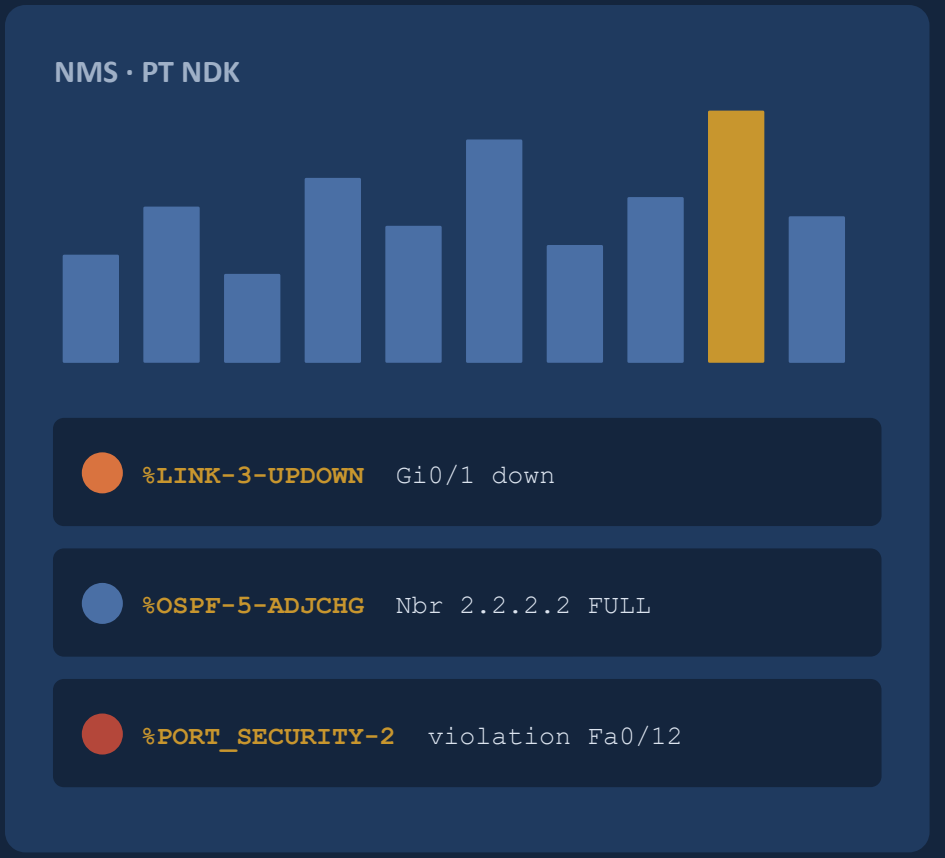
ENTERPRISE NETWORKING · PERTEMUAN 14

Monitoring & Troubleshooting

SNMP dan syslog — dari menunggu keluhan menjadi mendeteksi lebih dulu

Sub-CPMK 4.2 · CPL-8, CPL-11 · Bab 14 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	**Dari reaktif ke proaktif**	Mengapa pemantauan manual tidak cukup
02	**SNMP**	Manager, agent, MIB, OID; polling & trap; versi
03	**Syslog**	Delapan level keparahan dan anatomi pesan
04	**NMS & konfigurasi**	Dashboard terpusat, perintah Cisco IOS, NTP
05	**Metodologi troubleshooting**	Langkah, pendekatan, dan kotak alat perintah
06	**Studi kasus & praktikum**	NMS terpusat PT NDK dan diagnosis gangguan

Setelah pertemuan ini, mahasiswa mampu…

Sub-CPMK 4.2

Mampu melakukan pemantauan (monitoring) dan diagnosis dasar (troubleshooting) jaringan enterprise menggunakan SNMP dan syslog.

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

1
Menjelaskan kebutuhan pemantauan proaktif

2
Menguraikan arsitektur SNMP: polling (GET) dan trap

3
Menjelaskan delapan level keparahan syslog

4
Menjelaskan NMS sebagai penyatu SNMP & syslog

5
Mengonfigurasi SNMP dan syslog di Cisco IOS

6
Menganalisis monitoring terpusat multi-lokasi

01

Dari reaktif ke proaktif

Jangan menunggu pengguna menelepon untuk tahu ada masalah

Login satu per satu ke puluhan perangkat setiap pagi

Reaktif

- Teknisi memeriksa perangkat satu per satu
- Masalah di antara jadwal pemeriksaan terlewat
- Tahu ada gangguan setelah pengguna mengeluh
- Jam-jam downtime yang sebenarnya tidak perlu

Proaktif

- Perangkat melapor sendiri saat ada kejadian
- Status semua lokasi terlihat di satu layar
- Tim IT tahu sebelum pengguna menyadarinya
- Tren data untuk merencanakan kapasitas

'Notifikasi otomatis' yang sudah kita sebut

Bab 6
EtherChannel gagal terbentuk

Bab 7
HSRP failover

Bab 10
Port security violation

Hari ini: mekanismenya.

Jaringan yang tidak dipantau bukanlah jaringan yang bebas masalah — ia hanyalah jaringan yang masalahnya belum diketahui.

Buku Ajar Enterprise Networking, Bab 14

02

SNMP

Simple Network Management Protocol: bertanya berkala, menerima laporan mendadak

SNMP dan syslog: dua alat yang saling melengkapi

SNMP memungkinkan sistem pusat (Manager) memantau — dan pada kasus tertentu mengonfigurasi — perangkat jaringan (Agent) dari jarak jauh.

Syslog mengirim catatan peristiwa (log) dari perangkat ke server terpusat, masing-masing dengan **level keparahan 0–7**.



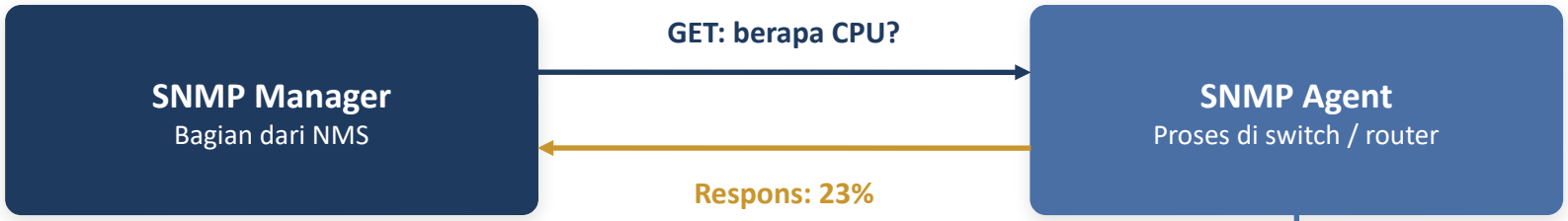
Analogi: rumah sakit

Cek detak jantung berkala → Polling SNMP
Tren dari waktu ke waktu

Alarm darurat berbunyi → Trap SNMP
Kejadian mendadak, langsung dilaporkan

Buku catatan medis berlabel → Syslog
Setiap peristiwa, dari rutin hingga darurat

Manager bertanya, Agent menjawab dari MIB-nya



SNMP Manager Sistem pusat yang melakukan polling dan menerima trap

SNMP Agent Perangkat yang menjalankan SNMP dan menjawab Manager

MIB Management Information Base: kumpulan data status

OID Object Identifier: alamat unik setiap item data

MIB

Struktur data status perangkat; tiap item punya OID unik

sysUpTime
`1.3.6.1.2.1.1.3.0`

ifOperStatus
`1.3.6.1.2.1.2.2.1.8`

Port yang dipakai

`UDP 161`
Manager → Agent (GET)

`UDP 162`
Agent → Manager (trap)

`UDP 514`
Syslog ke server

Dua cara komunikasi, dipakai bersama



Polling (GET)

Manager bertanya berkala, mis. tiap 60 detik

- Ideal untuk tren jangka panjang: grafik CPU, bandwidth
- Masalah baru diketahui paling cepat di polling berikutnya



Trap

Agent langsung melapor tanpa ditanya

- Ideal untuk kejadian mendadak: interface down
- Jauh lebih cepat mendeteksi masalah tiba-tiba

Praktik terbaik: pakai keduanya — polling untuk visibilitas tren, trap untuk respons cepat.

Keamanan adalah pembeda utama

Versi	Autentikasi	Enkripsi	Status
SNMPv1	Community string	**Tidak — teks polos**	Usang
SNMPv2c	Community string	**Tidak — teks polos**	Masih umum, tidak aman untuk produksi
SNMPv3	Username + autentikasi (mis. SHA)	**Ya (mis. AES)**	**Direkomendasikan untuk enterprise**



Community string = kata sandi teks polos. Siapa pun yang menyadap trafik bisa membacanya. Default 'public'/'private' lebih parah: bisa ditebak tanpa menyadap.

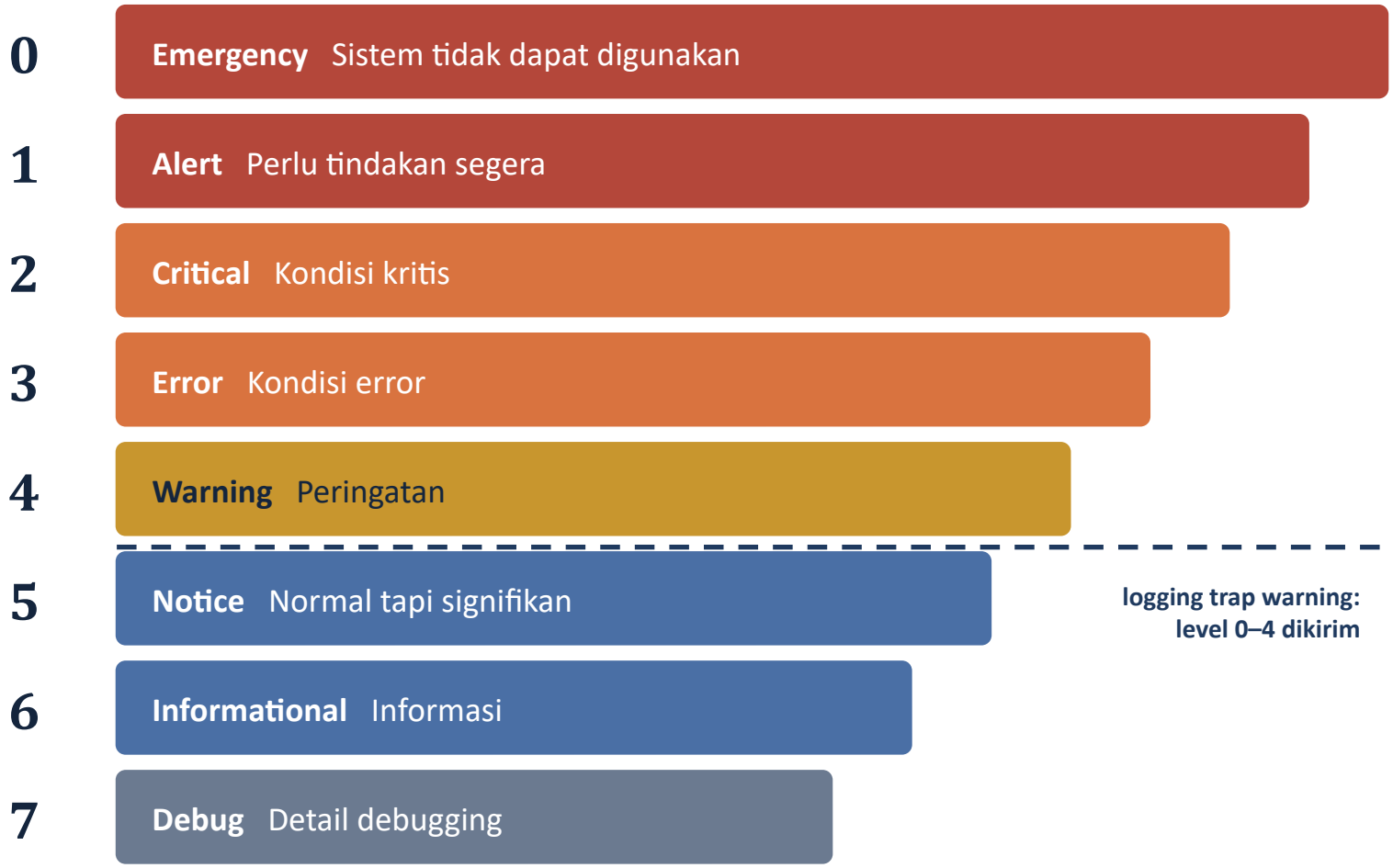
RO vs RW: community RW mengizinkan perangkat diubah lewat SNMP. Berikan hanya jika benar-benar perlu.

03

Syslog

Delapan level keparahan: makin kecil angkanya, makin gawat

0 paling kritis, 7 paling detail



Level 0–1

Mengancam operasional sistem secara keseluruhan

Level 2–4

Perlu perhatian, belum tentu darurat

Level 5–7

Informatif / detail untuk debugging

Angka severity tertulis di dalam nama pesannya

```
*Oct  9 21:30:15.123: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
```

Timestamp
Kapan terjadi — butuh NTP agar akurat

Facility
Sumber: LINK, OSPF, PORT_SECURITY, …

Severity
Angka 0–7 di tengah

Mnemonic
Kode singkat jenis kejadian

Latihan membaca: level berapa, dan apakah terkirim dengan logging trap warning (≤ 4)?

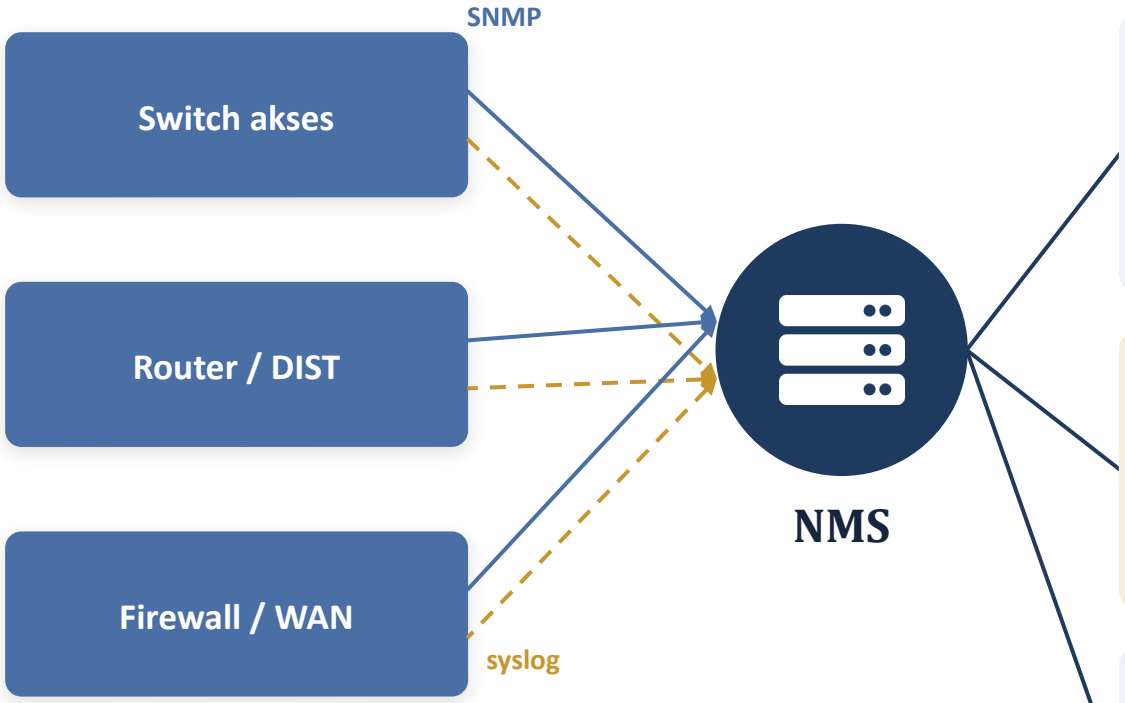
Pesan	Level	Dengan logging trap warning
`%LINK-3-UPDOWN`	3 · Error	Terkirim
`%LINEPROTO-5-UPDOWN`	5 · Notice	Tidak terkirim
`%OSPF-5-ADJCHG`	5 · Notice	Tidak terkirim
`%PORT_SECURITY-2-PSECURE_VIOLATION`	2 · Critical	Terkirim

04

NMS & konfigurasi

Menyatukan SNMP dan syslog, lalu mengonfigurasi setiap perangkat

Satu layar untuk seluruh jaringan



Dashboard real-time
Status seluruh perangkat di semua lokasi dalam satu layar

Notifikasi & alerting
Email, SMS, atau integrasi lain saat kejadian kritis

Riwayat & laporan tren
Dasar perencanaan kapasitas jangka panjang

SNMPv2c dari buku, SNMPv3 untuk produksi

Dari buku ajar (SNMPv2c)

```
snmp-server community NDK-ReadOnly RO
snmp-server host 10.10.10.100
   version 2c NDK-ReadOnly
snmp-server enable traps
snmp-server enable traps snmp linkdown linkup
```

Tambahan: SNMPv3 (autentikasi + enkripsi)

```
snmp-server group NMS-GRP v3 priv
snmp-server user nmsadmin NMS-GRP v3
   auth sha <kata-sandi-auth>
   priv aes 128 <kata-sandi-priv>
```

Verifikasi: `show snmp`



Tambahan praktis: batasi siapa yang boleh bertanya dengan ACL — `snmp-server community NDK-ReadOnly RO 10` (ACL 10 hanya mengizinkan IP server NMS).

Kirim log ke server, dengan waktu yang bisa dipercaya

Dari buku ajar

```
logging host 10.10.10.100
logging trap warning
logging source-interface loopback 0
```

`logging host` Alamat syslog server tujuan

`logging trap warning` Kirim level 0–4 saja

`source-interface loopback 0` Alamat sumber stabil; loopback 0 harus sudah ada

Tambahan: sinkronisasi waktu (NTP)

```
ntp server 10.10.10.1
service timestamps log datetime msec
clock timezone WIB 7
```



Mengapa NTP penting?

Tanpa jam yang sinkron, log dari DIST-HQ, DIST-SBY, dan DIST-MDN tidak bisa diurutkan — kronologi gangguan jadi menyesatkan.

Perintah inti dan saat monitoring tidak bekerja

Perintah	Fungsi
`snmp-server community <str> RO|RW`	Community SNMP read-only / read-write
`snmp-server host <ip> version <v> <str>`	Alamat Manager penerima trap
`snmp-server enable traps`	Mengaktifkan pengiriman trap
`logging host <ip>`	Alamat syslog server
`logging trap <level>`	Level minimum yang dikirim ke server
`show logging` · `show snmp`	Buffer log lokal & status SNMP

Trap / log tidak sampai?

1. Community string Manager ≠ Agent
1. ACL memblokir UDP 161/162/514
1. Server tidak terjangkau (ping, rute)
1. logging trap terlalu ketat untuk level yang diharapkan
1. Trap belum diaktifkan (enable traps) atau host belum diset

Empat kebiasaan dari buku ajar

SNMPv3 di produksi

Autentikasi dan enkripsi, bukan community string teks polos.

Community sulit ditebak

Bukan 'public'/'private'; RW hanya bila benar-benar perlu.

logging trap warning / error

Seimbang antara visibilitas dan volume pesan yang bisa dikelola.

Sinkronkan waktu dengan NTP

Sebelum mengandalkan timestamp untuk menyusun kronologi.

05

Metodologi troubleshooting

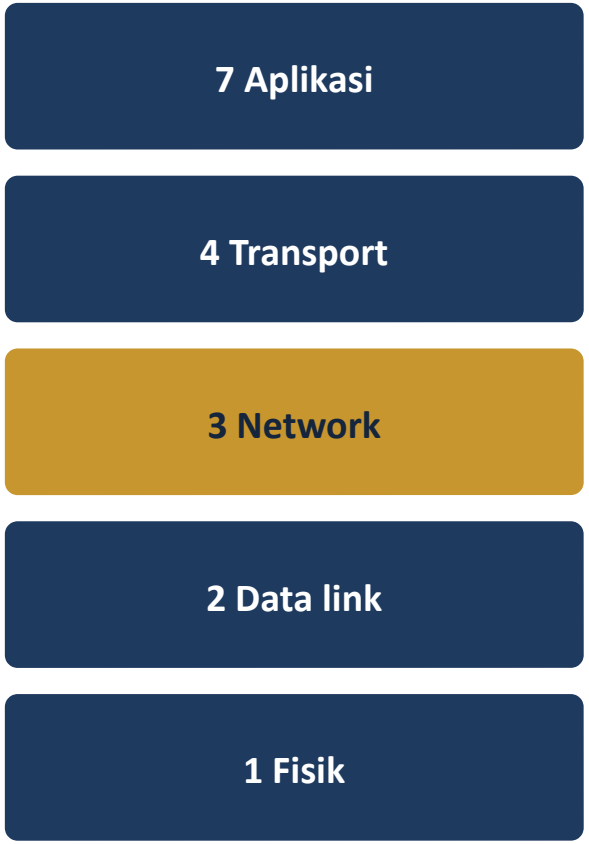
Tambahan untuk praktikum: mendiagnosis gangguan secara sistematis

Enam langkah dari gejala sampai dokumentasi



Kalau hipotesis salah: kembalikan perubahan, lalu kembali ke langkah 3. Jangan menumpuk perubahan yang belum terbukti.

Mulai dari mana? Tiga pendekatan berbasis layer OSI



Bottom-up Mulai dari layer 1 ke atas: kabel, status port, VLAN, IP…

Cocok saat gejala menunjukkan masalah fisik/link, atau penyebabnya belum jelas sama sekali

Top-down Mulai dari aplikasi ke bawah

Cocok saat hanya satu aplikasi yang bermasalah sementara lainnya normal

Divide & conquer Mulai dari tengah (mis. ping di layer 3), lalu naik atau turun

Paling cepat untuk teknisi berpengalaman: satu ping membelah masalah jadi dua

Perintah verifikasi sepanjang semester

Layer 1–2

`show interfaces status`
Port up/down, err-disabled

`show vlan brief` · `show interfaces trunk`
VLAN & trunk (P2)

`show spanning-tree` · `show etherchannel summary`
STP & EtherChannel (P6)

`show port-security`
Violation (P10)

Layer 3

`ping` · `traceroute`
Jangkauan & jalur

`show ip route`
Rute ada? (P3–P5)

`show ip ospf neighbor`
Adjacency OSPF (P4–P5)

`show standby brief`
HSRP (P7)

Layanan & monitoring

`show access-lists`
Counter ACL (P9)

`show policy-map interface`
QoS (P11)

`show ip nat translations`
NAT/PAT (P12)

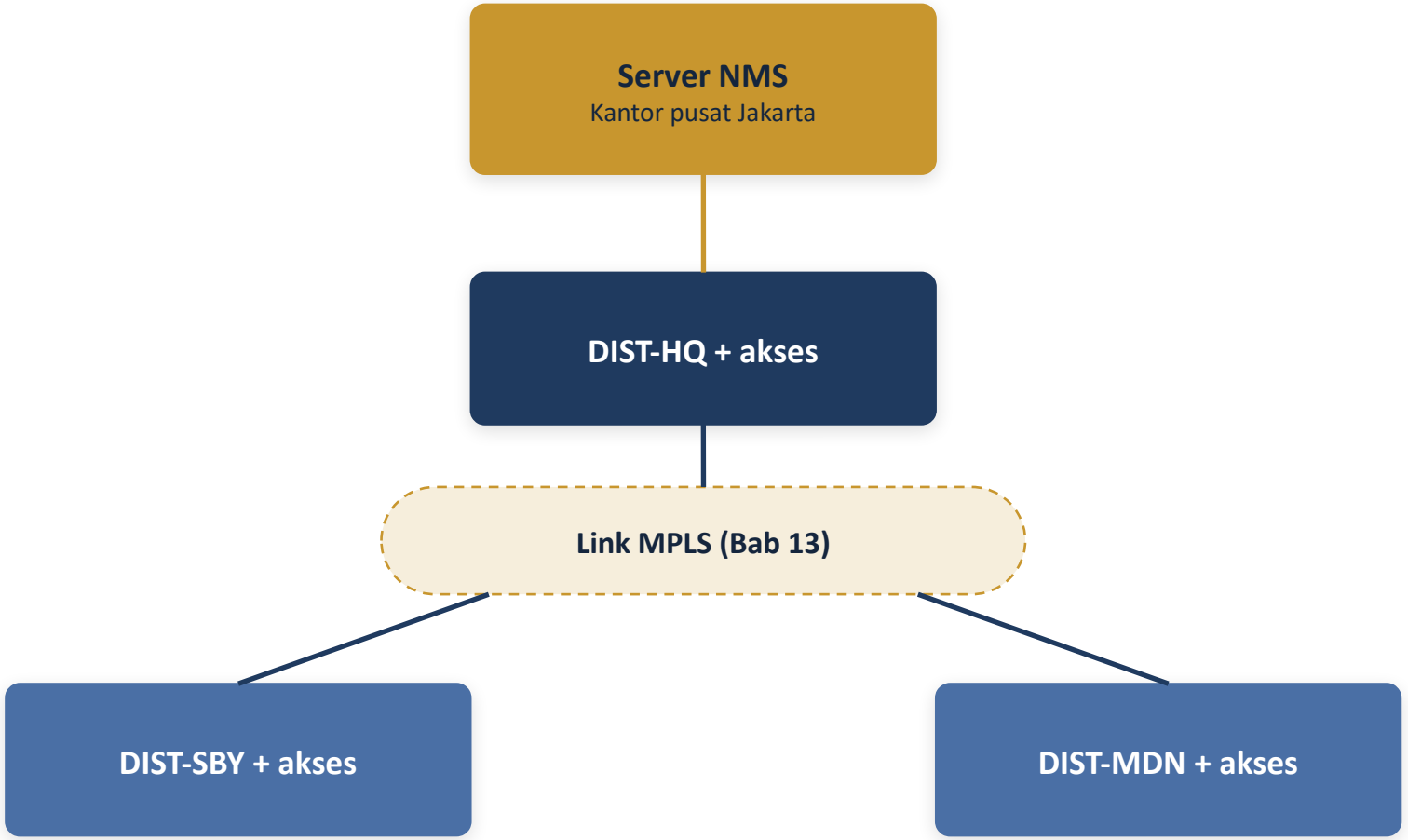
`show logging`
Jejak kejadian (P14)

06

Studi kasus & praktikum

NMS terpusat PT Nusantara Digital Kreasi

Satu NMS di Jakarta memantau tiga kota



Trap SNMP
Gi0/1 DIST-SBY down → tim IT di Jakarta tahu dalam hitungan detik

Syslog
Setiap port security violation tercatat di dashboard — jejak audit tanpa login ke switch

Polling SNMP
Tren CPU & bandwidth WAN → upgrade kapasitas sebelum jadi bottleneck

PERTANYAAN KRITIS

Bagaimana trap keluar lewat link yang baru saja putus?

Telusuri kejadiannya

Jika Gi0/1 DIST-SBY adalah link ke MPLS
Satu-satunya jalan menuju NMS di Jakarta

Trap linkDown & syslog dibuat
Tapi dikirim lewat UDP — tanpa konfirmasi, tanpa kirim ulang

Jalur ke Jakarta sudah putus
Pesan hilang; VPN cadangan pun belum tentu membawa rute (P13)

Lalu bagaimana Jakarta tahu?
Polling berikutnya ke DIST-SBY tidak dijawab

Diskusikan di kelas

1. Mengapa 'tidak ada jawaban polling' justru informasi yang berharga?
1. Di mana log kejadian itu masih bisa ditemukan setelah link pulih?
1. Bagaimana desain monitoring bisa dibuat lebih tahan terhadap kasus seperti ini?

Kelebihan dan tantangan monitoring terpusat

Kelebihan

- Dari reaktif menjadi proaktif
- Notifikasi hampir real-time
- Data historis untuk perencanaan kapasitas
- Satu dashboard, tanpa login manual

Tantangan

- SNMPv1/v2c tanpa enkripsi berisiko
- Volume data besar butuh penyimpanan
- Konfigurasi tak konsisten → visibilitas timpang
- NMS sendiri titik kegagalan kritis

Prinsip desain

Standar sejak awal, aman, dan redundan.

Konfigurasi monitoring seragam di semua perangkat, SNMPv3 dengan akses terbatas, dan NMS yang tidak menjadi titik kegagalan tunggal — ia 'mata dan telinga' seluruh jaringan.

Konfigurasi monitoring, lalu diagnosis gangguan

1. Pakai topologi gabungan (VLAN, OSPF, HSRP, ACL, NAT) + 1 server NMS/syslog
2. Syslog: logging host & trap warning; cek pesan masuk di server
3. SNMP: community RO + host; query sysUpTime/interface dari NMS
4. Dosen menyisipkan 3–4 gangguan (mis. port shutdown, VLAN salah, ACL salah, NAT terbalik)
5. Diagnosis dengan log + kotak alat; satu perubahan per pengujian
6. Dokumentasi: gejala, hipotesis, bukti perintah, perbaikan, verifikasi

Rubrik penilaian

Rancangan skema monitoring	20%
Keberhasilan konfigurasi & troubleshooting	40%
Pengujian diagnosis gangguan	20%
Kelengkapan dokumentasi	20%

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

Enam hal yang dibawa pulang

01

Pemantauan proaktif wajib untuk jaringan enterprise berskala besar

02

SNMP: Manager–Agent–MIB–OID; polling untuk tren, trap untuk kejadian mendadak

03

SNMPv3 mengenkripsi; v1/v2c mengirim community dalam teks polos

04

Syslog 0–7: makin kecil makin kritis; level ada di %FACILITY-SEV-MNEMONIC

05

NMS: dashboard, alerting, laporan tren — dan perlu redundansi

06

Troubleshooting: gejala → isolasi → hipotesis → uji → perbaiki → catat

Uji pemahaman sebelum praktikum

Analisis

Perangkat tidak mengirim trap meski sudah dikonfigurasi. Sebutkan tiga kemungkinan penyebab.

Analisis

Syslog server kebanjiran ribuan pesan tidak relevan per menit. Konfigurasi apa yang disesuaikan?

Konfigurasi

Tulis perintah syslog untuk mengirim level Error (3) ke atas ke server 172.16.1.50.

Reflektif

Mengapa NMS sendiri perlu redundansi? Apa risikonya jika NMS tunggal gagal?

PERTEMUAN BERIKUTNYA

Pertemuan 15 — Proyek Kolaboratif

Saatnya menyatukan semuanya: merancang, mengonfigurasi, mendokumentasikan, dan mempresentasikan jaringan enterprise terintegrasi dalam tim. Sub-CPMK 4.3.

Terima kasih — sampai jumpa di laboratorium

Referensi

- Buku Ajar Enterprise Networking, Bab 14 — Prodi D3 TK PNP
- IETF (2009). RFC 5424: The Syslog Protocol
- IETF (2002). RFC 3411: SNMP Management Frameworks
- Odom, W. (2023). CCNA 200-301 Official Cert Guide, Vol. 1. Cisco Press
- Cisco NetAcad — ENSA, modul Network Management & Troubleshooting