**Jurnal Pengembangan Rekayasa dan Teknologi**
Vol.9, No.2, November 2025, pp. 34 – 47
p-ISSN: 1410-9840 & e-ISSN: 2580-8850
https://journals.usm.ac.id/index.php/jprt
DOI : https://doi.org/10.26623/jprt.v10i1.10528



# Analisis Troubleshooting Jaringan LAN Menggunakan ICMP pada Cisco Packet Tracer

**Michael*[1], Johannes Hamonangan Siregar[2]**
Universitas Pembangunan Jaya
michael@student.upj.ac.id[1] , johanes.siregar@upj.ac.id[2]

**Informasi Artikel**

Dikirim :29-09-2025
Direview :30-10-2025
Diterbitkan :30-11-2025

**Kata Kunci**

ICMP, Cisco Packet Tracer, Troubleshooting, LAN, Traceroute

**Abstrak**

Protokol Internet Control Message Protocol (ICMP) merupakan protokol pendukung pada lapisan jaringan yang berfungsi menyediakan informasi kendali serta pelaporan kesalahan dalam proses pengiriman paket IP. Pada jaringan Local Area Network (LAN), ICMP banyak digunakan sebagai alat troubleshooting dasar untuk menguji konektivitas, mendeteksi jalur paket, dan menganalisis kegagalan komunikasi antarperangkat. Penelitian ini bertujuan untuk menganalisis efektivitas ICMP dalam menangani permasalahan konektivitas jaringan melalui simulasi LAN menggunakan Cisco Packet Tracer. Metode penelitian dilakukan dengan merancang topologi jaringan sederhana, melakukan konfigurasi IP dan routing, serta mensimulasikan berbagai skenario gangguan seperti kesalahan konfigurasi IP, gateway tidak tersedia, dan pemutusan link jaringan. Pengujian dilakukan menggunakan perintah ping dan traceroute untuk mengamati respon pesan ICMP. Hasil penelitian menunjukkan bahwa ICMP mampu memberikan informasi diagnostik yang jelas melalui pesan echo reply, destination unreachable, dan request timed out, sehingga memudahkan identifikasi sumber permasalahan jaringan. Penelitian ini menegaskan bahwa ICMP merupakan alat fundamental dalam troubleshooting jaringan berbasis TCP/IP, khususnya untuk pembelajaran dan simulasi jaringan.

## 1. PENDAHULUAN

Konektivitas jaringan merupakan komponen fundamental dalam keberlangsungan sistem komunikasi digital modern. Pada jaringan berbasis TCP/IP, proses pengiriman data bersifat connectionless, sehingga tidak terdapat mekanisme bawaan untuk memastikan apakah suatu paket berhasil mencapai tujuan. Oleh karena itu, diperlukan protokol pendukung yang mampu memberikan informasi diagnostik ketika terjadi gangguan dalam proses komunikasi data. Salah satu protokol yang memegang peranan penting dalam hal tersebut adalah Internet Control Message Protocol (ICMP).

Menurut penelitian yang dilakukan oleh (Kumar, Appathurai, & Nagarajan, 2020),ICMP berfungsi sebagai mekanisme pelaporan kesalahan yang bekerja bersama protokol IP untuk menyediakan informasi ketika pengiriman paket tidak berhasil atau ketika suatu host tidak merespons. Mereka menjelaskan bahwa ICMP dapat melaporkan kondisi seperti destination unreachable, time exceeded, hingga error pada header paket IP. Selain itu, ICMP juga menyediakan pesan echo request dan echo reply yang menjadi dasar

dari perintah ping, salah satu alat diagnostik paling umum yang digunakan untuk mengevaluasi apakah sebuah perangkat tujuan dapat dijangkau.

Manajemen distribusi paket data dan metode routing berpengaruh signifikan terhadap efisiensi jaringan, termasuk dalam konteks identifikasi masalah konektivitas ketika konfigurasi tidak sesuai. Analisis performa jaringan seperti itu merupakan landasan penting bagi teknik troubleshooting menggunakan protokol diagnostik seperti ICMP (Surono, Christanto, & Maulana, 2020).

Selanjutnya, penggunaan perintah ping dan traceroute tidak hanya dimanfaatkan sebagai teknik praktis dalam pemeriksaan konektivitas jaringan, tetapi juga telah menjadi objek kajian dalam penelitian jaringan komputer di Indonesia. Dalam penelitian Analisis Traffic pada Jaringan LAN, dijelaskan bahwa perintah ping digunakan untuk mengirimkan ICMP Echo Request guna mengukur waktu respons (delay) dan kehilangan paket, sedangkan traceroute berfungsi untuk menelusuri jalur paket dari sumber ke tujuan dengan mengidentifikasi setiap hop yang dilewati (Sandova & Prihantoro, 2021). Melalui analisis jalur hop tersebut, administrator jaringan dapat menentukan titik kegagalan komunikasi secara lebih sistematis, khususnya ketika paket berhenti atau mengalami keterlambatan pada perangkat tertentu. Temuan ini menunjukkan bahwa kombinasi penggunaan ping dan traceroute memberikan informasi diagnostik yang jelas dan terstruktur, sehingga sangat mendukung proses troubleshooting jaringan berbasis TCP/IP.

Dalam konteks pembelajaran dan simulasi jaringan, Cisco Packet Tracer digunakan sebagai media yang efektif untuk memahami mekanisme kerja ICMP secara aman dan terkontrol. Melalui simulasi ini, berbagai skenario gangguan jaringan seperti kesalahan konfigurasi IP, gateway tidak tersedia, hingga pemutusan link dapat direkayasa untuk mengamati respon ICMP secara langsung (Assyifaurrohmah, Mubin, & Tabrani, 2025)

Berdasarkan pemaparan tersebut, penelitian ini bertujuan untuk menganalisis peran ICMP dalam proses troubleshooting konektivitas jaringan melalui simulasi LAN berbasis Cisco Packet Tracer. Penelitian ini mengacu pada kajian ICMP sebagai protokol diagnostik (Kumar et al., 2020), dukungan analisis rekayasa jaringan dalam identifikasi masalah konektivitas (Surono et al., 2020), serta pendekatan simulasi jaringan untuk pengujian error komunikasi (Assyifaurrohmah et al., 2025).

Kontribusi utama penelitian ini adalah f(1) mengklasifikasikan respon ICMP berdasarkan jenis gangguan jaringan yang terjadi, seperti kesalahan konfigurasi IP, gateway tidak tersedia, serta pemutusan link antar-perangkat jaringan,(2) menganalisis keterkaitan antara pesan ICMP yang dihasilkan dengan lapisan jaringan (Layer 3) pada model OSI, khususnya dalam konteks proses pengalamatan, routing, dan pengendalian kesalahan; serta,(3) menunjukkan efektivitas ICMP sebagai alat diagnosis awal dalam troubleshooting konektivitas jaringan LAN berbasis TCP/IP melalui simulasi menggunakan Cisco Packet Tracer.

## TINJAUAN PUSTAKA

### 1.Protokol ICMP

ICMP adalah protokol pada lapisan Network (Layer 3) yang digunakan untuk memberikan informasi kendali (control messages) seperti error, unreachable, time exceeded, dan status konektivitas antar host. ICMP tidak membawa data aplikasi, melainkan menyediakan mekanisme diagnostik untuk mengetahui kondisi jaringan.

Dalam literatur ilmiah, Internet Control Message Protocol (ICMP) dijelaskan sebagai ICMP merupakan protokol pada lapisan jaringan (Layer 3) yang berfungsi untuk menyediakan informasi kendali dan pelaporan kesalahan ketika terjadi gangguan dalam

proses pengiriman paket IP. Protokokol ini mampu mengirimkan pesan diagnostik seperti destination unreachable ketika rute tidak tersedia dan time exceeded ketika nilai Time-to-Live (TTL) paket telah habis sebelum mencapai tujuan (Gezer, Warner, Technology, & Science, 2019)

Penelitian oleh (Finata & Nasution, 2024) juga menegaskan bahwa ICMP merupakan protokol yang paling umum digunakan dalam pemeriksaan konektivitas jaringan karena menyediakan respon langsung terhadap keberhasilan maupun kegagalan pengiriman paket dalam percobaan ping maupun traceroute.

2.Local Area Network (LAN) dan Topologi Hybrid

Local Area Network (LAN) merupakan jaringan komputer yang mencakup area terbatas seperti rumah, kantor, atau laboratorium. Dalam implementasi LAN, topologi yang paling umum digunakan adalah topologi star karena mudah dikelola dan isolasi masalah dapat dilakukan dengan cepat.

Dalam penelitian (Finata & Nasution, 2024), topologi star digunakan sebagai dasar penghubung perangkat melalui switch karena memberikan struktur jaringan yang rapi serta stabil. Ketika beberapa star network dihubungkan melalui router, terbentuklah topologi hybrid, yang merupakan kombinasi struktur star pada LAN dengan koneksi point-to-point antar router.

Hybrid topology ini sangat sesuai untuk eksperimen ICMP karena menyediakan jalur multipath yang memudahkan pengamatan perilaku paket ICMP ketika melewati beberapa router (Finata & Nasution, 2024).

3.Routing Statis dalam Analisis Konektivitas

Routing statis adalah metode routing yang dikonfigurasi secara manual oleh administrator. Dalam penelitian universitas Hasanuddin (2024), routing statis dijelaskan sebagai metode yang memberikan kontrol penuh terhadap jalur yang digunakan paket, sehingga memudahkan troubleshooting karena setiap rute telah ditentukan secara eksplisit.

Ketika rute tidak tersedia atau salah dikonfigurasi, ICMP akan menghasilkan pesan seperti destination unreachable, yang sangat membantu dalam proses analisis masalah konektivitas. Penelitian ini juga menekankan bahwa routing statis sangat cocok digunakan pada skenario pembelajaran dan simulasi seperti Packet Tracer, karena memberikan gambaran jelas tentang bagaimana paket melintasi jaringan (FALIQ, 2024).

4.Simulasi Jaringan Menggunakan Cisco Packet Tracer

Cisco Packet Tracer adalah simulator jaringan yang digunakan secara luas dalam pendidikan jaringan komputer. Simulator ini menyediakan Simulation Mode, yang memungkinkan pengguna melihat paket ICMP secara visual, termasuk identifikasi pesan echo, unreachable, dan TTL exceeded.

Dalam penelitian (Finata & Nasution, 2024),Packet Tracer terbukti efektif dalam memodelkan topologi star dan hybrid serta menjalankan perintah ping dan traceroute berbasis ICMP. Penelitian tersebut menunjukkan bahwa Packet Tracer mampu memperlihatkan detail struktur paket dan jalur yang dilalui oleh paket ICMP, sehingga sangat mendukung proses troubleshooting.

## 2. METODOLOGI

Metode penelitian ini menggunakan pendekatan eksperimen simulatif pada Cisco Packet Tracer untuk menganalisis perilaku ICMP dalam troubleshooting konektivitas jaringan. Pendekatan ini mengikuti praktik penelitian rekayasa jaringan modern yang menekankan simulasi terkontrol dan analisis paket (Qomarudin, Amrullah, Yogyakarta, & Yogyakarta, 2022) .

2.1.Pendekatan Penelitian

Penelitian menggunakan metode eksperimen simulatif, yaitu membangun jaringan virtual, menyusun konfigurasi, merekayasa gangguan, dan mengamati respon ICMP secara langsung. Pendekatan eksperimen ini terbukti efektif dalam menganalisis pola error ICMP seperti destination unreachable atau request timeout, sebagaimana ditunjukkan oleh studi monitoring ICMP pada jaringan server(Qomarudin et al., 2022).

2.2.Alat dan Bahan

Alat dan bahan pada penelitian ini disesuaikan secara spesifik dengan topologi simulasi yang digunakan dalam Cisco Packet Tracer. Seluruh perangkat dan koneksi dalam bagian ini berasal dari desain jaringan dua LAN yang saling terhubung melalui dua router, sebagaimana tampak pada topologi penelitian. Pendekatan berbasis simulasi seperti ini juga digunakan oleh (Ariyadi, 2023) untuk menganalisis perilaku ICMP dalam jaringan multihop.

Perangkat dan Kebutuhan yang Digunakan:

1.Perangkat Lunak

Cisco Packet Tracer versi 8.x Digunakan sebagai simulator utama untuk membangun topologi, melakukan konfigurasi jaringan, memvisualisasikan paket ICMP, dan menyusun skenario gangguan.

Ariyadi et al. (2023) menegaskan bahwa simulasi berbasis Packet Tracer atau Wireshark mampu menampilkan struktur paket ICMP secara akurat untuk keperluan troubleshooting.

2.Perangkat Jaringan

•2 Router-PT (Router 1 dan Router 2)

Router 1 ↔ Router 2 menggunakan Serial Se2/0

Router ke switch menggunakan interface Fa0/0 atau Fa0/1

•2 Switch (2960-24TT)

Switch1 untuk LAN 1

Switch0 untuk LAN 2

•4 PC-PT

PC1 dan PC2 pada LAN 1

PC3 dan PC4 pada LAN 2

Digunakan untuk pengujian ping dan traceroute.

3.Media Koneksi

•Copper Straight-Through

Dipakai untuk koneksi dari PC → Switch dan Switch → Router (fa interface).

•Copper Cross-Over (Opsional)

Digunakan hanya jika menghubungkan perangkat sejenis.

•Serial DCE/DTE Cable

Digunakan untuk menghubungkan Router 1 ↔ Router 2 via interface Se2/0, sesuai screenshot topologi yang kamu gunakan.

4.Parameter Konfigurasi

•Alamat IP statis untuk semua PC

LAN 1: 192.168.10.0/24

LAN 2: 192.168.20.0/24

•Alamat IP Serial Link antarrouter

10.10.10.0/30

•Static routing pada kedua router untuk menghubungkan kedua LAN.

•Simulation Mode sebagai alat analisis visual ICMP.

Metode observasi paket ini direkomendasikan dalam Wireshark ICMP Lab (2020).

Bagian ini sekaligus menyesuaikan struktur nyata perangkat dan koneksi dalam simulasi kamu, sehingga seluruh proses pengujian ICMP dilakukan dengan kondisi jaringan yang benar-benar identik.

2.3.Perancangan Topologi Jaringan

Topologi jaringan dirancang berdasarkan model dua LAN yang dihubungkan oleh dua router dengan koneksi serial. Struktur multihop seperti ini direkomendasikan dalam penelitian simulasi ICMP karena memungkinkan peneliti mengamati jalur routing dan perubahan respon ICMP akibat gangguan.

Topologi terdiri dari:

- LAN 1: PC1 dan PC2 → Switch1 → Router 1
- LAN 2: PC3 dan PC4 → Switch0 → Router 2
- Router 1 ↔ Router 2 via serial Se2/0

Pendekatan desain ini mendukung analisis lintas-subnet yang diperlukan dalam studi troubleshooting berbasis ICMP(Finata & Nasution, 2024).

2.4.Langkah-Langkah Penelitian

a. Konfigurasi IP Address

Proses konfigurasi dilakukan dengan menetapkan IP statis pada setiap PC dan router. Teknik IP statis dipilih karena memberikan alur yang deterministik ketika menganalisis kesalahan konfigurasi dan respon ICMP. Pendekatan konfigurasi seperti ini juga digunakan (FALIQ, 2024) dalam analisis routing dan ICMP pada topologi yang serupa.

Contoh konfigurasi:

- PC LAN 1: 192.168.10.x/24
- PC LAN 2: 192.168.20.x/24
- Router Serial Link: 10.10.10.0/30

(FALIQ, 2024) menegaskan bahwa konfigurasi IP manual menjadi dasar penting untuk menguji error-respons ICMP secara presisi.

b. Konfigurasi Static Routing

Routing statis ditambahkan untuk menghubungkan kedua subnet:

•Router 1 →

ip route 192.168.20.0 255.255.255.0 10.10.10.2

•Router 2 →

ip route 192.168.10.0 255.255.255.0 10.10.10.1

Teknik routing statis ini sejalan dengan praktik troubleshooting ICMP dalam analisis jaringan yang dilakukan oleh Ariyadi et al. (2023), yang menunjukkan bahwa static route memudahkan identifikasi sumber kegagalan jalur paket.

c. Baseline Test (Pengujian Awal)

Pengujian awal dilakukan sebelum gangguan direkayasa. Ping antar subnet harus menghasilkan echo reply. Jika tidak, konfigurasi dasar diperbaiki terlebih dahulu. Konsep baseline ini juga diterapkan dalam penelitian monitoring jaringan berbasis ICMP oleh (Qomarudin et al., 2022), di mana respons normal dicatat sebagai pembanding hasil gangguan.

2.5. Skenario Pengujian Troubleshooting

Pengujian troubleshooting dilakukan untuk mengamati bagaimana ICMP memberikan pesan diagnostik pada berbagai kondisi gangguan jaringan. Setiap skenario dirancang untuk memicu jenis pesan ICMP tertentu sehingga proses analisis kesalahan dapat diamati secara jelas. Pendekatan pengujian seperti ini banyak digunakan dalam penelitian simulasi jaringan berbasis ICMP (Ariyadi, 2023).

Skenario 1 — Kesalahan Konfigurasi IP dan Gateway

Pada skenario ini, dilakukan kesalahan konfigurasi jaringan pada sisi host, meliputi subnet mask yang tidak sesuai dan default gateway yang salah atau tidak dikonfigurasi. Kondisi ini menyebabkan host tidak memiliki jalur yang valid untuk mencapai jaringan tujuan sehingga paket ICMP tidak dapat diteruskan dengan benar.

Akibat kesalahan tersebut, router mengembalikan pesan ICMP Type 3 – Destination Host Unreachable, yang menandakan bahwa tujuan tidak dapat dijangkau melalui rute yang tersedia. Mekanisme ini sesuai dengan temuan (Ariyadi, 2023) yang menyatakan bahwa kesalahan konfigurasi IP dan gateway merupakan penyebab utama kegagalan konektivitas pada jaringan multihop, serta penelitian (Qomarudin et al., 2022) yang menjelaskan bahwa pesan destination unreachable muncul ketika jalur routing tidak ditemukan.

Skenario 2 — Link antarrouter & link antar switch-router diputus

Pada skenario ini dilakukan dua jenis pemutusan koneksi untuk mengamati perbedaan respon ICMP berdasarkan lokasi gangguan jaringan.

Pemutusan pertama dilakukan pada koneksi antar-router dengan menonaktifkan interface serial Se2/0 pada Router 1 menggunakan perintah shutdown. Kondisi ini menyebabkan Router 1 tidak lagi memiliki jalur aktif menuju Router 2 dan jaringan LAN 2. Pengujian menggunakan perintah ping dari PC1 ke PC4 menghasilkan pesan Destination Host Unreachable, yang dikirim oleh Router 1 sebagai indikasi tidak tersedianya rute ke host tujuan.

Pemutusan kedua dilakukan pada koneksi antara switch dan router (gateway). Pada kondisi ini, host tidak dapat menjangkau gateway sehingga proses ARP gagal dan paket ICMP tidak pernah mencapai router. Akibatnya, pengujian ping menghasilkan pesan Request Timed Out, karena tidak terdapat perangkat jaringan yang mengirimkan pesan kesalahan ICMP kembali ke pengirim.

Perbedaan respon ICMP ini menunjukkan bahwa jenis pesan yang dihasilkan bergantung pada titik kegagalan jaringan. Temuan ini memperkuat peran ICMP sebagai alat diagnostik untuk mengidentifikasi lokasi gangguan konektivitas, baik pada level gateway maupun jalur routing antar-perangkat jaringan. Hasil ini sejalan dengan penelitian (Razzanda & Koprawi, 2024) yang menyatakan bahwa ICMP mampu menunjukkan titik kegagalan komunikasi berdasarkan respon error yang dihasilkan.

### 2.6. Metode Analisis Data

Analisis data pada penelitian ini dilakukan dengan pendekatan deskriptif-komparatif, yaitu membandingkan hasil pengujian ICMP pada kondisi jaringan normal dan kondisi gangguan. Setiap skenario dianalisis berdasarkan jenis pesan ICMP, jalur paket, dan keberhasilan ping.

1. Identifikasi jenis pesan ICMP

Menentukan apakah pesan yang muncul berupa echo reply, request timed out, destination unreachable, atau time exceeded. Teknik identifikasi seperti ini digunakan juga dalam penelitian ICMP oleh (Ariyadi, 2023).

2. Menganalisis jalur paket (hop-by-hop)

Hasil traceroute dibandingkan antara kondisi normal dan kondisi gangguan untuk melihat perubahan jalur atau titik kegagalan. Pendekatan analisis hop digunakan dalam monitoring ICMP oleh (Qomarudin et al., 2022).

3. Mencocokkan hasil dengan penyebab gangguan

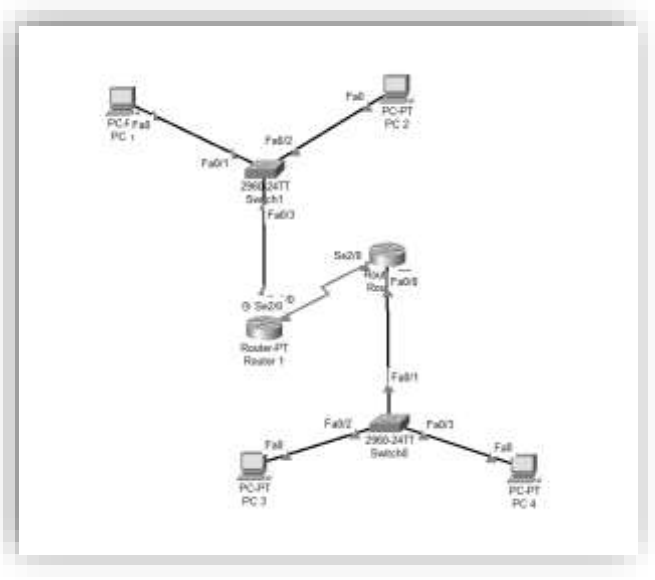
Pesan ICMP dikaitkan dengan konfigurasi yang sengaja diubah (misconfig IP, gateway salah, interface down). Pola hubungan error–penyebab ini selaras dengan pemetaan ICMP pada studi jaringan oleh (Razzanda & Koprawi, 2024).

Hasil dari ketiga langkah ini menjadi dasar penarikan kesimpulan mengenai efektivitas ICMP sebagai alat troubleshooting konektivitas jaringan pada topologi LAN multihop yang dibangun di Cisco Packet Tracer.

## 3. HASIL DAN PEMBAHASAN

Hasil penelitian disajikan berdasarkan tiga skenario troubleshooting yang telah dirancang, yaitu kesalahan konfigurasi IP, gateway tidak tersedia, dan pemutusan link antar-router. Setiap hasil pengujian dibandingkan dengan kondisi baseline, kemudian dianalisis menggunakan pesan ICMP yang muncul pada Packet Tracer Simulation Mode.

Gambar 1 menampilkan topologi jaringan simulasi LAN pada Cisco Packet Tracer yang digunakan sebagai skenario pengujian ICMP.




Gambar 1. Perancangan Topologi Jaringan

3.1 Hasil Baseline (Kondisi Normal)

Pada kondisi awal, seluruh perangkat telah dikonfigurasi menggunakan IP statis dan routing statis di kedua router. Uji ping antar-host (PC1 → PC4) menunjukkan echo reply tanpa kehilangan paket. Jalur traceroute juga menunjukkan paket melewati Router 1 → Router 2 sesuai desain.

Interpretasi:

Kondisi baseline yang berhasil menunjukkan bahwa konfigurasi dasar sudah benar, sehingga pesan ICMP pada skenario gangguan nantinya dapat dianalisis secara akurat. Hasil ini sejalan dengan metode baseline pada Qomarudin et al. (2022) yang menekankan pentingnya kondisi awal sebagai pembanding.

Gambar 2 menampilkan hasil pengujian konektivitas jaringan dalam kondisi normal, di mana perintah ping berhasil mendapatkan echo reply dari host tujuan.

Gambar 3 menampilkan hasil pengujian konektivitas jaringan dalam kondisi normal, di mana perintah tracert berhasil mendapatkan echo reply dari host tujuan.

Gambar 2. Hasil Ping Kondisi Normal (Baseline)

Gambar 3. Hasil Traceroute Kondisi Normal

3.2. Hasil Skenario 1 – Kesalahan Konfigurasi IP dan Gateway

Pada skenario ini, dilakukan perubahan konfigurasi jaringan berupa pengaturan subnet mask dan default gateway yang tidak sesuai pada salah satu PC. Kondisi tersebut menyebabkan host tidak dapat menentukan jalur komunikasi yang benar menuju jaringan tujuan.

Hasil Pengujian:

•Ping dari PC ke jaringan lain menghasilkan pesan Destination host unreachable

•Pesan ICMP dikirim oleh router gateway

•Tidak ditemukan echo reply dari host tujuan

Pembahasan:

Pesan destination host unreachable menunjukkan bahwa router tidak memiliki rute yang valid untuk meneruskan paket ke tujuan. Hal ini mengindikasikan bahwa kesalahan konfigurasi IP dan gateway pada host menyebabkan paket tidak dapat keluar dari subnet asal. Temuan ini mendukung hasil penelitian (Ariyadi, 2023) dan (Qomarudin et al., 2022) yang menyatakan bahwa ICMP Type 3 merupakan indikator utama kegagalan jalur komunikasi akibat kesalahan konfigurasi jaringan.

Gambar 4 menampilkan hasil pengujian ping IP tidak sesuai yang menghasilkan pesan destination host unreachable.

Gambar 4. Hasil Ping PC2 ke PC3 dengan Pesan Destination Host Unreachable

3.3. Hasil Skenario 2 – Link Antarrouter Diputus

Hasil Pengujian

Pada skenario ini dilakukan dua jenis pemutusan koneksi untuk mengamati perbedaan respon ICMP:

1.Pemutusan link antar-router Interface serial Se2/0 pada Router 1 dinonaktifkan menggunakan perintah:

2.interface se2/0

3.shutdown

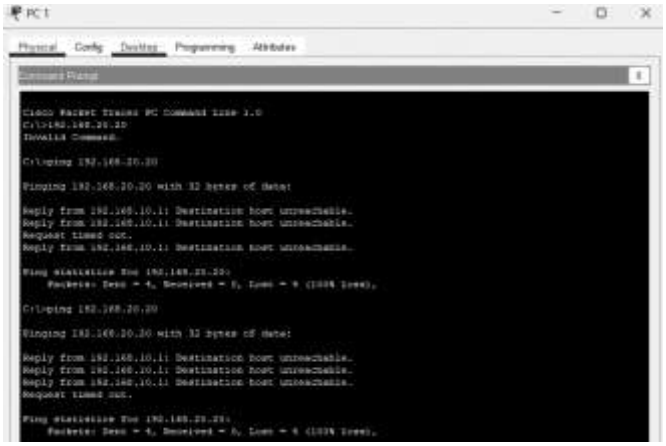
Pengujian dilakukan dengan mengirim perintah ping dari PC1 ke PC4.

Hasil pengujian menunjukkan bahwa pesan ICMP yang muncul adalah:

“Destination host unreachable”

Gambar 5 & 6 menampilkan hasil pengujian ping ketika koneksi antar-router diputus, yang menghasilkan pesan destination host unreachable.

Gambar 5. Interface Serial Router 1 dalam Keadaan Down



Gambar 6. Hasil Ping Destination Host Unreachable akibat Link Antarrouter Terputus

Pesan ini dikirim oleh Router 1 sebagai gateway karena router tidak lagi memiliki rute aktif menuju jaringan tujuan (LAN 2).

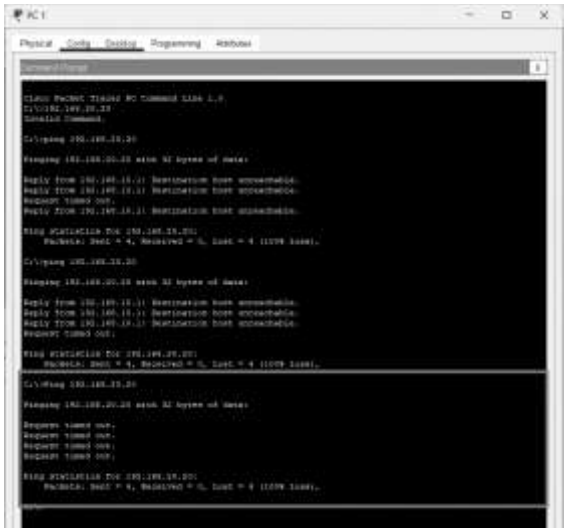
4.Pemutusan link antara switch dan router

Pada pengujian lanjutan, koneksi antara switch dan router pada sisi LAN diputus. Dalam kondisi ini, perintah ping dari PC menuju jaringan tujuan menghasilkan pesan:

“Request timed out”

Gambar 7 & 8 menampilkan hasil pengujian ping saat koneksi antara switch dan router dinonaktifkan, sehingga paket ICMP tidak menerima balasan dan menghasilkan pesan request timed out.

Gambar 7. Shutdown Interface Switch ke Router



Gambar 8.Hasil Ping Request Timed Out akibat Putusnya Koneksi Switch–Router

Tidak adanya respon ini menunjukkan bahwa paket ICMP tidak mendapatkan balasan apa pun karena host pengirim kehilangan akses ke gateway dan tidak menerima pesan error eksplisit dari router.

Pembahasan

Perbedaan hasil pengujian pada kedua kondisi tersebut menunjukkan bahwa jenis gangguan jaringan sangat memengaruhi jenis pesan ICMP yang dihasilkan.

Pada pemutusan link antar-router, Router 1 masih berfungsi sebagai gateway aktif bagi LAN 1. Namun, karena jalur menuju Router 2 terputus, router tidak dapat meneruskan paket ke jaringan tujuan. Dalam kondisi ini, router secara aktif mengirimkan pesan ICMP Type 3 – Destination Host Unreachable kepada host pengirim. Hal ini menunjukkan bahwa router mampu mendeteksi kegagalan jalur dan melaporkannya secara eksplisit melalui ICMP.

Sebaliknya, pada pemutusan link antara switch dan router, host pengirim kehilangan akses langsung ke gateway. Paket ICMP tidak pernah mencapai router, sehingga tidak ada perangkat jaringan yang mengirimkan pesan kesalahan kembali ke host. Akibatnya, pengirim hanya menunggu balasan hingga waktu habis dan menghasilkan pesan request timed out. Kondisi ini mencerminkan kegagalan komunikasi tanpa notifikasi error eksplisit dari jaringan.

Temuan ini memperlihatkan bahwa ICMP tidak hanya berfungsi sebagai alat uji konektivitas, tetapi juga mampu menunjukkan lokasi dan jenis gangguan jaringan berdasarkan pesan yang dihasilkan. Hasil pengujian ini sejalan dengan penelitian (Razzanda & Koprawi, 2024) yang menyatakan bahwa ICMP efektif dalam mengidentifikasi kegagalan jalur komunikasi dan membantu menentukan titik gangguan pada jaringan multihop.

Pembahasan Umum :

Tabel 1 menyajikan ringkasan respons ICMP pada berbagai skenario gangguan jaringan berdasarkan hasil pengujian ping.

Table 1. Ringkasan Respon ICMP terhadap Berbagai Skenario Gangguan Jaringan

| No | Skenario Pengujian | Kondisi Gangguan | Respon ICMP | Interpretasi |
|---|---|---|---|---|
| 1 | *Baseline* (Normal) | Tidak ada gangguan | *Echo Reply* | Konektivitas jaringan berjalan normal |
| 2 | Kesalahan IP / *Gateway* | *Gateway* salah / tidak tersedia | *Destination Host Unreachable* | Router tidak menemukan jalur ke jaringan tujuan |
| 3 | Link Switch–Router Putus | Host tidak mencapai router | *Request Timed Out* | Paket ICMP tidak mendapat balasan |
| 4 | Link Antarrouter Diputus | Jalur utama LAN 1–LAN 2 terputus | *Request Timed Out / Time Exceeded* | Paket berhenti di router terakhir yang aktif |

Berdasarkan seluruh skenario pengujian yang telah dilakukan, dapat diketahui bahwa protokol ICMP memberikan informasi diagnostik yang jelas dan konsisten terhadap berbagai jenis gangguan konektivitas jaringan LAN. Setiap jenis kesalahan konfigurasi maupun kegagalan jalur menghasilkan respon ICMP yang berbeda, sehingga administrator jaringan dapat mengidentifikasi sumber permasalahan secara sistematis.

Pada kondisi jaringan normal (baseline), pengujian menggunakan perintah ping dan traceroute menunjukkan keberhasilan komunikasi antar host lintas subnet dengan ditandai oleh munculnya echo reply. Hal ini menandakan bahwa konfigurasi IP, gateway, dan routing telah berjalan dengan benar. Kondisi baseline ini digunakan sebagai pembanding utama

dalam menganalisis hasil pada skenario gangguan, sebagaimana direkomendasikan oleh (Qomarudin et al., 2022) dalam studi monitoring jaringan berbasis ICMP.

Pada skenario kesalahan konfigurasi IP address dan gateway, respon ICMP yang muncul berupa Destination Host Unreachable atau Request Timed Out, tergantung pada lokasi gangguan. Ketika gateway salah atau tidak tersedia, router secara aktif mengembalikan pesan ICMP Type 3 (Destination unreachable), sedangkan ketika jalur komunikasi terputus sebelum mencapai router (misalnya pada link switch–router), paket ICMP tidak memperoleh balasan sehingga menghasilkan request timed out. Pola ini sejalan dengan temuan Ariyadi (2023) yang menyatakan bahwa perbedaan lokasi gangguan sangat mempengaruhi jenis pesan ICMP yang diterima oleh host pengirim.

Pada skenario pemutusan link antarrouter, ICMP menunjukkan kemampuannya dalam mengidentifikasi kegagalan jalur utama pada jaringan multihop. Hasil pengujian menunjukkan bahwa paket ICMP berhenti pada router terakhir yang masih aktif, dan pesan yang muncul dapat berupa request timed out, time exceeded (ICMP Type 11), atau network unreachable (ICMP Type 3), tergantung pada arah lalu lintas dan kondisi routing table. Temuan ini konsisten dengan penelitian Razzanda & Koprawi (2024) yang menegaskan bahwa ICMP efektif digunakan untuk mendeteksi gangguan konektivitas akibat kegagalan link antar-perangkat jaringan.

Secara keseluruhan, hasil pengujian membuktikan bahwa ICMP tidak hanya berfungsi sebagai alat uji konektivitas, tetapi juga sebagai mekanisme troubleshooting yang mampu menunjukkan lokasi dan jenis gangguan jaringan. Dengan memanfaatkan pesan ICMP yang dihasilkan dari perintah ping dan traceroute, administrator jaringan dapat melakukan analisis kesalahan secara lebih cepat dan terarah pada jaringan LAN berbasis TCP/IP.

Penelitian ini memiliki beberapa keterbatasan, antara lain simulasi jaringan dilakukan pada skala kecil menggunakan Cisco Packet Tracer sehingga belum sepenuhnya merepresentasikan kondisi jaringan nyata dengan trafik tinggi dan kompleksitas yang lebih beragam. Selain itu, penelitian ini hanya memanfaatkan protokol ICMP sebagai alat diagnosis dasar dalam proses troubleshooting, tanpa mengombinasikannya dengan protokol atau metode analisis jaringan lainnya seperti SNMP, NetFlow, atau analisis paket mendalam.

## 4. KESIMPULAN

Berdasarkan hasil penelitian dan simulasi yang telah dilakukan, dapat disimpulkan bahwa Internet Control Message Protocol (ICMP) terbukti efektif sebagai alat troubleshooting konektivitas jaringan LAN pada simulasi berbasis Cisco Packet Tracer. Melalui pengujian berbagai skenario gangguan jaringan, ICMP mampu memberikan informasi diagnostik yang jelas dan spesifik sesuai dengan jenis permasalahan yang terjadi.

Pada skenario kesalahan konfigurasi alamat IP dan gateway, ICMP menghasilkan pesan destination host unreachable atau request timed out, yang menunjukkan bahwa host tidak memiliki jalur yang valid untuk mencapai jaringan tujuan. Hal ini membuktikan bahwa ICMP dapat digunakan untuk mengidentifikasi kesalahan pada lapisan jaringan (Layer 3), khususnya terkait pengalamatan dan penentuan gateway.

Selanjutnya, pada skenario pemutusan link antarrouter, hasil pengujian menunjukkan bahwa paket ICMP berhenti pada hop terakhir yang masih aktif, dengan keluaran berupa request timed out, time exceeded, atau network unreachable, tergantung pada lokasi pemutusan link. Temuan ini menegaskan bahwa ICMP mampu membantu administrator jaringan menentukan titik gangguan secara cepat pada jaringan multihop.

Perbedaan hasil antara pemutusan link antarrouter dan pemutusan link antara switch dan router juga menunjukkan bahwa jenis gangguan jaringan sangat memengaruhi respon ICMP. Dengan demikian, interpretasi pesan ICMP menjadi kunci penting dalam proses troubleshooting, bukan hanya sekadar melihat apakah ping berhasil atau gagal.

Secara keseluruhan, penelitian ini membuktikan bahwa ICMP merupakan protokol fundamental dan relevan dalam analisis troubleshooting konektivitas jaringan LAN, baik dalam konteks pembelajaran maupun praktik administrasi jaringan. Simulasi menggunakan Cisco Packet Tracer juga terbukti efektif sebagai media eksperimen untuk memahami perilaku ICMP secara visual dan sistematis.

## DAFTAR PUSTAKA

Ariyadi. (2023). ANALISIS PAKET ICMP WEBSITE UNIVERSITAS BINADARMA, 2(2), 55–60.

Assyifaurrohmah, F., Mubin, A. F., & Tabrani, A. (2025). SKEMA JARINGAN TROUBLESHOOT MENGGUNAKAN, 19(1), 48–56.

FALIQ, M. N. (2024). Analisis Kinerja Protokol Routing OSPF Menggunakan Controller RYU Dan OPENDAYLIGHT Pada Jaringan Software Defined Network (SDN) Disusun.

Finata, K., & Nasution, K. (2024). Analisis Kinerja Protokol Routing Open Shortest Path First ( OSPF ) pada Jaringan Universitas Islam Sumatera Utara.

Gezer, A., Warner, G., Technology, T., & Science, C. (2019). Exploitation of ICMP Time Exceeded Packets for A Large-Scale Router Delay Analysis, 16(6), 1090–1097.

Kumar, M. A., Appathurai, K., & Nagarajan, P. (2020). Troubleshooting Networks Using Internet Control Message Protocol.

Qomarudin, M. F., Amrullah, A., Yogyakarta, U. A., & Yogyakarta, U. A. (2022). SISTEM MONITORING JARINGAN REALTIME BERBASIS INTERNET CONTROL MESSAGE PROTOCOL, 3(2), 67–80.

Razzanda, & Koprawi. (2024). Implementasi IDS dan IPS terhadap Serangan TCP Port Scanning dan ICMP Flooding Iqbal, 13(4), 6549–6562.

Sandova, D., & Prihantoro, C. (2021). ANALISIS TRAFFIC PADA JARINGAN LAN, 4(3), 329–337.

Surono, Christanto, F. W., & Maulana, C. (2020). Uji Komparasi Quality of Service Antara Metode Routing dan VLAN pada Distribusi Paket Data Jaringan Internet, 4(2), 183–190.