VERSI 2.0

SEPTEMBER 2025

PRAKTIKUM JARINGAN KOMPUTER

MODUL 5 DEMO PRAKTIKUM - IMPLEMENTASI PORT SECURITY DAN KONFIGURASI SWITCH SECURITY

DISUSUN OLEH:

Ir. Mahar Faiqurahman, S.Kom., M.T.

Taufiq Ramadhan

Sutrisno Adit Pratama

TIM LABORATORIUM INFORMATIKA

UNIVERSITAS MUHAMMADIYAH MALANG

PENDAHULUAN

TUJUAN

1. Mahasiswa mampu implementasi Port Security
2. Mahasiswa mampu memahami serangan Vlan
3. Mahasiswa mampu memahami serangan DHCP
4. Mahasiswa mampu memahami serangan ARP
5. Mahasiswa mampu memahami serangan STP

TARGET MODUL

1. Melakukan konfigurasi DTP dan Native VLAN untuk mitigasi serangan Vlan
2. Melakukan konfigurasi DHCP Snooping untuk mitigasi serangan DHCP
3. Melakukan konfigurasi inspeksi ARP untuk mitigasi serangan ARP
4. Melakukan konfigurasi PortFast dan BPDU Guard untuk mitigasi serangan STP

PERSIAPAN MATERI

1. Port Security
2. Vlan
3. DHCP
4. ARP
5. STP

PERSIAPAN SOFTWARE DAN HARDWARE

1. Komputer/Laptop
2. Sistem operasi Windows/ Linux/ MacOS
3. Simulator Packet Tracer - https://bit.ly/jarkom_2025_umm

KEYWORDS

Security, bpdu, vlan attack, stp, arp

DAFTAR ISI

DEMO PRAKTIKUM

Demo yang dilakukan yaitu mengerjakan Activity Lab Packet Tracer - Switch Security Configuration. Download file *Packet Tracer* pada link di bawah ini:
https://bit.ly/modul-5_jarkom_2025_umm
Praktikum dilakukan pada File Packet Tracer dengan mengikuti petunjuk yang sudah disediakan. Petunjuk pengerjaan praktikum juga dapat dilihat pada perintah di bawah. Praktikum akan dilaksanakan secara live configuration, yang akan dilakukan secara real time pada saat jam praktikum dilaksanakan. Harap persiapkan dengan baik dan belajar dengan sungguh-sungguh agar tidak menghambat kelancaran jalannya praktikum. Terimakasih.

Tabel VLAN

Switch	VLAN Number	VLAN Name	Port Membership	Network
SW-1	10	Admin	F0/1, F0/2	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	G0/1, G0/2	Kosong
	999	BlackHole	Semua port yang tidak terpakai	Kosong
SW-2	10	Admin	F0/1, F0/22	192.168.10.0/24
	20	Sales	F0/10	192.168.20.0/24
	99	Management	F0/24	192.168.99.0/24
	100	Native	None	Kosong
	999	BlackHole	Semua port yang tidak terpakai	Kosong

Tujuan

Bagian 1: Membuat Jalur *Trunk* yang Aman
Bagian 2: Mengamankan Port Switch yang Tidak Digunakan
Bagian 3: Menerapkan Keamanan Port (*Port Security*)
Bagian 4: Mengaktifkan DHCP Snooping
Bagian 5: Mengkonfigurasi Rapid PVST, PortFast, dan BPDU Guard

Latar Belakang

Anda akan meningkatkan keamanan pada dua buah *access switch* di sebuah jaringan yang baru terkonfigurasi sebagian. Anda akan menerapkan serangkaian fitur keamanan yang telah dibahas dalam modul ini sesuai dengan persyaratan yang diberikan. Perlu dicatat bahwa *routing* sudah dikonfigurasi pada jaringan ini, sehingga konektivitas antar-host di VLAN yang berbeda seharusnya berfungsi setelah semua pengaturan selesai.

INSTRUKSI

Langkah 1: Membuat Jalur *Trunk* yang Aman

a. **Hubungkan port G0/2 dari kedua *access layer switch*.**
b. **Konfigurasikan port G0/1 dan G0/2 sebagai *trunk* statis di kedua switch.**
c. **Matikan negosiasi DTP (*Dynamic Trunking Protocol*) pada kedua sisi link.**
d. **Buat VLAN 100 dan berikan nama Native di kedua switch.**
e. **Konfigurasikan semua port *trunk* di kedua switch agar menggunakan VLAN 100 sebagai *native VLAN*.**

Langkah 2: Mengamankan Port Switch yang Tidak Digunakan

a. **Matikan (shutdown) semua port switch yang tidak digunakan pada SW-1.**
b. **Buat VLAN 999 pada SW-1 dan berikan nama BlackHole. Pastikan nama yang dikonfigurasi sama persis dengan yang diminta.**
c. **Pindahkan semua port switch yang tidak digunakan ke dalam VLAN BlackHole.**

Langkah 3: Menerapkan Keamanan Port (*Port Security*)

a. **Aktifkan keamanan port pada semua port akses yang aktif di switch SW-1.**
b. **Konfigurasikan port-port aktif tersebut agar mengizinkan maksimal 4 alamat MAC untuk dipelajari pada setiap port.**
c. **Untuk port F0/1 di SW-1, konfigurasikan alamat MAC dari PC secara statis menggunakan keamanan port.**
d. **Konfigurasikan setiap port akses yang aktif agar secara otomatis menambahkan alamat MAC yang dipelajari ke dalam konfigurasi yang sedang berjalan (*running configuration*).**
e. **Konfigurasikan mode pelanggaran keamanan port untuk menjatuhkan (drop) paket dari alamat MAC yang melebihi batas maksimum. Mode ini juga harus menghasilkan log Syslog, tetapi tidak mematikan (disable) port.**

Langkah 4: Mengaktifkan DHCP Snooping

a. **Konfigurasikan port *trunk* pada SW-1 sebagai port terpercaya (*trusted port*).**
b. **Batasi port yang tidak terpercaya (*untrusted port*) pada SW-1 agar hanya menerima lima paket DHCP per detik.**
c. **Pada SW-2, aktifkan DHCP snooping secara global dan juga untuk VLAN 10, 20, dan 99.**

Catatan: Konfigurasi DHCP snooping mungkin tidak dinilai dengan benar di dalam Packet Tracer.

Langkah 5: Mengkonfigurasi Rapid PVST, PortFast, dan BPDU Guard

a. **Aktifkan PortFast pada semua port akses yang sedang digunakan di SW-1.**
b. **Aktifkan BPDU Guard pada semua port akses yang sedang digunakan di SW-1.**
c. **Konfigurasikan SW-2 agar semua port aksesnya menggunakan PortFast secara default.**

RUBRIK PENILAIAN

Pemahaman Materi	**30%**
Codelab	**20%**
Demo	**50%**