TRK — ENTERPRISE NETWORKING • PERTEMUAN 2

Virtual LAN (VLAN) dan Trunking IEEE 802.1Q

Segmentasi Jaringan dan Konektivitas Antar-Switch — Sub-CPMK 1.2



Program Studi D3 — Teknik Komputer
Politeknik Negeri Padang

Dosen Pengampu: Ir. H. A. Mooduto, M.Kom. & Ideva Gaputra, S.Kom., M.Kom.

PETA KONSEP PERTEMUAN

Alur Pembahasan Hari Ini

Melanjutkan Bab 1: dari kebutuhan segmentasi menuju mekanisme VLAN & trunking IEEE 802.1Q.

01

Mengapa Perlu VLAN?

Satu switch fisik, banyak broadcast domain terpisah — bagaimana caranya?

02

Definisi & Jenis VLAN

Data, default, native, management, voice VLAN

03

Access Port vs Trunk Port

Mode konfigurasi port switch dan fungsinya masing-masing

04

Tagging IEEE 802.1Q

Struktur TPID, PCP, DEI, VID pada frame Ethernet

05

Native VLAN & Keamanan

Risiko VLAN hopping dan praktik terbaik mitigasinya

06

Konfigurasi & Studi Kasus

Praktik CLI serta implementasi VLAN PT Nusantara Digital Kreasi

CAPAIAN PEMBELAJARAN

Sub-CPMK 1.2 & Tujuan Pembelajaran

Sub-CPMK 1.2 Mampu mengonfigurasi VLAN dan trunking (802.1Q) untuk segmentasi jaringan enterprise. (Mendukung CPL-2, CPL-8)

1. Menjelaskan konsep VLAN sebagai mekanisme segmentasi broadcast domain, beserta jenis-jenisnya (data, native, default, management, voice).
2. Membedakan fungsi access port dan trunk port pada switch, serta kapan masing-masing digunakan.
3. Menguraikan mekanisme tagging IEEE 802.1Q pada frame Ethernet, termasuk struktur TPID, PCP, DEI, dan VLAN ID.
4. Menjelaskan konsep dan risiko keamanan terkait native VLAN pada trunk link.
5. Mengonfigurasi VLAN, access port, dan trunk port secara konseptual menggunakan perintah dasar Cisco IOS.
6. Menganalisis penerapan segmentasi VLAN pada studi kasus organisasi nyata.

PENDAHULUAN

Satu Switch, Tiga Divisi — Bagaimana Memisahkannya?

Pada Bab 1, **PT Nusantara Digital Kreasi** merancang ulang jaringannya dengan rencana segmentasi VLAN untuk memisahkan Divisi Keuangan, Umum, dan Tamu/Guest. Namun satu pertanyaan teknis belum terjawab:

> *Bagaimana caranya satu switch fisik yang sama dapat melayani tiga broadcast domain yang benar-benar terpisah? Dan bagaimana switch akses dapat 'berbicara' dengan switch distribusi menggunakan tiga VLAN sekaligus, padahal di antara keduanya hanya ada satu kabel fisik?*

Jawabannya: Virtual LAN (VLAN) untuk segmentasi logis, dan trunking IEEE 802.1Q untuk membawa banyak VLAN melalui satu link fisik.

Tanpa VLAN: setiap segmen butuh switch fisik terpisah. Tanpa trunking: setiap VLAN butuh kabel sendiri antar-switch.

KONSEP DASAR

Definisi VLAN & Analogi Interkom Gedung

Virtual LAN (VLAN) — metode membagi satu jaringan fisik menjadi beberapa broadcast domain logis yang terpisah, tanpa memerlukan switch fisik terpisah untuk setiap segmen. Lalu lintas broadcast, multicast, dan unknown-unicast pada satu VLAN tidak diteruskan ke VLAN lain kecuali melalui perangkat Layer 3.

Analogi: Sistem Interkom Gedung

Tanpa pembagian, pengumuman dari lantai mana pun terdengar di seluruh gedung — persis seperti broadcast pada jaringan flat.

Dengan VLAN, gedung dibagi menjadi beberapa 'saluran interkom' independen: pengumuman Divisi Keuangan hanya terdengar oleh ruangan yang terhubung ke saluran itu — meski kabel fisiknya tetap berbagi jalur yang sama di dalam dinding.

Prinsip Kunci

- Pemisahan terjadi secara logis, bukan dengan menarik kabel fisik baru
- Keanggotaan VLAN umumnya ditentukan berdasarkan port (port-based VLAN)
- Pendekatan port-based paling umum di industri karena kesederhanaannya, dibanding berbasis MAC address/protokol

Jenis-Jenis VLAN dalam Arsitektur Enterprise

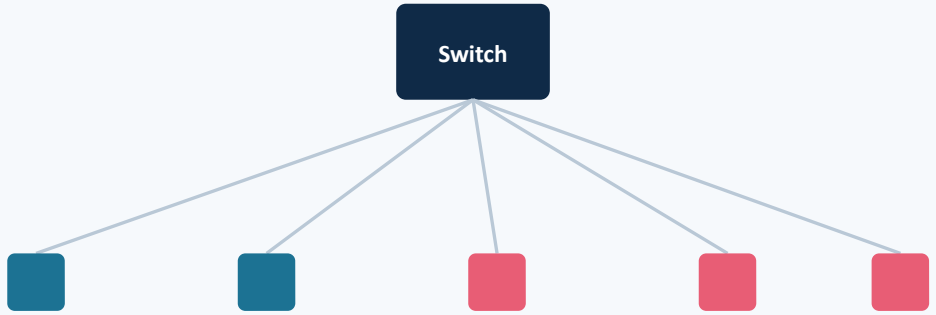
Jenis VLAN	Fungsi	Contoh
Data VLAN	Membawa lalu lintas data pengguna biasa (dokumen, aplikasi bisnis, web browsing)	VLAN 10 (Umum), VLAN 20 (Keuangan)
Default VLAN	VLAN bawaan pabrik pada semua port switch Cisco sebelum dikonfigurasi ulang	Selalu VLAN 1
Native VLAN	VLAN pada trunk link yang lalu lintasnya TIDAK diberi tag 802.1Q	Diarahkan ke VLAN khusus, bukan VLAN 1
Management VLAN	Membawa lalu lintas manajemen perangkat (akses SSH/Telnet ke switch)	VLAN 99
Voice VLAN	Membawa lalu lintas telepon IP, sering diprioritaskan dengan QoS	VLAN 50

Keanggotaan VLAN pada switch umumnya ditentukan berdasarkan port (port-based VLAN) — setiap port fisik dikonfigurasi menjadi anggota satu VLAN tertentu.

Segmentasi Broadcast Domain dengan VLAN

TANPA VLAN

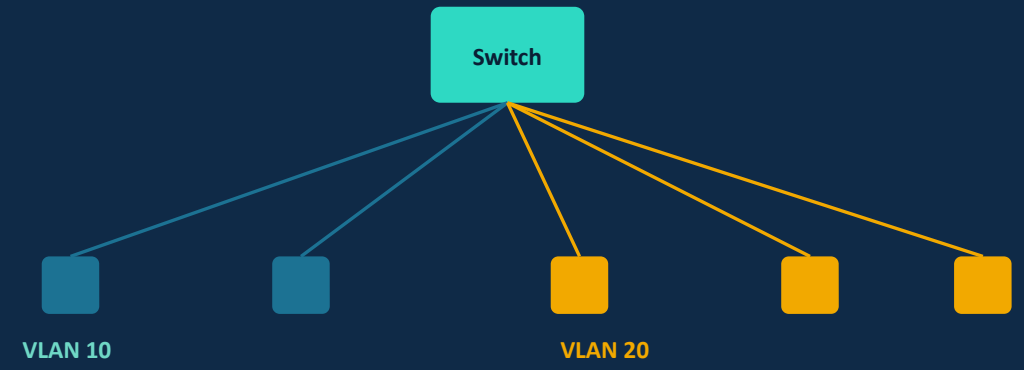
Satu Broadcast Domain Tunggal



Broadcast dari komputer Umum diteruskan ke SELURUH port — termasuk ke komputer Keuangan yang tidak berkepentingan.

DENGAN VLAN

Dua Broadcast Domain Terpisah



Broadcast dari VLAN 10 hanya beredar di antara anggota VLAN 10 — sama sekali tidak terlihat oleh port anggota VLAN 20.

Access Port vs. Trunk Port

Access Port

Anggota satu VLAN tunggal. Menghubungkan perangkat pengguna akhir (PC, printer, AP). Frame yang lewat TIDAK membawa tag VLAN.

Trunk Port

Membawa banyak VLAN sekaligus melalui satu link fisik. Menghubungkan switch-ke-switch atau switch-ke-router. Setiap frame diberi tag, kecuali dari native VLAN.



Tanpa trunking, skenario ini memerlukan TIGA kabel fisik terpisah antar-switch — satu untuk setiap VLAN.

Mekanisme Tagging IEEE 802.1Q

Empat byte tambahan (tag 802.1Q) disisipkan tepat setelah field Source MAC Address pada frame Ethernet standar.



↑ Disisipkan di sini, setelah Source MAC Address

TPID

16 bit

Tag Protocol Identifier — nilai tetap 0x8100 yang menandakan frame ini membawa tag 802.1Q.

PCP

3 bit

Priority Code Point — menandakan prioritas QoS frame saat terjadi kongesti.

DEI

1 bit

Drop Eligible Indicator — menandakan apakah frame boleh dibuang lebih dulu saat jaringan padat.

VID

12 bit

VLAN Identifier — menyimpan nomor VLAN asal frame (1–4094; 0 dan 4095 dicadangkan).

Native VLAN & Risiko VLAN Hopping

Pengecualian penting: frame dari native VLAN melintasi trunk link TANPA tag sama sekali. Dirancang untuk kompatibilitas dengan perangkat lama, namun pada praktiknya menjadi celah keamanan yang dikenal sebagai **VLAN hopping** — penyerang dapat mengirim frame yang memanfaatkan ketiadaan tag untuk 'melompat' antar-VLAN.

Mengapa Berisiko?

Tag 802.1Q hanya ada selama frame melintasi trunk link antar-switch. Begitu sampai di access port menuju pengguna akhir, tag dilepas — perangkat pengguna tidak pernah melihat tag VLAN.

Namun karena native VLAN tidak ditandai sama sekali, penyerang dapat menyisipkan tag palsu untuk mengelabui switch agar mengira frame berasal dari VLAN lain.

Praktik Terbaik Mitigasi

- Arahkan native VLAN pada SELURUH trunk ke satu VLAN khusus (mis. VLAN 999), bukan VLAN 1 default
- Pastikan VLAN khusus tersebut tidak memiliki anggota access port sama sekali
- Nonaktifkan Dynamic Trunking Protocol (DTP) dengan switchport nonegotiate
- Batasi VLAN yang diizinkan pada trunk (switchport trunk allowed vlan)

Konfigurasi VLAN & Trunk pada Cisco IOS

```
! Membuat VLAN
Switch(config)# vlan 10
Switch(config-vlan)# name UMUM
Switch(config)# vlan 20
Switch(config-vlan)# name KEUANGAN
! Access port
Switch(config)# interface gi0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
! Trunk port
Switch(config)# interface gi0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 99
Switch(config-if)# switchport trunk allowed vlan 10,20,99
! Verifikasi
Switch# show vlan brief
Switch# show interfaces trunk
```

Referensi Perintah

`vlan <id>`

Membuat VLAN baru pada database VLAN switch

`switchport access vlan <id>`

Menetapkan VLAN anggota untuk access port

`switchport mode trunk`

Menetapkan port sebagai trunk port

`switchport trunk native vlan <id>`

Menetapkan native VLAN pada trunk

`switchport trunk allowed vlan <daftar>`

Membatasi VLAN yang diizinkan melintasi trunk

`switchport nonegotiate`

Menonaktifkan DTP pada trunk manual

`show vlan brief / show interfaces trunk`

Verifikasi VLAN & status trunk

Praktik Konfigurasi & Kesalahan Umum

Praktik Konfigurasi Umum

1. Nonaktifkan DTP (switchport nonegotiate) pada trunk yang dikonfigurasi manual
2. Batasi VLAN yang diizinkan pada tiap trunk hanya untuk VLAN yang benar-benar diperlukan
3. Arahkan native VLAN seluruh trunk ke satu VLAN khusus yang konsisten (mis. VLAN 999)
4. Dokumentasikan pemetaan VLAN ID terhadap fungsi/divisi pada tabel referensi terpusat

VLAN Mismatch — Kesalahan Tersering

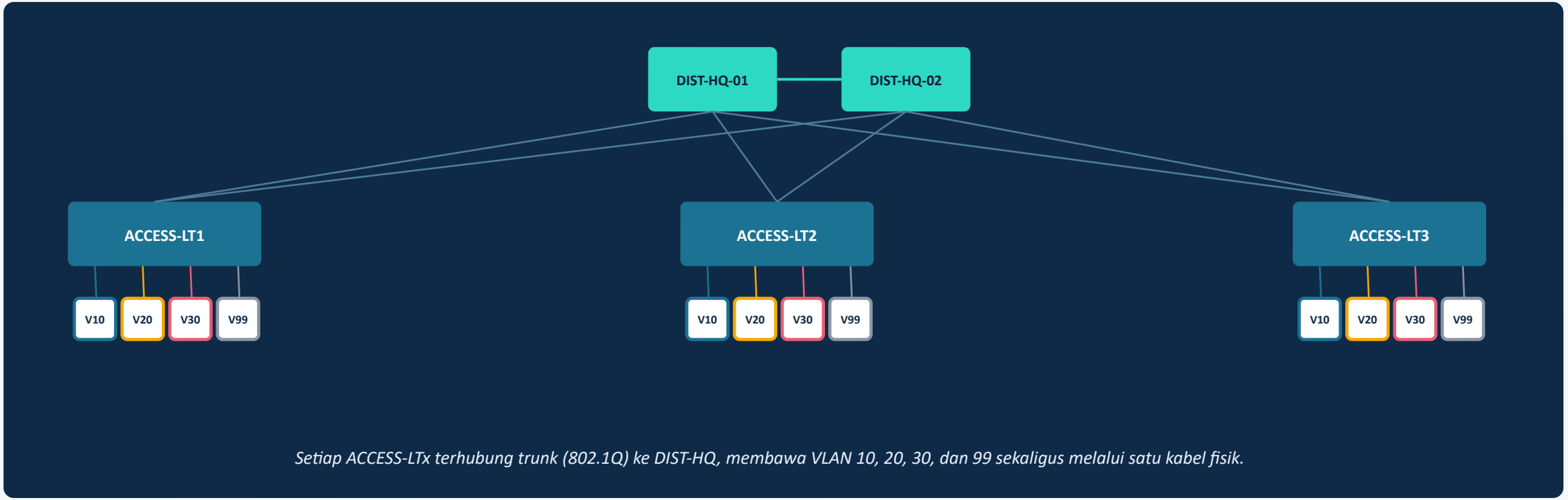
Terjadi ketika native VLAN pada kedua ujung trunk link berbeda — misalnya SWITCH-A menggunakan native VLAN 99, sementara SWITCH-B masih default VLAN 1.

Akibat: peringatan pada log switch dan potensi kebocoran lalu lintas antar-VLAN yang tidak disengaja.

Verifikasi wajib: show interfaces trunk
pada KEDUA ujung link setelah konfigurasi.

Implementasi VLAN di Kantor Pusat PT Nusantara Digital Kreasi

Tiga switch akses (per lantai) terhubung trunk ke pasangan switch distribusi redundan DIST-HQ-01/02 dari Bab 1, membawa VLAN 10 (Umum), 20 (Keuangan), 30 (Tamu/Guest), dan 99 (Management/Native).



Setiap ACCESS-LTx terhubung trunk (802.1Q) ke DIST-HQ, membawa VLAN 10, 20, 30, dan 99 sekaligus melalui satu kabel fisik.

Kelebihan, Kekurangan & Pertimbangan Desain

Kelebihan

- Efisiensi infrastruktur — satu switch & trunk melayani banyak segmen logis
- Keamanan berlapis — isolasi broadcast domain antar-divisi
- Fleksibilitas penempatan — keanggotaan ditentukan konfigurasi port, bukan lokasi kabel
- Kemudahan pengelolaan — QoS/ACL berbeda untuk tiap segmen

Kekurangan & Tantangan

- Kompleksitas konfigurasi bertambah pada jaringan berskala besar (puluhan VLAN)
- Risiko keamanan VLAN hopping jika native VLAN tidak dikonfigurasi hati-hati
- Komunikasi antar-VLAN memerlukan perangkat Layer 3 tambahan (dibahas Bab 3)
- VLAN mismatch pada trunk dapat menyebabkan gangguan yang sulit dilacak

RANGKUMAN

Poin-Poin Kunci Pertemuan Ini

1. VLAN membagi satu jaringan fisik menjadi beberapa broadcast domain logis terpisah
2. Lima jenis VLAN: data, default (selalu VLAN 1), native, management, voice
3. Access port = satu VLAN tanpa tag; trunk port = banyak VLAN dengan tag, kecuali native VLAN
4. IEEE 802.1Q menyisipkan tag 4 byte (TPID, PCP, DEI, VID) setelah Source MAC Address
5. Native VLAN berisiko VLAN hopping — arahkan ke VLAN khusus, bukan VLAN 1
6. Konfigurasi VLAN: buat VLAN pada database, lalu tetapkan mode access/trunk per port
7. VLAN mismatch adalah kesalahan tersering — wajib verifikasi show interfaces trunk di kedua ujung

AKTIVITAS PEMBELAJARAN

Praktikum Lab: Konfigurasi VLAN & Trunk

Metode: Ceramah, Demonstrasi & Praktikum Lab | **Waktu:** 270 menit

Pengalaman Belajar Mahasiswa

Mengonfigurasi VLAN dan trunk link pada simulator jaringan (Cisco Packet Tracer/GNS3) sesuai topologi yang diberikan, kemudian menguji konektivitas antar-perangkat.

Kriteria & Indikator Penilaian

Ketepatan konfigurasi VLAN & trunk; keberhasilan pengujian konektivitas antar-VLAN sejenis

- Bobot 2% dari total nilai
- CPL-2, CPL-8

Instruksi Praktikum

1. Buka topologi latihan pada Packet Tracer/GNS3 (2 switch, 6 PC)
2. Buat VLAN 10, 20, dan 99 pada kedua switch beserta penamaannya
3. Konfigurasikan access port sesuai pemetaan VLAN yang diberikan
4. Konfigurasikan trunk port antar-switch dengan native VLAN 99
5. Uji konektivitas: PC pada VLAN sama harus terhubung, PC beda VLAN tidak
6. Verifikasi dengan show vlan brief dan show interfaces trunk



TERIMA KASIH

Sampai Jumpa di Bab 3: Inter-VLAN Routing

Referensi Utama

Cisco Systems (2023). CCNA 200-301 Official Cert Guide. Cisco Press.
Froom, Frahim & Sivasubramanian (2022). Implementing Cisco IP Switched Networks (SWITCH). Cisco Press.
Lammle, T. (2021). CCNA Routing and Switching Complete Study Guide (3rd ed.). Sybex.
Odom, W. (2023). CCNA 200-301 Official Cert Guide, Vol. 1 (2nd ed.). Cisco Press.