Sebatik Vol. 29 No. 1 June 2025
ISSN: 1410-3737(p) 2621-069X(e)
[bagian header jangan di isi] "Judul", Sebatik, 00(0).
Open access article licensed under CC-BY
Submitted: 0000/00/00 Accepted: 0000/00/00 Published: 0000/00/00
DOI:10.46984/sebatik.v29i1.0000

Building Network Security Using DHCP Snooping, VLAN, and ACL Methods Through Cisco Packet Tracer Simulation

Randitya Rizki Ramadhani[1)], H. Pajar Pahrudin[2)], dan **Pitrasacha Adytia[3)]**

Teknik Informatika, STMIK Widya Cipta Dharma
Jl. M. Yamin No.25, Samarinda, 75123
E-mail: 1943055@wicida.ac.id[1)], pajar@wicida.ac.id[2)], pitra@wicida.ac.id[3)]

ABSTRACT

Randitya Rizki Ramadhani, 2026, Building Network Security Using DHCP Snooping, VLAN, and ACL Methods Through Cisco Packet Tracer Simulation, Sekolah Tinggi Manajemen Informatika dan Komputer Widya Cipta Dharma, Main Supervisor: H. Pajar Pahrudin, S.Kom., M.H., Co-Supervisor: Pitrasacha Adytia, S.T., M.T. This study aims to build local network security at STMIK Widya Cipta Dharma campus against DHCP Rogue attacks by implementing DHCP Snooping, VLAN, and Access Control Lists (ACL) using Cisco Packet Tracer simulations. DHCP Rogue attacks can cause the distribution of invalid IP addresses, IP conflicts, connectivity disruptions, and decreased network performance. The system development method used in this study is the Network Development Life Cycle (NDLC), which includes the stages of analysis, design, simulation, implementation, monitoring, and management. The results of the study indicate that the implemented network security system effectively enhances network protection, where clients only receive IP addresses from legitimate DHCP servers, thereby minimizing IP conflicts and connectivity disruptions

***Keywords**: DHCP Snooping, VLAN, ACL, network security*

Membangun Keamanan Jaringan Dengan Metode DHCP Snooping, VLAN, dan ACL Menggunakan Simulasi Cisco Packet Tracer

ABSTRAK

Randitya Rizki Ramadhani, 2026, Membangun Keamanan Jaringan Dengan Metode DHCP Snooping, VLAN, dan ACL Menggunakan Simulasi Cisco Packet Tracer, Sekolah Tinggi Manajemen Informatika dan Komputer Widya Cipta Dharma, Dosen Pembimbing Utama: H. Pajar Pahrudin, S.Kom., M.H., Dosen Pembimbing Pendamping: Pitrasacha Adytia, S.T., M.T. Penelitian ini bertujuan membangun keamanan jaringan lokal kampus STMIK Widya Cipta Dharma terhadap serangan DHCP Rogue dengan menerapkan DHCP Snooping, VLAN, dan Access Control List (ACL) menggunakan simulasi Cisco Packet Tracer. Serangan DHCP Rogue dapat menyebabkan distribusi alamat IP tidak valid, konflik IP, gangguan konektivitas, dan penurunan kinerja jaringan. Metode pengembangan yang digunakan adalah Network Development Life Cycle (NDLC) yang meliputi tahap analisis, desain, simulasi, implementasi, monitoring, dan manajemen. Hasil penelitian menunjukkan bahwa sistem keamanan yang diterapkan efektif meningkatkan perlindungan jaringan, di mana klien hanya menerima alamat IP dari DHCP Server yang sah sehingga konflik IP dan gangguan koneksi dapat diminimalkan.

Kata Kunci: DHCP *Snooping*, VLAN, ACL, Keamanan jaringan

1. PENDAHULUAN

Perkembangan internet yang semakin pesat membuat teknologi informasi menjadi bagian penting dalam kehidupan manusia terutama dalam proses mengelola data menjadi informasi sehingga mempercepat pelaksanaan pekerjaan. Seiring dengan meningkatnya jumlah pengguna internet, kebutuhan akan keamanan jaringan internet juga semakin penting. Namun, meningkatnya ketergantungan terhadap jaringan komputer turut diikuti oleh berkembangnya berbagai ancaman keamanan jaringan. Salah satu permasalahan yang sering terjadi pada jaringan local di lingkungan kampus adalah serangan DHCP *Rogue* atau DHCP Palsu. Serangan ini terjadi Ketika terdapat perangkat tidak sah yang bertindak sebagai DHCP *Server* di dalam jaringan, sehingga membagikan Alamat IP yang tidak sesuai kepada *client*.

Pada lingkungan kampus seperti STMIK Widya Cipta Dharma yang memiliki banyak pengguna serta perangkat jaringan resiko munculnya serangna DHCP *Rogue* semakin tinggi, khususnya pada jaringan yang digunakan untuk administrasi dan keuangan, laboratorium komputer, serta akses publik karena banyaknya pengguna dan perangkat yang terhubung dalam jaringan tersebut. Besarnya jumlah pengguna dan perangkat yang terhubung dalam jaringan tersebut menciptakan kesempatan bagi pengguna jaringan lainnya untuk menghubungkan perangkat penyedia layannan DHCP ke dalam jaringan kampus secara sengaja dengan tujuan tertentu, akibatnya

perangkat tersebut berfungsi sebagai DHCP *Server* palsu (DHCP *Rogue*) yang membagikan alamat IP secara tidak sah sehingga menyebabkan konlik IP, dan gangguan konektivitas jaringan.

Oleh karena itu, diperlukan sistem keamanan jaringan yang efektif untuk mencegah dan mengurangi resiko dari DHCP *Rogue.* Cara yang bisa diterapakan adalah dengan mengaktifkan DHCP *Snooping* sebagai fitur keamanan pada *switch* yang akan memantau dan membatasi aktivitas DHCP di jaringan serta otomatis menolak layanan DHCP yang tidak sah. Selain itu, *Virtual Local Area Network* (VLAN) digunakan untuk memisahkan bagian jaringan berdasarkan fungsi dan kebutuhan pengguna sehingga dapat mengecilkan potensi serangan. Penggunaan *Access Control List* (ACL) penting untuk membatasi akses antar jaringan

2. RUANG LINGKUP

Dalam penelitian ini permasalahan mencakup:

1. Rumusan Masalah

Berdasarkan latar belakang di atas maka terdapat rumusan masalah yang dapat dibahas adalah sebagai berikut : " Bagaimana membangun keamanan jaringan dengan metode DHCP Snooping, VLAN, dan ACL menggunakan simulasi Cisco Packet Tracer ".

2. Batasan penelitian

Berdasarkan rumusan masalah diatas terdapat beberapa batasan masalah agar ruang lingkup penelitian tidak terlalu luas. Beberapa batasan masalah tersebut adalah Rancangan sistem akan dibuat dalam bentuk simulasi di Cisco Packet Tracer; Metode keamanan jaringan yang diterapkan meliputi DHCP Snooping, Virtual Local Area Network (VLAN), dan Access Control List (ACL); Penelitian difokuskan pada perancangan dan simulasi keamanan jaringan untuk mengatasi serangan DHCP Rogue.

3. Tujuan Penelitian

Tujuan penelitian ini adalah untuk merancang sistem keamanan jaringan menggunakan metode DHCP Snooping, VLAN, dan Access Control List (ACL) guna meningkatkan keamanan jaringan kampus. Selain itu, penelitian ini bertujuan mengimplementasikan dan mensimulasikan penerapan DHCP Snooping, VLAN, dan ACL menggunakan Cisco Packet Tracer. Penelitian ini juga bertujuan untuk mengetahui efektivitas penerapan ketiga metode tersebut dalam mencegah konflik alamat IP serta menjaga kestabilan konektivitas jaringan. Di samping itu, penelitian ini menganalisis potensi dan dampak serangan DHCP Rogue pada jaringan kampus STMIK Widya Cipta Dharma melalui simulasi serangan DHCP Rogue pada topologi jaringan kampus menggunakan Cisco Packet Tracer. Hasil penelitian diharapkan dapat menjadi rekomendasi dalam penerapan sistem keamanan jaringan kampus yang lebih andal dan terstruktur.

3. BAHAN DAN METODE

Untuk memperkuat hasil penelitian, diperlukan landasan konseptual yang digunakan dalam perumusan definisi-definisi pendukung kegiatan penelitian, baik yang bersumber dari teori dasar maupun teori umum.

3.1 Jaringan Komputer

Menurut Astuti, I. K. (2018), Jaringan komputer adalah jaringan komunikasi yang memungkinkan komputer untuk berkomunikasi satu sama lain dengan bertukar data. Jaringan komputer dibangun dengan kombinasi perangkat keras dan perangkat lunak. Ketikan dua komputer atau lebih berkomunikasi satu sama lain atau bertukar data, terdapat bagian-bagian dalam jaringan komputer yang berperan sebagai pihak yang menerima atau meminta layanan, yang disebut klien, dan pihak yang menyediakan atau mengirim layanan disebut sebagai server. Ada tiga tipe jenis jaringan yang bisa digunakan, yaitu :

1. Local Area Network (LAN)

Local Area Network (LAN) jaringan yang bersifat lokal dalam jarak/area dan menggabungkan perangkat keras dan perangkat lunak untuk berkomunikasi satu sama lain dalam area terbatas. Jaringan ini biasanya disiapkan untuk kantor, lembaga pendidikan, atau departemen dalam perusahaan Noviani, Y. D. (2020).

Manfaat LAN meliputi berbagi sumber daya, namun masalah manajemen, keamanan, dan komunikasi data dapat timbul. Tantangan ini muncul dengan banyaknya pengguna terhubung dan komunikasi data yang membaik, sehingga diperlukan pengelolaan jaringan yang baik untuk menjaga kinerja dan mencegah penurunan kecepatan jaringan.

2. Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) adalah jenis jaringan komputer yang memiliki cakupan wilayah yang lebih luas dan tingkat kompleksitas yang lebih tinggi dibandingkan dengan *Local Area* Network (LAN). Jaringan MAN dirancang untuk menghubungkan beberapa jaringan LAN yang berada dalam satu wilayah metropolitan, seperti antar gedung, kawasan industri, kampus, hingga antar kota dalam satu provinsi. Oleh karena itu, jaringan ini disebut *Metropolitan Area Network* karena sering dimanfaatkan untuk menghubungkan jaringan komputer dari satu kota ke kota lain guna mendukung pertukaran data, komunikasi, dan layanan informasi secara cepat dan efisien. Dalam membangun jaringan MAN, operator telekomunikasi biasanya memanfaatkan infrastruktur jaringan berskala besar seperti serat optik, microwave, atau jaringan nirkabel berkapasitas tinggi, serta perlu terhubung langsung dengan berbagai jaringan komputer. Sugiyanta, L., & Raja, B. (2017).

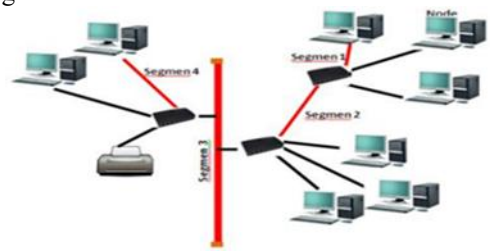
3. Wide Area Network (WAN)

Wide Area Network (WAN) adalah jaringan komputer yang mencakup wilayah geografis yang luas, seperti wilayah jaringan antar komputer, kota, atau bahkan negara. Ini juga dapat digambarkan sebagai jaringan yang memerlukan router dan saluran komunikasi publik. Tujuan dari WAN adalah untuk membangun konektivitas antara jaringan area lokal yang berbeda, memungkinkan pengguna dan komputer di satu lokasi untuk

berkomunikasi dengan orang-orang di lokasi lain. Sugiyanta, L., & Raja, B. (2017).

3.2 Topologi Jaringan

Menurut Syafrizal, M. (2020), Topologi jaringan merupakan gambaran desain hubungan antar komputer dalam suatu jaringan area lokal, di mana kabel jaringan, kartu Ethernet, dan perangkat pendukung lainnya digunakan sebagai media transmisi data. Pemilihan jenis aplikasi yang digunakan dapat mempengaruhi bentuk hubungan antarperangkat serta kelebihan dan kekurangan dari topologi jaringan yang diterapkan. Pada jaringan kampus STMIK Widya Cipta Dharma (WICIDA), topologi yang digunakan adalah topologi tree. Berikut ini merupakan gambaran topologi tree yang dapat dilihat pada gambar di bawah ini.



Gambar 1. Topologi Tree

Menurut Madcoms. (2017), Topologi tree adalah hasil penggabungan dari topologi bus dan topologi star. Umumnya, topologi tree digunakan untuk interkoneksi antara hirarki dengan pusat yang berbeda-beda.

3.3 *Virtual Local Area Network* (VLAN)

VLAN adalah subnet yang dapat mengelompokan sekumpulan perangkat di jaringan terpisah. LAN adalah sekelompok komputer dan perangkat yang berbagi jalur komunikasi melalui koneksi kabel atau nirkabel di lokasi geografis yang sama. VLAN memungkinkan *administrator* jaringan dengan mudah mensegmentasi jaringan berdasarkan kebutuhan fungsional serta persyaratan keamanan sistem tanpa harus membuat kabel baru atau melakukan perubahan besar ke infrastruktur jaringan. VLAN sering digunakan oleh bisnis besar untuk menditribusikan perangkat mereka guna meningkatkan manajemen lalu lintas data Anam, M. C., dkk (2024).

VLAN adalah subnet yang dapat mengelompokan sekumpulan perangkat di jaringan terpisah. LAN adalah sekelompok komputer dan perangkat yang berbagi jalur komunikasi melalui koneksi kabel atau nirkabel di lokasi geografis yang sama. VLAN memungkinkan *administrator* jaringan dengan mudah mensegmentasi jaringan berdasarkan kebutuhan fungsional serta persyaratan keamanan sistem tanpa harus membuat kabel baru atau melakukan perubahan besar ke infrastruktur jaringan. VLAN sering digunakan oleh bisnis besar untuk menditribusikan perangkat mereka guna meningkatkan manajemen lalu lintas data Anam, M. C., dkk (2024).

Menurut Sutanto, P. H. (2018), cara kerja VLAN didasarkan pada metode pengelompokan tertentu seperti *port*, alamat MAC, dan metode lainnya. Informasi penandaan VLAN (*tagging*) disimpan dalam *database switch,* di mana pada VLAN berbasis *port, database* mencatat *port* yang terhubung dalam VLAN tertentu Pengelolaan VLAN umumnya menggunakan *switch* yang dapat dikonfigurasi untuk menyimpan dan menyinkronkan informasi VLAN. *Switch* menentukan jalur pengiriman data, sedangkan komunikasi antar VLAN memerlukan *router* atau perangkat layer 3. Beberapa kelebihan penggunaan VLAN antara lain :

1) Keamanan jaringan. Keamanan dalam suatu jaringan dapat berupa pemisahan logis dari segmentasi jaringan.
2) Penghematan anggaran. Dapat menghemat anggaran dengan menggunakan *bandwith* yang ada atau peningkatan perluasan jaringan
3) Peningkatan kemapuan jaringan. Membagi jaringan layer 2 menjadi beberapa grup *broadcast domain* yang lebih kecil, yang tentunya mengurangi lalu lintas paket yang tidak perlu dalam jaringan.
4) Memperkecil broadcast domain. Membagi jaringan kedalam VLAN akan mengurangi jumlah perangkat yang terlibat dalam *broadcast strom.* Hal ini disebabkan oleh keterbatasan broadcast domain.
5) Mengembangkan dan mengelola teknologi jaringan dengan lebih efisien. VLAN memfasilitasi manajemen jaringan dengan membagi pengguna yang membutuhkan sumber daya yang diperlukan ke dalam segmen yang sama.

3.4 DHCP

DHCP adalah protokol berbasis arsitektur klien atau *server* yang digunakan untuk memfasilitasi penetapan alamat IP pada suatu jaringan. DHCP memfasilitasi transfer data ke PC klien lain atau PC *server* dan menyediakan alamat IP dinamis dan konfigurasi lainnya. Alamat IP DHCP klien tidak dapat digunakan oleh klien lainnya, tetapi *server* dapat menggunakan alamat IP klien untuk periode tertentu. DHCP juga menghemat tenaga dan waktu saat memberikan IP dan mencegah konflik IP. Namun, DHCP untuk konfigurasi IP bergantung pada *server*. Jika *server* mati maka semua komputer akan terputus Sungkar, M. S., & Sabara, M. A. (2019).

3.5 DHCP Snooping

Menurut Ariyadi, T. (2017), DHCP *Snooping* adalah serangkaian teknik yang diterapkan untuk meningkatkan keamanan jaringan DHCP. Ketika *server* DHCP memberikan alamat IP klien di jaringan lokal, DHCP *Snooping* dapat konfigurasi pada *switch* LAN untuk bisa mengizinkan klien dengan alamat IP dan MAC tertentu yang memiliki akses ke jaringan. DHCP *Snooping* dapat memastikan integritas IP di *domain* peralihan Lapisan dua. Dengan DHCP *Snooping*, alamat IP dan informasi alamat MAC yang sesuai disimpan dalam *database*. DHCP *Snooping* dapat digunakan untuk fitur keamanan lainnya seperti perlindungan sumber daya IP dan ARP *dinamis,* menjadikannya bagian penting dari keamanan akses jaringan lokal. DHCP *Snooping* juga dapat mencegah penyerang menambahkan server DHCP ke

jaringan, sehingga merusak jaringan dan menambahkan komponen yang tidak sah.

DHCP *Snooping* bekerja seperti *firewall* yang fungsi dan tugas utamanya adalah membedakan antara sumber IP tepercaya dan tidak tepercaya. Metode ini memungkinkan membedakan antara sumber tepercaya dan tidak tepercaya dari database yang telah dikonfigurasi dan terdaftar sebelumnya. Basis data ini menyimpan alamat IP sumber tepercaya dan menolak sumber yang bukan sumber tersebut. Biasanya, DHCP *Snooping* digunakan di jaringan komputer perusahaan. Sumber tepercaya adalah saklar di bawah kendali administrator perusahaan, termasuk *router* dan *server* yang terhubung dan terdaftar ke jaringan perusahaan Medianto, M. (2020).

3.6 *Access Control List*

Access Control List (ACL) adalah teknologi pemantauan paket yang populer dan lama. ACL memeriksa isi paket dan menerapkan aturan untuk menentukan apakah paket tersebut ditolak atau diizinkan. Meskipun menggunakan beberapa fitur header TCP/IP, ACL ini berfokus pada pemfilteran berdasarkan alamat IP sumber atau tujuan. Pengaturan ACL yang efektif memungkinkan *administrator* jaringan mengontrol lalu lintas dengan lebih baik dan menerapkan kebijakan keamanan ketat Azmi, F., dkk (2022). *Access Control List* (ACL) melibatkan pengelompokan paket berdasarkan kategori yang berbeda. *Access Control List* (ACL) bisa sangat berguna untuk mengontrol lalu lintas jaringan. *Access Control List* juga menjadi alat pilihan untuk pengambilan keputusan dalam situasi ini. *Access Control List* (ACL) hanya digunakan untuk mengizinkan atau melarang paket dari suatu host ke tujuan tertentu. *Access Control List* (ACL) mencakup aturan dan ketentuan yang menentukan lalu lintasjaringan dan menentukan prosedur di *router* apakah paket diteruskan atau tidak. Penggunaan *Access Control List* (ACL) yang paling umum dan paling mudah adalah untuk memfilter paket yang tidak diinginkan saat menerapkan kebijakan keamanan Simanjuntak, P., dkk (2017).

Cara kerja metode *Access Control List* ini adalah dengan membagi kategori pengguna dan *bandwidth* berdasarkan penggunanya, kategori pengguna ini dikelompokkan berdasarkan kebutuhan pengguna dan juga membatasi hak aksesnya untuk memanfaatkan layanan internet dengan merata sehingga mengatasi permasalahan *bandwidth* yang tidak stabil. Dengan penerapan pengelompokan dan pembatasan tersebut, administrator jaringan dapat mengontrol penggunaan sumber daya jaringan secara lebih efisien, mencegah terjadinya dominasi bandwidth oleh pengguna tertentu, serta menjaga kualitas layanan internet agar tetap optimal bagi seluruh pengguna.

Berikut ini tipe *Access List* yang digunakan pada penelitian ini yaitu :

1. *Extended* ACL

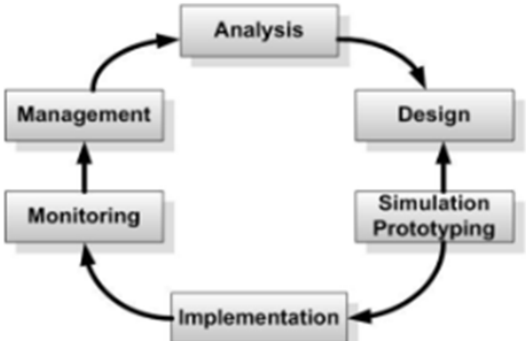
Extended ACL adalah jenis ACL yang kompleks dibanding dengan *Standard* ACL. *Extended* ACL memungkinkan kontrol lalu lintas jaringan berdasarkan IP, protokol, dan *port* sehingga memberikan pengaturan keamanan dan pengelolaan trafik jaringan yang lebih spesifik dan efektif. Dengan kemampuan tersebut, administrator jaringan dapat menentukan kebijakan akses secara lebih detail sesuai kebutuhan dan kondisi jaringan yang ada.

3.7 Cisco Packet Tracer

Cisco Packet Tracer adalah aplikasi virtualisasi jaringan yang memungkinkan pengguna untuk mengembangkan dan mensimulasikan jaringan virtual. Dengan aplikasi ini, pengguna dapat menggunakan perangkat keras virtual Cisco tanpa harus membelinya. Aplikasi ini menyediakan antarmuka pengguna yang mudah digunakan dan memungkinkan pengguna untuk belajar mengkonfigurasi perangkat Cisco di dalam jaringan. Dengan Cisco Packet Tracer, pengguna mendapatkan pengalaman langsung dalam membuat dan mengelola jaringan, yang penting untuk mengembangkan keterampilan jaringan komputer. Cisco Packet Tracer dikembangkan oleh Cisco Systems Inc dan banyak digunakan oleh mahasiswa yang mengikuti program kursus CCNA dan CCNP. Aplikasi ini memungkinkan pengguna untuk mensimulasikan jaringan komputer nyata dan menganalisis masalah jaringan tanpa menggunakan jaringan fisik Medianto, M. (2020).

3.8 Metode Pengembangan Sistem

Network Development Life Cycle (NDLC) merupakan metode untuk mengembangkan atau merancang sistem jaringan komputer dan memungkinkan pemantauan terhadap sistem yang sedang dirancang atau dikembangkan agar dapat diketahui kinerjanya. NDLC juga merupakan metode yang bergantung pada proses pembangunan sebelumnya seperti perencaan strategi bisnis, daur hidup pengembangan aplikasi dan analisa pedistribusian data Ahmad, U. A., dkk (2021).



Gambar 2. ***Network Development Life Cycle***

Adapun tahapan – tahapan NDLC sebagai berikut :

1. *Analysis,* pada tahap ini dilakukan analisa kebutuhan, analisa permasalahan yang muncul, analisa keinginan user dan analisa topologi jaringan yang ada. Tahap ini bertujuan untuk memperoleh gambaran menyeluruh mengenai kondisi jaringan sehingga dapat dirumuskan solusi yang tepat sesuai dengan kebutuhan pengguna.
2. *Design,* pada tahap ini merupakan gambar desain topologi jaringan koneksi yang akan dibuat. diharapkan

gambar ini dapat memberikan gambaran lengkap mengenai kebutuhan yang ada.
3. *Simulation Prototype,* Pada tahap ini simulasi menggunakan alat khusus seperti Cisco Packet Tracer.
4. *Implementation,* Pada tahap ini segala sesuatu yang telah direncanakan dan dirancang sebelumnya dilaksanakan.
5. *Monitoring,* pada tahap ini dilakukan pemantauan agar komputer dan jaringan komunikasi dapat beroperasi secara optimal.
6. *Management,* Pada tahap ini manajemen membuat agar sistem yang telah dibangun berfungsi baik dapat bertahan lama dan tetap terjaga.

4. PEMBAHASAN

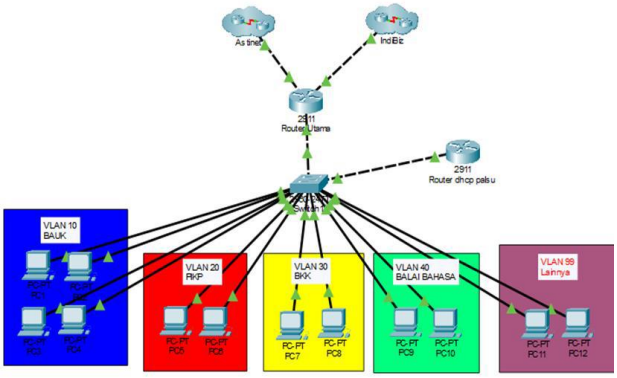
Pada pembahasan ini akan di paparkan hasil dari penelitian dalam Membangun keamanan jaringan dengan metode DHCP *Snooping*, VLAN, dan ACL pada Kampus STMIK Widya Cipta Dharma, Dengan metode NDLC dengan tahapan yaitu Analisis, desain, Simulasi Prototipe, Implementasi, *Monitoring.*

4.1 Analisis

Dalam analisis peneliti melakukan wawancara kepada staff Puskom Wicida dan melihat topologi dan manajemen jaringan yang diterapkan oleh Kampus STMIK Widya Cipta Dharma. Meskipun secara struktur jaringan telah menerapkan segmentasi VLAN, masih ditemukan beberapa permasalahan yang berpotensi mengganggu keamanan dan kinerja jaringan. Masalah yang terjadi adalah belum optimalnya pengamanan layanan DHCP, sehingga memungkinkan terjadinya serangan DHCP *Rogue*. Kondisi ini dapat terjadi apabila terdapat pengguna atau perangkat yang secara sengaja maupun tidak sengaja mengaktifkan layanan DHCP *Server* di dalam jaringan kampus. Akibatnya, perangkat klien berpotensi memperoleh alamat IP yang tidak valid, *gateway* yang salah, atau bahkan diarahkan ke jaringan yang tidak semestinya.
Untuk mencegah terjadinya serangan DHCP *Rogue* pada jaringan kampus, diperlukan penerapan mekanisme keamanan jaringan yang mampu membatasi serta mengendalikan proses pendistribusian alamat IP kepada setiap klien. Salah satu langkah utama yang dapat diterapkan adalah mengaktifkan fitur DHCP *Snooping* pada perangkat *switch*, yang berfungsi untuk memantau dan memfilter lalu lintas DHCP sehingga hanya DHCP *Server* yang sah yang diperbolehkan memberikan alamat IP kepada klien. Selain itu, penerapan *Access Control List* (ACL) pada router digunakan untuk membatasi hak akses antar VLAN dan mengontrol lalu lintas jaringan sehingga hanya komunikasi yang diizinkan sesuai kebijakan jaringan yang dapat berlangsung, serta mencegah akses tidak sah antar segmen jaringan. Dengan menerapkan langkah-langkah ini, potensi risiko serangan DHCP Rogue dapat diminimalisir.

4.2 Desain

Desain topologi menggunakan aplikasi Cisco Packet Tracer, berikut merupakan desain topologi yang telah dibuat. Dapat dilihat pada gambar dibawah merupakan rancangan dari topologi yang telah dibuat. Topologi ini dirancang untuk merepresentasikan kondisi jaringan secara nyata, yang terdiri dari beberapa perangkat jaringan seperti router, switch, dan PC yang saling terhubung, sehingga dapat digunakan sebagai media simulasi untuk pengujian konfigurasi, analisis kinerja jaringan, serta penerapan fitur keamanan jaringan sesuai dengan skenario yang telah direncanakan



Gambar 3. Rancangan Topologi

Pada rancangan topologi jaringan yang dibuat, jaringan kampus terhubung kedua ISP yang dikonfigurasikan menggunakan sistem *failover*, di mana satu ISP berfungsi sebagai jalur akses internet utama dan ISP lainnya sebagai jalur cadangan. Kedua ISP tersebut terhubung ke *router* utama yang berperan sebagai pengelola lalu lintas jaringan sekaligus sebagai penghubung antar VLAN. *Router* utama kemudian terhubung ke sebuah *switch* yang berfungsi sebagai pusat distribusi jaringan. *Switch* tersebut menghubungkan beberapa segmen jaringan yang dipisahkan menggunakan Virtual Local Area Network (VLAN), yaitu VLAN 10 (BAUK), VLAN 20 (PIKP), VLAN 30 (BKK), VLAN 40 (Balai Bahasa), dan VLAN 99 (Lainnya), masing-masing dengan jumlah PC sesuai dengan kebutuhan unit kerja. Berikut ini merupakan daftar IP Address yang digunakan Penerapan VLAN ini bertujuan untuk meningkatkan keamanan, efisiensi pengelolaan jaringan, serta mengurangi lalu lintas *broadcast* antar unit kerja. Berikut ini merupakan daftar IP Address yang digunakan.

Tabel 1. Daftar *Address List*

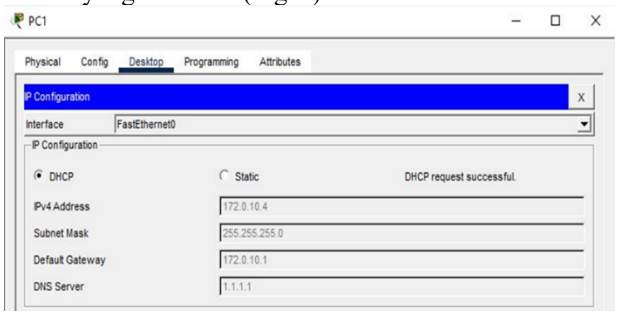
No	VLAN ID	*NETWORK*
1	VLAN 10	192.168.10.0/24
2	VLAN 20	192.168.20.0/24
3	VLAN 30	192.168.30.0/24
4	VLAN 40	192.168.40.0/24
5	VLAN 99	192.168.99.0/24

Selain itu, pada topologi juga ditambahkan sebuah *router* DHCP palsu sebagai simulasi serangan DHCP *Rogue*. Keberadaan perangkat ini digunakan untuk menguji efektivitas penerapan mekanisme keamanan jaringan. khususnya DHCP *Snooping* dalam mencegah distribusi alamat IP yang tidak sah dan *Access Control List*

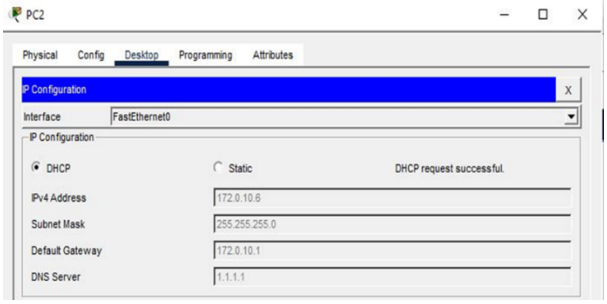
(ACL) untuk membatasi serta mengontrol lalu lintas antar jaringan

4.3 Simulasi

Setelah melakukan desain topologi, selanjutnya dilakukan simulasi jaringan dengan melakukan pengujian layanan DHCP pada masing-masing PC. Pengujian ini dilakukan sebelum DHCP *Snooping* diaktifkan dan sesudah DHCP *Snooping* diaktifkan. Pada kondisi sebelum DHCP *Snooping* diaktifkan, alamat IP pada PC1 hingga PC12 diatur menggunakan DHCP sehingga setiap PC akan menerima alamat IP secara otomatis. Namun, terdapat perbedaan sumber alamat IP yang diterima oleh masing-masing PC, di mana beberapa PC memperoleh alamat IP dari server DHCP yang terpercaya (trusted), sementara PC lainnya menerima alamat IP dari server DHCP yang tidak sah (rogue).

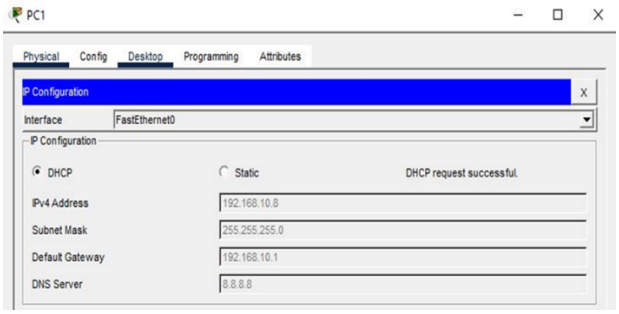


Gambar 4. Pengujian PC tanpa DHCP Snooping

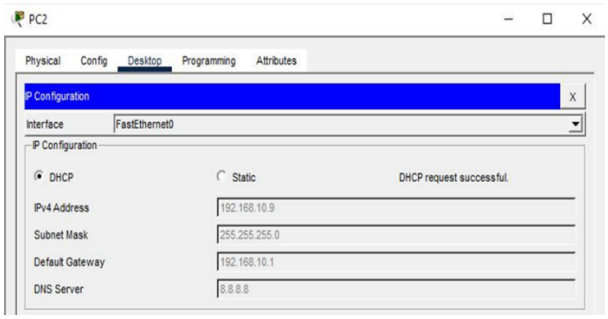


Gambar 5. Pengujian PC tanpa DHCP Snooping

Setelah DHCP *Snooping* diaktifkan pada *switch*, terlihat perubahan signifikan pada distribusi alamat IP. Semua PC yang sebelumnya menerima IP dari DHCP *Rogue* kini hanya mendapatkan alamat IP dari DHCP *Trusted.* Hal ini menunjukkan bahwa DHCP *Snooping* berhasil memblokir *server* DHCP yang tidak sah (*Rogue*) dan memastikan hanya *server* resmi yang dapat memberikan alamat IP kepada klien. Dengan demikian, keamanan jaringan meningkat karena mencegah kemungkinan konflik IP, gangguan konektivitas, dan potensi serangan berbasis DHCP yang dapat merusak komunikasi antar perangkat dalam jaringan, serta menjaga stabilitas dan keandalan sistem jaringan secara keseluruhan. Selain itu, penerapan DHCP Snooping juga memungkinkan administrator jaringan untuk melakukan pemantauan yang lebih efektif terhadap lalu lintas DHCP, mendeteksi dan mencatat aktivitas server yang mencurigakan, serta menerapkan kebijakan manajemen alamat IP yang lebih terstruktur, sehingga tidak hanya meningkatkan keamanan, tetapi juga mempermudah troubleshooting, pengendalian akses, dan perencanaan kapasitas jaringan untuk mendukung kinerja optimal di seluruh infrastruktur.



Gambar 6. Pengujian PC setelah DHCP *Snooping* diaktifkan



Gambar 7. Pengujian PC setelah DHCP *Snooping* diaktifkan

4.4 Implementasi

Tahap implementasi merupakan proses konfigurasi *switch*, *router*, dan ISP. Pada tahap awal dilakukan pembuatan lima VLAN pada *switch*, yaitu VLAN 10 (BAUK), VLAN 20 (PIKP), VLAN 30 (BKK), VLAN 40 (Balai Bahasa), dan VLAN 99 (Lainnya). Untuk pembagian *port* pada *Switch* VLAN 10 masuk dalam *port* Fa0/1 sampai Fa0/4, VLAN 20 masuk dalam *port* Fa0/5 sampai Fa0/6, VLAN 30 masuk dalam *port* Fa0/7 sampai Fa0/8, VLAN 40 masuk dalam *port* Fa0/9 sampai Fa0/10, VLAN 99 masuk dalam *port* Fa0/11 sampai Fa0/22. Konfigurasi ini dilakukan untuk memastikan setiap perangkat terhubung ke VLAN yang sesuai sehingga komunikasi data antar unit kerja dapat berjalan dengan terstruktur, aman, dan efisien. Berikut merupakan konfigurasi VLAN pada *Switch* dapat dilihat pada gambar dibawah.

```
Switch>enable
Switch#configure terminal
Switch(config)#VLAN 10
Switch(config-vlan)#Name BAUK
Switch(config-vlan)#exit
```

Gambar 8. Konfigurasi VLAN 10

```
Switch(config)#VLAN 20
Switch(config-vlan)#Name PIKP
Switch(config-vlan)#exit
```

Gambar 9. Konfigurasi VLAN 20

```
Switch(config)#VLAN 30
```

```
Switch(config-vlan)#Name BKK
Switch(config-vlan)#exit
```

Gambar 10. Konfigurasi VLAN 30

```
Switch(config)#VLAN 40
Switch(config-vlan)#Name Balai_bahasa
Switch(config-vlan)#exit
```

Gambar 11. Konfigurasi VLAN 40

```
Switch(config)#VLAN 99
Switch(config-vlan)#Name Lainnya
Switch(config-vlan)#exit
```

Gambar 12. Konfigurasi VLAN 99

Selanjutnya adalah konfigurasi *port access* dan *trunk. Port access* melewatkan data di VLAN yang sama, sedangkan *port trunk* melewatkan data dari beberapa VLAN berbeda ke *router*. konfigurasi *trunk* ke *Router* Utama dan *Route*r *Rogue. port* Fa0/24 terhubung ke *router* utama, dan *port* Fa0/23 terhubung ke *Router Rogue.* Berikut konfigurasi *port access* dan *trunk* pada *switch* dan hasil konfigurasi dapat dilihat pada gambar dibawah.

```
Switch(config)#inteface range Fa0/1-4
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#inteface range Fa0/5-6
Switch(config-if)#switchport access vlan 20
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#inteface range Fa0/7-8
Switch(config-if)#switchport access vlan 30
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#inteface range Fa0/9-10
Switch(config-if)#switchport access vlan 40
Switch(config-if)#switchport mode access
Switch(config-if)#exit
Switch(config)#inteface range Fa0/11-22
Switch(config-if)#switchport access vlan 99
Switch(config-if)#switchport mode access
Switch(config-if)#exit
```

Gambar 13. Konfigurasi Port Access

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

Gambar 14. Konfigurasi *Trunk* ke *Router* Utama dan *Router Rogue*

Setelah melakukan konfigurasi *interface* VLAN, tahap selanjutnya adalah mengaktifkan *port* pada *router* yang terhubung ke *switch,* sehingga *interface* tersebut dapat berfungsi secara optimal dalam meneruskan lalu lintas data dari setiap VLAN serta memastikan komunikasi jaringan antara *router* dan *switch* berjalan dengan baik. Langkah ini juga diperlukan agar router dapat menjalankan fungsi inter-VLAN *routing* dan bertindak sebagai *default gateway* bagi masing-masing VLAN.

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

Gambar 15. Mengaktifkan *port* ke *switch*

Selanjutnya dilakukan konfigurasi IP *address* pada *router* untuk koneksi ke ISP, di mana *port GigabitEthernet0/1* dihubungkan ke *Router* ISP Utama (Astinet) dan *port GigabitEthernet0/2* dihubungkan ke *Router* ISP Cadangan (IndiBiz), sehingga *router* dapat mengelola koneksi internet utama dan cadangan sesuai dengan mekanisme *failover* yang diterapkan Pengaturan ini bertujuan menjamin ketersediaan layanan internet saat salah satu jalur mengalami gangguan. Berikut konfigurasi IP *Address* pada kedua ISP yang dapat dilihat pada gambar dibawah.

```
Router>enable
Router#configure terminal
Router(config)#int g0/1
Router(config-subif)#ip address 100.10.10.2 255.255.255.252
Router(config-subif)#exit
Router(config)#int g0/2
Router(config-subif)#ip address 200.20.20.2 255.255.255.252
```

Gambar 16. konfigurasi IP *address* pada *router* untuk koneksi ke ISP

Kemudian masuk ke *Router* ISP Utama berikan alamat IP pada *Port* G0/1 yang mengarah ke *Router* Utama. Berikut konfigurasi yang dapat dilihat pada gambar dibawah.

```
Router>enable
Router#configure terminal
Router(config)#int g0/1
Router(config-subif)#ip address 100.10.10.1 255.255.255.252
Router(config-subif)#exit
```

Gambar 17. Mengaktifkan *port* ke *Router* Utama

Selanjutnya masuk ke *Router* ISP Cadangan berikan alamat IP pada *Port* G0/2 yang mengarah ke *Router* Utama. Berikut konfigurasi yang dapat dilihat pada gambar dibawah.

```
Router>enable
Router#configure terminal
Router(config)#int g0/2
Router(config-subif)#ip address 200.20.20.1 255.255.255.252
Router(config-subif)#exit
```

Gambar 18. Mengaktifkan *port* ke *Router* Utama

Setelah IP *Address* pada masing masing ISP diberikan kemudian konfigurasi *Failover* pada *Router* Utama. Sebagai contoh ketika ISP utama mengalami gangguan dan *user* dibawahnya tidak dapat mengakses

internet maka *failover* akan secara otomatis berpindah jalur ke ISP cadangan agar *user* tetap dapat mengakses internet. Berikut konfigurasi *default router* yang dapat dilihat pada gambar dibawah.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 100.10.10.1
Router(config)#ip route 0.0.0.0 0.0.0.0 200.20.20.1 10
```

Gambar 19. Konfigurasi default route

Kemudian melakukan konfigurasi *sub-interface* untuk menghubungkan setiap VLAN pada *Router* Utama. Konfigurasi *sub-interface* ini agar dapat melayani komunikasi antar VLAN serta berfungsi sebagai *default gateway* bagi masing-masing VLAN. Berikut konfigurasi *sub-interface* pada *Router* Utama yang dapat dilihat pada gambar dibawah.

```
Router>enable
Router#configure terminal
Router(config)#int g0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add 192.168.10.1 255.255.255.0
Router(config-subif)#exit
```

Gambar 20. *Sub-Interface* VLAN 10 pada *Router* Utama

```
Router(config)#int g0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip add 192.168.20.1 255.255.255.0
Router(config-subif)#exit
```

Gambar 21. *Sub-Interface* VLAN 20 pada *Router* Utama

```
Router(config)#int g0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip add 192.168.30.1 255.255.255.0
Router(config-subif)#exit
```

Gambar 22. *Sub-Interface* VLAN 30 pada *Router* Utama

```
Router(config)#int g0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip add 192.168.40.1 255.255.255.0
Router(config-subif)#exit
```

Gambar 23. *Sub-Interface* VLAN 40 pada *Router* Utama

```
Router(config)#int g0/0.99
Router(config-subif)#encapsulation dot1Q 99
Router(config-subif)#ip add 192.168.99.1 255.255.255.0
Router(config-subif)#exit
```

Gambar 24. *Sub-Interface* VLAN 99 pada *Router* Utama

Selanjutnya menambahkan IP DHCP *Pool* pada *Router* Utama untuk menentukan *range* IP *Address* yang akan didistribusikan otomatis oleh DHCP *Server* pada VLAN 10, VLAN 20, VLAN 30, VLAN 40, dan VLAN 99 lengkap dengan parameter jaringan lainnya seperti *default gateway*, *subnet mask*, DNS *server*. Konfigurasi ini bertujuan agar setiap perangkat klien memperoleh alamat IP yang sesuai dengan segmentasi VLAN sehingga pengelolaan jaringan menjadi lebih terstruktur. Berikut konfigurasi ip dhcp *pool* 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
```

Gambar 25. Konfigurasi IP DHCP *Pool* VLAN 10

```
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
```

Gambar 26. Konfigurasi IP DHCP *Pool* VLAN 20

```
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
```

Gambar 27. Konfigurasi IP DHCP *Pool* VLAN 30

```
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
```

Gambar 28. Konfigurasi IP DHCP *Pool* VLAN 40

```
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
```

Gambar 29. Konfigurasi IP DHCP *Pool* VLAN 99

Selanjutnya masuk ke *Router Rogue* untuk mengaktifkan *port* yang terhubung ke *switch*, kemudian dilakukan penambahan konfigurasi *sub-interface* untuk menghubungkan VLAN pada *Router Rogue.* Konfigurasi ini bertujuan untuk mensimulasikan keberadaan *router* tidak resmi (*rogue*) yang mencoba melayani beberapa VLAN dalam jaringan sebagai bagian dari pengujian keamanan. Melalui simulasi ini, dapat dianalisis dampak keberadaan perangkat tidak sah terhadap kestabilan dan keamanan jaringan. Hasil pengujian ini menjadi dasar penerapan mekanisme pengamanan jaringan. Berikut

merupakan konfigurasi untuk mengaktifkan *port* ke *switch* dan *sub-interface* pada *Router Rogue.*

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

Gambar 30. Mengaktifkan *port* ke *switch*

```
Router>enable
Router#configure terminal
Router(config)#int g0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add 172.0.10.1 255.255.255.0
Router(config-subif)#exit
```

Gambar 31. *Sub-Interface* VLAN 10 pada *Router Rogue*

```
Router(config)#int g0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip add 172.0.20.1 255.255.255.0
Router(config-subif)#exit
```

Gambar 32. *Sub-Interface* VLAN 20 pada *Router Rogue*

```
Router(config)#int g0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip add 172.0.30.1 255.255.255.0
Router(config-subif)#exit
```

Gambar 33. *Sub-Interface* VLAN 30 pada *Router Rogue*

```
Router(config)#int g0/0.40
Router(config-subif)#encapsulation dot1Q 40
Router(config-subif)#ip add 172.0.40.1 255.255.255.0
Router(config-subif)#exit
```

Gambar 34. *Sub-Interface* VLAN 40 pada *Router Rogue*

```
Router(config)#int g0/0.99
Router(config-subif)#encapsulation dot1Q 99
Router(config-subif)#ip add 172.0.99.1 255.255.255.0
Router(config-subif)#exit
```

Gambar 35. *Sub-Interface* VLAN 99 pada *Router Rogue*

Kemudian konfigurasi IP DHCP *Pool* pada *Router Rogue* untuk menentukan rentang IP *address* palsu secara otomatis oleh DHCP *Server* pada VLAN 10, VLAN 20, VLAN 30, VLAN 40, dan VLAN 99 sebagai bagian dari simulasi serangan DHCP *Rogue.* Berikut konfigurasi IP DHCP *Pool* pada *Router Rogue* seperti gambar dibawah ini.

```
Router(config)#ip dhcp pool BAUK
Router(dhcp-config)#network 172.0.10.0 255.255.255.0
Router(dhcp-config)#default-router 172.0.10.1
Router(dhcp-config)#dns-server 1.1.1.1
Router(dhcp-config)#exit
```

Gambar 36. Konfigurasi IP DHCP *Pool* VLAN 10

```
Router(config)#ip dhcp pool PIKP
Router(dhcp-config)#network 172.0.20.0 255.255.255.0
Router(dhcp-config)#default-router 172.0.20.1
Router(dhcp-config)#dns-server 1.1.1.1
```

Gambar 37. Konfigurasi IP DHCP *Pool* VLAN 20

```
Router(config)#ip dhcp pool BKK
Router(dhcp-config)#network 172.0.30.0 255.255.255.0
Router(dhcp-config)#default-router 172.0.30.1
Router(dhcp-config)#dns-server 1.1.1.1
Router(dhcp-config)#exit
```

Gambar 38. Konfigurasi IP DHCP *Pool* VLAN 30

```
Router(config)#ip dhcp pool Balai_bahasa
Router(dhcp-config)#network 172.0.40.0 255.255.255.0
Router(dhcp-config)#default-router 172.0.40.1
Router(dhcp-config)#dns-server 1.1.1.1
Router(dhcp-config)#exit
```

Gambar 39. Konfigurasi IP DHCP *Pool* VLAN 40

```
Router(config)#ip dhcp pool Lainnya
Router(dhcp-config)#network 172.0.99.0 255.255.255.0
Router(dhcp-config)#default-router 172.0.99.1
Router(dhcp-config)#dns-server 1.1.1.1
Router(dhcp-config)#exit
```

Gambar 40. Konfigurasi IP DHCP *Pool* VLAN 99

Setelah itu, IP Address pada PC1 hingga PC12 diset menggunakan DHCP, sehingga alamat IP yang diperoleh oleh masing-masing PC berbeda. Kondisi ini menyebabkan beberapa PC mendapatkan alamat IP dari DHCP *Trusted,* sedangkan PC lainnya menerima alamat IP dari DHCP *Rogue*. Kondisi tersebut terjadi karena belum diterapkannya mekanisme keamanan pada jaringan untuk membatasi dan memverifikasi sumber DHCP yang diperbolehkan memberikan alamat IP kepada klien. Tanpa adanya fitur pengamanan seperti DHCP Snooping, switch tidak mampu membedakan antara server DHCP yang sah dan server DHCP yang tidak sah. Hal ini berpotensi menimbulkan masalah jaringan, seperti konflik alamat IP, kesalahan konfigurasi gateway, hingga ancaman keamanan berupa serangan man-in-the-middle.

Oleh karena itu, penerapan DHCP Snooping menjadi sangat penting karena berfungsi sebagai mekanisme keamanan pada switch untuk memverifikasi dan membatasi sumber DHCP yang diperbolehkan, mencegah masuknya DHCP Rogue, serta memastikan

setiap klien memperoleh konfigurasi jaringan yang benar sehingga keamanan, kestabilan, dan keandalan jaringan dapat terjaga secara optimal. Dengan adanya fitur ini, administrator jaringan juga dapat memonitor dan mencatat setiap aktivitas DHCP yang terjadi pada jaringan, mengidentifikasi potensi ancaman atau kesalahan konfigurasi secara dini, serta menerapkan kebijakan pengelolaan alamat IP yang lebih efisien, sehingga tidak hanya mencegah gangguan layanan dan konflik IP, tetapi juga meningkatkan performa jaringan dan meminimalkan risiko downtime yang dapat berdampak pada produktivitas pengguna dan operasional organisasi secara keseluruhan.

Berikut merupakan hasil yang diperoleh ketika fitur DHCP *Snooping* belum diaktifkan, sebagaimana ditampilkan pada tabel di bawah ini.

Tabel 2. Sebelum DHCP *Snooping* diaktifkan

Device	VLAN	IP Address	Subnetmask	Gateway	DNS
	10	192.168.10.1	255.255.255.0	192.168.10.1	8.8.8.8
	20	192.168.20.1	255.255.255.0	192.168.20.1	8.8.8.8
RTR_Utama	30	192.168.30.1	255.255.255.0	192.168.30.1	8.8.8.8
	40	192.168.40.1	255.255.255.0	192.168.40.1	8.8.8.8
	99	192.168.99.1	255.255.255.0	192.168.99.1	8.8.8.8
	10	172.0.10.1	255.255.255.0	172.0.10.1	1.1.1.1
	20	172.0.20.1	255.255.255.0	172.0.20.1	1.1.1.1
RTR_Rogue	30	172.0.30.1	255.255.255.0	172.0.30.1	1.1.1.1
	40	172.0.40.1	255.255.255.0	172.0.40.1	1.1.1.1
	99	172.0.99.1	255.255.255.0	172.0.99.1	1.1.1.1
PC1	10	172.0.10.4	255.255.255.0	172.0.10.1	1.1.1.1
PC2	10	172.0.10.6	255.255.255.0	172.0.10.1	1.1.1.1
PC3	10	192.168.10.7	255.255.255.0	192.168.10.1	8.8.8.8
PC4	10	172.0.10.3	255.255.255.0	172.0.10.1	1.1.1.1
PC5	20	172.0.20.3	255.255.255.0	172.0.20.1	1.1.1.1
PC6	20	192.168.20.4	255.255.255.0	192.168.20.1	8.8.8.8
PC7	30	172.0.30.3	255.255.255.0	172.0.30.1	1.1.1.1
PC8	30	192.168.30.4	255.255.255.0	192.168.30.1	8.8.8.8
PC9	40	172.0.40.2	255.255.255.0	172.0.40.1	1.1.1.1
PC10	40	172.0.40.3	255.255.255.0	172.0.40.1	1.1.1.1
PC11	99	172.0.99.4	255.255.255.0	172.0.99.1	1.1.1.1
PC12	99	192.168.99.3	255.255.255.0	192.168.99.1	8.8.8.8

Pada tabel konfigurasi di atas dapat dilihat ada beberapa PC diantaranya PC1, PC2, PC4, PC5, PC7, PC9, PC10, PC11 mendapat IP *Address, Gateway* dan *Domain Name Server* dari DHCP *Rogue* sedangkan PC lainnya mendapat IP Address, Gateway dan *Domain Name Server* dari DHCP *Trusted.*

Perancangan berikutnya mengkonfigurasi *Switch* menggunakan DHCP *Snooping*. Konfigurasi ini bertujuan untuk memastikan bahwa hanya *port* yang dipercaya (*trusted*) yang diperbolehkan mendistribusikan alamat IP kepada *client*. Berikut merupakan konfigurasi DHCP *Snooping* pada *switch*.

```
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 fa0/24
Switch (config-if)#description "DHCP Trust"
Switch (config-if)#exit
Switch (config)#ip dhcp snooping
Switch (config)#int fa0/24
Switch (config-if)#ip dhcp snooping trust
```

Gambar 41. Konfigurasi DHCP *Snooping*

Pada konfigurasi di atas, perintah IP DHCP *Snooping* mengaktifkan metode keamanan DHCP *Snooping* hanya *port* Fa0/24 yang dapat dipercaya sebagai DHCP *server* dengan deskripsi DHCP *Trust*. Hasil dari konfigurasi ditampilkan pada tabel di bawah.

Tabel 3. Sesudah DHCP *Snooping* diaktifkan

Device	VLAN	IP Address	Subnetmask	Gateway	DNS
	10	192.168.10.1	255.255.255.0	192.168.10.1	8.8.8.8
	20	192.168.20.1	255.255.255.0	192.168.20.1	8.8.8.8
RTR_Utama	30	192.168.30.1	255.255.255.0	192.168.30.1	8.8.8.8
	40	192.168.40.1	255.255.255.0	192.168.40.1	8.8.8.8
	99	192.168.99.1	255.255.255.0	192.168.99.1	8.8.8.8
	10	172.0.10.1	255.255.255.0	172.0.10.1	1.1.1.1
	20	172.0.20.1	255.255.255.0	172.0.20.1	1.1.1.1
RTR_Rogue	30	172.0.30.1	255.255.255.0	172.0.30.1	1.1.1.1
	40	172.0.40.1	255.255.255.0	172.0.40.1	1.1.1.1
	99	172.0.99.1	255.255.255.0	172.0.99.1	1.1.1.1
PC1	10	192.168.10.8	255.255.255.0	192.168.10.1	8.8.8.8
PC2	10	192.168.10.9	255.255.255.0	192.168.10.1	8.8.8.8
PC3	10	192.168.10.7	255.255.255.0	192.168.10.1	8.8.8.8
PC4	10	192.168.10.10	255.255.255.0	192.168.10.1	8.8.8.8
PC5	20	192.168.20.5	255.255.255.0	192.168.20.1	8.8.8.8
PC6	20	192.168.20.4	255.255.255.0	192.168.20.1	8.8.8.8
PC7	30	192.168.30.5	255.255.255.0	192.168.30.1	8.8.8.8
PC8	30	192.168.30.4	255.255.255.0	192.168.30.1	8.8.8.8
PC9	40	192.168.40.3	255.255.255.0	192.168.40.1	8.8.8.8
PC10	40	192.168.40.4	255.255.255.0	192.168.40.1	8.8.8.8
PC11	99	192.168.99.4	255.255.255.0	192.168.99.1	8.8.8.8
PC12	99	192.168.99.3	255.255.255.0	192.168.99.1	8.8.8.8

Berdasarkan hasil konfigurasi DHCP *Snooping* di atas, dapat dilihat bahwa semua PC berhasil mendapat IP *Address,* DNS *server* dan *Gateway* dari DHCP Utama, kemudian PC1, PC2, PC4, PC5, PC7, PC9, PC10, PC11 tidak lagi mendapat IP *Address*, DNS *server* dan *Gateway* dari DHCP *Rogue.*

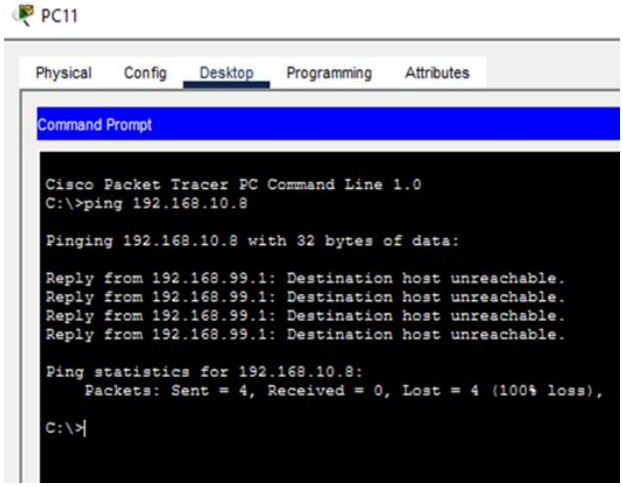
Tahap selanjutnya dilakukan konfigurasi *Access Control List* (ACL) pada *Router* Utama dengan tujuan untuk membatasi jaringan dari VLAN 99 menuju VLAN 10, sehingga komunikasi dari VLAN tersebut ke jaringan VLAN 10 tidak diperbolehkan sesuai dengan kebijakan keamanan yang diterapkan. Konfigurasi ini dilakukan untuk meningkatkan keamanan jaringan dengan mencegah akses yang tidak sah serta memastikan setiap

VLAN hanya dapat berkomunikasi sesuai dengan fungsi dan perannya masing-masing dalam infrastruktur jaringan. Berikut konfigurasi ACL pada *Router* Utama.

```
Router>enable
Router#configure terminal
Router(config)#access-list access-list 100 deny ip 192.168.99.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config)# access-list 100 permit ip any any
Router(config)#int g0/0.99
Router(config-subif)# ip access-group 100 in
```

Gambar 42. Konfigurasi *Access Control List*

Setelah konfigurasi *Access Control List* tahap selanjutnya uji *ping* dari PC 11 VLAN 99 ke IP *Address* PC1 VLAN 10. Berikut hasil uji *ping* seperti gambar dibawah ini.



Gambar 43. Uji *ping* dari VLAN 99 ke VLAN 10

Munculnya pesan *Destination host unreachable* menandakan bahwa *router* secara sengaja menolak dan tidak meneruskan paket ICMP menuju VLAN 10 sebagai akibat dari kebijakan keamanan yang diterapkan melalui *Access Control List* (ACL).

4.5 Monitoring

Pada tahap ini, dilakukan monitoring dengan cara melakukan pengecekan DHCP *Snooping* pada *switch*, VLAN dan pembagian *port switch,* koneksi *trunk* antara *switch* dan *router*, *Access Control List* (ACL) pada *router*, serta *monitor failover* ISP untuk memastikan seluruh konfigurasi keamanan dan ketersediaan jaringan berjalan sesuai dengan perancangan.

Perintah *show ip dhcp snooping* pada switch digunakan untuk menampilkan status dan konfigurasi DHCP *Snooping*, termasuk VLAN yang dilindungi, pengaturan *interface trusted* dan *untrusted*, serta informasi keamanan untuk mencegah DHCP server tidak sah dalam proses pemberian alamat IP. Berikut tampilan nya seperti gambar dibawah ini.

```
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20,30,40,99
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
-----------------------    -------    ----------------
FastEthernet0/1            no         unlimited
FastEthernet0/7            no         unlimited
FastEthernet0/9            no         unlimited
FastEthernet0/10           no         unlimited
FastEthernet0/11           no         unlimited
FastEthernet0/2            no         unlimited
FastEthernet0/4            no         unlimited
FastEthernet0/5            no         unlimited
FastEthernet0/12           no         unlimited
FastEthernet0/24           yes        unlimited
FastEthernet0/23           no         unlimited
```

Gambar 44. *Monitoring* DHCP *Snooping*

Perintah show vlan brief pada switch digunakan untuk menampilkan ringkasan VLAN, meliputi daftar VLAN, nama, status, dan port yang tergabung, sehingga memudahkan administrator dalam memeriksa konfigurasi, memastikan penempatan port sudah sesuai, serta melakukan troubleshooting untuk menjaga stabilitas jaringan. Informasi yang ditampilkan dari perintah ini sangat penting dalam proses pengelolaan jaringan karena membantu mengidentifikasi kesalahan konfigurasi VLAN, port yang belum terkonfigurasi dengan benar, maupun potensi masalah konektivitas antar perangkat dalam jaringan. Berikut tampilan nya seperti gambar dibawah ini.

```
Switch>enable
Switch#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Gig0/1, Gig0/2
10   bauk                              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
20   pikp                              active    Fa0/5, Fa0/6
30   bkk                               active    Fa0/7, Fa0/8
40   balai_bahasa                      active    Fa0/9, Fa0/10
99   lainnya                           active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                 Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                 Fa0/19, Fa0/20, Fa0/21, Fa0/22
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
Switch#
```

Gambar 45. Monitoring VLAN

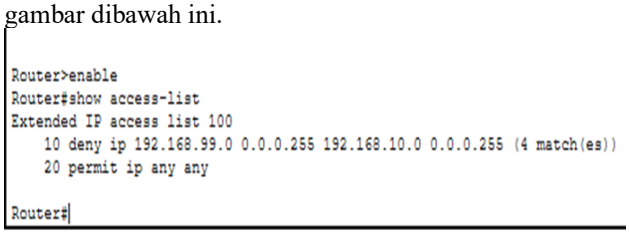
Perintah *show interface trunk* pada *switch* digunakan untuk menampilkan informasi mengenai interface yang berfungsi sebagai *trunk*, termasuk status *trunking*, mode *trunk, encapsulation* (seperti 802.1Q), VLAN yang diizinkan**,** VLAN yang aktif dan sedang diteruskan, serta VLAN *native*. Perintah ini sangat berguna untuk memastikan koneksi *trunk* antar *switch* atau antara *switch* dan *router* berjalan dengan benar, sehingga lalu lintas data dari berbagai VLAN dapat dilewatkan tanpa masalah. Berikut tampilan nya seperti gambar dibawah ini.

```
Switch#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/23      on           802.1q         trunking      1
Fa0/24      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/23      1-1005
Fa0/24      1-1005

Port        Vlans allowed and active in management domain
Fa0/23      1,10,20,30,40,99
Fa0/24      1,10,20,30,40,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/23      1,10,20,30,40,99
Fa0/24      1,10,20,30,40,99
```

Gambar 46. Interface Trunk

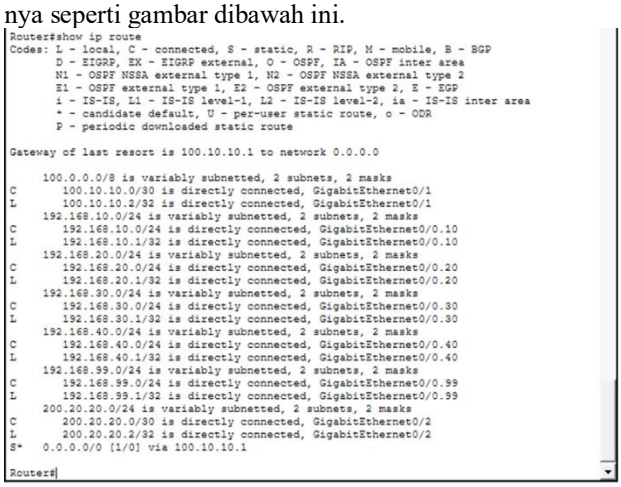
Perintah *show access-lists* pada *router* digunakan untuk menampilkan daftar *Access Control List* (ACL) yang telah dikonfigurasikan seperti ACL *extended,* beserta aturan (*permit* atau *deny*) yang berfungsi untuk mengontrol dan memfilter lalu lintas jaringan, sehingga *administrator* dapat memantau, memverifikasi, dan

melakukan troubleshooting terhadap kebijakan keamanan yang diterapkan pada *switch.* Berikut tampilan nya seperti gambar dibawah ini.



Gambar 47. *Monitoring* ACL

Perintah *show ip route* digunakan untuk menampilkan tabel *routing* pada perangkat jaringan seperti *router,* yang berisi informasi mengenai rute-rute jaringan yang diketahui perangkat tersebut. Melalui perintah ini, *administrator* dapat melihat jaringan tujuan, *next hop, interface* yang digunakan, serta jenis rute (*static, connected*, atau *dynamic*), sehingga sangat berguna untuk memverifikasi konfigurasi *routing* dan melakukan *troubleshooting* ketika terjadi masalah komunikasi antarjaringan. Informasi yang ditampilkan membantu administrator dalam menganalisis alur pengiriman paket data, memastikan rute yang digunakan telah sesuai dengan perancangan jaringan, serta mengidentifikasi kesalahan konfigurasi atau rute yang tidak aktif. Berikut tampilan nya seperti gambar dibawah ini.



Gambar 48. *Monitoring failover* ISP

5. KESIMPULAN

Berdasarkan hasil perancangan dan simulasi keamanan jaringan menggunakan metode DHCP Snooping, VLAN, dan Access Control List (ACL) pada Cisco Packet Tracer, dapat disimpulkan bahwa penerapan DHCP Snooping terbukti efektif dalam mencegah serangan DHCP Rogue dengan memastikan hanya DHCP Server resmi yang berwenang mendistribusikan alamat IP kepada klien, sehingga keamanan jaringan menjadi lebih terjaga dari gangguan DHCP server palsu. Selain itu, penerapan VLAN mampu mengelompokkan jaringan berdasarkan VLAN ID atau grup yang telah ditentukan, sehingga perangkat yang berada di luar kelompok tersebut tidak dapat saling berkomunikasi dalam satu jaringan yang sama. Penggunaan Access Control List (ACL) juga terbukti efektif dalam membatasi akses antar VLAN, khususnya dalam melindungi jaringan sensitif seperti VLAN 10 pada bagian BAUK.

6. SARAN

Saran yang dapat diberikan untuk pengembangan penelitian berikutnya yaitu disarankan untuk melakaukan peningkatan pengamanan pada Layer 2 sebagai langkah antisipasi terhadap potensi ancaman dengan menambahkan DHCP *Starvation*, sehingga diharapkan dapat meningkatkan sistem keamanan jaringan secara menyeluruh. Selain itu, penelitian selanjutnya juga dapat mengkaji penerapan fitur keamanan Layer 2 lainnya, seperti Port Security dan Dynamic ARP Inspection, guna memperkuat perlindungan jaringan kampus secara lebih komprehensif.

7. REFERENSI

Ahmad, U. A., Saputra, R. E., & Pangestu, Y. (2021). *Perancangan Infrastruktur Jaringan Komputer Menggunakan Fiber Optik Dengan Metode Network Development Life Cycle (NDLC)*.

Ariyadi, T. (2017). Desain Keamanan DHCP Snooping Untuk Mengurangi Serangan Local Area Network (LAN). *JUSIKOM*, *2*(1).

Azmi, F., Umi Kalsum, T., & Alamsyah, H. (2022). Analysis and Application of Access Control List (ACL) Methods on Computer Networks Analisa dan Penerapan Metode Access Control List (ACL) pada Jaringan Komputer. *JURNAL KOMITEK*, *2*(1), 81–88. https://doi.org/10.53697/jkomitek.v2i1

Fahri, M., Fiade, A., & Suseno, H. B. (2018). Simulasi Jaringan Virtual Local Area Network (VLAN) Menggunakan Pox Controller. *JURNAL TEKNIK INFORMATIKA*, *10*(1), 85–90. https://doi.org/10.15408/jti.v10i1.6821

Madcoms. (2017). *Membangun Sistem Jaringan Komputer dengan Mikrotik*. Andi

Medianto, M. (2020). *Analisis Keamanan Jaringan Local Area Network yang Menggunakan DHCP Server Berbasis Cisco dengan metode Penetration Testing Medianto*.

Miftah, Z. (2018). SIMULASI KEAMANAN JARINGAN DENGAN METODE DHCP SNOOPING DAN VLAN. *Faktor Exacta*, *11*(2), 167. https://doi.org/10.30998/faktorexacta.v11i2.2456

Noviani, Y. D. (2020). *Analisis Pengembangan Virtual Local Area Network (VLAN) di SMK Asy-Syarifiy Pandanwangi-Lumajang*. *02*, 61–66.

Simanjuntak, P., Suharyanto, C. E., & Jamilah, J. (2017). Analisis Penggunaan Access Control List (ACL) Dalam Jaringan Komputer Di Kawasan Batamindo Industrial Park Batam. *Journal Information System Development (ISD)*, *2*(2).

Sugiyanta, L., & Raja, B. (2017). Kualitas Jaringan Pada Jaringan Virtual Local Area Network (VLAN)

Yang Menerapkan Linux Terminal Server Project (LTSP). *PINTER : Jurnal Pendidikan Teknik Informatika Dan Komputer*, *1*(2), 82–89. https://doi.org/10.21009/pinter.1.2.1

Sungkar, M. S., & Sabara, M. A. (2019). *Rancang Bangun Jaringan LAN Dengan Sistem Routing Protokol IGRP dan DHCP Server Menggunakan Router Cisco Untuk Melakukan Pengiriman Data Di Kantor Sekretariat Kabupaten Brebes*. *8*(1).

STMIK Widya Cipta Dharma. (2025). Panduan Penulisan Tugas Akhir Skripsi.

Syafrizal, M. (2020). *Pengantar Jaringan Komputer*. Andi.