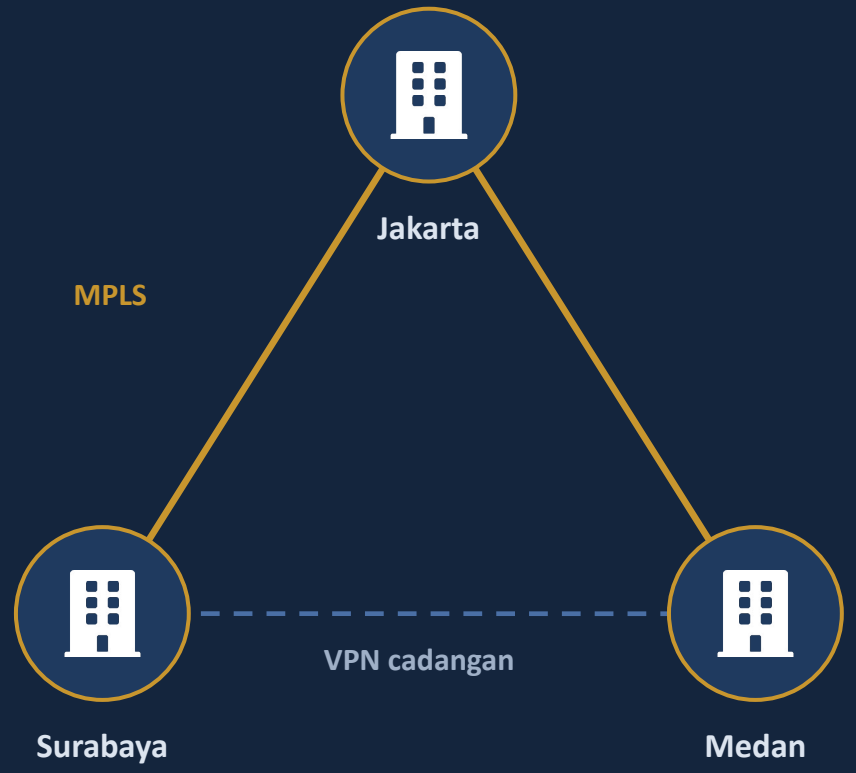
ENTERPRISE NETWORKING · PERTEMUAN 13

Teknologi WAN

Leased Line, MPLS, dan VPN Site-to-Site — menghubungkan kantor yang terpisah ratusan kilometer

Sub-CPMK 4.1 · CPL-8, CPL-11 · Bab 13 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

Alur pembahasan hari ini

01	**Membuka kotak hitam WAN**	Dari LAN milik sendiri ke jaringan sewaan
02	**Istilah & spektrum WAN**	CE, PE, P, SLA, IPsec
03	**Leased line & MPLS**	Sirkuit dedicated dan label switching
04	**VPN site-to-site (IPsec)**	Enkapsulasi, dua fase, konfigurasi
05	**Memilih teknologi WAN**	Perbandingan dan strategi berlapis
06	**Studi kasus & tugas**	WAN PT NDK dan tugas analisis

Setelah pertemuan ini, mahasiswa mampu…

Sub-CPMK 4.1

Mampu menjelaskan dan merancang gambaran umum teknologi WAN (leased line, MPLS, VPN site-to-site) untuk konektivitas enterprise.

CPL-8 · CPL-11
Bobot tugas: 1,5% nilai akhir

1
Membedakan LAN dan WAN, termasuk peran penyedia layanan

2
Menguraikan leased line sebagai sirkuit dedicated

3
Menjelaskan label switching dan konektivitas any-to-any MPLS

4
Menjelaskan enkapsulasi dan enkripsi VPN IPsec

5
Membandingkan biaya, keandalan, skalabilitas ketiganya

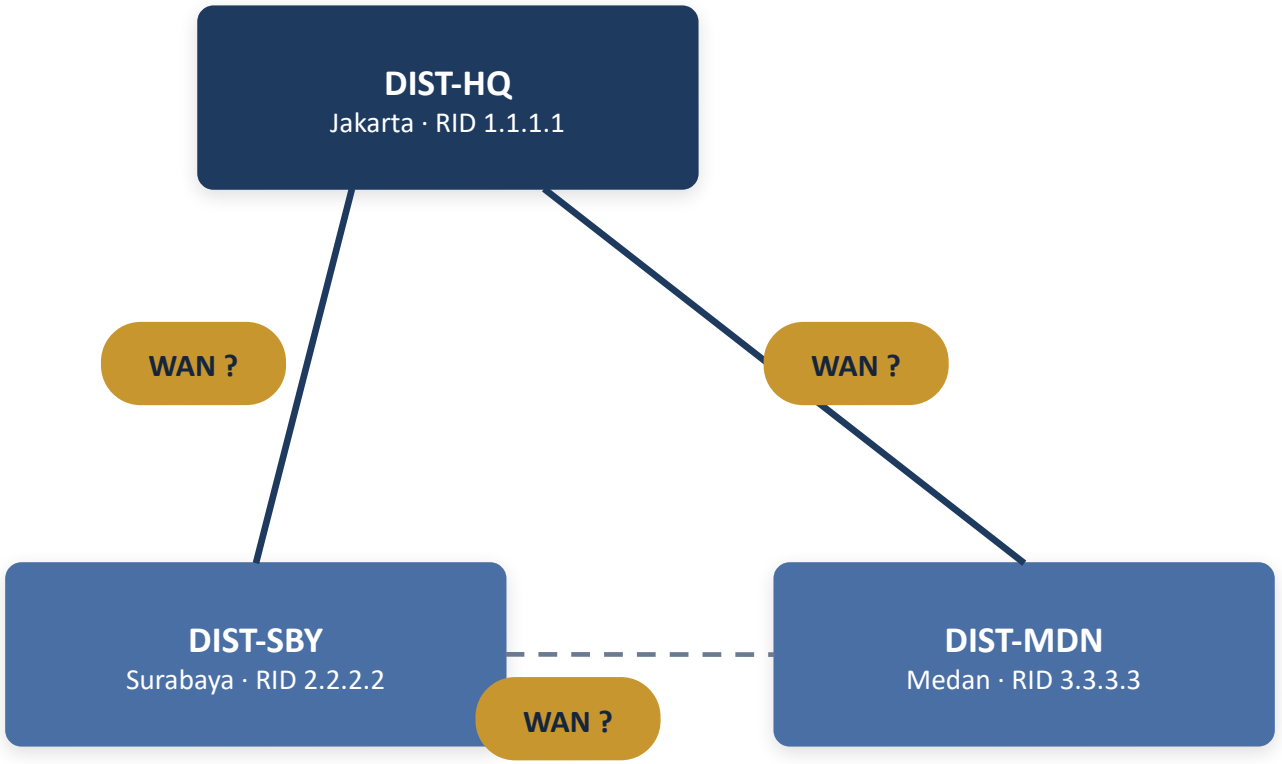
6
Menganalisis strategi WAN berlapis multi-lokasi

01

Membuka kotak hitam WAN

Sejak Bab 4 kita menggambar 'WAN Link' — hari ini kita lihat isinya

Garis 'WAN Link' yang belum pernah dijelaskan



Bab 4–5

OSPF bertukar rute MELALUI link ini; jalur cadangan SBY –MDN

Bab 11

QoS di link WAN untuk voice & video

Bab 13

Teknologi APA yang membentuk link itu sendiri?

Milik sendiri vs menyewa kapasitas



LAN

Seperti mobil pribadi di jalan kompleks sendiri

Infrastruktur	**Milik organisasi**
Jangkauan	**Satu gedung / kompleks**
Kendali	**Penuh, ujung ke ujung**
Biaya	**Investasi perangkat sekali beli**



WAN

Seperti transportasi umum antar-kota: beli tiket, bukan rel

Infrastruktur	**Milik carrier / ISP**
Jangkauan	**Antar-kota, antar-pulau**
Kendali	**Sebagian; diatur lewat SLA**
Biaya	**Sewa berulang (bulanan)**

Memilih teknologi WAN bukan soal mencari yang 'terbaik' secara mutlak — melainkan mencocokkan karakteristik teknologi dengan kebutuhan bisnis spesifik pada setiap koneksi.

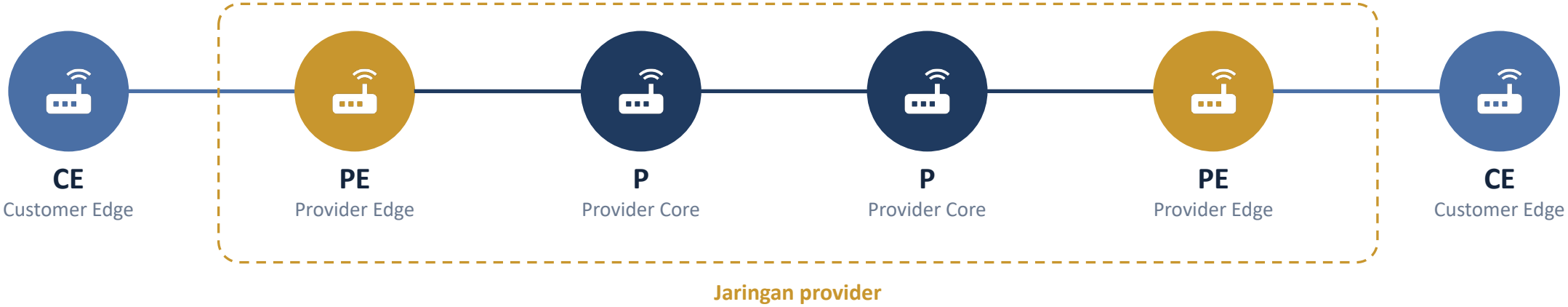
Buku Ajar Enterprise Networking, Bab 13

02

Istilah & spektrum WAN

Siapa memegang apa, dan apa yang dijanjikan provider

CE, PE, P: batas tanggung jawab pelanggan dan provider



CE

Router milik pelanggan, titik keluar-masuk ke WAN

PE

Router provider yang menghubungkan CE

P

Router inti provider antar-PE (khusus MPLS)

SLA

Janji tertulis: bandwidth, uptime, waktu perbaikan

IPsec

Protokol enkripsi & autentikasi trafik IP — dasar VPN

SPEKTRUM TRADE-OFF

Tiga teknologi, tiga titik di spektrum biaya–keandalan

← Biaya rendah, best-effort

Biaya tinggi, terjamin →



VPN site-to-site

Terowongan terenkripsi di atas internet publik

Murah · cepat dipasang · performa tak dijamin

MPLS

Jaringan privat virtual di backbone bersama milik provider

Any-to-any · QoS end-to-end · biaya menengah

Leased line

Sirkuit fisik dedicated antara dua titik

Paling konsisten · paling mahal · tak skalabel

03

Leased line & MPLS

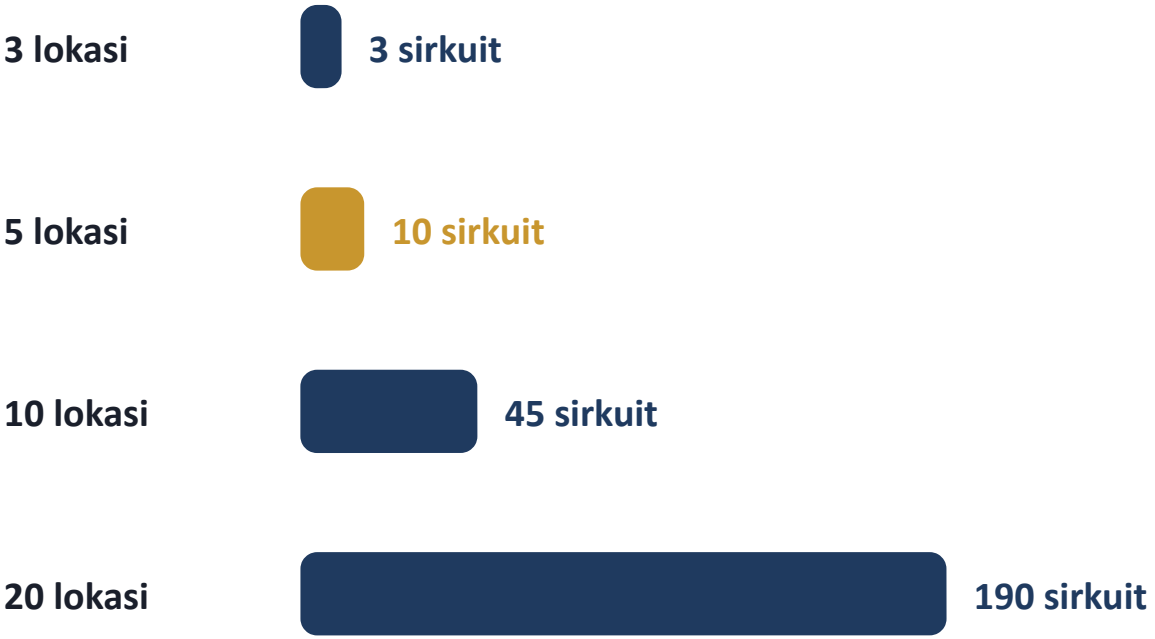
Satu sirkuit per pasangan lokasi, atau satu cloud untuk semua

Andal untuk dua lokasi, mahal untuk banyak lokasi



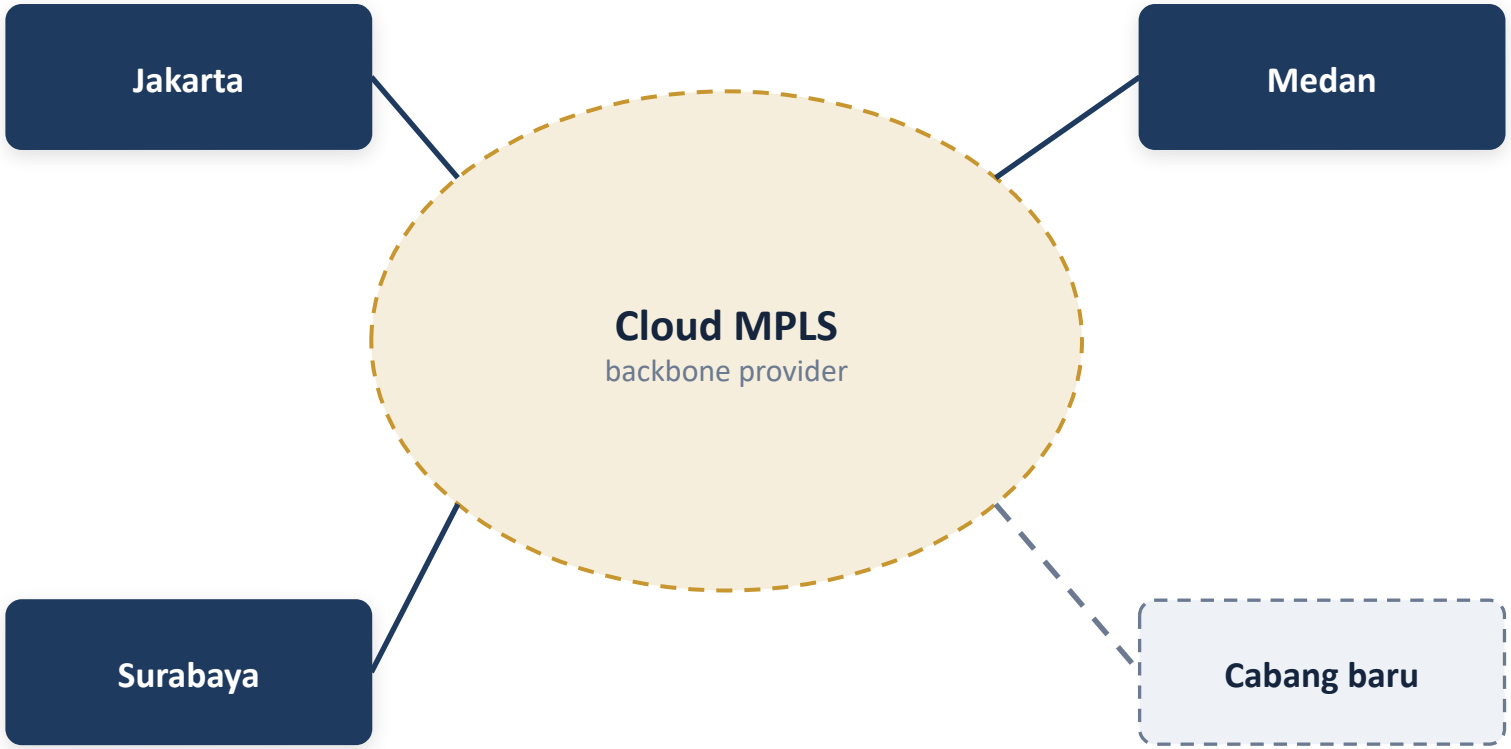
- Bandwidth simetris dijamin
- Latensi sangat konsisten
- Tidak dibagi dengan pelanggan lain
- Biaya tertinggi, instalasi lebih lama

Jumlah sirkuit untuk full mesh = n(n−1)/2



Lima cabang = 10 sirkuit terpisah, masing-masing dengan biaya bulanan.

Satu koneksi per lokasi, semua bisa saling bicara



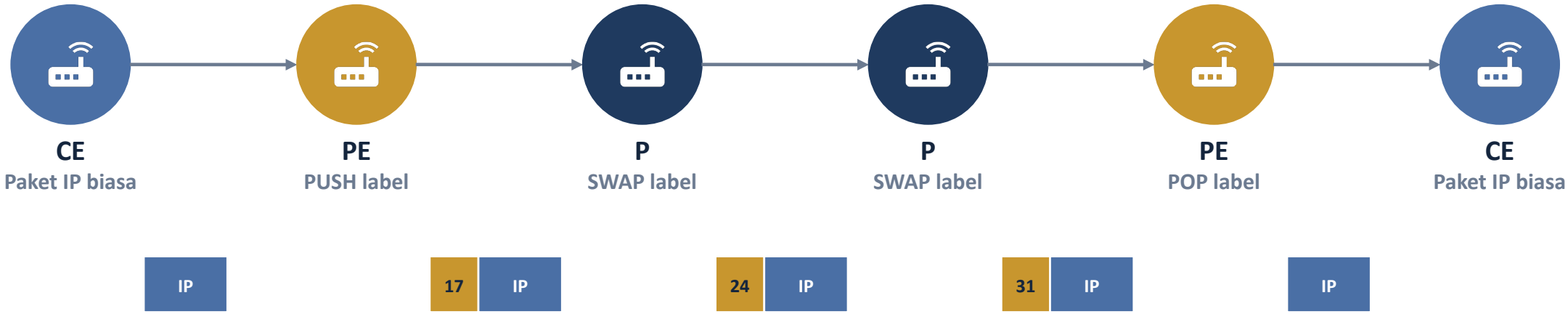
Any-to-any
Setiap lokasi terhubung ke semua lokasi lain lewat satu cloud

Skalabel
Cabang baru cukup satu koneksi ke PE terdekat

QoS end-to-end
Prioritas voice/video (Bab 11) bisa dijaga di backbone

Satu provider
Seluruh cloud bergantung pada satu penyedia

PE menempel & melepas label, P hanya menukar label



Paket di setiap segmen (angka label hanya ilustrasi)

Router P

Hanya membaca & menukar label — tidak memeriksa tabel routing IP lengkap

Label Switched Path

Jalur label yang sudah ditentukan dari PE masuk ke PE keluar

Transparan bagi CE

CE mengirim & menerima paket IP biasa; label tak pernah sampai ke CE

04

VPN site-to-site (IPsec)

Terowongan terenkripsi di atas internet yang tidak dipercaya

Paket asli dienkripsi, lalu dibungkus header publik baru

Paket asli (di LAN)



Di internet (setelah IPsec, tunnel mode)



Yang terlihat di internet
Hanya dua alamat publik router VPN dan header ESP

Yang tersembunyi
Alamat IP privat asli dan seluruh isi payload

Fungsi ESP

Encapsulating Security Payload

Membawa paket asli yang terenkripsi, serta informasi untuk memeriksa keaslian dan integritasnya.

Kenalan & sepakat dulu, baru kirim data

Fase 1
ISAKMP / IKE

Kedua router saling mengautentikasi (mis. pre-shared key) dan membangun saluran aman untuk bernegosiasi.

```
encryption aes 256
authentication pre-share
group 14
```

Verifikasi: `show crypto isakmp sa`

Fase 2
IPsec SA

Menyepakati cara mengenkripsi DATA sebenarnya, lalu trafik 'interesting' mulai dienkripsi.

```
transform-set esp-aes esp-sha-hmac
match address 101
set peer 203.0.113.20
```

Verifikasi: `show crypto ipsec sa`

VPN site-to-site berbasis crypto map

```
! Fase 1
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 14
crypto isakmp key KunciRahasia123
   address 203.0.113.20

! Fase 2
crypto ipsec transform-set TS-VPN
   esp-aes esp-sha-hmac
```

```
! Trafik yang dienkripsi + crypto map
access-list 101 permit ip 192.168.0.0
   0.0.255.255 192.168.99.0 0.0.0.255
crypto map CM-VPN 10 ipsec-isakmp
 set peer 203.0.113.20
 set transform-set TS-VPN
 match address 101
interface gigabitEthernet 0/1
 crypto map CM-VPN
```



Periksa ACL 101: tujuannya 192.168.99.0/24 adalah VLAN 99 Management milik HQ, bukan subnet cabang; sumbernya juga mencakup tujuan itu. Seharusnya: subnet lokal → subnet lokasi lawan.

05

Memilih teknologi WAN

Cocokkan karakteristik teknologi dengan kebutuhan setiap koneksi

PERBANDINGAN

Leased line vs MPLS vs VPN site-to-site

Aspek	Leased line	MPLS	VPN site-to-site
Topologi	Point-to-point (2 lokasi)	Any-to-any dalam cloud	Terowongan di atas internet
Bandwidth & latensi	**Terjamin, paling konsisten**	**Terjamin sesuai SLA**	**Best-effort, bervariasi**
Biaya	**Paling tinggi**	Menengah	**Paling rendah**
Skalabilitas banyak lokasi	**Rendah (n(n–1)/2 sirkuit)**	**Tinggi**	**Tinggi, di mana ada internet**
QoS end-to-end	**Ya**	**Ya**	**Tidak terjamin di internet**
Keamanan	Sirkuit dedicated	Terpisah per pelanggan	Bergantung enkripsi IPsec
Waktu implementasi	**Lama**	Sedang	**Cepat**

Tiga pertanyaan sebelum memilih



Seberapa kritikal trafiknya?
VoIP, video, ERP inti

→ **Butuh jaminan → MPLS atau leased line**



Berapa banyak lokasi?
Dua lokasi vs banyak cabang

→ **Dua → leased line bisa masuk akal; banyak → MPLS**



Seberapa sering jalur dipakai?
Utama vs cadangan / kantor kecil

→ **Jarang atau anggaran ketat → VPN internet**

Jalur utama yang andal, jalur cadangan yang murah



Jalur utama

MPLS atau leased line

Membawa trafik kritikal sehari-hari: voice, video, aplikasi bisnis



Jalur cadangan

VPN site-to-site via internet

Idle sebagian besar waktu, aktif saat jalur utama gagal

Mengapa berlapis?

Keandalan maksimal pada anggaran wajar.

Daripada membayar premium untuk dua jalur mahal, jalur kedua cukup murah karena jarang dipakai. Routing dinamis (OSPF, Bab 4–5) memilih jalur utama lewat cost dan beralih saat gagal.

PRAKTIK TERBAIK

Empat kebiasaan saat memilih & menerapkan WAN

Evaluasi kebutuhan dulu

Bandwidth dan sensitivitas latensi tiap koneksi menentukan teknologinya.

Rancang berlapis

Jalur utama andal + VPN internet sebagai cadangan murah, selaras dengan OSPF.

Negosiasikan SLA jelas

Bandwidth, uptime, dan waktu respons perbaikan untuk leased line & MPLS.

Enkripsi mengikuti standar terkini

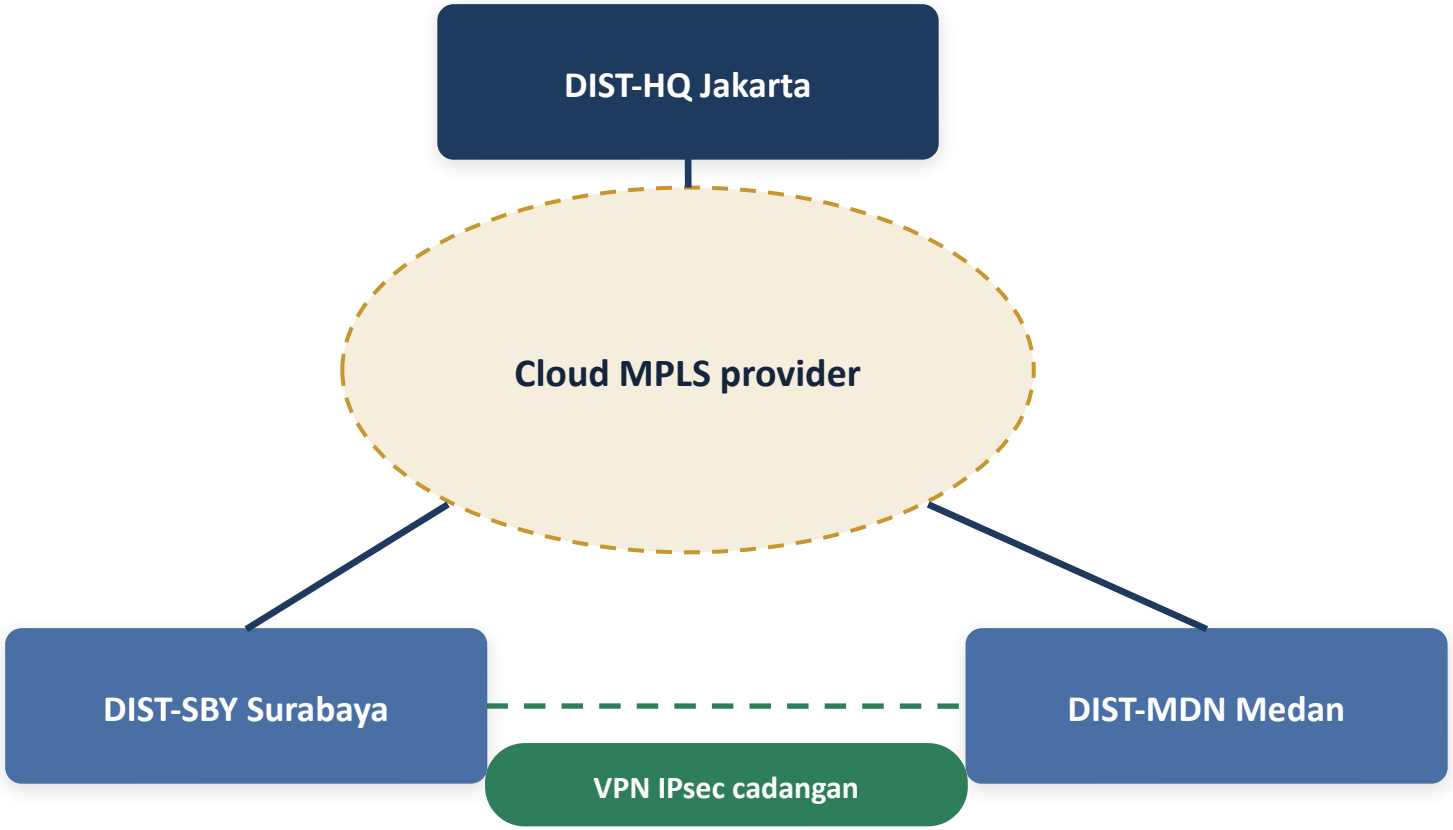
Algoritma & panjang kunci VPN diperbarui; enkripsi lama bisa menjadi rentan.

06

Studi kasus & tugas

Strategi WAN berlapis PT Nusantara Digital Kreasi

MPLS sebagai jalur utama, VPN sebagai cadangan



Mengapa MPLS di jalur utama?

- Any-to-any tanpa sirkuit per pasangan
- QoS end-to-end selaras WAN-QOS (Bab 11)
- Skalabel untuk ekspansi cabang

Mengapa VPN untuk SBY–MDN?

- Hanya dipakai saat failover yang jarang
- Tidak sepadan membayar MPLS tambahan
- OSPF cost memilih MPLS saat normal

PERTANYAAN KRITIS

Bisakah OSPF berjalan di atas VPN crypto map?

Fakta yang perlu dihubungkan

Klaim buku
OSPF otomatis beralih ke VPN cadangan saat MPLS gagal

Cara OSPF menemukan tetangga
Hello dikirim ke alamat multicast 224.0.0.5

Crypto map
Hanya mengenkripsi unicast yang cocok dengan ACL 101; multicast tidak ikut lewat

Akibatnya
Adjacency OSPF tidak terbentuk lewat terowongan — tidak ada rute cadangan untuk dipilih

Diskusikan di kelas

1. Jika adjacency OSPF tidak terbentuk lewat VPN, apa yang terjadi saat link MPLS Surabaya putus?
1. Teknik apa yang membuat VPN bisa membawa trafik routing dinamis? (petunjuk: GRE over IPsec, VTI)
1. Jika DIST-SBY juga menjalankan PAT, apa yang harus dikecualikan?

Kelebihan dan kekurangan tiap teknologi

Leased line

Kelebihan

- Bandwidth & latensi paling terjamin
- Keamanan tinggi: sirkuit dedicated

Kekurangan

- Biaya paling tinggi
- Tidak skalabel, instalasi lama

MPLS

Kelebihan

- Any-to-any efisien
- QoS end-to-end, skalabel

Kekurangan

- Biaya menengah
- Bergantung satu provider

VPN site-to-site

Kelebihan

- Biaya paling rendah
- Cepat dipasang, di mana pun ada internet

Kekurangan

- Best-effort tanpa SLA
- Latensi & jitter bervariasi

Usulkan WAN untuk ekspansi PT NDK

Skenario

PT NDK membuka:

- Cabang Makassar — 60 karyawan, VoIP, video conference, ERP terpusat di Jakarta
- 8 kantor perwakilan kecil — 3–5 orang, email & aplikasi web
- Anggaran WAN terbatas; Makassar tidak boleh putus lebih dari 1 jam

Yang dikumpulkan:

1. Analisis kebutuhan tiap koneksi (bandwidth, latensi, keandalan, biaya, skalabilitas)
1. Usulan teknologi utama & cadangan per lokasi, dengan diagram
1. Argumentasi & laporan tertulis 3–5 halaman

Rubrik penilaian

Ketepatan analisis kebutuhan konektivitas WAN	40%
Kesesuaian usulan teknologi WAN	30%
Kualitas argumentasi & laporan	30%

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

Enam hal yang dibawa pulang

01

WAN menghubungkan LAN yang terpisah jauh lewat infrastruktur milik provider

02

Leased line: sirkuit dedicated, paling terjamin, paling mahal, tak skalabel

03

MPLS: label switching, any-to-any, QoS end-to-end, skalabel

04

Router P hanya membaca label; CE tidak pernah melihat label

05

VPN IPsec: paket asli dienkripsi & dibungkus IP publik baru; dua fase

06

Strategi berlapis: utama andal + VPN cadangan murah

Uji pemahaman

Analisis

Lima cabang butuh saling terhubung dengan anggaran terbatas. Teknologi apa yang masuk akal, dan mengapa bukan leased line penuh?

Analisis

VoIP di jalur VPN buruk saat jam sibuk. Apa penyebab teknisnya, dikaitkan dengan QoS Bab 11?

Teknis

Jelaskan urutan Fase 1 dan Fase 2 pembentukan terowongan IPsec beserta fungsinya.

Reflektif

Kapan organisasi kecil boleh memakai VPN sebagai satu-satunya jalur WAN? Trade-off apa yang diterima?

PERTEMUAN BERIKUTNYA

Pertemuan 14 — Monitoring & Troubleshooting

Jaringan multi-lokasi sudah terbangun. Berikutnya: bagaimana memantaunya dan mendiagnosis gangguan dengan SNMP dan syslog. Sub-CPMK 4.2.

Terima kasih — selamat mengerjakan tugas studi kasus

Referensi

- Buku Ajar Enterprise Networking, Bab 13 — Prodi D3 TK PNP
- Odom, W. (2023). CCNA 200-301 Official Cert Guide, Vol. 1. Cisco Press
- Doyle & Carroll (2021). Routing TCP/IP, Vol. 2, 2nd ed. Cisco Press
- IETF (2005). RFC 4301: Security Architecture for the Internet Protocol
- Cisco NetAcad — ENSA, modul WAN Concepts & VPN