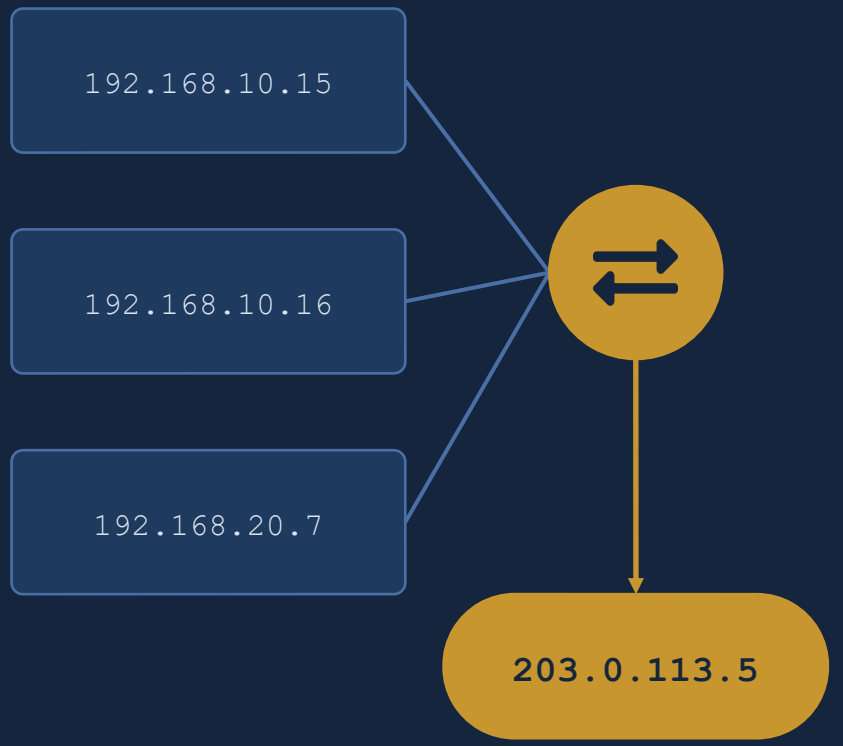
ENTERPRISE NETWORKING · PERTEMUAN 12

NAT dan PAT

Network Address Translation — menjembatani alamat privat internal dengan internet publik

Sub-CPMK 3.4 · CPL-8, CPL-11 · Bab 12 Buku Ajar



Dosen Pengampu

Ir. H. A. Mooduto, M.Kom. · Ideva Gaputra, S.Kom., M.Kom.

Program Studi D3 Teknik Komputer — Politeknik Negeri Padang · Ganjil 2026/2027

PETA PERTEMUAN

Alur pembahasan hari ini

01	**Alamat privat & internet**	RFC 1918 dan mengapa tidak routable
02	**Konsep & terminologi NAT**	Inside/outside, local/global
03	**Static, Dynamic, PAT**	Tiga cara memetakan alamat
04	**Tabel translasi PAT**	Peran nomor port membedakan sesi
05	**Konfigurasi Cisco IOS**	Tiga langkah, verifikasi, troubleshooting
06	**Studi kasus & praktikum**	Gerbang internet PT NDK

Setelah pertemuan ini, mahasiswa mampu…

Sub-CPMK 3.4

Mampu mengonfigurasi Network Address Translation (NAT) dan Port Address Translation (PAT) pada jaringan enterprise.

CPL-8 · CPL-11
Bobot tugas: 2% nilai akhir

1
Menjelaskan mengapa alamat RFC 1918 tidak dirutekan di internet

2
Membedakan Static NAT, Dynamic NAT, dan PAT

3
Menjelaskan tabel translasi PAT dan peran nomor port

4
Menjelaskan inside local, inside global, outside global

5
Mengonfigurasi Static NAT dan PAT di Cisco IOS

6
Menganalisis kombinasi NAT & PAT dengan server publik

01

Alamat privat & internet

192.168.10.15 dipakai jutaan jaringan sekaligus — internet tidak tahu yang mana

RFC 1918

Tiga rentang alamat privat

10.0.0.0/8

10.0.0.0 – 10.255.255.255

Satu blok besar, populer di enterprise besar

172.16.0.0/12

172.16.0.0 – 172.31.255.255

Sering dipakai jaringan menengah

192.168.0.0/16

192.168.0.0 – 192.168.255.255

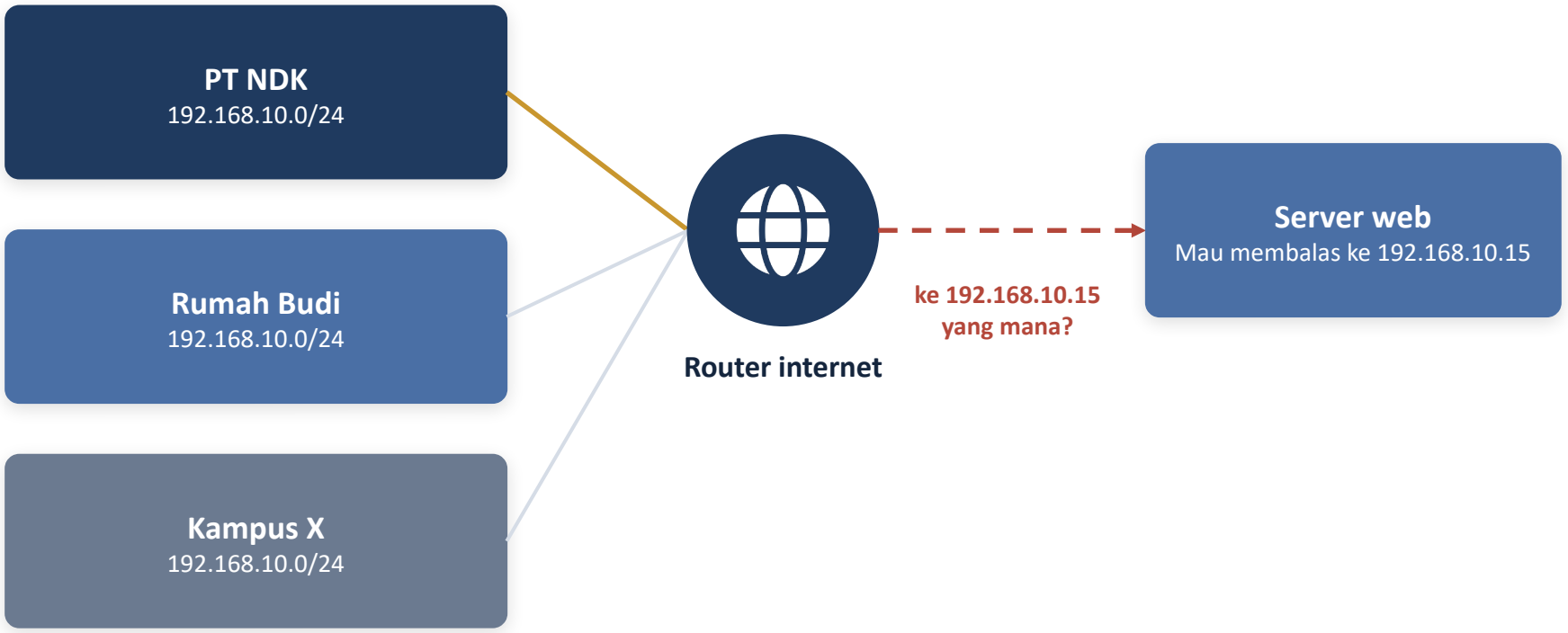
Dipakai PT NDK sejak Bab 1

≈ 4,3 miliar

alamat IPv4 secara teoretis — jauh lebih sedikit dari jumlah perangkat yang terhubung hari ini

Bebas dipakai siapa pun, tanpa perlu didaftarkan atau unik secara global — konsekuensinya, tidak pernah dirutekan oleh router internet publik.

Balasan tidak tahu jalan pulang



Bukan diblokir kebijakan keamanan, melainkan tidak ada jalur kembali (return path) yang valid.

Solusi: NAT

Ganti alamat privat dengan alamat publik yang valid tepat sebelum paket meninggalkan jaringan, lalu terjemahkan kembali saat balasan tiba.

NAT adalah penerjemah di gerbang perbatasan — ia menerjemahkan bahasa internal organisasi menjadi bahasa universal yang dipahami seluruh dunia, tanpa perlu mengungkap peta lengkap dari dalam rumahnya.

Buku Ajar Enterprise Networking, Bab 12

02

Konsep & terminologi NAT

Menerjemahkan alamat di header paket saat melintasi batas jaringan

Apa itu Network Address Translation?

NAT menerjemahkan alamat IP pada **header paket** saat paket melintasi batas dua jaringan — umumnya jaringan privat organisasi dan internet publik.

Dijalankan di **router atau firewall di tepi (edge)** jaringan.

Keluar: alamat privat → publik. **Masuk:** publik → privat.



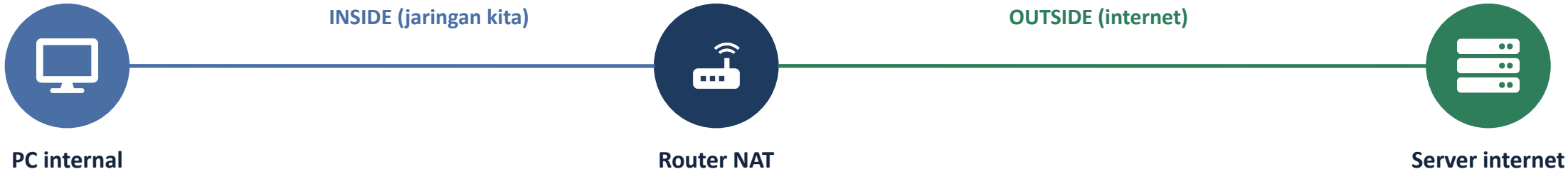
Analogi: resepsionis & PABX

Ekstensi 101, 102, 103 → Alamat privat
Hanya berlaku di dalam gedung

Nomor utama gedung → Alamat publik
Yang terlihat oleh penelepon luar

PABX tahu ekstensi tujuan → Tabel translasi
Balasan diteruskan ke orang yang tepat

Empat nama untuk alamat dalam satu percakapan



Inside local

`192.168.10.15`

Alamat privat asli PC internal

Inside global

`203.0.113.5`

Alamat publik yang mewakili PC itu di internet

Outside global

`198.51.100.7`

Alamat publik asli server tujuan

Outside local

`198.51.100.7`

Alamat tujuan seperti terlihat dari dalam — umumnya sama dengan outside global

Cara mengingat: inside/outside = milik siapa perangkatnya · local/global = dilihat dari sisi mana

03

Static NAT, Dynamic NAT, PAT

Tiga cara memetakan alamat privat ke publik

Pemetaan, jumlah host per IP publik, dan kegunaannya

Static NAT

1 : 1 permanen

Host per IP publik

1

Satu IP publik khusus untuk satu host, selamanya

Server yang harus selalu ditemukan di alamat yang sama

Dynamic NAT

1 : 1 dari pool, sementara

Host per IP publik

1

Per host yang sedang aktif; pool habis = host lain menunggu

Jarang dipakai sekarang — digantikan PAT

PAT (Overload)

Banyak : 1 dibedakan port

Host per IP publik

Ribuan

Semua host berbagi satu IP publik bersamaan

Akses internet umum: standar de facto

Pertanyaan pertama: siapa yang memulai koneksi?

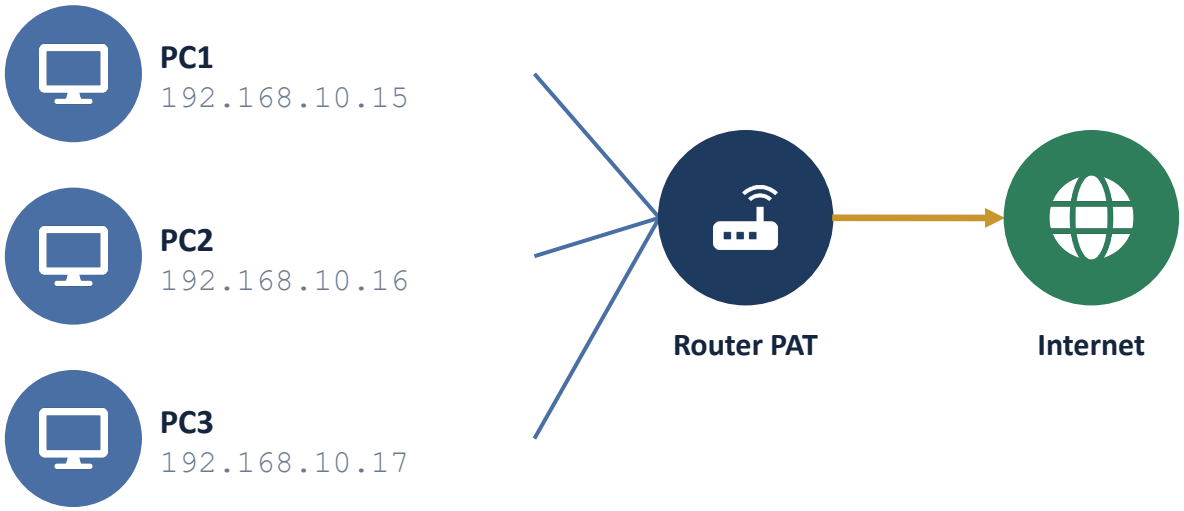


04

Tabel translasi PAT

Nomor port yang membuat ribuan host bisa berbagi satu alamat

Tiga PC, satu alamat publik, port berbeda



Tabel translasi di router

Inside local	Inside global
192.168.10.15:49152	**203.0.113.5:1025**
192.168.10.16:49152	**203.0.113.5:1026**
192.168.10.17:50211	**203.0.113.5:1027**

IP publik sama

Ketiga PC tampil sebagai 203.0.113.5

Port pembeda

Router memberi port sumber berbeda per sesi

Entri sementara

Dibuat saat sesi mulai, dihapus saat idle/ditutup

Bagaimana balasan menemukan PC yang tepat

1. **PC2 mengirim**
   `Src 192.168.10.16:49152 → Dst 198.51.100.7:443`
2. **Router menerjemahkan**
   `Src diganti 203.0.113.5:1026; entri dicatat di tabel`
3. **Server membalas**
   `Dst 203.0.113.5:1026 — alamat publik, rutenya valid`
4. **Router mencocokkan**
   `Port 1026 → milik 192.168.10.16:49152 → diteruskan ke PC2`

Konsekuensi penting

Paket yang datang dari internet tanpa entri di tabel (tidak diawali dari dalam) tidak punya tujuan internal — itulah sebabnya PAT saja tidak cukup untuk server publik.

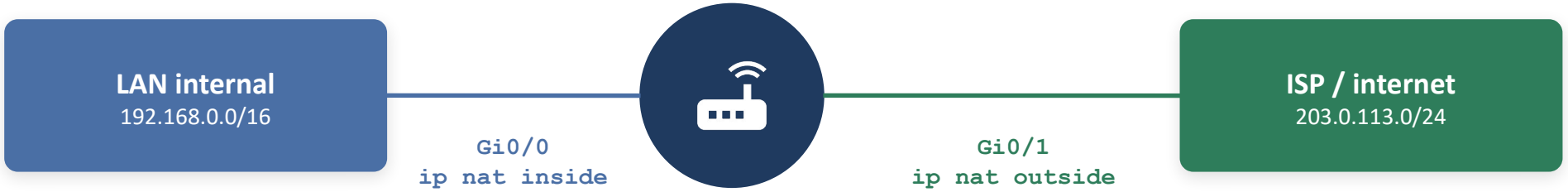
05

Konfigurasi NAT di Cisco IOS

Tandai sisi, tentukan siapa yang diterjemahkan, tulis aturannya

TIGA LANGKAH

Pola konfigurasi semua jenis NAT



Langkah 1

Tandai sisi

ip nat inside / ip nat outside di interface yang tepat

Langkah 2

Tentukan siapa

ACL standar memilih alamat yang boleh ditranslasi

Langkah 3

Tulis aturannya

ip nat inside source … static / pool / overload

Ingat Pertemuan 9: di sini ACL dipakai untuk MEMILIH alamat, bukan memblokir lalu lintas. permit = ikut ditranslasi.

PAT untuk semua LAN, Static NAT untuk satu server

```
! Langkah 1: tandai sisi
interface gigabitEthernet 0/0
 description LAN Internal
 ip nat inside
interface gigabitEthernet 0/1
 description Menuju ISP
 ip nat outside

! Verifikasi
show ip nat translations
show ip nat statistics
```

PAT (NAT overload)

```
access-list 1 permit 192.168.0.0 0.0.255.255
ip nat inside source list 1
   interface gigabitEthernet 0/1 overload
```

Static NAT untuk server

```
ip nat inside source static
   192.168.20.50 203.0.113.10
```

overload = kata kunci yang mengubah NAT biasa menjadi PAT. Perintah ip nat inside source … ditulis satu baris; di sini dipotong agar terbaca.

NAT dengan pool alamat publik

```
ip nat pool NDK-POOL 203.0.113.20 203.0.113.30
   netmask 255.255.255.0
access-list 2 permit 192.168.10.0 0.0.0.255
ip nat inside source list 2 pool NDK-POOL
```

Pool 11 alamat (203.0.113.20–30) untuk host di VLAN 10. Langkah 1 (inside/outside) tetap sama.



Batasnya

Host ke-12 yang aktif bersamaan tidak mendapat alamat sampai ada entri yang kedaluwarsa. Itu sebabnya Dynamic NAT jarang dipakai.

Aturan ip nat inside source …	Hasil
`list 2 pool NDK-POOL`	Dynamic NAT: 1 host aktif = 1 IP dari pool
`list 2 pool NDK-POOL overload`	PAT memakai alamat dari pool
`list 1 interface gi0/1 overload`	PAT memakai IP interface outside

show ip nat translations

```
Pro Inside global      Inside local       Outside local      Outside global
tcp 203.0.113.5:1025   192.168.10.15:49152 198.51.100.7:443   198.51.100.7:443
tcp 203.0.113.5:1026   192.168.10.16:49152 198.51.100.7:443   198.51.100.7:443
--- 203.0.113.10       192.168.20.50      ---                ---
```

Baris tcp …:1025/1026

Entri PAT dinamis — muncul saat PC mengakses internet, hilang saat idle

Baris --- 203.0.113.10

Entri Static NAT — selalu ada, tanpa protokol dan port

Tabel kosong?

Belum ada lalu lintas, atau inside/outside/ACL salah — mulai troubleshooting

Perintah NAT yang perlu dihafal

Perintah	Fungsi
`ip nat inside | ip nat outside`	Menandai interface sebagai sisi internal / eksternal
`ip nat inside source list <acl> interface <intf> overload`	PAT memakai IP interface outside
`ip nat inside source static <local> <global>`	Static NAT permanen 1:1
`ip nat pool <nama> <awal> <akhir> netmask <mask>`	Pool alamat publik untuk Dynamic NAT
`ip nat inside source list <acl> pool <nama>`	Dynamic NAT dari pool
`show ip nat translations | statistics`	Tabel translasi aktif / statistik NAT
`clear ip nat translation *`	Menghapus entri dinamis (berguna saat uji)

Saat host tidak bisa keluar ke internet

1

Inside/outside terbalik

Penyebab paling umum NAT tidak bekerja sama sekali

2

ACL tidak mencakup subnet

Pakai ACL yang mencakup SELURUH subnet internal, bukan satu subnet

3

Alamat Static & PAT bertumpuk

Alamat publik Static NAT tidak boleh dipakai juga oleh PAT/pool

4

Tidak ada rute default ke ISP

NAT tidak menggantikan routing; paket tetap perlu jalan keluar



Urutan cek

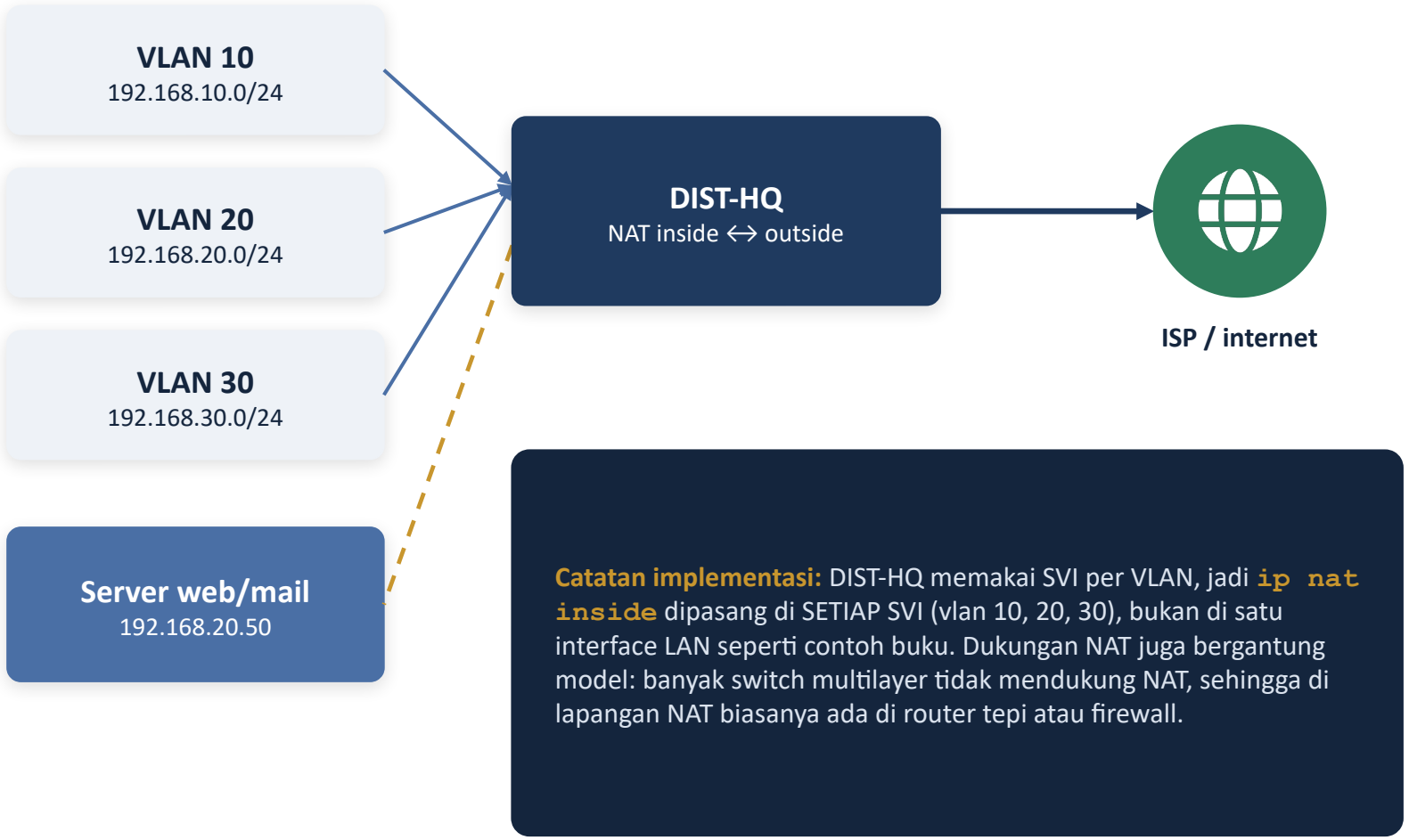
1. show run | include ip nat — sisi interface
1. show ip nat translations — entri terbentuk?
1. show access-lists — counter ACL NAT bertambah?
1. show ip route — ada rute default?

06

Studi kasus & praktikum

Gerbang internet PT Nusantara Digital Kreasi

PAT untuk karyawan, Static NAT untuk server



Catatan implementasi: DIST-HQ memakai SVI per VLAN, jadi `ip nat inside` dipasang di SETIAP SVI (vlan 10, 20, 30), bukan di satu interface LAN seperti contoh buku. Dukungan NAT juga bergantung model: banyak switch multilayer tidak mendukung NAT, sehingga di lapangan NAT biasanya ada di router tepi atau firewall.

PAT

`Semua VLAN internal → 203.0.113.5`

Outbound massal karyawan

Static NAT

`192.168.20.50 ↔ 203.0.113.10`

Inbound ke web & mail

PERTANYAAN KRITIS

Server publik di VLAN Keuangan?

Telusuri dampaknya

192.168.20.0/24 = VLAN 20 Keuangan
Subnet server publik sama dengan data paling sensitif

Static NAT 1:1 membuka semua port
Bukan hanya 80/443/25 — SSH, RDP, SMB ikut terjangkau

Server diretas dari internet
Penyerang langsung berada di dalam VLAN Keuangan

ACL BLOK-TAMU (Pertemuan 9)
Menjaga dari tamu internal, tidak dari internet

Diskusikan di kelas

1. Di segmen mana sebaiknya server yang dapat diakses dari internet ditempatkan?
1. Bagaimana membatasi Static NAT agar hanya port layanan yang terbuka?
1. Apakah NAT bisa dianggap pengganti firewall?

Kelebihan dan keterbatasan NAT



Kelebihan

- Ribuan host berbagi satu IP publik
- Struktur alamat internal tersembunyi
- Alamat internal bisa diubah tanpa mengubah alamat publik
- Server tetap terjangkau di alamat konsisten



Keterbatasan

- Protokol yang menyisipkan IP di payload butuh ALG
- Troubleshooting & korelasi log lebih sulit
- Sedikit menambah latensi pemrosesan
- Konektivitas end-to-end murni hilang

NAT & IPv6

NAT adalah solusi sementara.

IPv6 menyediakan alamat yang cukup agar setiap perangkat kembali memiliki alamat unik global — mengembalikan prinsip konektivitas end-to-end.

Static NAT, Dynamic NAT, dan PAT

1. Topologi: LAN (2 VLAN + 1 server) – router tepi – router ISP – server 'internet'
2. Tandai ip nat inside/outside; pastikan rute default ke ISP ada
3. Static NAT server lokal → uji akses dari server internet ke IP publiknya
4. Dynamic NAT dengan pool kecil (mis. 3 alamat) → uji 4 host, amati yang gagal
5. Ganti ke PAT (overload) → semua host berhasil; bandingkan tabel translasi
6. Dokumentasikan show ip nat translations/statistics tiap skema

Rubrik penilaian

Rancangan skema NAT statis, dinamis, PAT	20%
Keberhasilan konfigurasi & fungsionalitas	40%
Pengujian konektivitas ke internet	20%
Kelengkapan dokumentasi	20%

Sangat Baik 85–100 · Baik 70–84 · Cukup 55–69 · Kurang < 55

Enam hal yang dibawa pulang

01

Alamat RFC 1918 tidak dirutekan di internet: tidak unik, tak ada jalur kembali

02

NAT menerjemahkan alamat di header saat paket melintasi tepi jaringan

03

Inside local = privat asli; inside global = publik yang mewakilinya

04

Static 1:1 untuk server; Dynamic dari pool (jarang); PAT banyak:1 untuk internet

05

PAT membedakan sesi dengan nomor port di tabel translasi sementara

06

Konfigurasi: inside/outside → ACL → ip nat inside source; cek show ip nat translations

Uji pemahaman sebelum praktikum

Analisis

Server email harus selalu bisa diakses dari internet dengan alamat yang sama. Jenis NAT apa yang tepat, dan mengapa?

Analisis

Host internal tidak bisa ke internet meski NAT sudah dikonfigurasi. Sebutkan tiga hal yang perlu diperiksa.

Konfigurasi

Tulis konfigurasi PAT untuk 10.0.0.0/8 dengan Gi0/0 inside dan Gi0/1 outside.

Reflektif

Mengapa NAT disebut solusi sementara, dan apa kaitannya dengan IPv6?

PERTEMUAN BERIKUTNYA

Pertemuan 13 — Teknologi WAN

CPMK-3 selesai. Berikutnya kita menghubungkan kantor pusat dan cabang: leased line, MPLS, dan VPN site-to-site. Sub-CPMK 4.1.

Terima kasih — sampai jumpa di laboratorium

Referensi

- Buku Ajar Enterprise Networking, Bab 12 — Prodi D3 TK PNP
- IETF (1996). RFC 1918: Address Allocation for Private Internets
- Odom, W. (2023). CCNA 200-301 Official Cert Guide, Vol. 1. Cisco Press
- Lammle, T. (2021). CCNA Routing and Switching Complete Study Guide. Sybex
- Cisco NetAcad — ENSA, modul Network Address Translation