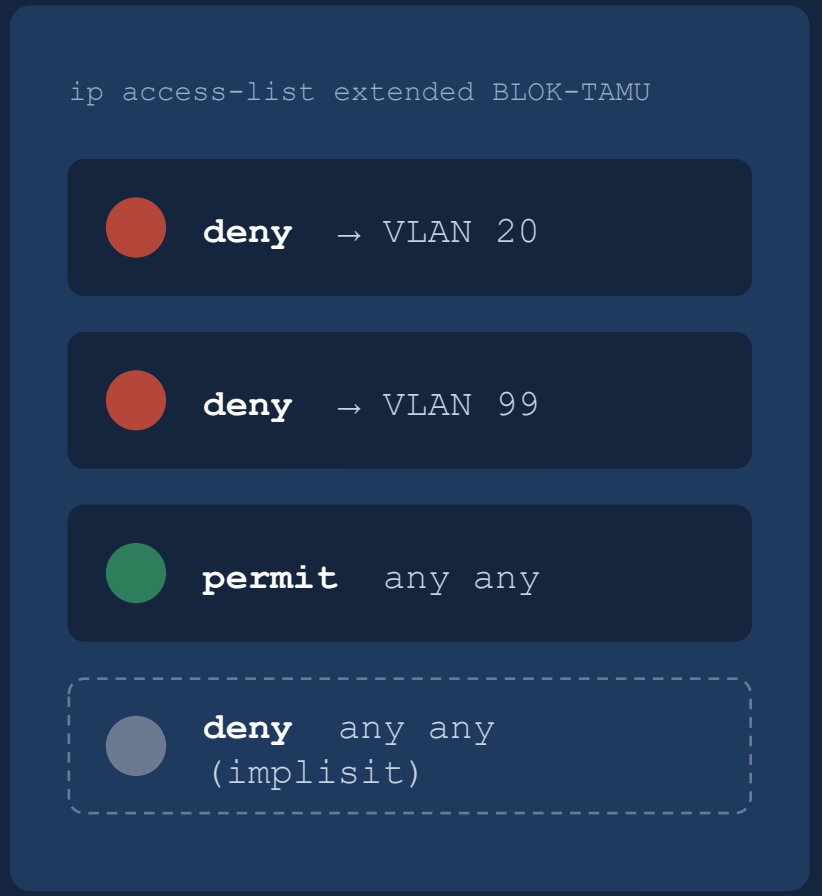
ENTERPRISE NETWORKING · PERTEMUAN 9

Access Control List (ACL)

Standard & Extended — menyaring lalu lintas antar-VLAN dan antar-jaringan

Sub-CPMK 3.1 · CPL-8, CPL-11 · Bab 9 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	**Terhubung ≠ aman**	Celah keamanan sejak inter-VLAN routing
02	**Konsep ACL**	Permit/deny, implicit deny, jenis ACL
03	**Cara kerja ACL**	Top-down, penempatan, arah in/out
04	**Wildcard mask**	Menentukan cakupan alamat IP
05	**Konfigurasi Cisco IOS**	Standard, Extended, verifikasi, praktik terbaik
06	**Studi kasus & praktikum**	Membatasi VLAN Tamu di PT NDK

Setelah pertemuan ini, mahasiswa mampu…

Sub-CPMK 3.1

Mampu merancang dan menerapkan Access Control List (ACL) standar dan extended untuk keamanan jaringan enterprise.

CPL-8 · CPL-11
Bobot tugas: 2,5% nilai akhir

1
Menjelaskan konsep ACL dan logika top-down dengan implicit deny

2
Membedakan Standard dan Extended ACL beserta aturan penempatannya

3
Menghitung dan menerapkan wildcard mask

4
Menjelaskan arah pemrosesan ACL: inbound dan outbound

5
Mengonfigurasi Standard dan Extended ACL di Cisco IOS

6
Menganalisis ACL untuk membatasi akses antar-VLAN

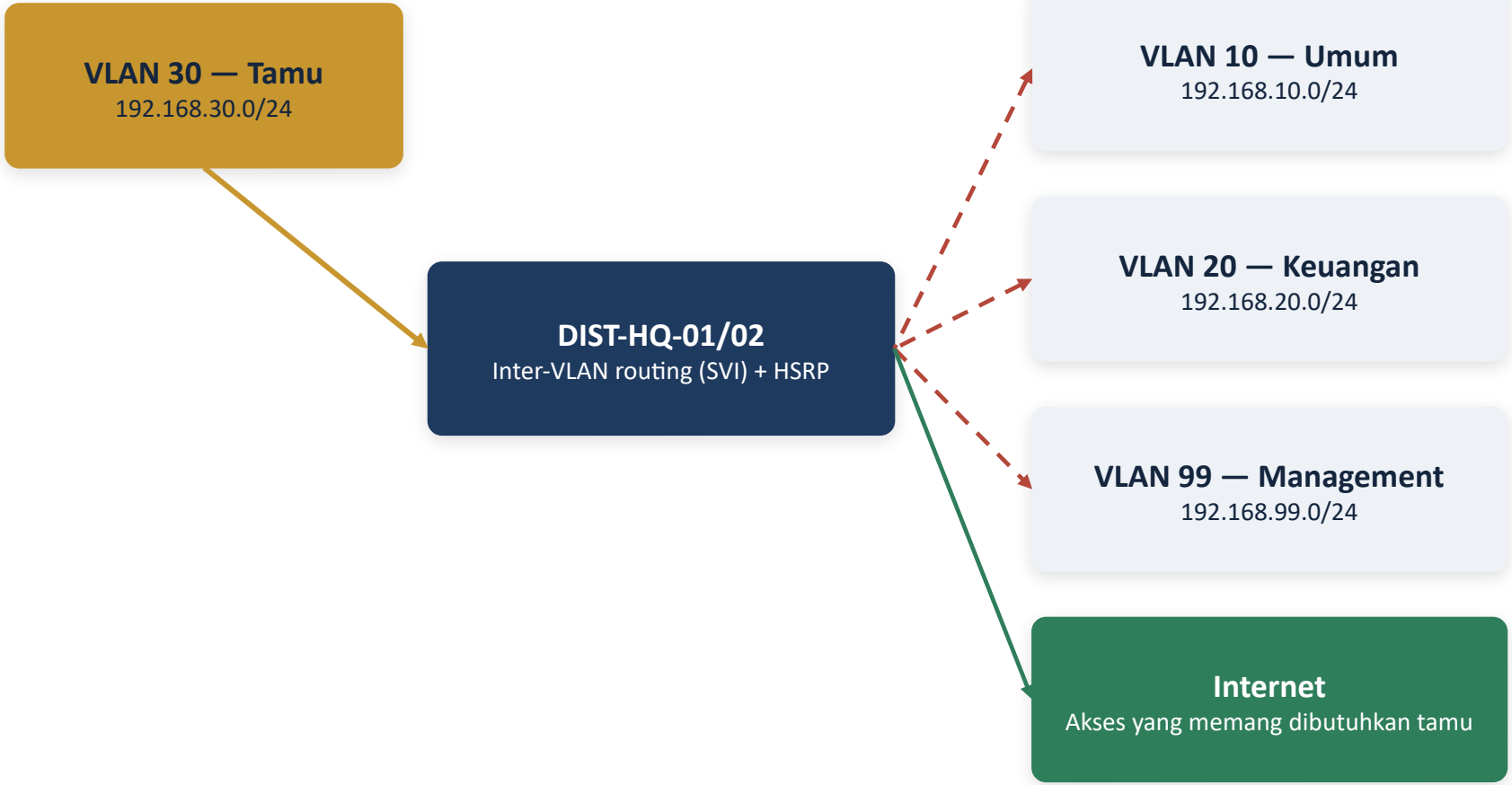
01

Terhubung tidak sama dengan aman

Semakin baik konektivitas, semakin luas jalur yang bisa disalahgunakan

MASALAH

Tamu di Wi-Fi kantor bisa menjangkau semuanya



Garis merah putus-putus = akses yang seharusnya tidak ada

Peringatan sejak Bab 3

Setelah inter-VLAN routing aktif, VLAN Tamu secara teknis dapat menjangkau server Keuangan dan antarmuka manajemen perangkat.

Konektivitas tanpa kontrol bukanlah jaringan yang baik — ia hanyalah pintu yang terbuka lebar bagi siapa saja yang kebetulan berhasil masuk.

Buku Ajar Enterprise Networking, Bab 9

02

Konsep dasar ACL

Daftar aturan permit/deny yang diperiksa sebelum paket diteruskan

DEFINISI

Apa itu Access Control List?

ACL adalah kumpulan pernyataan berurutan yang **mengizinkan (permit)** atau **menolak (deny)** lalu lintas berdasarkan kriteria tertentu.

Kriteria yang bisa dipakai:

alamat IP sumber · alamat IP tujuan · protokol · nomor port

Pemeriksaan berhenti pada **pernyataan pertama yang cocok** — sisa daftar tidak diperiksa lagi.



Analogi: daftar tamu acara

Daftar tamu di pintu → ACL
Diperiksa dari atas ke bawah

Nama cocok dengan entri → First match
Petugas langsung bertindak

Nama tidak ada di daftar → Implicit deny
Default-nya: tidak boleh masuk

Baris terakhir yang tidak pernah terlihat

ACL yang ditulis administrator

```
10  deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255

20  deny ip 192.168.30.0 0.0.0.255 192.168.99.0 0.0.0.255

    deny ip any any   ← implicit deny, otomatis
```

Akibatnya: ACL ini memblokir SELURUH lalu lintas VLAN Tamu, termasuk ke internet — bukan hanya ke VLAN 20 dan 99.

Perbaikannya

Jika tujuan ACL hanya memblokir hal tertentu, akhiri dengan pernyataan permit eksplisit:

```
30  permit ip any any
```

Kesalahan nomor satu pemula — dan jawaban soal analisis B.1.

Standard, Extended, dan Named ACL

Standard

Kriteria filter

Hanya alamat IP sumber

Rentang nomor

`1–99`
`1300–1999`

Sederhana, tapi tidak bisa membedakan tujuan

Extended

Kriteria filter

Sumber, tujuan, protokol (TCP/UDP/ICMP), port

Rentang nomor

`100–199`
`2000–2699`

Paling fleksibel; fokus utama hari ini

Named

Kriteria filter

Sama seperti Standard/Extended, diberi nama

Rentang nomor

`Tanpa nomor`
`mis. BLOK-TAMU`

Lebih mudah dibaca saat troubleshooting

03

Cara kerja ACL

Urutan pemeriksaan, lokasi penempatan, dan arah pemrosesan

First match: berhenti di baris pertama yang cocok

Paket masuk
Src 192.168.30.25 → Dst 192.168.99.1

```
10  deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
```
Tidak cocok → lanjut

```
20  deny ip 192.168.30.0 0.0.0.255 192.168.99.0 0.0.0.255
```
COCOK → paket ditolak, berhenti

```
30  permit ip any any
```
Tidak pernah diperiksa

```
    deny ip any any (implisit)
```
Tidak pernah diperiksa

Aturan emas

Pernyataan paling spesifik di atas, paling umum (permit ip any any) di paling bawah.

Pernyataan spesifik harus mendahului yang umum

Urutan salah

Baris 20 tidak pernah tercapai: HTTPS ke server Keuangan sudah ditangkap baris 10 dan ditolak.

```
10  deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
20  permit tcp 192.168.10.0 0.0.0.255 host 192.168.20.10 eq 443
30  permit ip any any
```

Urutan benar

Pengecualian (HTTPS ke satu server) diperiksa lebih dulu, baru blokir umum ke subnet Keuangan.

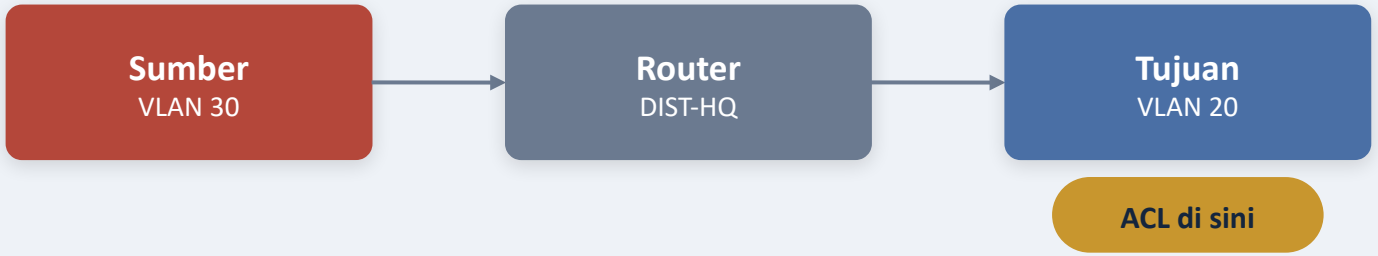
```
10  permit tcp 192.168.10.0 0.0.0.255 host 192.168.20.10 eq 443
20  deny ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
30  permit ip any any
```

Standard dekat tujuan, Extended dekat sumber

Standard ACL

Hanya melihat sumber

Jika dipasang dekat sumber, VLAN 30 terblokir ke SEMUA tujuan — Standard ACL tidak bisa membedakan tujuan.

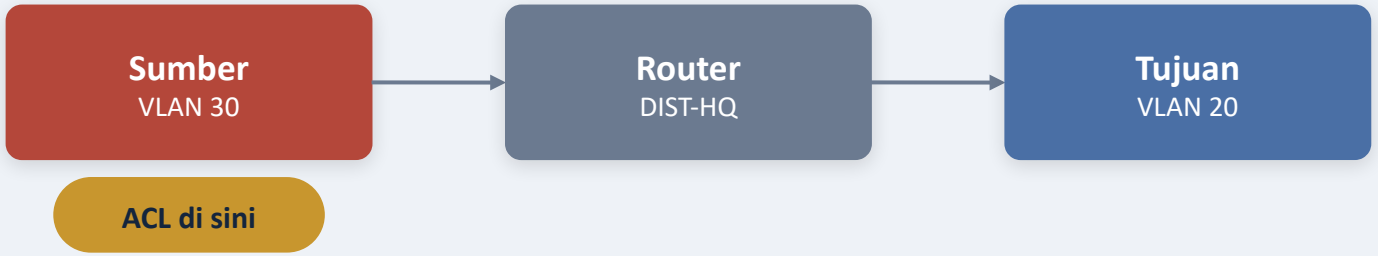


Diterapkan pada interface menuju tujuan (VLAN 20)

Extended ACL

Melihat sumber + tujuan

Paket yang pasti ditolak dibuang sedini mungkin, menghemat bandwidth di sepanjang jalur.

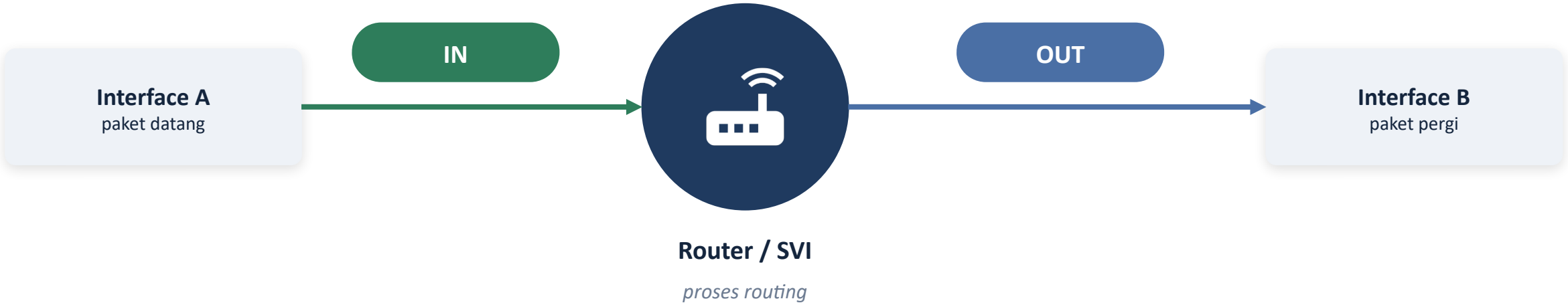


Diterapkan pada interface sumber (VLAN 30)

ARAH PEMROSESAN

Inbound atau outbound?

`Perintah:  ip access-group <nomor/nama> in | out`



Inbound (in)
Paket diperiksa saat MASUK ke interface, sebelum keputusan routing. Paket yang ditolak tidak sempat diproses routing.

Outbound (out)
Paket diperiksa saat AKAN KELUAR dari interface, setelah keputusan routing.

04

Wildcard mask

Kebalikan subnet mask: 0 = harus cocok, 1 = abaikan

KONSEP

Wildcard mask adalah kebalikan dari subnet mask



Bit 0 Harus sama persis dengan alamat di ACL

Bit 1 Boleh bernilai apa saja (don't care)

Konversi umum dan dua kata kunci pintas

Subnet mask	Wildcard mask	Cakupan
255.255.255.255 (/32)	**0.0.0.0**	Satu host spesifik
255.255.255.0 (/24)	**0.0.0.255**	Seluruh host satu subnet /24
255.255.252.0 (/22)	**0.0.3.255**	Rentang 4 subnet /24 sekaligus
0.0.0.0	**255.255.255.255**	Seluruh alamat IP

```
192.168.20.10 0.0.0.0
= host 192.168.20.10
```

```
0.0.0.0 255.255.255.255
= any
```

Latihan cepat: berapa wildcard mask untuk /26 (255.255.255.192) dan /28 (255.255.255.240)?

05

Konfigurasi ACL di Cisco IOS

Buat daftarnya, pasang di interface, lalu verifikasi

Blok Tamu ke Keuangan, dipasang dekat tujuan

```
! 1. Buat ACL
access-list 10 deny 192.168.30.0 0.0.0.255
access-list 10 permit any

! 2. Pasang di SVI tujuan, arah keluar
interface vlan 20
 ip access-group 10 out
```

`deny 192.168.30.0 0.0.0.255`
Tolak semua sumber dari subnet Tamu

`permit any`
Izinkan sumber lain (hindari implicit deny)

`vlan 20 … out`
Diperiksa saat router mengirim paket ke host Keuangan



Catatan untuk buku ajar: contoh di Bab 9 memakai ip access-group 10 in pada VLAN 20. Arah in di SVI VLAN 20 hanya memeriksa paket DARI host VLAN 20, sehingga trafik Tamu → Keuangan tidak tersaring. Yang tepat adalah out.

BLOK-TAMU: dipasang dekat sumber, arah masuk

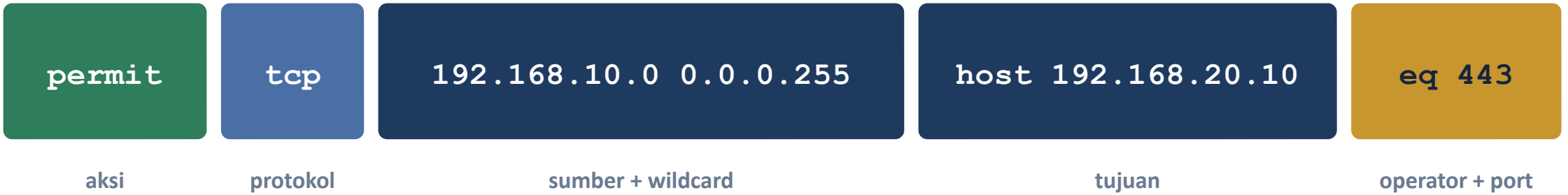
```
ip access-list extended BLOK-TAMU
 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
 deny ip 192.168.30.0 0.0.0.255 192.168.99.0 0.0.0.255
 permit ip any any
exit

interface vlan 30
 ip access-group BLOK-TAMU in
```

- Tamu → Keuangan — Ditolak
- Tamu → Management — Ditolak
- Tamu → Internet & lainnya — Diizinkan

Verifikasi: show access-lists

Diketik di mode configure terminal. Prompt sub-mode ACL: (config-ext-nacl)#

Membaca satu baris Extended ACL



Protokol

ip · tcp · udp · icmp — ip berarti semua protokol IP

Operator port

eq (sama dengan) · neq · gt · lt · range

Port umum

21 FTP · 22 SSH · 23 Telnet · 53 DNS · 80 HTTP · 443 HTTPS

Lima perintah ACL yang perlu dihafal

Perintah	Fungsi
`access-list <no> permit|deny <src> <wildcard>`	Membuat pernyataan Standard ACL bernomor
`ip access-list extended <nama>`	Membuat Extended ACL bernama, masuk sub-mode
`permit|deny <proto> <src> <dst> [eq port]`	Pernyataan Extended: protokol, sumber, tujuan
`ip access-group <no|nama> in|out`	Memasang ACL di interface beserta arahnya
`show access-lists`	Menampilkan ACL dan jumlah paket cocok per baris

Contoh keluaran show access-lists — counter matches membuktikan ACL bekerja

```
Extended IP access list BLOK-TAMU
    10 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255 (12 matches)
    20 deny ip 192.168.30.0 0.0.0.255 192.168.99.0 0.0.0.255 (4 matches)
    30 permit ip any any (230 matches)
```

Empat kebiasaan baik, tiga kesalahan klasik

Akhiri dengan permit ip any any

Bila tujuannya hanya memblokir hal tertentu

Gunakan Named ACL

BLOK-TAMU-KE-KEUANGAN lebih jelas dari 110

Uji di jam sepi / out-of-band

Salah ACL di interface manajemen bisa mengunci Anda sendiri

Verifikasi counter

show access-lists: apakah tiap baris benar-benar ter-match?

Kesalahan klasik

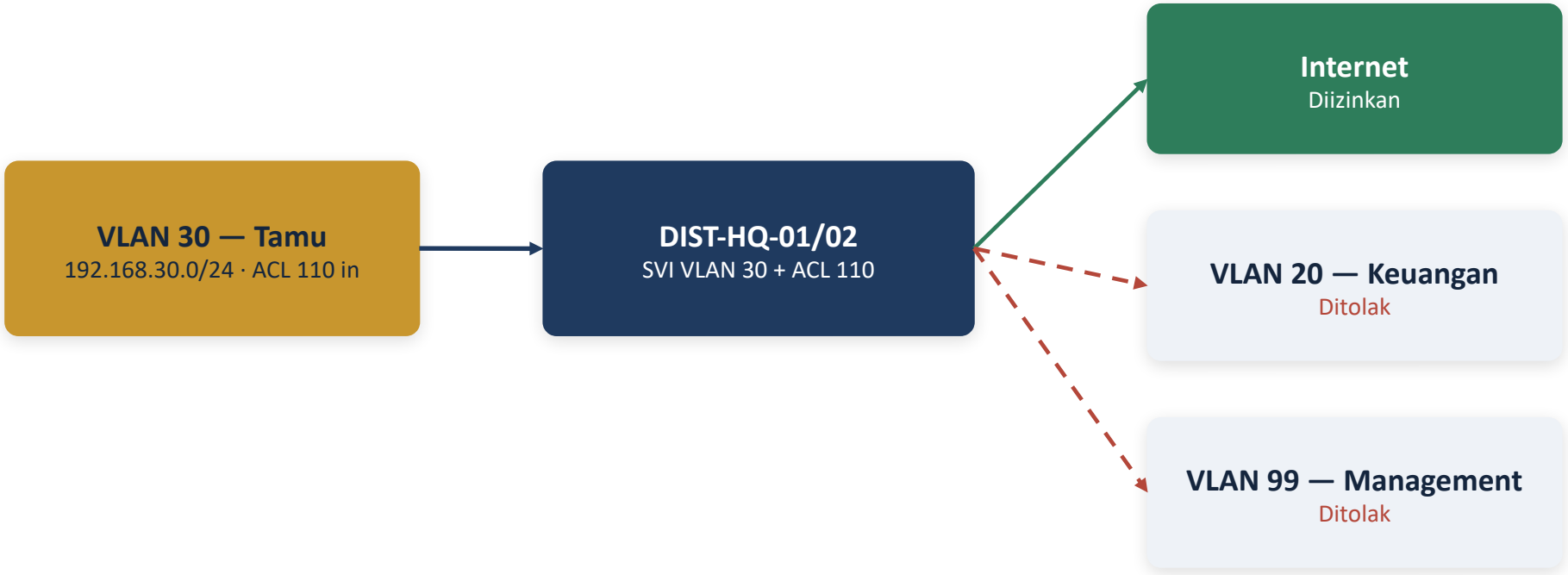
1. Lupa permit di akhir → semua lalu lintas terblokir
1. Standard ACL terlalu dekat sumber → tujuan lain ikut terblokir
1. Salah hitung wildcard → cakupan filter meleset

06

Studi kasus & praktikum

Extended ACL membatasi VLAN Tamu di PT Nusantara Digital Kreasi

ACL 110 pada SVI VLAN 30, arah inbound




```
access-list 110 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 110 deny ip 192.168.30.0 0.0.0.255 192.168.99.0 0.0.0.255
access-list 110 permit ip any any
```

Mengapa Extended?

Butuh filter berdasarkan tujuan spesifik. Standard ACL tak bisa membedakan Keuangan dari Internet.

Mengapa VLAN 30 in?

Sedekat mungkin dengan sumber; paket ditolak sebelum di-routing.

PERTANYAAN KRITIS

Apakah tamu benar-benar hanya bisa ke internet?

Telusuri paket ini terhadap ACL 110

`192.168.30.25 → 192.168.20.5`
Baris 1 cocok · **Ditolak**

`192.168.30.25 → 192.168.99.1`
Baris 2 cocok · **Ditolak**

`192.168.30.25 → 8.8.8.8`
Baris 3 cocok · **Diizinkan**

`192.168.30.25 → 192.168.10.20`
Baris 3 cocok · **Diizinkan?!**

Diskusikan di kelas

1. VLAN 10 (Umum) tidak disebut di ACL 110. Apa artinya bagi keamanan?
1. Ubah ACL agar tamu benar-benar hanya bisa ke internet. Pernyataan apa yang ditambahkan, dan di baris ke berapa?
1. Pendekatan mana yang dipakai NDK: permit by default atau deny by default?

Kelebihan, keterbatasan, dan filosofi kebijakan

Kelebihan

- Kontrol granular: alamat, protokol, port
- Tanpa perangkat tambahan: langsung di router/switch L3
- Fondasi NAT (Bab 12) dan QoS (Bab 11)

Keterbatasan

- Implicit deny tak terlihat — sumber kesalahan
- ACL panjang membebani CPU router low-end
- Stateless: tidak mengingat status koneksi

Dua filosofi kebijakan

Deny by default, permit by exception

Hanya izinkan yang dibutuhkan. Untuk data sangat sensitif.

Permit by default, deny by exception

Izinkan umumnya, blokir yang berisiko. Dipakai NDK.

Rancang dan terapkan ACL antar-segmen

1. Bangun topologi: switch L3 dengan VLAN 10 Umum, 20 Keuangan, 30 Tamu, 99 Management + 1 PC tiap VLAN
2. Uji baseline: semua VLAN saling ping (inter-VLAN routing aktif)
3. Standard ACL: blok Tamu → Keuangan; bandingkan hasil arah in vs out di SVI VLAN 20
4. Extended ACL BLOK-TAMU di SVI VLAN 30 in: tolak VLAN 20 & 99, izinkan sisanya
5. Uji efektivitas: ping/akses dari PC Tamu ke tiap VLAN; cek counter show access-lists
6. Perbaiki celah VLAN 10; dokumentasikan topologi, konfigurasi, dan hasil uji

Rubrik penilaian



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

Enam hal yang dibawa pulang

01

ACL: daftar permit/deny yang diperiksa top-down, berhenti di kecocokan pertama

02

Implicit deny menolak semua yang tak cocok — tambahkan permit bila perlu

03

Standard: sumber saja (1–99) · Extended: sumber, tujuan, protokol, port (100–199)

04

Standard dekat tujuan, Extended dekat sumber

05

Wildcard = 255 − subnet mask; 0 cocok persis, 1 abaikan; host & any

06

Pasang dengan ip access-group … in/out; verifikasi dengan show access-lists

Uji pemahaman sebelum praktikum

Analisis

ACL berhasil memblokir yang dimaksud, tetapi semua lalu lintas lain ikut terblokir. Apa penyebabnya?

Analisis

Mengapa tim IT NDK memilih Extended ACL, bukan Standard ACL, untuk VLAN Tamu?

Konfigurasi

Buat Extended ACL BLOK-FTP: tolak FTP (port 21) dari 192.168.40.0/24 ke host 192.168.20.50, izinkan lainnya, pasang di VLAN 40 in.

Reflektif

Kapan 'deny by default' lebih tepat daripada 'permit by default'?

PERTEMUAN BERIKUTNYA

Pertemuan 10 — Port Security & NAC Dasar

Setelah menyaring lalu lintas di Layer 3, kita turun ke port switch: siapa yang boleh tersambung, dan apa yang terjadi saat terjadi pelanggaran akses. Sub-CPMK 3.2.

Terima kasih — sampai jumpa di laboratorium

Referensi

- Buku Ajar Enterprise Networking, Bab 9 — Prodi D3 TK PNP
- Odom, W. (2023). CCNA 200-301 Official Cert Guide, Vol. 1. Cisco Press
- Lammle, T. (2021). CCNA Routing and Switching Complete Study Guide. Sybex
- Teare, Vachon & Graziani (2021). ROUTE Foundation Learning Guide. Cisco Press
- Cisco NetAcad — modul Access Control Lists