OPTIMALISASI KONEKTIVITAS JARINGAN KAMPUS MELALUI SIMULASI ARP DAN DHCP MENGGUNAKAN *CISCO PACKET TRACER*

Harry Pribadi Fitrian, Fitri Anisa, Mayasari Agustina, Neneng Masitoh, Arya Gunawan
Teknik Informatika, Universitas Teknologi Digital Bandung
Jl. Cibogo No.Indah III, Rancasari, Kota Bandung
harrypribadi@digitechuniversity.ac.id

ABSTRAK

Tujuan dari penelitian ini adalah untuk menganalisis optimalisasi konektivitas jaringan kampus melalui simulasi protokol ARP dan DHCP menggunakan *Cisco Packet Tracer*. Mengingat pentingnya jaringan yang efisien untuk mendukung kegiatan akademis dan administratif, penelitian ini mengidentifikasi beberapa masalah umum, termasuk kemacetan jaringan dan kesulitan dalam mengelola alamat IP. Metodologi yang digunakan meliputi analisis persyaratan jaringan, desain topologi, simulasi dan evaluasi kinerja jaringan berdasarkan parameter throughput, latensi, dan keamanan. Penelitian telah menunjukkan bahwa penerapan protokol ARP untuk resolusi alamat dan DHCP untuk manajemen alamat IP dapat secara signifikan meningkatkan efisiensi koneksi, mengurangi kemacetan, dan membuat jaringan berskala besar lebih mudah dikelola. Studi ini menghasilkan hasil yang sangat baik dalam menilai kinerja jaringan, yang menunjukkan bahwa *Cisco Packet Tracer* merupakan alat yang efektif untuk merancang dan menguji model jaringan kampus sebelum implementasi sebenarnya, sehingga meminimalkan risiko kesalahan dan biaya. Disimpulkan bahwa ini merupakan alat.

Kata kunci: *Jaringan Komputer, Cisco Packet Tracer, Konektivitas, Optimasi, ARP, DHCP.*

1. PENDAHULUAN

Jaringan komputer telah menjadi elemen penting dalam menunjang berbagai kegiatan akademik dan administrasi di lembaga pendidikan. Dalam konteks ini, penting untuk mengoptimalkan konektivitas jaringan agar proses komunikasi dan transfer data dapat dilakukan secara efisien. Aspek penting dari manajemen jaringan adalah penggunaan Address Resolusi Protocol (ARP) dan Dynamic Host Configuration Protocol (DHCP). Ini bertanggung jawab untuk mengelola alamat IP dan mengonfigurasi perangkat di jaringan Anda. Jaringan yang efisien sangat penting untuk mendukung proses belajar mengajar dan pengelolaan kampus. Kualitas koneksi yang baik meningkatkan produktivitas dan pengalaman pengguna [1].

Seiring bertambahnya jumlah pengguna dan perangkat yang terhubung ke jaringan kampus , tantangan dalam mengelola jaringan menjadi lebih kompleks. Masalah seperti kecepatan akses yang lambat, kehilangan paket, dan kesulitan dalam mengelola alamat IP dapat memengaruhi kualitas koneksi yang diharapkan [4].

Peran ARP dan DHCP sangat penting untuk manajemen jaringan. ARP digunakan untuk memetakan alamat IP ke alamat fisik (MAC), sementara DHCP memfasilitasi manajemen alamat IP dengan secara otomatis menetapkan alamat ke perangkat yang terhubung[2].

Menggunakan Cisco Packet Tracer sebagai alat simulasi, perancang jaringan dapat menguji berbagai konfigurasi dan topologi tanpa terlebih dahulu menjalankan implementasi fisik. Dengan cara ini, masalah potensial seperti kemacetan jaringan atau keterbatasan skala dapat diidentifikasi sebelum penerapan sebenarnya [5].

Tujuan dari penelitian ini adalah untuk menganalisis dan mengembangkan model jaringan yang dapat mengoptimalkan konektivitas menggunakan simulasi ARP dan DHCP. Pendekatan ini bertujuan untuk menemukan solusi efektif untuk meningkatkan efisiensi jaringan kampus [3].

Studi ini juga mencakup desain topologi, simulasi dan evaluasi kinerja jaringan berdasarkan parameter throughput, latensi, dan keamanan. Hasil penelitian ini diharapkan dapat memberikan kontribusi yang signifikan terhadap pengembangan jaringan komputer di lingkungan kampus [3].

Mengoptimalkan konektivitas jaringan kampus melalui penggunaan ARP dan DHCP serta simulasi dengan Cisco Packet Tracer merupakan langkah penting dalam mengatasi tantangan yang ada. Pendekatan ini bertujuan untuk meningkatkan kualitas jaringan dan dengan demikian mendukung kegiatan akademis dan administratif secara lebih efektif.

2. TINJAUAN PUSTAKA

2.1. Router

Router adalah perangkat yang mengirimkan paket data ke tujuannya melalui jaringan atau Internet melalui proses yang disebut perutean Proses perutean berjalan pada Level 3 pada koneksi sistem terbuka. Router berfungsi sebagai penghubung antara dua atau lebih jaringan meneruskan data dari satu jaringan ke jaringan lainnya. Router berbeda dengan switch. Sakelar adalah perangkat yang menghubungkan beberapa perangkat ke jaringan area lokal (LAN). Untuk menjelaskan perbedaan fungsional antara router dan switch, adalah jalan dan router adalah penghubung antara jalan. Setiap rumah di Jalan diberi alamat dalam urutan tertentu.

Demikian pula, sakelar menghubungkan beberapa perangkat dan setiap perangkat dalam LAN memiliki alamat IP-nya sendiri. Router sering digunakan dalam jaringan yang didasarkan pada teknologi protokol TCP/IP dan jenis router ini juga disebut router IP Selain router IP, ada juga router AppleTalk dan banyak jenis router lainnya. Router memungkinkan Anda menghubungkan banyak jaringan yang lebih kecil ke jaringan yang lebih besar, yang disebut internetwork, atau membagi jaringan besar menjadi beberapa subjaringan untuk kinerja yang lebih baik dan administrasi yang lebih mudah. Anda bisa. Router juga dapat digunakan untuk menghubungkan LAN ke layanan komunikasi, seperti komunikasi leased-line atau digital subscriber line (DSL). Router yang digunakan untuk menghubungkan LAN ke koneksi leased-line seperti T1 atau T3 sering disebut server akses. Router yang digunakan untuk menghubungkan jaringan lokal ke koneksi DSL juga dikenal sebagai router DSL.Jenis router ini biasanya memiliki fungsi firewall yang menyaring paket berdasarkan alamat sumber dan tujuan paket, tetapi beberapa router tidak memiliki fungsi ini. Router dengan kemampuan penyaringan paket juga dikenal sebagai router penyaring paket. Router biasanya memblokir lalu lintas keluar untuk mencegah badai siaran yang dapat menurunkan kinerja jaringan.

2.2. Subneting

Subnet mask adalah istilah teknologi informasi dalam bahasa Inggris yang merujuk pada angka biner 32-bit yang digunakan untuk membedakan antara ID jaringan dan ID host, dan menunjukkan lokasi host, baik di jaringan lokal maupun jaringan eksternal. Subnet mask (juga dikenal sebagai masker alamat) adalah nilai 32-bit yang digunakan untuk membedakan antara ID jaringan dan ID host dalam alamat IP. Subnet mask biasanya ditulis dalam notasi desimal bertitik, seperti alamat IP. Setelah semua bit ditetapkan untuk bagian dari ID jaringan dan ID host, nilai 32-bit yang dihasilkan diubah ke notasi desimal bertitik .Perhatikan bahwa subnet mask bukanlah alamat IP, meskipun direpresentasikan dalam notasi desimal bertitik sebagai subnet mask default adalah berdasarkan kelas alamat IP digunakan dalam jaringan TCP/IP.

2.3. Address Resolusi Protocol (ARP)

Address Resolusi Protocol (ARP) adalah protokol yang digunakan dalam jaringan komputer untuk memetakan alamat Internet Protocol (IP) ke alamat Media Access Control (MAC). ARP bertindak sebagai jembatan antara lapisan jaringan (Layer 3) dan lapisan data link (Layer 2) dari model Open Systems Interconnection (OSI), yang memungkinkan perangkat di jaringan lokal berkomunikasi secara efektif satu sama lain.

Jaringan lokal memiliki protokol yang disebut ARP (Address Resolusi Protocol). Fungsi protokol ARP adalah untuk mengubah alamat IP menjadi alamat MAC (Agrawal et al., belum dikonfirmasi). Paket permintaan ARP disiarkan dan menyertakan alamat IP host tujuan. Ketika host tujuan menerima paket permintaan ARP, ia mengirimkan paket balasan ARP unicast ke host pengirim. Host pengirim menyimpan alamat IP dan alamat MAC host tujuan dalam tabel cache ARP-nya. Tabel cache ARP memiliki batas waktu penyimpanan yang berbeda pada sistem operasi yang berbeda. ARP tidak memiliki kewarganegaraan. Artinya, h. Keakuratan setiap balasan ARP yang diterima tidak diperiksa, sehingga alamat IP dan alamat MAC paket balasan ARP segera disimpan dalam tabel cache ARP. Protokol ARP tidak memiliki kemampuan untuk memverifikasi apakah respons ARP yang diterima dikirimkan sebagai respons terhadap paket permintaan ARP sebelumnya[9].

ARP bersifat stateless dan tidak memerlukan autentikasi sehingga rentan terhadap berbagai serangan pada jaringan komputer. Protokol ARP rentan terhadap serangan yang disebut ARP spoofing atau keracunan ARP yang disebabkan oleh kerentanan keamanan pada protokol. Oleh karena itu, proses deteksi serangan penting untuk melindungi inangnya sebelum melakukan tindakan pencegahan[6].

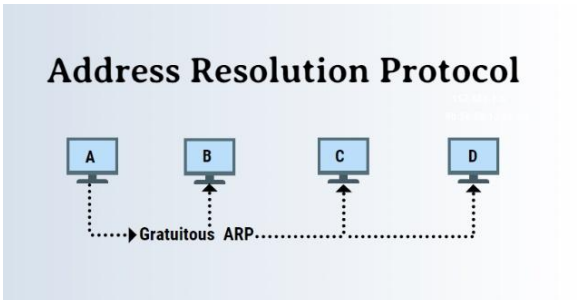
Penggunaan paket permintaan gema ICMP dan paket balasan gema ICMP untuk secara aktif mendeteksi serangan spoofing ARP, namun metode ini menghabiskan banyak sumber daya dalam jaringan. Switch Cisco juga menerapkan metode inspeksi ARP dinamis untuk meningkatkan keamanan, namun biaya implementasinya sangat tinggi. Sistem deteksi spoofing ARP yang baik tidak mengubah protokol ARP, tidak memerlukan instalasi tambahan pada setiap host yang terhubung ke jaringan, menggunakan sumber daya jaringan minimal, dan dapat mendeteksi semua jenis spoofing ARP tanpa menunda sistem pengiriman paket yang dapat mendeteksi serangan ARP. Untuk mendeteksi serangan spoofing ARP, sistem deteksi melakukan inspeksi antara header Ethernet dan ARP, mendeteksi transmisi paket ARP yang berlebihan, dan mengidentifikasi pasangan IP dan alamat MAC yang jahat.

Oleh karena itu, dalam penelitian ini, kami mengusulkan metode untuk secara aktif menganalisis lalu lintas paket ARP dan mendeteksi serangan spoofing ARP. Metode ini menggunakan satu host, yang disebut detektor host, untuk mendeteksi dan memeriksa paket ARP dalam lalu lintas jaringan. Detektor Host memeriksa header Ethernet dan paket ARP, menghitung jumlah paket ARP untuk mendeteksi paket redundan, menentukan apakah beberapa alamat MAC sumber alamat IP digunakan, dan mengidentifikasi alamat IP dan pasangan alamat MAC sudah benar. Detektor host juga mengimplementasikan metode ARP stateful, yang memeriksa setiap paket respons ARP yang diterima untuk menentukan apakah paket tersebut terkait dengan permintaan sebelumnya [6].

Address Resolusi Protocol (ARP) adalah protokol yang digunakan untuk memetakan alamat IP ke alamat MAC. ARP merupakan protokol penting untuk komunikasi jaringan LAN, terutama saat berkomunikasi melalui Ethernet. Alamat MAC adalah alamat unik 48-bit yang biasa digunakan sebagai pengenal di Ethernet. Alamat MAC bersifat unik dan terdiri dari tiga oktet Pengidentifikasi Unik Organisasi (OUI) yang mengidentifikasi produsen perangkat dan tiga oktet tambahan yang disediakan oleh produsen perangkat [3].

Konsep dasar keracunan ARP atau spoofing adalah menggunakan cache ARP untuk memberikan pengguna jaringan server palsu atau ID/alamat gateway, yang memungkinkan penyerang mengubah lalu lintas jaringan [5].

Jika dibiarkan, serangan ini dapat mengganggu lalu lintas jaringan dan mengganggu konektivitas Internet pada perangkat yang terhubung ke jaringan tersebut. Oleh karena itu, perlu adanya penelitian yang dapat mendeteksi perilaku serangan keracunan ARP [9].



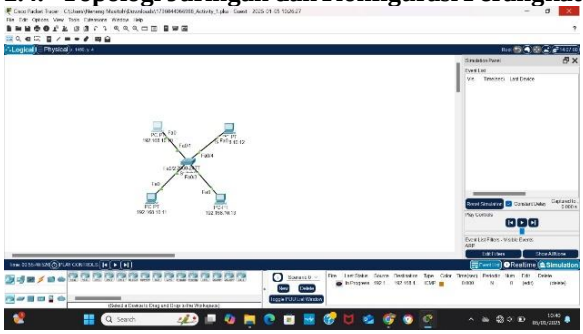
Gambar 1. Konsep ARP

Pada gambar 1 menggambarkan konsep Address Resolution Protocol (ARP**)**, khususnya mengenai Gratuitous ARP. Berikut adalah penjelasan untuk elemen yang terdapat dalam gambar :

a. Perangkat A, B, C, dan D :
   - Ini mewakili berbagai perangkat dalam jaringan yang saling terhubung. Masing-masing perangkat memiliki alamat IP dan alamat MAC yang unik.

b. Gratuitous ARP :
   - Ini adalah jenis permintaan ARP yang dikirim oleh perangkat (dalam hal ini, perangkat A) tanpa permintaan dari perangkat lain.
   - Tujuannya adalah untuk memberi tahu perangkat lain di jaringan tentang alamat MAC dan IP yang baru atau diperbarui.
   - Ini biasanya terjadi ketika perangkat baru ditambahkan ke jaringan atau ketika alamat IP perangkat diubah.

2.4. Topologi Jaringan dan Konfigurasi Perangkat



Gambar 2. Topologi Star

Pada gambar 2 menggambarkan konfigurasi jaringan yang terdiri dari beberapa perangkat komputer yang terhubung melalui switch. Berikut adalah penjelasan elemen-elemen yang ada dalam gambar:

a. Perangkat PC :
   - (Gambar menunjukkan beberapa PC yang terhubung ke jaringan. Setiap PC memiliki alamat IP yang unik, yang digunakan untuk identifikasi dalam jaringan).

b. Switch :
   - (Switch berfungsi sebagai perangkat penghubung yang mengarahkan lalu lintas data antara PC. Ia menggunakan alamat MAC untuk mengirimkan data ke perangkat yang tepat).

c. Proses ARP
   - (Ketika salah satu PC ingin berkomunikasi dengan PC lain, ia akan mengirimkan permintaan ARP untuk menemukan alamat MAC dari PC yang memiliki alamat IP tujuan).
   - (Permintaan ARP disiarkan ke seluruh jaringan, dan perangkat yang memiliki alamat IP yang dicari akan merespons dengan mengirimkan alamat MAC-nya).

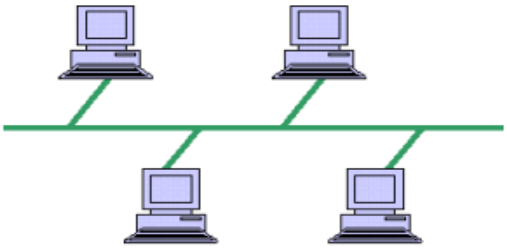
d. Konektivitas
   - (Gambar menunjukkan konektivitas antara PC dan switch, menciptakan jaringan lokal yang memungkinkan komunikasi antar perangkat).

Keuntungan dari pemakaian topologi bintang adalah :

- Mudah untuk mengubah dan menambah node baru ke dalam jaringan yang menggunakan topologi bintang tanpa mengganggu aaktivitas jaringan yang sedang berlangsung.
- Apabila terdapa node yang mengalami kerusakan dalam jaringan maka node tersebut tidak akan membuat mati keseluruhan jaringan bintang (hanya node tersebut yang mati).
- Dapat menggunakan lebih dari 1 jenis kabel di dalam jaringan yang sama, dengan hub yang dapat mengakomodasi tipe kabel yang berbeda-beda.

Kelemahan dari topologi bintang adalah :

- Memiliki satu kelemahan utama yang terletak pada hub. Jika terjadi kegagalan pada hub pusat, maka seluruh jaringan akan gagal untuk beroperasi.
- Membutuhkan lebih banyak kabel karena semua kabel di jaringan harus ditarik ke satu titik pusat. Jumlah terminal terbatas, tergantung dari jumlah port yang bisa ditampung oleh hub.
- Lalulintas data yang padat dapat menyebabkan jaringan bekerja lebih lambat.



Gambar 3. Topologi Bus

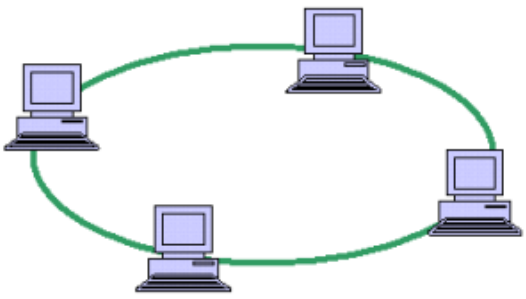
Pada gambar 3 menggambarkan konfigurasi jaringan terdiri dari beberapa perangkat komputer (PC) yang terhubung melalui kabel utama, meskipun dalam praktiknya menggunakan switch sebagai pusat penghubung.

Keuntungan dari topologi bus adalah sebagai berikut :

- Topologi yang sederhana
- Kabel yang digunakan untuk menghubungkan setiap node berjumlah sedikit.
- Biaya yang diperlukan untuk melakukan penyusunan kabel dengan topologi ini relative murah.
- Cukup mudah apabila ingin dilakukan perluasan pada topologi.

Sedangkan kelemahan-kelemahan dari topologi ini yaitu:

- Traffic (lalu lintas) jaringan yang padat akan sangat memperlambat bus.
- Keseluruhan jaringan akan mati (shut down) apabila terdapat kerusakan pada kabel.
- Sangat sulit untuk melakukan pemeriksaan apabila terdapat salah satu node yang rusak.
- Bukan merupakan solusi untuk digunakan pada jaringan komputer skala besar.



Gambar 4. Topologi Ring

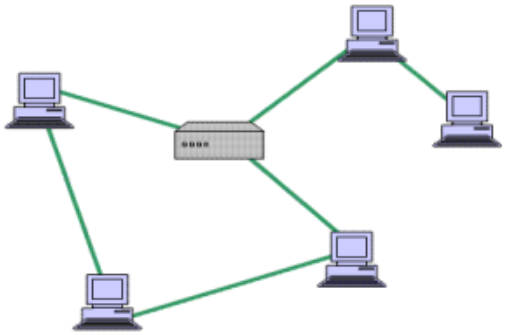
Pada gambar 4 menggambarkan konfigurasi jaringan terdiri dari beberapa perangkat komputer (PC) yang terhubung melalui kabel utama, meskipun dalam praktiknya menggunakan switch sebagai pusat penghubung.

Keuntungan dari pemakaian topologi cincin adalah :

- Data mengalir satu arah sehingga collision dapat dihindarkan.
- Aliran pesan dapat mengalir lebih cepat karena setiap node dapat melayani pesan dari kiri ataupun kanan.
- Waktu yang digunakan untuk mengakses data lebih optimal.
- Sangat sederhana dalam penerapannya.

Kelemahan dari pemakaian topologi cincin adalah :

- Apabila ada satu node dalam cincin yang gagal berfungsi, maka akan mempengaruhi kinerja keseluruhan jaringan.
- Menambah atau mengurangi komputer akan mengacaukan kinerja jaringan.
- Sulit untuk melakukan konfigurasi ulang.



Gambar 5. Topologi Mesh

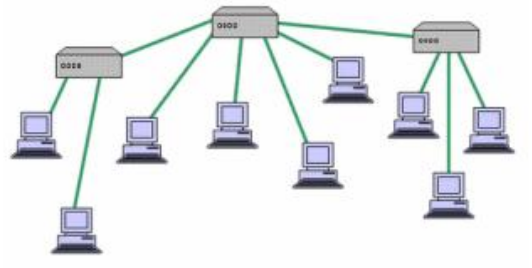
Pada gambar 5 menggambarkan konfigurasi setiap perangkat dalam jaringan terhubung langsung ke beberapa perangkat lainnya. Ini menciptakan jaringan yang sangat terhubung di mana data dapat dikirim melalui berbagai jalur, meningkatkan keandalan dan fleksibilitas komunikasi.

Keuntungan dari penggunaan topologi acak adalah :

- Mudah dalam menangani kegagalan-kegagalan yang mungkin terjadi dalam jaringan (fault tolerance yang tinggi).
- Relatif mudah untuk melakukan pencarian terhadap node yang mengalami kegagalan.

Kelemahan dari topologi ini adalah :

- Membutuhkan biaya yang relatif besar.
- Sulit untuk melakukan konfigurasi ulang dan instalasi node baru pada saat jumlah node yang terkoneksi berjumlah banyak.



Gambar 6. Topologi Pohon

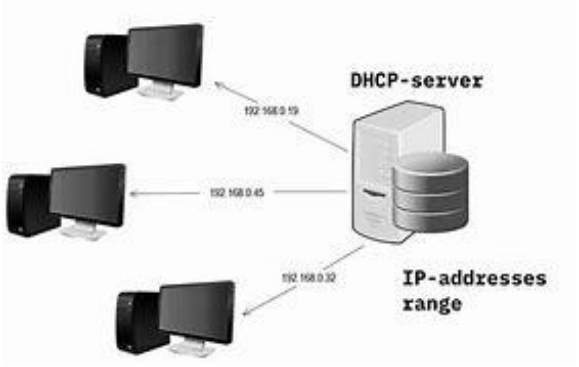
Pada gambar 6 menggambarkan konfigurasi dari topologi star dan bus. Ini terdiri dari beberapa perangkat yang terhubung dalam struktur hierarkis, mirip dengan cabang-cabang pohon.
Keuntungan dari topologi pohon adalah:

- Mendukung pengembangan lebih lanjut dari jaringan dari pada topologi bus (terbatas pada jumlah perangkat dikarenakan traffic yang mungkin muncul) dan topologi bintang (terbatas pada jumlah port pada hub).
- Didukung oleh beberapa vendor perangkat lunak dan perangkat keras.

Kelemahan dari topologi pohon adalah :

- Panjang keseluruhan dari setiap bagian tergantung dari jenis kabel yang digunakan.
- Jika terjadi kegagalan pada bus, maka seluruh jaringan akan gagal berfungsi.
- Lebih susah diterapkan dan dikonfigurasi dari topologi lainnya.

2.5. Dynamic Host Configuration Protocol



Gambar 7. DHCP server

Pada gambar 7 menggambarkan tampilan dari DHCP server. Konfigurasi otomatis alamat IP menggunakan Dynamic Host Configuration Protocol (DHCP) sangat penting dalam manajemen jaringan. Hal ini sangat penting jika Anda perlu menyiapkan jaringan untuk 30 hingga 100 PC atau lebih. DHCP memungkinkan administrator jaringan untuk secara efisien menetapkan alamat IP ke perangkat yang terhubung, mengurangi kesalahan manual dan menghemat waktu selama pengaturan jaringan.

Alamat IP (alamat Protokol Internet) terdiri dari sekumpulan bilangan biner 32-bit yang dibagi menjadi empat bagian yang disebut oktet. Setiap oktet memiliki panjang 8 bit dan biasanya direpresentasikan dalam format desimal sebagai empat angka yang dipisahkan oleh titik. Misalnya alamat IP yang umum digunakan adalah 192.168.1.1. Setiap angka dalam alamat IP ini berkisar antara 0 hingga 255 dan merupakan representasi desimal dari nilai biner 8-bit. Alamat IP berfungsi sebagai pengenal unik untuk setiap host yang terhubung ke jaringan Internet. Dalam konteks ini, sangat penting bahwa tidak ada dua host di jaringan yang memiliki alamat IP yang sama. Hal ini dapat menyebabkan konflik alamat IP dan mengganggu konektivitas jaringan. Jika dua perangkat mencoba menggunakan alamat IP yang sama, satu perangkat mungkin tidak dapat terhubung ke jaringan atau mengalami masalah komunikasi.

2.6. Analisis Protocol Jaringan ARP dan DHCP

Tabel 1. Tabel *Address Resolution Protocol*

Alamat IP	Alamat MAC	Age (menit)	Tipe
192.168.1.1	00:1A:2B:3C:4D:5E 0	0	Dinamis
192.168.1.2	00:E0:BB:B1:AA:AA	10	Statis
192.168.1.3	00:FF:CC:DD:EE:11 5	5	Dinamis

Dari Tabel 1 dapat dilihat bahwa Tabel ARP (Address Resolution Protocol) yang ditampilkan berfungsi untuk mengaitkan alamat IP dengan alamat MAC di dalam jaringan.
Alamat IP Ini adalah alamat yang digunakan untuk mengidentifikasi perangkat di jaringan. Dalam contoh ini, ada tiga alamat IP:

- 192.168.1.1
- 192.168.1.2
- 192.168.1.3

Alamat MAC terdiri dari 12 digit hexadecimal dan bersifat unik untuk setiiap perangkat.Contoh alamat MAC yang ditampilkan :

- 00:1A:2B:3C:4D:5E
- 00:E0:BB:1A:AA:AA
- 00:FF:CC:DD:EE:11

Age (menit): Kolom ini menunjukkan berapa lama (dalam menit) sejak entri alamat IP dan MAC ini ditambahkan ke tabel ARP. Nilai ini penting karena entri ARP memiliki masa berlaku tertentu; jika tidak digunakan dalam waktu tertentu, entri tersebut akan dihapus.Contoh nilai dalam tabel:

- 192.168.1.1: 0 menit
- 192.168.1.2: 10 menit
- 192.168.1.3: 5 menit

Type: Ini menunjukkan apakah entri tersebut bersifat dinamis atau statis.

- Dinamis: Entri yang dibuat secara otomatis oleh ARP ketika perangkat saling berkomunikasi. Enti

ini bisa dihapus secara otomatis setelah periode tertentu.
- Statis: Entri yang ditambahkan secara manual dan tidak akan dihapus secara otomatis. Ini berguna untuk perangkat yang selalu ada di jaringan.

Tabel 2. Tabel *Dynamic Host Configuration Protocol*

Alamat IP	Alamat MAC	Age (menit)	Tipe
192.168.1.100	00:1A:1B:3C:4D:5E	24 jam	Aktif
192.168.1.101	00:E0:BB:B1:AA:AA	12 jam	Aktif
192.168.1.102	00:FF:CC:DD:EE:11	8 jam	Pending

Dari Tabel 2 dapat dilihat bahwa Tabel DHCP berfungsi untuk menunjukkan informasi tentang perangkat yang terhubung ke jaringan dan telah mendapatkan alamat IP melalui protokol DHCP.
Alamat IP Ini adalah alamat IP yang diberikan kepada perangkat dalam jaringan. Contohnya:
- 192.168.1.100
- 192.168.1.101
- 192.168.1.102

Alamat MAC (Media Access Control) adalah alamat fisik yang unik untuk setiap perangkat jaringan. Ini digunakan untuk mengidentifikasi perangkat di jaringan lokal. Contohnya:
- 00:1A:1B:3:C4:D5
- 00:0E:BB:1B:4A:A4
- 00:FF:CC:DD:EE:11

Age (menit) Kolom ini menunjukkan berapa lama alamat IP telah diberikan kepada perangkat dalam satuan waktu (dalam menit). Ini penting untuk mengelola sewa alamat IP. Contohnya:
- 24 jam (atau 1440 menit)
- 12 jam (atau 720 menit)
- 8 jam (atau 480 menit)

Tipe Kolom ini menunjukkan status atau tipe dari alamat IP yang diberikan. Tipe dapat berupa:
- Aktif: Menunjukkan bahwa perangkat tersebut masih terhubung dan menggunakan alamat IP.
- Pending: Menunjukkan bahwa alamat IP sedang menunggu konfirmasi atau belum sepenuhnya aktif.

3. METODE PENELITIAN

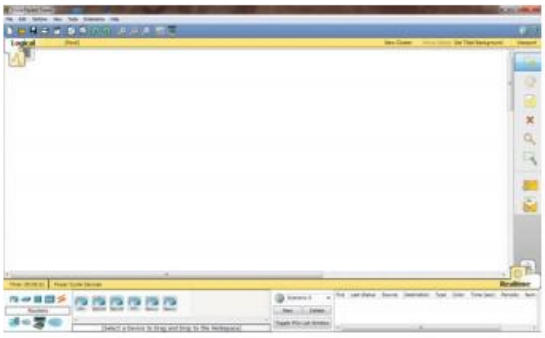
Penelitian ini menggunakan teknik tinjauan literatur sebagai pendekatan utama dalam merancang dan mengembangkan model jaringan komputer kampus menggunakan Cisco Packet Tracer. Metode penelitian kepustakaan adalah suatu teknik yang didasarkan pada pengumpulan, analisis, dan sintesis berbagai sumber informasi yang relevan guna menciptakan landasan teoritis dan praktis bagi penelitian yang akan dilakukan. Dalam konteks ini, mempelajari literatur menjadi sangat penting karena memberikan wawasan yang mendalam mengenai topik-topik yang berkaitan dengan jaringan komputer.

Langkah-Langkah Metodologi Penelitian Kepustakaan :

a. Pengumpulan Data meliputi pencarian dan pengumpulan berbagai sumber literatur seperti buku, artikel jurnal, disertasi, dan dokumen teknis yang berkaitan dengan jaringan komputer. Sumber daya ini membantu peneliti memahami konsep dasar jaringan, topologi yang digunakan, dan teknologi yang dapat diterapkan dalam jaringan kampus.
b. Menganalisis dan mengevaluasi informasi yang diperoleh. Hal ini termasuk menilai kualitas dan keandalan sumber serta relevansi informasi dengan tujuan penelitian. Peneliti juga membandingkan temuan dari pendekatan yang berbeda dan sumber yang berbeda untuk memperoleh perspektif yang lebih komprehensif.
c. Peneliti mengatur informasi yang dikumpulkan dan dianalisis ke dalam kerangka yang koheren. Proses sintesis ini penting untuk mengintegrasikan konsep dan ide yang berbeda ke dalam model yang utuh. Dalam hal ini peneliti dapat merancang model jaringan komputer kampus yang menggabungkan berbagai elemen seperti topologi jaringan, penggunaan virtual local area network (VLAN), dan penerapan routing dinamis.

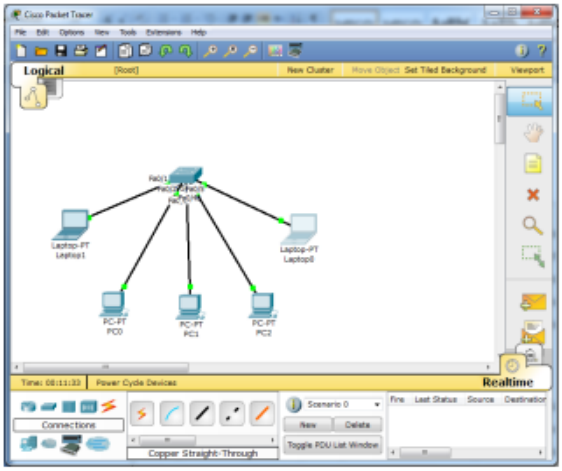
4. HASIL DAN PEMBAHASAN

4.1. Membuat Topologi Jaringan ARP dan DHCP



Gambar 8. Software Cisco Packet Tracer

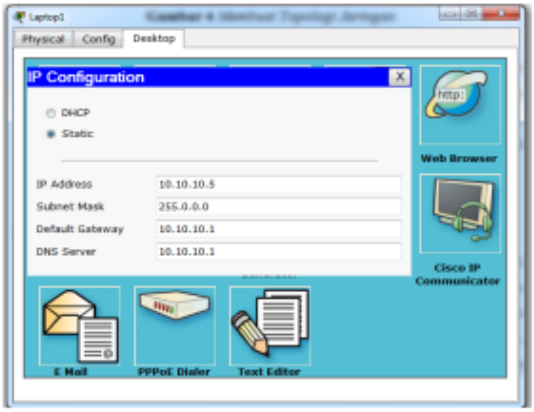
Pada gambar 8 menggambarkan tampilan dari Software Cisco Packet Tracer.



Gambar 9. Membuat Topologi Jaringan

Pada gambar 9 Area kerja dapat digunakan untuk membuat model topologi jaringan komputer yang akan digunakan. Dengan menggunakan cisco packet tracer, pilih end device dan gunakan concentrator sesuai kebutuhan. Kemudian gunakan fasilitas penghubung untuk menghubungkan setiap end device ke concentrator.

4.2. Menentukan Alamat IP Addres

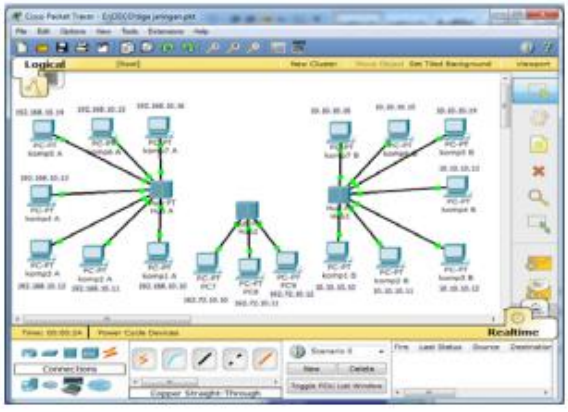


Gambar 10. Menentukan Alamat IP Address

Pada gambar 10, dijelaskan bahwa IP address adalah identitas perangkat dalam jaringan komputer. alamat IP dapat dibuat dengan mengklik dua kali pada perangkat yang diinginkan. lalu pergi ke desktop, pilih Konfigurasi IP, dan kemudian masukkan nomor IP berdasarkan kelas yang telah ditentukan..

4.3. Simulasi Jaringan Komputer ARP dan DHCP

Sebuah jaringan komputer terdiri dari sejumlah komputer yang terhubung satu sama lain, dan satu jaringan komputer akan terhubung ke jaringan komputer yang lain melalui jaringan, baik lokal maupun internasional.

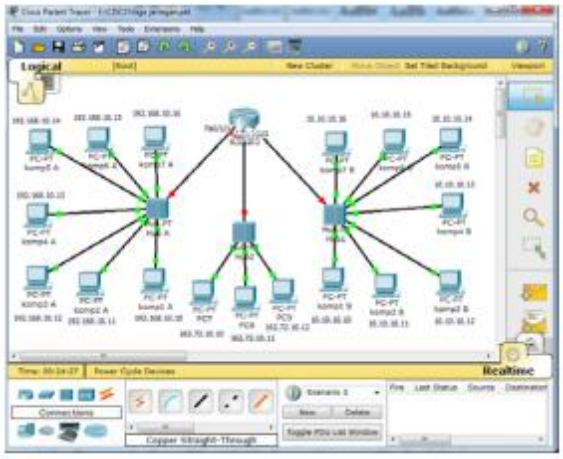


Gambar 11. Simulasi Jaringan

Gambar 11, menunjukkan bahwa router adalah alat yang diperlukan untuk mengatur sistem pertukaran data agar terjadi komunikasi data dalam jaringan Satu jaringan komputer pada kenyataannya terdiri dari sejumlah komputer yang terhubung satu sama lain, dan satu jaringan komputer akan terhubung ke jaringan komputer yang lain melalui jaringan, baik lokal maupun internasional.

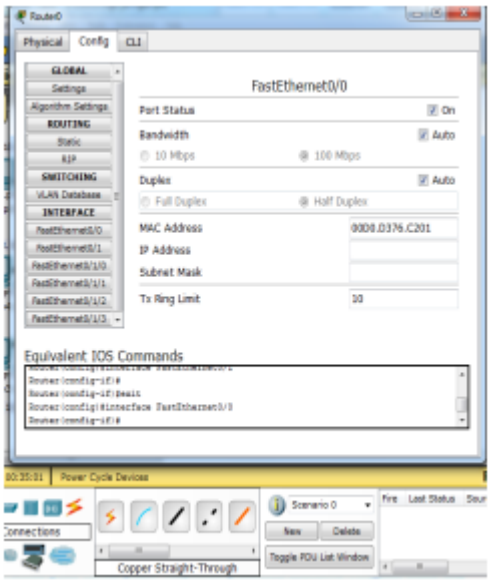
Jaringan yang terpisah, masing-masing membentuk jaringan komputer sendiri. Agar jaringan dapat saling berhubungan satu sama lain, jaringan harus dihubungkan. Ini terjadi jika masing-masing jaringan menggunakan kelas IP address yang berbeda. Namun, jika kelas IP address masing-masing jaringan berbeda, maka untuk menghubungkan jaringan ini harus menggunakan peralatan seperti switch.

4.4. Setting Router



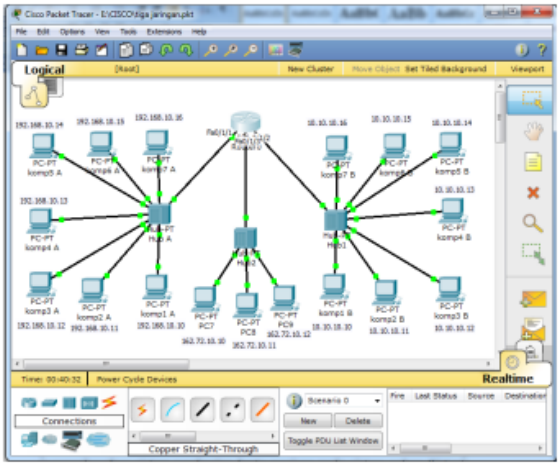
Gambar 12. Pemakaian Router

Pada gambar 12, untuk memanfaatkan router dalam suatu jaringan, router harus dikonfigurasi sehingga setiap jaringan yang terhubung padanya dan membentuk jaringan yang lebih besar dapat mencapai. Cara untuk mengkonfigurasi router adalah dengan mengklik ganda padanya. Kemudian, dalam menu setting, pilih perintah config. Tentukan posisi port yang digunakan dan centang pilihan on pada port status.



Gambar 13. Setting Router

Pada gambar 13, merupakan tahapan memasasukkan nomor IP address dan subnetmask setelah posisi alat on. Setelah tahapan konfigurasi router selesai, jaringan komputer yang terhubung dapat berkomunikasi data dengan jaringan komputer lain.



Gambar 14. Koneksi Router

Pada gambar 14, merupakan gambaran dalam simulasi, titik hijau akan menunjukkan setiap koneksi yang terhubung dan tidak ada kesalahan dalam pengaturan jaringan; titik merah akan menunjukkan komputer yang mengalami masalah.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa mengoptimalkan konektivitas jaringan kampus melalui simulasi ARP dan DHCP menggunakan Cisco Packet Tracer sangat penting untuk meningkatkan efisiensi, keandalan, dan keamanan manajemen jaringan Masu. Dalam penelitian ini, dengan menerapkan metode simulasi, kami berhasil mengidentifikasi dan menganalisis beberapa masalah umum dalam manajemen jaringan, seperti kemacetan lalu lintas dan kesulitan dalam mengelola alamat IP. Hasil simulasi menunjukkan bahwa penggunaan protokol ARP untuk resolusi alamat dan DHCP untuk pengelolaan alamat IP dapat meningkatkan kinerja jaringan kampus secara signifikan, mengurangi kemacetan, dan menyederhanakan pengelolaan jaringan besar.

Alat simulasi seperti Cisco Packet Tracer memungkinkan perancang jaringan menguji berbagai konfigurasi dan topologi tanpa risiko kehilangan yang disebabkan oleh implementasi fisik. Oleh karena itu, penelitian ini memberikan kontribusi yang signifikan terhadap perkembangan jaringan komputer di lingkungan akademik dan membuka peluang penelitian lebih lanjut di bidang pengelolaan jaringan yang efisien dan aman, untuk Saran Pengujian Berkelanjutan: Lembaga pendidikan disarankan untuk melakukan pengujian berkelanjutan pada jaringan nyata berdasarkan hasil simulasi untuk memastikan kinerja optimal dalam lingkungan kampus yang dinamis. Pendidikan dan Pelatihan: Diperlukan program pendidikan dan pelatihan bagi teknisi jaringan dan mahasiswa untuk meningkatkan pemahaman mereka tentang manajemen jaringan, termasuk penggunaan alat simulasi seperti Cisco Packet Tracer.

Penelitian Lanjutan: Penelitian lebih lanjut disarankan untuk mengeksplorasi teknologi dan metode baru dalam manajemen jaringan yang efisien dan aman, serta untuk mengadaptasi solusi yang ada dengan perkembangan teknologi terkini.Implementasi Keamanan: Penting untuk menerapkan langkah-langkah keamanan yang lebih ketat dalam jaringan kampus, termasuk penggunaan firewall dan sistem deteksi intrusi, untuk melindungi data dan infrastruktur jaringan dari ancaman yang semakin kompleks.Dengan mengikuti saran-saran ini, diharapkan jaringan kampus dapat beroperasi dengan lebih efisien dan aman, mendukung kegiatan akademis dan administratif secara lebih efektif.

DAFTAR PUSTAKA

[1] Adjei, H. A., Shunhua, M. T., Agordzo, G. K., Li, Y., Peprah, G., & Gyarteng, E. S. (2021, February). SSL stripping technique (DHCP snooping and ARP spoofing inspection). In *2021 23rd International Conference on Advanced Communication Technology (ICACT)* (pp. 187-193). IEEE.

[2] Nurfaishal, M. D., & Akbar, Y. (2024). Analisis Efektivitas Keamanan Jaringan Layer 2: Port Security, VLAN Hopping, DHCP Snooping. *Jurnal Indonesia: Manajemen Informatika dan Komunikasi*, *5*(3), 3278-3290.

[3] Dandotiya, M., Dandotiya, A. S., Dandotiya, N., & Sahu, A. (2022). A Secure Detection Framework for ARP, DHCP, and DoS Attacks on Kali Linux. *Int J Res Appl Sci Eng Technol*, *10*(7), 3044-3053.

[4] Firmansyah, F., & Pratama, Y. H. (2023). Analisis Simulasi Mitigasi Ancaman ARP Dan Round Trip Time Pada Lalu Lintas DHCP VTP. *Progresif: Jurnal Ilmiah Komputer*, *19*(1), 137-144.

[5] Rahman, Taufik, Teguh Rahmat Zaini, and

[6] Giatika Chrisnawati. "Perancangan Jaringan Virtual Local Area Network (Vlan) & Dhcp Pada Pt. Navicom Indonesia Bekasi." JIKA (Jurnal Informatika) 4.1 (2020): 36-41.

[7] Gowda, S., & Dayananda, R. B. (2023, July). Detection And Prevention of ARP Attack in Software Defined Networks. In *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.

[8] Novianto, D., Japriadi, Y. S., & Tommy, L. (2024). MITIGASI DHCP STARVATION ATTACK PADA ROUTERBOARD MIKROTIK DAN PENGARUHNYA

TERHADAP PERFORMANSI. *Jurnal Ilmiah Informatika Global*, *15*(2), 52-57.

[9] Ishtiaq, H. U., Bhutta, A. A., & Mian, A. N. (2024). DHCP DoS and starvation attacks on SDN controllers and their mitigation. *Journal of Computer Virology and Hacking Techniques*, *20*(1), 15-25.

[10] Suethanuwong, E. (2025). An Effective Prevention Approach against ARP Cache Poisoning Attacks in MikroTik-based Networks. *ECTI Transactions on Computer and Information Technology (ECTI-CIT)*, *19*(1), 1-12.

[11] Marcus, Ronald David, Hudan Eka Rosyadi, and Fandi Yulian Pamuji. "Prototype sistem administrasi dan keamanan jaringan komputer berbasis DHCP server mikrotik." Briliant: Jurnal Riset dan Konseptual 6.3 (2021): 685-695.