ENTERPRISE NETWORKING · PERTEMUAN 10

Port Security & NAC Dasar

Mengamankan titik akses fisik ke jaringan — dari MAC address hingga IEEE 802.1X

Sub-CPMK 3.2 · CPL-8, CPL-11 · Bab 10 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	**Celah di port fisik**	Apa yang tidak bisa dijangkau ACL
02	**Konsep port security**	MAC secure: static, dynamic, sticky
03	**Cara kerja & violation**	Protect, restrict, shutdown, err-disabled
04	**NAC & IEEE 802.1X**	Autentikasi identitas sebelum akses
05	**Konfigurasi Cisco IOS**	Perintah, verifikasi, pemulihan port
06	**Studi kasus & praktikum**	Port ruang rapat PT NDK

Setelah pertemuan ini, mahasiswa mampu…

Sub-CPMK 3.2

Mampu menerapkan port security dan mekanisme kontrol akses jaringan (Network Access Control) dasar.

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

1
Menjelaskan risiko akses fisik yang tidak dikendalikan pada port switch

2
Menguraikan port security dan jenis MAC secure: static, dynamic, sticky

3
Membandingkan mode violation protect, restrict, shutdown

4
Menjelaskan konsep NAC melalui kerangka IEEE 802.1X

5
Mengonfigurasi port security dengan perintah Cisco IOS

6
Menganalisis port security pada area publik/rentan

01

Celah di port fisik

ACL menjaga lalu lintas antar-VLAN, bukan siapa yang boleh masuk ke VLAN

SKENARIO

Satu kabel printer, satu laptop asing, akses penuh ke VLAN

ACCESS-LT1
Port Fa0/12 aktif · VLAN 10



Laptop pribadi orang tak berwenang

Asumsi tersembunyi ACL: ACL hanya mengendalikan paket yang SUDAH berada di dalam jaringan, dan memfilter lalu lintas ANTAR-VLAN. Perangkat asing di port aktif langsung menjadi anggota sah VLAN tersebut.

1 Colok

Kabel printer di ruang rapat kosong dicabut, dipasang ke laptop asing

2 DHCP

Laptop langsung mendapat alamat IP VLAN 10

3 ARP

Bisa menemukan host lain di VLAN yang sama

4 Akses

Semua yang diizinkan untuk VLAN 10 kini terbuka

Istilahnya: rogue device — akses tidak sah melalui port fisik. Risiko paling mendasar, tetapi sering diabaikan di jaringan enterprise.

ACL menjaga ke mana lalu lintas boleh pergi setelah masuk jaringan. Port Security menjaga siapa yang boleh masuk sejak awal.

Buku Ajar Enterprise Networking, Bab 10

02

Konsep port security

Membatasi jumlah dan identitas MAC address di setiap port

Apa itu port security?

Port Security adalah fitur Layer 2 switch yang membatasi **jumlah** dan/atau **identitas MAC address** yang boleh mengirim lalu lintas melalui suatu port.

Switch mempelajari MAC perangkat yang terhubung sampai batas maksimum (default **1**). MAC baru setelah batas tercapai memicu **security violation**.



Analogi: kunci sidik jari

Sidik jari terdaftar → **Secure MAC**
Bebas keluar-masuk

Jumlah orang terdaftar → **Maximum**
Batas yang ditetapkan

Orang asing mencoba masuk → **Violation**
Alarm, catat, atau kunci pintu

Static, dynamic, dan sticky

Static

Cara belajar

Dimasukkan manual oleh engineer

Masuk konfigurasi?

Ya, permanen

Setelah reboot

Tetap ada

Aman tapi terlalu manual untuk ratusan port

Dynamic

Cara belajar

Dipelajari otomatis dari perangkat pertama

Masuk konfigurasi?

Tidak

Setelah reboot

Hilang

Mudah, tapi daftar hilang setiap reboot

Sticky

Cara belajar

Dipelajari otomatis, lalu ditulis ke running-config

Masuk konfigurasi?

Ya, bila disimpan ke startup-config

Setelah reboot

Tetap ada

Paling populer: otomatis + persisten

Tiga angka yang perlu diingat

1

MAC address

Maximum default saat port security diaktifkan

Shutdown

Mode violation

Default: port langsung err-disabled

Access

Mode port

Port harus diset switchport mode access dulu



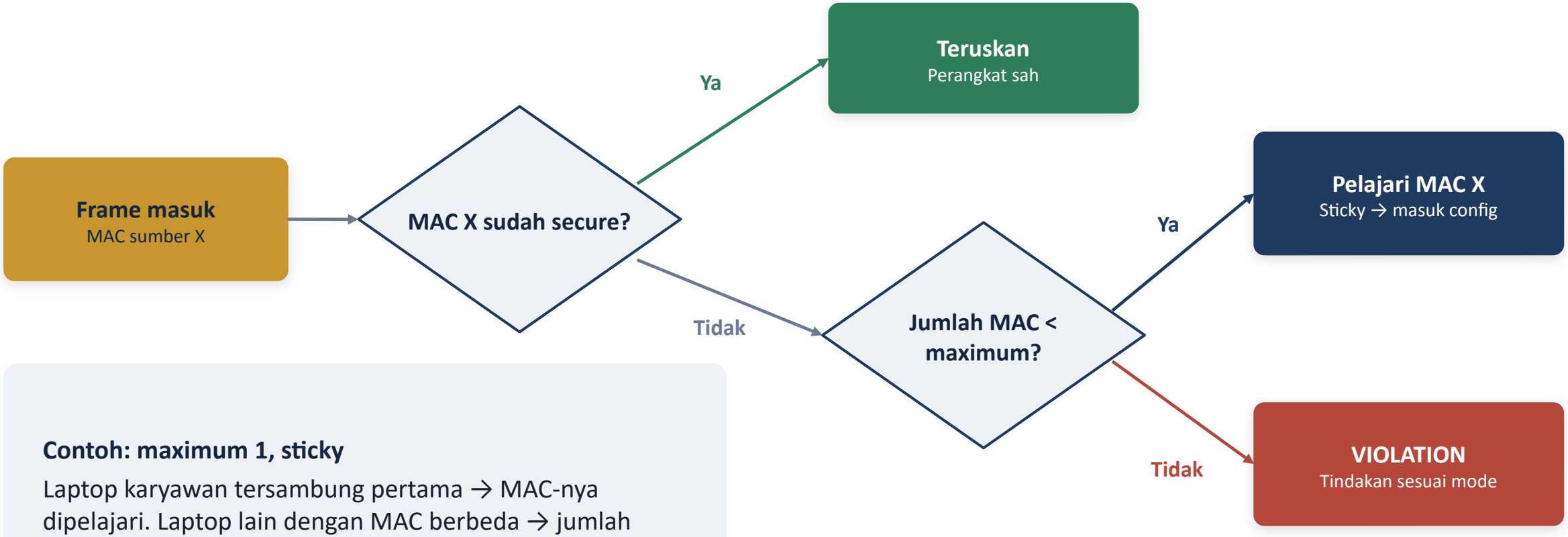
Implikasinya: cukup mengetik switchport port-security saja sudah menghasilkan port yang menerima satu MAC dan mati total jika ada MAC kedua. Sadari default ini sebelum menerapkannya ke banyak port sekaligus.

03

Cara kerja & mode violation

Apa yang dilakukan switch saat MAC tak dikenal muncul

Setiap frame yang masuk ke port diperiksa



Contoh: maximum 1, sticky

Laptop karyawan tersambung pertama → MAC-nya dipelajari. Laptop lain dengan MAC berbeda → jumlah sudah 1 = maximum → violation.

Protect, restrict, shutdown: apa bedanya?

Tindakan switch	Protect	Restrict	Shutdown (default)
Buang frame dari MAC tak dikenal	Ya	Ya	Ya
Kirim log syslog / SNMP trap	Tidak	Ya	Ya
Tambah counter violation	Tidak	Ya	Ya
Perangkat sah tetap terlayani	Ya	Ya	Tidak
Port masuk err-disabled	Tidak	Tidak	Ya

Ringkasnya

Drop diam-diam
Tidak ada jejak — tim IT tidak tahu ada percobaan

Drop + log
Layanan jalan, visibilitas tetap ada

Matikan port
Paling tegas; perangkat sah ikut terputus

Trade-off antara ketersediaan dan ketegasan

← Ketersediaan layanan diutamakan

Ketegasan keamanan diutamakan →



Protect

Cocok untuk

Jarang dipakai: pelanggaran tidak terlihat

Restrict

Cocok untuk

Area kerja karyawan tetap yang jarang ganti perangkat

Shutdown

Cocok untuk

Area berisiko tinggi: ruang rapat publik, lobi

Memulihkan port setelah shutdown violation

Manual

Engineer memulihkan setelah investigasi

```
interface fastEthernet 0/12
 shutdown
 no shutdown
```

Cocok untuk area berisiko tinggi: ada kesempatan memeriksa log dulu.

Otomatis

Port hidup lagi setelah jeda

```
errdisable recovery cause psecure-violation
errdisable recovery interval 300
```

Cocok untuk port yang sering violation karena kesalahan wajar, mis. ganti laptop.

04

NAC & IEEE 802.1X

Dari mencocokkan MAC menuju membuktikan identitas

Port security adalah NAC paling sederhana

NAC adalah konsep luas untuk mengendalikan perangkat mana yang boleh mengakses jaringan, **kapan**, dan dengan **hak akses apa**.

Kelemahan: MAC spoofing



Laptop sah
`00d0.5866.9b12`



Penyerang meniru
`00d0.5866.9b12`

Switch hanya melihat MAC. Bila MAC tiruan identik dan perangkat asli sedang tidak tersambung, port security meloloskannya.

MAC address relatif mudah dipalsukan dari sisi software.



Solusi lebih kuat

IEEE 802.1X

Port baru dibuka setelah identitas pengguna/perangkat terbukti — lewat username/password, sertifikat digital, atau metode lain.

Tiga entitas mengendalikan satu port



Supplicant

Perangkat pengguna dengan client 802.1X

Authenticator

Switch yang menjaga port tetap tertutup

Authentication Server

Umumnya server RADIUS yang memvalidasi kredensial

Sebelum: Unauthorized

Hanya lalu lintas EAP untuk autentikasi yang diizinkan lewat

Sesudah: Authorized

RADIUS mengonfirmasi kredensial valid → akses jaringan penuh

Implementasi mendalam 802.1X (konfigurasi RADIUS, integrasi direktori pengguna) di luar cakupan mata kuliah ini.

PERBANDINGAN

Port security vs IEEE 802.1X

Aspek	Port Security	IEEE 802.1X
Yang diperiksa	MAC address	Identitas: kredensial atau sertifikat
Tahan MAC spoofing	**Tidak**	**Ya**
Infrastruktur tambahan	Tidak perlu — fitur switch	Server RADIUS + client di perangkat
Kompleksitas	Rendah	Tinggi
Cocok untuk	Langkah awal di semua access port	Area publik/berisiko tinggi, organisasi dengan SDM & anggaran

Bukan pilihan salah satu: port security memberi perlindungan dasar hari ini; 802.1X menjadi tujuan migrasi bertahap.

05

Konfigurasi port security

Lima baris di interface, dua perintah verifikasi

Sticky, maximum 1, violation shutdown pada Fa0/12

```
interface fastEthernet 0/12
 switchport mode access
 switchport port-security
 switchport port-security maximum 1
 switchport port-security mac-address sticky
 switchport port-security violation shutdown
exit
```

`mode access`	Wajib lebih dulu; port dinamis/trunk ditolak
`port-security`	Mengaktifkan fitur (tanpa ini, baris lain tak berlaku)
`maximum 1`	Hanya satu MAC; sama dengan default
`sticky`	MAC pertama ditulis ke running-config
`violation shutdown`	Sama dengan default; ditulis agar desain jelas

Jangan lupa: `copy running-config startup-config` — tanpa ini MAC sticky hilang saat switch reboot.

Banyak port sekaligus, lalu periksa hasilnya

Tujuh port ruang rapat dalam satu langkah

```
interface range fa0/10 - 16
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
```

Diterapkan ke Fa0/10 s.d. Fa0/16 sekaligus; maximum & violation memakai default (1, shutdown).

show port-security interface fa0/12 (setelah violation)

```
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 00d0.5866.9b12:10
Security Violation Count   : 1
```

Status port: Secure-up normal · Secure-down tidak ada link · Secure-shutdown err-disabled · Daftar MAC: `show port-security address`

Perintah port security yang perlu dihafal

Perintah	Fungsi
`switchport port-security`	Mengaktifkan port security (port harus mode access)
`switchport port-security maximum <n>`	Jumlah maksimum MAC yang diizinkan
`switchport port-security mac-address sticky`	Sticky learning: MAC disimpan ke konfigurasi
`switchport port-security violation <mode>`	protect | restrict | shutdown
`show port-security interface <intf>`	Status port, jumlah MAC, counter violation
`show port-security address`	Daftar MAC secure yang sudah dipelajari

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 00d0.5866.9b12 on port
FastEthernet0/12.
```

Empat kebiasaan dari buku, satu tambahan

Sticky untuk port pengguna

Seimbang antara kemudahan (bukan static) dan persistensi (bukan dynamic).

errdisable recovery

Jeda mis. 300 detik untuk port yang sering violation karena kesalahan wajar.

Hanya di access port

Jangan di trunk: trunk membawa banyak MAC dari switch lain.

Dokumentasikan

Port mana ber-port security dan mode apa — mempercepat troubleshooting.

Tambahan: port tak terpakai

```
interface fa0/20
 shutdown
 switchport access vlan 999
```

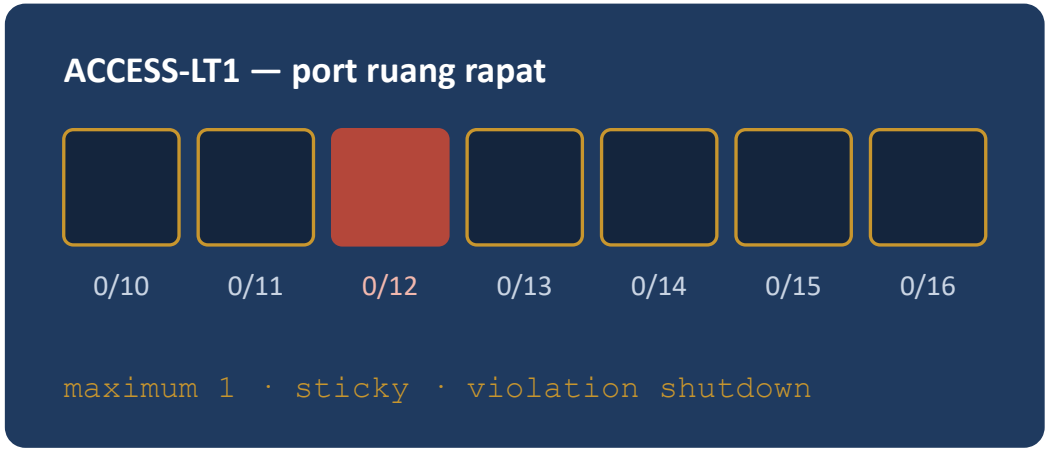
Port yang tidak dipakai lebih aman dimatikan dan dipindah ke VLAN kosong. Praktik umum, tidak dibahas di Bab 10.

06

Studi kasus & praktikum

Port security di ruang rapat PT Nusantara Digital Kreasi

Ruang rapat lantai 1: area berisiko tinggi



Mengapa shutdown?

Ruang rapat dipakai tamu eksternal dan sering tidak diawasi. Di area ini keamanan lebih diutamakan daripada ketersediaan tanpa gangguan.

Pagi
Laptop karyawan di Fa0/12 untuk presentasi → MAC dipelajari via sticky

Sore
Ruangan kosong; orang tak berwenang colok laptop pribadi ke Fa0/12

Seketika
Violation → Fa0/12 err-disabled, syslog dikirim, perangkat asing terblokir

Setelahnya
Tim IT investigasi log, pulihkan port manual; pertimbangkan migrasi ke 802.1X

PERTANYAAN KRITIS

Besok pagi, presenter lain datang ke ruang yang sama…

Telusuri kejadiannya

Hari 1, pagi
Laptop karyawan A → MAC A jadi sticky di Fa0/12

Hari 1, sore
Laptop asing → err-disabled (sesuai harapan)

Hari 2
Tim IT memulihkan port. MAC A masih tersimpan

Hari 2, pagi
Presenter tamu B colok laptop → MAC B ≠ A → err-disabled lagi?!



Diskusikan di kelas

1. Apakah sticky + maximum 1 cocok untuk port yang dipakai bergantian oleh banyak presenter?
1. Apa yang sebenarnya dibutuhkan tamu presenter: akses penuh ke VLAN karyawan, atau cukup internet?
1. Usulkan desain yang lebih tepat untuk port ruang rapat.

Kelebihan dan keterbatasan port security



Kelebihan

- Mencegah perangkat asing di port aktif
- Konfigurasi sederhana, terutama dengan sticky
- Mode violation fleksibel sesuai tingkat risiko
- Lapisan defense in depth bersama ACL



Keterbatasan

- Bisa ditembus MAC spoofing
- Shutdown mengganggu bila sering terpicu
- Butuh dokumentasi & proses matang di skala besar
- Tidak cocok untuk trunk atau hub/switch tak terkelola

Konfigurasi port security dan uji violation

1. Topologi: 1 switch akses, 3 PC sah, 1 laptop "penyusup" (MAC berbeda)
2. Fa0/1: sticky, max 1, shutdown → colok PC sah, cek show port-security address
3. Ganti dengan laptop penyusup → amati Secure-shutdown, counter, dan syslog
4. Pulihkan port: shutdown / no shutdown; lalu uji errdisable recovery 30 s
5. Fa0/2: restrict & Fa0/3: protect → ulangi uji; bandingkan log & counter
6. Dokumentasikan topologi, konfigurasi, hasil uji tiap mode dalam tabel

Rubrik penilaian

Rancangan skema port security & NAC	20%
Keberhasilan konfigurasi & fungsionalitas	40%
Pengujian respons terhadap violation	20%
Kelengkapan dokumentasi	20%

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

RANGKUMAN

Enam hal yang dibawa pulang

01

Port security membatasi MAC di port switch — celah yang tak dijangkau ACL

02

MAC secure: static (manual), dynamic (hilang saat reboot), sticky (persisten)

03

Violation: protect (drop diam), restrict (drop + log), shutdown (err-disabled, default)

04

Default: maximum 1, violation shutdown, port harus mode access

05

802.1X: Supplicant – Authenticator – RADIUS; identitas dibuktikan sebelum akses

06

Pilih mode sesuai risiko area: shutdown untuk area publik, restrict untuk area kerja

Uji pemahaman sebelum praktikum

Analisis

Port shutdown terus err-disabled tiap karyawan ganti laptop. Sebutkan dua solusi konfigurasi.

Analisis

Penyerang memalsukan MAC laptop sah untuk melewati port security. Mengapa bisa, dan apa solusinya?

Konfigurasi

Tulis perintah port security di Gi0/8: maximum 2, sticky, violation restrict.

Reflektif

Kapan organisasi sebaiknya bermigrasi dari port security ke 802.1X?

PERTEMUAN BERIKUTNYA

Pertemuan 11 — Quality of Service (QoS) Dasar

Jaringan sudah terhubung dan terkendali. Berikutnya: memastikan suara dan video tetap lancar saat jaringan padat. Sub-CPMK 3.3.

Terima kasih — sampai jumpa di laboratorium

Referensi

- Buku Ajar Enterprise Networking, Bab 10 — Prodi D3 TK PNP
- Odom, W. (2023). CCNA 200-301 Official Cert Guide, Vol. 1. Cisco Press
- Froom, Frahim & Sivasubramanian (2022). SWITCH Foundation Learning Guide. Cisco Press
- IEEE (2020). Std 802.1X-2020: Port-Based Network Access Control
- Cisco NetAcad — SRWE, Switch Security Configuration