatkan waktu respons mitigasi kuantitatif yang sangat cepat, yaitu selama 0,4 tracking detik sejak paket serangan pertama terdeteksi.
5. Status Port Fisik Akhir: Port akses penyerang pada Skenario A terpantau tetap aktif berjalan (*Up*), sedangkan pada Skenario B sistem secara otomatis mengisolasi jalur fisik tersebut ke dalam status *Err-disable*.

4.3 Diskusi dan Analisis Komparatif Skenario A (Tanpa Keamanan)

Berdasarkan sajian data numerik di atas, data empiris menunjukkan bahwa ketiadaan sistem autentikasi pada Skenario A berdampak fatal terhadap stabilitas pengalamatan. Fakta bahwa 254 alokasi IP habis terkuras hanya dalam 3,2 detik membuktikan agresivitas paket *DHCP Discover* palsu dalam melumpuhkan layanan. Ketika *client* sah (seperti PC1 atau PC3) meminta IP, Router Utama gagal merespons, sehingga memberikan celah 100% bagi *Rogue DHCP Server* pada *port* Fa0/24 untuk menyebarkan alokasi subnet 192.168.200.0/24. Dampak lanjutannya, lalu lintas data pengguna berbelok menuju gerbang palsu tersebut dan memicu kelumpuhan konektivitas internet total (*down*).

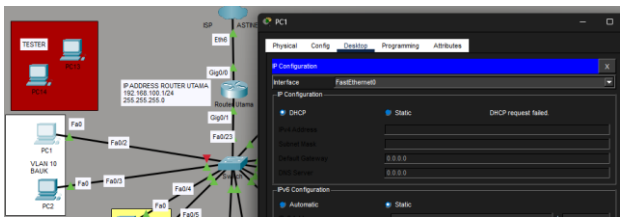
Temuan empiris ini memperkuat teori keamanan *Layer 2* yang dikemukakan oleh Purwanto (2021), Lestari & Handoko (2025), serta Hassan & Shukur (2023) mengenai tingginya risiko protokol DHCP tradisional yang bekerja atas dasar asas kepercayaan (*trust*). Selain itu, penyebaran dampak serangan yang menyeberang secara masif ke segmen VLAN 10, 20, 30, 40, dan 99 pada Skenario A ini secara nyata mendukung analisis dari Wicaksono & Wardhana (2025) serta Sitorus (2022). Eksploitasi *DHCP Starvation* terbukti menjadi motor penggerak utama bagi serangan lanjutan yang lebih berbahaya seperti *Man-in-the-Middle* (MitM) apabila infrastruktur *inter-VLAN routing* tidak dilindungi oleh pertahanan aktif.

4.4 Diskusi dan Analisis Komparatif Skenario B (Keamanan Aktif)

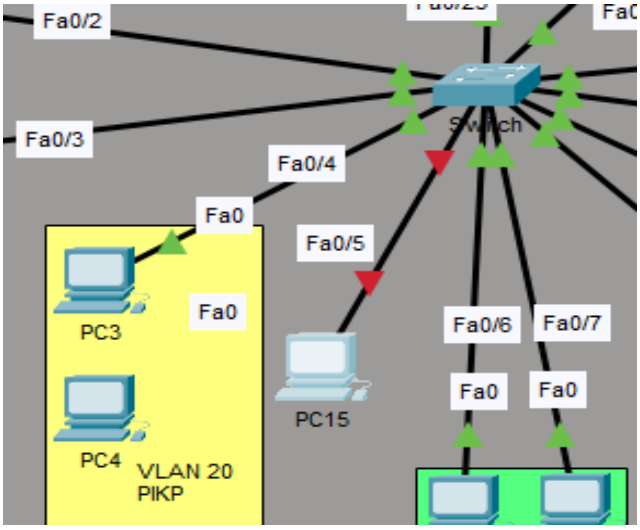
Sebaliknya, pada Skenario B, integrasi pertahanan berlapis terbukti memberikan efektivitas proteksi mutlak sebesar 100%. Batasan kuantitatif *rate limiting* sebesar 2 pps pada fitur *DHCP Standard Snooping* terbukti andal membuang (*drop*) banjir paket ilegal secara *real-time*, sehingga alokasi 254 IP tetap utuh. Temuan ini sejalan dengan penelitian Azis (2021) serta Utomo & Rahman (2022) yang memposisikan *DHCP Snooping* sebagai *firewall* perimeter *Layer 2* terbaik untuk mengunci fungsionalitas server legal dan menolak paket respon dari *port untrusted* (Fa0/24).

Namun, aspek kebaruan (*novelty*) dan kontribusi ilmiah utama dari riset ini terletak pada kedalaman analisis respons fisik port melalui *Port Security maximum 1 MAC address*. Ketika riset terdahulu oleh Azis (2021) serta Adani & Syafria (2022) mengabaikan manipulasi fisik alamat MAC, penelitian ini berhasil menutup celah tersebut. Data menunjukkan *switch* hanya membutuhkan durasi waktu respons mitigasi yang sangat singkat, yaitu 0,4 detik, untuk mengeksekusi parameter *violation shutdown* dan mengisolasi port penyerang ke status *err-disable* (ditandai dengan indikator kabel merah pada lingkungan simulator). Waktu respons 0,4 detik ini jauh lebih efisien dari batas aman toleransi gangguan jaringan yang ditentukan (< 1 detik). Temuan integrasi pengamanan fisik ini sejalan dengan hasil riset Alhajahmad (2025) serta Alsaadi & Abdul-Zahra (2022) yang membuktikan efektivitas kombinasi fitur *switch* dalam mengisolasi perangkat penyerang secara instan.

Selain itu, keberhasilan pengujian pada arsitektur multisegmentasi VLAN yang dinamis ini berhasil memecahkan keterbatasan metodologi pada riset Sinaga (2021), Sopian (2022), serta Hidayat & Nugroho (2023) yang sebelumnya menguji sistem pertahanan sejenis hanya pada topologi homogen berskala kecil. Melalui kestabilan konektivitas semua *user* pasca-mitigasi, riset ini membuktikan secara kuantitatif bahwa kombinasi pengamanan otomatis ini sangat stabil, efisien, dan siap direplikasi secara aman pada lingkungan jaringan riil (*production network*) tanpa menurunkan performa bawaan sistem (Prasetyo, 2023; Saputra & Wijaya, 2024). Keberhasilan pembuktian pertahanan fisik dan logis ini secara otentik terekam melalui log sistem pada Gambar 4 dan Gambar 5.



Gambar 4. Hasil Dhcp Snooping
Figure 4. DHCP Snooping Results



Gambar 5. Hasil Port Security
Figure 5. Port Security Results

Pada gambar 4 dan 5 di atas merupakan hasil dari mkonfigurasi DHCP Snooping dan Port Security yang telah berhasil aktif.

5. KESIMPULAN

Hasil perancangan, implementasi, dan pengujian komparatif pada simulator *Cisco Packet Tracer* membuktikan bahwa protokol DHCP tradisional pada arsitektur jaringan VLAN memiliki kerentanan kritis terhadap serangan *DHCP Starvation* dan infiltrasi *Rogue DHCP Server* akibat ketiadaan mekanisme autentikasi di layer kedua (*Data Link Layer*). Masalah celah keamanan (*research gap*) tersebut berhasil diatasi secara tuntas melalui penerapan fitur keamanan berlapis yang menunjukkan efektivitas sebesar 100%. Mekanisme *Rate Limiting* pada *DHCP Snooping* sukses menahan banjir paket serangan (*flooding*), sementara parameter *violation shutdown* pada *Port Security* mampu mengisolasi port fisik penyerang secara otomatis ke dalam status *err-disable*. Integritas jaringan semakin diperkuat oleh kemampuan *DHCP Snooping* dalam memblokir distribusi IP ilegal dari router palsu pada port Fa0/24, sehingga ketersediaan *address pool* pada router utama tetap aman dan pengguna legal di seluruh segmen VLAN mendapatkan alokasi pengalamatan yang valid serta konektivitas internet yang stabil. Sebagai agenda pengembangan ke depan (*future works*), penelitian ini dapat diperluas dengan menganalisis dampak beban kerja komputasi (*CPU Utilization*) switch saat fitur keamanan diaktifkan pada infrastruktur perangkat keras fisik (*real device*) berskala korporasi.

6. SARAN

Berdasarkan hasil penelitian yang telah dicapai, terdapat beberapa arah pengembangan yang dapat dilakukan pada penelitian selanjutnya (*future works*). Pertama, implementasi metode mitigasi ini perlu diterapkan langsung pada infrastruktur perangkat keras fisik (*real* hardware) untuk memberikan visualisasi

performa dan respons sistem yang valid pada kondisi jaringan dunia nyata. Dampak dari pengujian fisik ini akan memberikan cetak biru (*blueprint*) pertahanan yang lebih adaptif bagi para praktisi jaringan. Kedua, penelitian berikutnya disarankan untuk mengintegrasikan fitur *DHCP Snooping* dan *Port Security* dengan mekanisme *Dynamic ARP Inspection* (DAI) serta *IP Source Guard*. Langkah integrasi ini berdampak signifikan pada terciptanya ekosistem perlindungan layer kedua yang menyeluruh terhadap ancaman tingkat lanjut seperti *ARP Spoofing*. Terakhir, analisis mendalam mengenai dampak beban kerja komputasi (*CPU Utilization*) pada *Core Switch* wajib dieksplorasi ketika fitur keamanan ini diaktifkan dalam skala korporasi besar. Evaluasi ini sangat krusial agar administrator jaringan dapat memprediksi ambang batas performa perangkat sebelum mengimplementasikan kebijakan keamanan pada ratusan *client*.

7. REFERENSI

Afriady, M., Adytia, P., & Fahmi, M. (2024). *Analisis penerapan metode hirarchical token bucket untuk management bandwidth jaringan internet (Studi kasus: STMIK Widya Cipta Dharma)* (Skripsi, STMIK Widya Cipta Dharma).

Adani, M. R., & Syafria, F. (2022). Analisis perbandingan performa jaringan VLAN menggunakan metode DHCP snooping dan non-DHCP snooping terhadap serangan rogue DHCP server. *Jurnal Edukasi dan Penelitian Informatika (JEPIN)*, *8*(2), 211–218.

Alhajahmad, B. (2025). Improving Switch Security Against MITM Attacks Using DHCP Snooping and Port Security. International Journal of Management Information Systems and Computer Science, 9(2), 157–174.

Alsaadi, R. R., & Abdul-Zahra, D. S. (2022). Comprehensive Design of Secure Local Area Networks (LAN) Against MitM and Rogue DHCP Attacks. Journal of Network Security and Computer Applications, 1(2), 1–12.

Azis, I. F. (2021). *Implementasi dan analisis kinerja DHCP snooping untuk fungsi pengamanan pada Dynamic Host Configuration Protocol* [Tugas Akhir, Telkom University]. Telkom University Repository.

Buamona, N. Q. (2023). Analisis dan implementasi keamanan jaringan menggunakan metode DHCP snooping dan switch port security. *Jurnal Teknik Informatika (J-Tifa)*, *6*(1), 23–31.

Dara, Y. C., Hariadi, F., & Lede, P. A. R. L. (2022). Analisis penerapan sistem keamanan jaringan menggunakan metode DHCP snooping dan switch port security. *Jurnal Inovatif*, *1*(3), 187–196.

Dewi, S., Firmansyah, F., & Hasan, U. (2022). Penerapan metode access control list pada jaringan VLAN menggunakan router Cisco. *IMTechno: Journal of Industrial Management and Technology*, *3*(1), 37–41.

Fahmi, A., & Setiawan, B. (2023). Pencegahan serangan DHCP starvation menggunakan kombinasi fitur DHCP snooping dan port security pada switch Cisco catalyst. *Jurnal Komputer dan Teknologi Informasi (JUKANTI)*, *6*(1), 12–20.

Gunawan, I., & Pratama, R. A. (2024). Pengamanan infrastruktur local area network berbasis virtual local area network (VLAN) dari ancaman serangan layer 2 mac flooding dan DHCP spoofing. *Jurnal Informatika dan Rekayasa Perangkat Lunak (JAIRO)*, *5*(2), 104–113.

Hassan, M. A., & Shukur, Z. (2023). An Analysis of DHCP Vulnerabilities, Attacks, and Countermeasures. IEEE Xplore / International Conference on Business and Technology (ICBT), 1–12. doi:10.1109/ICBT58133.2023.10201458.

Hidayat, T., & Nugroho, S. (2023). Simulasi dan analisis mitigasi serangan man-in-the-middle dan DHCP starvation menggunakan DHCP snooping pada jaringan berbasis Cisco Packet Tracer. *Jurnal Teknik Elektro dan Komputer Triac*, *10*(2), 75–82.

Kurniawan, D., & Mustofa, A. (2022). Penerapan port security dan dynamic ARP inspection (DAI) sebagai penguat fitur DHCP snooping dalam mengatasi serangan internal jaringan. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, *6*(4), 589–597.

Lestari, W., & Handoko, P. (2025). Analisis efektivitas pengamanan inter-VLAN routing terhadap serangan network starvation menggunakan pengamatan fitur dynamic host configuration protocol snooping. *Jurnal Sistem Informasi dan Ilmu Komputer (JSIK)*, *4*(1), 34–42.

Pamungkas, D. S. (2023). Analisis keamanan jaringan switch port security dan DHCP snooping dalam mengatasi serangan DHCP starvation. *Jurnal Edukasi Elektro*, *7*(1), 45–52.

Prasetyo, B. E. (2023). *Analisis dan implementasi sistem mitigasi rogue DHCP server dan DHCP starvation di jaringan kampus menggunakan arsitektur VLAN dan switch port security* [Skripsi, Universitas Negeri Semarang]. UNNES Institutional Repository.

Purwanto, H. S. (2021). Analisis efektivitas switch port security terhadap serangan MAC flooding dan DHCP starvation. *Jurnal Sistem Komputer dan Informatika (JSON)*, *3*(1), 22–29.

Ramadhani, R. R. (2026). *Building network security using DHCP snooping, VLAN, and ACL methods through Cisco Packet Tracer simulation* [Karya Ilmiah, STMIK Widya Cipta Dharma]. WICIDA Institutional Repository.

Saputra, R., & Wijaya, M. C. (2024). Evaluasi performa throughput dan delay jaringan local area network pasca implementasi policy DHCP snooping dan limitasi mac address. *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, *8*(3), 312–321.

Sinaga, A. S. R. M. (2021). Analisis dan implementasi keamanan jaringan dengan metode DHCP snooping dan switch port security. *Jurnal Informasi dan Teknologi (JIDT)*, *3*(2), 78–83.

Sitorus, M. B. R. (2022). Simulasi pertahanan layer 2 terhadap ancaman rogue DHCP server berbasis VLAN. *Jurnal Ilmiah Teknologi Informasi dan Robotika*, *4*(2), 89–96.

Sopian, A. (2022). *Penerapan sistem keamanan jaringan komputer dengan menggunakan metode DHCP snooping dan VLAN* [Skripsi, Universitas Sebelas April]. Scribd Repository.

Utomo, P., & Rahman, A. (2022). Eksperimen keamanan switchport layer 2 menggunakan serangan yersinia dan langkah preventif melalui konfigurasi DHCP snooping. *Jurnal Infomedia: Teknik Informatika, Data Mining, dan Multimedia*, *7*(2), 61–68.

Wicaksono, G., & Wardhana, A. (2025). Pengamanan arsitektur switch berbasis VLAN dari ancaman DHCP exhaustion attack menggunakan fitur mitigasi port-security. *Jurnal Telekomunikasi, Elektronika, komputasi, dan Kontrol (JTEKK)*, *5*(1), 18–27.