

ARP/ND, ICMP, DHCP, DNS, NAT, dan Packet Flow

Materi Kuliah Antar Jaringan (13S3121) – Minggu 3

Albert Sagala, S.T., M.T.

Program Studi Sarjana Teknik Elektro
Institut Teknologi Del

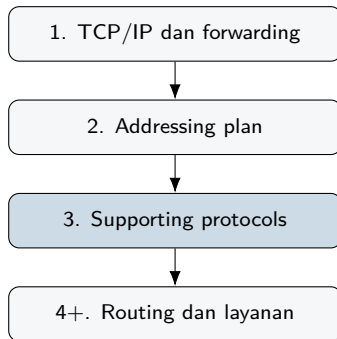
Semester Gasal Tahun Akademik 2026/2027

Posisi Materi Minggu 3

Fokus pertemuan

Mahasiswa memahami protokol pendukung yang membuat packet flow dapat terjadi secara operasional: **ARP/Neighbor Discovery, ICMP, DHCP, DNS**, dan **NAT**.

- Minggu 1: fungsi layer, host-switch-router, local/remote delivery.
- Minggu 2: IPv4/IPv6 addressing, subnetting, VLSM, summarization.
- Minggu 3: layanan pendukung dan urutan packet flow nyata.

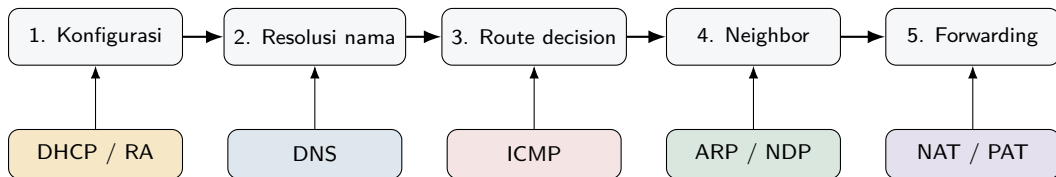


Capaian Pembelajaran Pertemuan

Setelah mengikuti materi ini, mahasiswa diharapkan mampu:

- ➊ Menjelaskan fungsi ARP pada IPv4 dan Neighbor Discovery pada IPv6.
- ➋ Membedakan fungsi ICMP untuk testing, error reporting, traceroute, dan path MTU discovery.
- ➌ Menjelaskan proses DHCPv4 DORA, DHCP relay, serta perbedaan SLAAC dan DHCPv6.
- ➍ Menjelaskan proses DNS resolution dan fungsi record dasar seperti A, AAAA, CNAME, NS, MX, PTR, dan TXT.
- ➎ Menjelaskan konsep NAT/PAT, translation table, manfaat, dan batasan desainnya.
- ➏ Menggambar packet flow end-to-end dari host kampus ke layanan internal dan Internet.

Peta Konsep: Dari Nama Layanan ke Packet Flow



Packet flow end-to-end: konfigurasi host → DNS → routing → neighbor resolution → forwarding

Inti slide

Protokol pendukung tidak berdiri sendiri. Setiap protokol menjawab satu pertanyaan operasional dalam aliran paket.

Kamus Singkatan Minggu 3

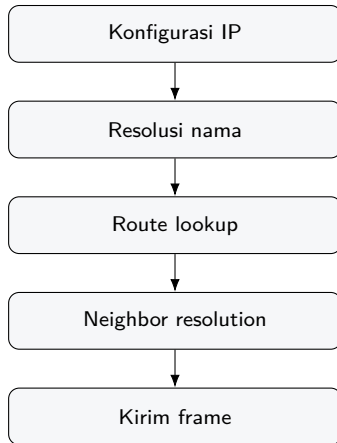
Singkatan	Kepanjangan dan makna ringkas
ARP	Address Resolution Protocol; IPv4 address menjadi MAC lokal.
NDP/ND	Neighbor Discovery Protocol; fungsi neighbor pada IPv6.
RS	Router Solicitation; host meminta router mengirim RA.
RA	Router Advertisement; router mengumumkan prefix/default router.
NS	Neighbor Solicitation; host mencari tetangga atau melakukan DAD.
NA	Neighbor Advertisement; jawaban terhadap NS.

Singkatan	Kepanjangan dan makna ringkas
DAD	Duplicate Address Detection; cek alamat IPv6 tidak duplikat.
ICMP	Internet Control Message Protocol; pesan kontrol dan diagnosis.
TTL/HL	Time To Live / Hop Limit; batas umur packet.
MTU	Maximum Transmission Unit; ukuran frame/packet maksimum link.
PAT	Port Address Translation; banyak host berbagi satu IP publik.
SVI	Switch Virtual Interface; gateway VLAN pada Layer-3 switch.

Masalah Dasar: Host Belum Siap Mengirim Paket

Pertanyaan operasional sebelum komunikasi

- 1 Berapa IP address, prefix, gateway, dan DNS server saya?
- 2 Nama tujuan diterjemahkan ke IP berapa?
- 3 Tujuan local atau remote?
- 4 MAC address tujuan lokal atau next-hop gateway berapa?
- 5 Apakah ada error, unreachable, TTL expired, atau MTU issue?
- 6 Apakah alamat diubah oleh NAT ketika keluar jaringan?

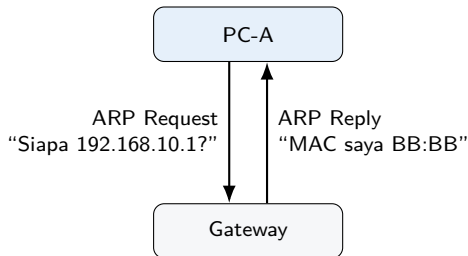


ARP: Address Resolution Protocol pada IPv4

Fungsi utama

ARP menerjemahkan **IPv4 address lokal** menjadi **MAC address** pada satu broadcast domain Ethernet.

- Digunakan hanya untuk tujuan yang dianggap berada pada link lokal.
- Untuk remote destination, host melakukan ARP terhadap **default gateway**.
- ARP Request dikirim sebagai Layer-2 broadcast.
- ARP Reply biasanya unicast dari pemilik IP yang diminta.



Switch mem-flood broadcast ARP, lalu belajar source MAC pada MAC table.

ARP untuk Local Delivery dan Remote Delivery

Local delivery

Host mencari MAC milik destination host.

- PC-A: 192.168.10.10/24
- PC-B: 192.168.10.20/24
- Destination MAC frame: MAC PC-B

Remote delivery

Host mencari MAC milik default gateway.

- PC-A: 192.168.10.10/24
- Server: 10.10.30.50/24
- Gateway PC-A: 192.168.10.1
- Destination MAC frame pertama: MAC gateway

Kesalahan umum

Source host tidak membutuhkan MAC address server remote. MAC address hanya bermakna pada link Layer 2 lokal.

ARP Cache dan Dampaknya terhadap Troubleshooting

- Hasil ARP disimpan sementara pada **ARP cache** atau neighbor table.
- Cache mempercepat komunikasi karena host tidak perlu broadcast setiap kali mengirim.
- Entry dapat menjadi stale ketika perangkat berpindah port, IP berubah, atau terjadi konflik IP.
- Saat troubleshooting, clear cache dapat membantu membedakan masalah konfigurasi dan cache lama.

Evidence minimum

- IP address dan prefix host.
- Default gateway.
- ARP/neighbor table.
- Packet capture ARP Request/Reply.
- MAC table switch bila diperlukan.

Neighbor Discovery pada IPv6

Gagasan utama

IPv6 tidak menggunakan ARP. IPv6 memakai **Neighbor Discovery Protocol (NDP)** berbasis ICMPv6 untuk menemukan router, menemukan tetangga, dan memeriksa alamat duplikat.

Pesan utama

- **RS** – Router Solicitation: host meminta informasi router.
- **RA** – Router Advertisement: router mengumumkan prefix dan default router.
- **NS** – Neighbor Solicitation: mencari alamat link-layer tetangga.
- **NA** – Neighbor Advertisement: jawaban terhadap NS.

Fungsi operasi

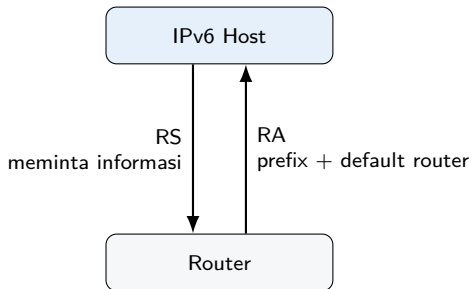
- Router discovery: host menemukan default router.
- Address resolution: IPv6 address menjadi link-layer address.
- DAD: Duplicate Address Detection sebelum alamat dipakai.
- Redirect: router memberi next-hop yang lebih tepat.

Router Advertisement dan SLAAC

Router Advertisement (RA)

Router mengumumkan prefix, default router, dan parameter jaringan. Host memakai informasi ini untuk membentuk alamat IPv6.

- **RS** = Router Solicitation: permintaan dari host.
- **RA** = Router Advertisement: pengumuman dari router.
- **SLAAC** membentuk address dari prefix /64 dan interface identifier.
- **DAD** memeriksa agar alamat IPv6 tidak duplikat.



Setelah RA diterima:

1. host membentuk alamat IPv6;
2. host melakukan DAD;
3. host memakai router sebagai default gateway.

ARP versus IPv6 Neighbor Discovery

Aspek	ARP pada IPv4	NDP pada IPv6
Protokol dasar	ARP, bukan ICMP	ICMPv6
Discovery alamat L2	IPv4 ke MAC	IPv6 ke link-layer address
Broadcast	Menggunakan L2 broadcast	Tidak ada broadcast; memakai multicast
Router discovery	Tidak dilakukan ARP	RA/RS bagian dari NDP
Duplicate detection	Umumnya ARP probe/defense	DAD bagian standar NDP
Dampak filtering	ARP perlu tetap berjalan di LAN	ICMPv6 kritis untuk operasi IPv6

ICMP: Bukan Sekadar Ping

Fungsi ICMP

ICMP digunakan untuk **control dan diagnostic messaging**: error reporting, echo test, TTL exceeded, unreachable, dan path MTU discovery.

- Echo Request/Reply: dasar perintah ping.
- Destination Unreachable: tujuan, port, atau network tidak dapat dicapai.
- Time Exceeded: TTL habis, digunakan oleh traceroute.
- Fragmentation Needed: penting untuk Path MTU Discovery.

Prinsip troubleshooting

Jangan hanya membaca pesan error; periksa **siapa** yang mengirim ICMP error dan pada hop mana error muncul.

Contoh

“Destination unreachable” dari gateway lokal berbeda makna dengan unreachable dari router remote.

Ping: Apa yang Sebenarnya Diuji?

Ping sukses membuktikan

- Source dapat mengirim Echo Request.
- Destination atau perangkat tujuan merespons Echo Reply.
- Forward path dan return path bekerja untuk ICMP.

Ping gagal belum membuktikan

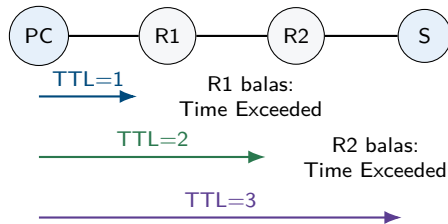
- Link fisik pasti rusak.
- Server aplikasi pasti mati.
- DNS pasti bermasalah.
- Semua protokol pasti gagal.

Catatan

ICMP dapat diblok oleh policy. Karena itu ping adalah indikator awal, bukan satu-satunya bukti konektivitas aplikasi.

Traceroute dan TTL/Hop Limit

- IPv4 menggunakan **TTL**; IPv6 menggunakan **Hop Limit**.
- Setiap router menurunkan nilainya satu.
- Jika nilai menjadi nol, router membuang packet dan mengirim ICMP **Time Exceeded**.
- Traceroute mengirim probe dengan nilai TTL/Hop Limit bertahap untuk menemukan hop Layer 3.



Setiap balasan mengungkapkan alamat router pada hop tersebut.

Masalah

Paket yang terlalu besar dapat gagal melewati link dengan MTU lebih kecil, terutama jika fragmentasi tidak tersedia atau tidak diinginkan.

- IPv4 dapat menggunakan ICMP “Fragmentation Needed” ketika DF bit aktif.
- IPv6 tidak melakukan fragmentasi oleh router; host harus menyesuaikan ukuran paket.
- Blocking ICMP secara buta dapat menyebabkan koneksi TCP tampak “hang” pada ukuran payload tertentu.

Implikasi desain keamanan

Policy firewall perlu membedakan ICMP yang berbahaya dari ICMP yang diperlukan untuk operasi jaringan normal.

DHCPv4: Mengotomasi Konfigurasi Host

Fungsi DHCPv4

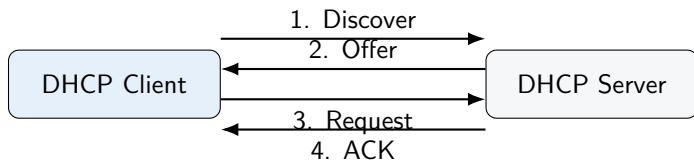
DHCPv4 memberikan parameter jaringan seperti IP address, subnet mask, default gateway, DNS server, lease time, dan opsi lain.

- Mengurangi konfigurasi manual.
- Mendukung address pool dan lease.
- Memerlukan perencanaan scope yang konsisten dengan VLAN/subnet.
- Broadcast DHCP tidak melewati router tanpa DHCP relay.

Parameter penting

- IP address dan prefix/mask.
- Default gateway.
- DNS server.
- Lease duration.
- Domain name atau opsi vendor bila diperlukan.

DHCPv4 DORA

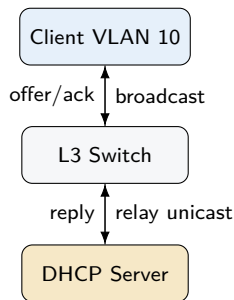


Makna DORA

Discover mencari server, Offer menawarkan konfigurasi, Request memilih tawaran, ACK mengesahkan lease. Setelah itu host dapat menggunakan alamat sesuai lease.

DHCP Relay pada Jaringan Bertingkat

- DHCP Discover awalnya broadcast dalam VLAN lokal.
- Router atau Layer-3 switch dapat bertindak sebagai **DHCP relay**.
- Relay meneruskan permintaan ke DHCP server pusat sebagai unicast.
- Server memilih scope berdasarkan informasi interface/relay.



Kesalahan umum

DHCP server pusat tidak akan menerima broadcast dari VLAN lain tanpa relay atau desain Layer 2 khusus.

DHCPv6, SLAAC, dan DNS Information

Mode	Address host	Default gateway	Informasi tambahan	
SLAAC saja	Dibentuk dari RA	Dari RA	Bisa melalui RA option tertentu	
SLAAC + DHCPv6 stateless	Dibentuk dari RA	Dari RA	DNS/domain DHCPv6	dari
DHCPv6 stateful	Dari DHCPv6	Tetap dari RA	DNS/domain DHCPv6	dari

Perbedaan penting dari DHCPv4

Pada IPv6, default gateway secara normal diperoleh melalui Router Advertisement. DHCPv6 tidak membawa informasi default gateway seperti DHCPv4.

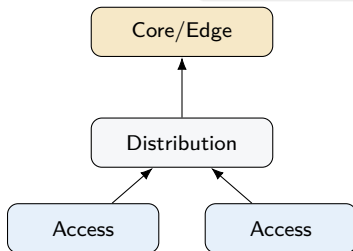
Address Assignment dan Hierarchical LAN

Access layer

- VLAN per fungsi: Student, Faculty, Lab, Server, IoT, Guest.
- DHCP scope mengikuti VLAN/subnet.
- First-hop gateway biasanya berada pada SVI di distribution layer.

Distribution/Core/Edge

- Distribution melakukan inter-VLAN routing dan relay DHCP.
- Core menghubungkan distribution block.
- Edge/firewall melakukan NAT dan policy menuju Internet.

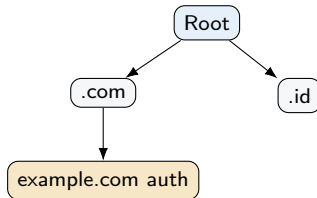


DNS: Nama Menjadi Alamat

Fungsi DNS

DNS menerjemahkan nama domain menjadi alamat IP dan menyediakan informasi lain yang diperlukan aplikasi jaringan.

- Manusia memakai nama:
`www.example.org`.
- Aplikasi membutuhkan IP address tujuan.
- DNS bersifat hierarkis: root, TLD, authoritative server.
- Resolver melakukan caching berdasarkan TTL record.



DNS Resolution: Recursive dan Iterative

Recursive query

Client meminta resolver memberikan jawaban final. Resolver melakukan proses pencarian ke server lain bila cache belum ada.

- Umum pada host ke DNS resolver kampus/ISP.
- Resolver menyimpan cache.

Iterative query

Server DNS dapat menjawab dengan referensi ke server lain yang lebih otoritatif.

- Digunakan resolver ketika berjalan melalui root, TLD, dan authoritative server.
- Mengikuti delegasi zone.

Catatan operasi

Gangguan DNS sering tampak seperti gangguan Internet, padahal IP connectivity mungkin masih berjalan.

DNS Record yang Sering Ditemui

Record	Fungsi	Contoh penggunaan
A	Nama ke IPv4	web.example.id -> 203.0.113.10
AAAA	Nama ke IPv6	web.example.id -> 2001:db8::10
CNAME	Alias nama	www -> web.example.id
NS	Name server zone	Delegasi DNS zone
MX	Mail exchanger	Server email domain
PTR	Reverse lookup	IP ke nama
TXT	Teks/verifikasi	SPF, DKIM, domain verification
SRV	Service location	Lokasi layanan tertentu

DNS, IPv4, dan IPv6 pada Dual-Stack

- Record **A** mengarah ke IPv4.
- Record **AAAA** mengarah ke IPv6.
- Client dual-stack dapat mencoba IPv6 lebih dahulu bergantung sistem dan policy.
- Jika IPv6 tidak lengkap, aplikasi dapat tampak lambat atau gagal walaupun IPv4 berjalan.

Diagnosis cepat

Bandingkan hasil:

- resolusi A dan AAAA;
- ping IPv4 dan ping IPv6;
- traceroute IPv4 dan traceroute IPv6;
- akses aplikasi pada kedua stack.

NAT: Network Address Translation

Definisi

NAT mengubah alamat IP pada packet ketika melewati perangkat boundary, umumnya firewall atau router edge.

- Banyak digunakan untuk menghubungkan private IPv4 ke Internet publik.
- Translation dapat bersifat static, dynamic, atau port-based.
- NAT memerlukan state table untuk memetakan koneksi.
- NAT bukan pengganti firewall policy.

Istilah umum

- Inside local: alamat private host internal.
- Inside global: alamat publik hasil translasi.
- Outside global: alamat tujuan di luar jaringan.
- PAT/NAPT: banyak host berbagi satu IP publik dengan port berbeda.

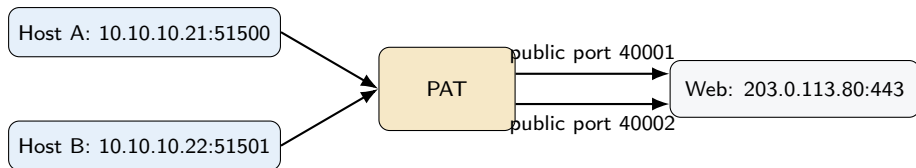
Jenis NAT

Jenis	Mekanisme	Contoh penggunaan
Static NAT	Pemetaan satu private IP ke satu public IP tetap	Publikasi server internal tertentu
Dynamic NAT	Private IP dipetakan ke pool public IP secara dinamis	Banyak host dengan pool publik terbatas
PAT/NAPT	Banyak host berbagi satu atau beberapa public IP dengan pembeda port	Akses Internet dari jaringan kampus/rumah
Destination NAT	Mengubah destination IP/port dari sisi luar ke server internal	Port forwarding ke layanan internal

Catatan

NAT mengubah packet flow karena alamat yang dilihat oleh server luar bukan alamat private asli host internal.

Contoh PAT: Banyak Host, Satu Public IP



Translation table sederhana

Inside local	Inside global
10.10.10.21:51500	198.51.100.5:40001
10.10.10.22:51501	198.51.100.5:40002

Prinsip

Port berbeda memungkinkan banyak koneksi internal berbagi satu public IPv4.

Manfaat dan Batasan NAT

Manfaat

- Menghemat penggunaan public IPv4.
- Memungkinkan private addressing internal.
- Membantu renumbering internal tanpa mengubah alamat publik.
- Umum pada edge network dan firewall.

Batasan

- Memecah prinsip end-to-end addressing.
- Membutuhkan state table dan timeout.
- Dapat mengganggu protokol yang membawa IP/port dalam payload.
- Bukan kontrol keamanan yang cukup tanpa firewall policy.

Packet Flow 1: Host ke Host pada Satu VLAN

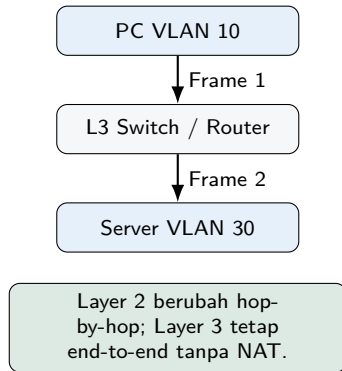
- 1 PC-A memiliki IP, prefix, gateway, dan DNS configuration.
- 2 PC-A menentukan destination berada pada subnet yang sama.
- 3 PC-A mengecek ARP cache untuk IP PC-B.
- 4 Jika belum ada, PC-A mengirim ARP Request broadcast.
- 5 PC-B menjawab ARP Reply dengan MAC address-nya.
- 6 PC-A mengirim frame langsung ke MAC PC-B.

Karakteristik

Router tidak terlibat dalam forwarding data antarhost pada subnet yang sama, tetapi switch tetap meneruskan frame berdasarkan MAC table.

Packet Flow 2: Host ke Server pada VLAN Berbeda

- 1 PC-A menentukan server berada pada subnet berbeda.
- 2 PC-A memilih default gateway sebagai next hop.
- 3 PC-A melakukan ARP untuk MAC gateway.
- 4 Frame pertama: MAC PC-A ke MAC gateway; IP PC-A ke IP server.
- 5 L3 switch/router melakukan route lookup dan membuat frame baru menuju server VLAN.
- 6 Server mengirim reply melalui gateway-nya; return path harus valid.



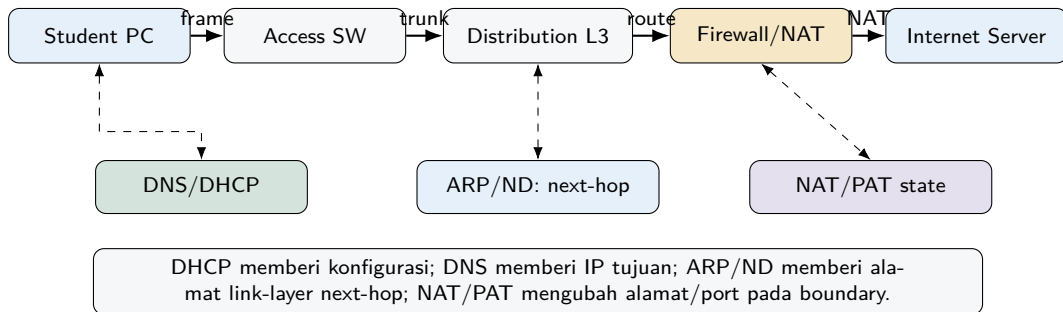
Packet Flow 3: Akses Website Internet dengan DNS dan NAT

- 1 Host memperoleh IP configuration melalui DHCP.
- 2 User mengetik nama domain; host bertanya ke DNS resolver.
- 3 Resolver mengembalikan A/AAAA record sesuai cache atau resolusi hierarkis.
- 4 Host menentukan tujuan remote dan mengirim frame ke default gateway.
- 5 Packet melewati distribution/core menuju firewall edge.
- 6 Firewall melakukan NAT/PAT dari private IPv4 ke public IPv4.
- 7 Server Internet melihat source sebagai public IP NAT, bukan private IP host.
- 8 Reply kembali ke public IP NAT; firewall menggunakan translation table untuk mengirim ke host internal.

Titik diagnosis

Kegagalan dapat terjadi pada DHCP, DNS, default gateway, routing internal, firewall policy, NAT state, Internet routing, atau server tujuan.

Diagram Packet Flow: Kampus ke Internet



Packet Flow IPv6: Tanpa ARP dan Umumnya Tanpa NAT

- 1 Host menerima RA dari router atau mengirim RS.
- 2 Host membentuk IPv6 address, melakukan DAD, dan mengetahui default router.
- 3 Host mendapatkan DNS information melalui RA option atau DHCPv6.
- 4 DNS mengembalikan AAAA record untuk layanan tujuan.
- 5 Host menggunakan Neighbor Discovery untuk menemukan link-layer address gateway.
- 6 Packet dikirim end-to-end dengan IPv6 source dan destination.

Perbedaan kunci

- Tidak ada ARP.
- Tidak ada broadcast.
- ICMPv6 adalah bagian kritis operasi jaringan.
- NAT bukan asumsi default dalam desain IPv6.

Checklist Troubleshooting Berbasis Packet Flow

Tahap	Evidence yang diperiksa
Konfigurasi host	IP/prefix, gateway, DNS server, IPv6 RA/DHCPv6 status
Layer 2 lokal	Link status, VLAN, MAC table, ARP/ND table
Neighbor resolution	ARP Request/Reply atau NS/NA berhasil
Routing lokal	Default route host, SVI/router interface, route table
DNS	A/AAAA record, resolver, cache, TTL, authoritative response bila perlu
ICMP	Echo, unreachable, TTL exceeded, path MTU indications
NAT/firewall	Translation table, session table, policy allow/deny, log
Return path	Route balik, NAT state, asymmetric path, security policy

Kesalahan Konseptual yang Sering Terjadi

- ❶ Mengira ARP dapat mencari MAC server di Internet.
- ❷ Menganggap ICMP boleh selalu diblok tanpa dampak operasional.
- ❸ Menganggap DHCP hanya memberikan IP address, padahal gateway dan DNS juga kritis.
- ❹ Menganggap DNS gagal berarti jaringan fisik pasti bermasalah.
- ❺ Menganggap NAT adalah mekanisme keamanan utama.
- ❻ Mengabaikan return path saat mendiagnosis ping atau akses aplikasi.
- ❼ Mencampur konsep IPv4 ARP dengan IPv6 Neighbor Discovery.

Studi Kasus Singkat: Student VLAN ke Web Server

Skenario

PC mahasiswa pada VLAN 10 ingin mengakses `https://server.kampus.local`. Server berada pada VLAN 30. DNS dan DHCP berada pada Server VLAN.

- 1 DHCP: PC memperoleh IP, gateway VLAN 10, dan DNS server.
- 2 DNS: PC menanyakan nama server ke DNS.
- 3 Route decision: server berada di subnet berbeda.
- 4 ARP: PC mencari MAC gateway VLAN 10.
- 5 Inter-VLAN routing: L3 switch meneruskan packet ke VLAN 30.
- 6 Return: server menjawab melalui gateway VLAN 30.

Pertanyaan diagnosis

Jika nama tidak bisa diakses tetapi IP server bisa di-ping, lapisan masalah paling mungkin berada pada DNS atau policy aplikasi, bukan pada routing dasar.

Studi Kasus Singkat: Student VLAN ke Internet

Skenario

PC mahasiswa pada VLAN 10 ingin membuka `https://www.example.org`. Jaringan kampus menggunakan private IPv4 dan PAT pada firewall edge.

- 1 PC mendapatkan konfigurasi dari DHCP.
- 2 DNS resolver mengembalikan A/AAAA record.
- 3 PC mengirim traffic ke default gateway.
- 4 Distribution/core meneruskan packet ke firewall.
- 5 Firewall mengevaluasi policy dan membuat NAT/PAT entry.
- 6 Server Internet menerima traffic dari public IP firewall.
- 7 Reply diterjemahkan kembali berdasarkan NAT state table.

Ringkasan Materi Minggu 3

- ARP menyelesaikan IPv4-to-MAC pada link lokal; IPv6 memakai Neighbor Discovery berbasis ICMPv6.
- ICMP adalah mekanisme diagnosis dan error reporting, bukan hanya ping.
- DHCPv4 mengotomasi konfigurasi host; DHCP relay diperlukan ketika server berada di subnet lain.
- IPv6 memakai kombinasi RA, SLAAC, dan/atau DHCPv6 untuk address assignment dan informasi tambahan.
- DNS menerjemahkan nama menjadi alamat dan dapat menjadi sumber masalah yang tampak seperti gangguan jaringan.
- NAT/PAT mengubah alamat/port pada boundary, terutama untuk private IPv4 ke Internet.
- Packet flow yang benar harus menjelaskan DNS, routing decision, ARP/ND, forwarding, NAT, dan return path.

Dua Pertanyaan Mendasar untuk Menguji Pemahaman

Pertanyaan 1

Seorang host IPv4 pada 192.168.10.25/24 ingin mengakses server 10.10.30.50. Jelaskan secara berurutan: keputusan local/remote, alamat MAC yang dicari dengan ARP, alamat IP source/destination pada packet, dan apa yang berubah ketika packet melewati router.

Pertanyaan 2

Dalam jaringan dual-stack, user dapat mengakses layanan menggunakan alamat IPv4, tetapi gagal ketika menggunakan nama domain. Jelaskan kemungkinan peran DNS A/AAAA record, IPv6 reachability, ICMPv6/ND, dan firewall policy dalam kasus tersebut.

Referensi

-  D. Plummer, “Ethernet Address Resolution Protocol,” RFC 826, 1982.
-  J. Postel, “Internet Control Message Protocol,” RFC 792, 1981.
-  A. Conta, S. Deering, and M. Gupta, “Internet Control Message Protocol (ICMPv6),” RFC 4443, 2006.
-  T. Narten et al., “Neighbor Discovery for IP version 6,” RFC 4861, 2007.
-  R. Droms, “Dynamic Host Configuration Protocol,” RFC 2131, 1997.
-  T. Mrugalski et al., “Dynamic Host Configuration Protocol for IPv6,” RFC 8415, 2018.
-  P. Mockapetris, “Domain Names - Concepts and Facilities,” RFC 1034, 1987.
-  P. Mockapetris, “Domain Names - Implementation and Specification,” RFC 1035, 1987.
-  P. Srisuresh and K. Egevang, “Traditional IP Network Address Translator,” RFC 3022, 2001.