PRAKTIKUM JARINGAN KOMPUTER

LAPORAN PRAKTIKUM

PERCOBAAN 3

CONFIGURE VLANS AND TRUNKING - PHYSICAL MODE

Alexander Lawrensius

TI A

2315061013

PROGRAM STUDI TEKNIK INFORMATIKA

JURUSAN TEKNIK ELEKTRO

FAKULTAS TEKNIK

UNIVERSITAS LAMPUNG

2025

I. JUDUL PERCOBAAN

CONFIGURE VLANS AND TRUNKING - PHYSICAL MODE

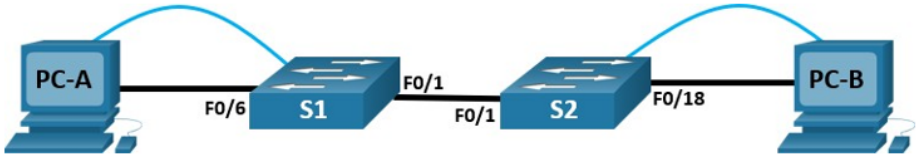
II. TUJUAN PERCOBAAN

Adapun tujuan dari percobaan ini adalah sebagai berikut.

1. Membangun Jaringan dan Mengonfigurasi Pengaturan Perangkat Dasar.
2. Membuat VLAN dan Menetapkan Port Switch.
3. Pertahankan Penugasan Port VLAN dan Basis Data VLAN.
4. Konfigurasikan Trunk 802.1Q Antar Switch.

TUGAS AKHIR

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.4	255.255.255.0	192.168.10.1

Gambar 1 Topologi dan Tabel Pengalamatan

Bagian 1: Membangun Jaringan dan Mengonfigurasi Pengaturan Perangkat Dasar

Langkah 1: Bangun jaringan seperti yang ditunjukkan dalam topologi

a. Klik dan seret kedua sakelar S1 dan S2 ke Rak
b. Klik dan seret PC-A dan PC-B ke Tabel dan gunakan tombol daya untuk menyalakannya
c. Sediakan konektivitas jaringan dengan menghubungkan kabel Tembaga Straight-through , seperti yang ditunjukkan dalam topologi
d. Hubungkan Kabel Konsol dari perangkat PC-A ke S1 dan dari perangkat PC-B ke S2

Langkah 2: Konfigurasikan pengaturan dasar untuk setiap sakelar

a. Dari Tab Desktop di setiap PC, gunakan Terminal untuk masuk ke setiap sakelar dan aktifkan mode EXEC istimewa

   Switch> enable

   Fungsinya: Masuk ke privileged EXEC mode, yaitu mode dengan akses penuh untuk melihat dan mengonfigurasi perangkat.
b. Masuk ke mode konfigurasi

   Switch# config terminal

Fungsinya: Masuk ke global configuration mode, tempat semua konfigurasi perangkat dilakukan.

c. Tetapkan nama perangkat untuk setiap sakelar

Switch(config)# hostname S1
Switch(config)# hostname S2

Fungsinya: Mengubah nama perangkat agar mudah dikenali dalam jaringan atau dokumentasi.

d. Tetapkan kelas sebagai kata sandi EXEC terenkripsi yang memiliki hak istimewa

S1(config)# enable secret class
S2(config)# enable secret class

Fungsinya: Mengatur password terenkripsi untuk masuk ke privileged EXEC mode (enable secret lebih aman dibanding enable password).

e. Tetapkan cisco sebagai kata sandi konsol dan aktifkan login

S1(config)# line console 0
S1(config-line)# password cisco
S1(config-line)# login
S2(config)# line console 0
S2(config-line)# password cisco
S2(config-line)# login

Fungsinya: Masuk ke konfigurasi konsol fisik (port console), Mengatur password untuk akses melalui konsol atau VTY (telnet/SSH), Mengaktifkan penggunaan password agar akses konsol/VTY tidak bebas.

f. Tetapkan cisco sebagai kata sandi vty dan aktifkan login

S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S2(config)# line vty 0 4
S2(config-line)# password cisco
S2(config-line)# login

Fungsinya: Masuk ke konfigurasi Virtual Terminal Lines, digunakan untuk akses telnet/SSH, Mengatur password untuk akses melalui

konsol atau VTY (telnet/SSH), Mengaktifkan penggunaan password agar akses konsol/VTY tidak bebas.

g. Enkripsikan kata sandi teks biasa

S1(config)# service password-encryption
S2(config)# service password-encryption

Fungsinya: Mengenkripsi password plaintext sehingga tidak terlihat dalam konfigurasi.

h. Buat spanduk yang memperingatkan siapa pun yang mengakses perangkat bahwa akses tanpa izin dilarang

S1(config)# banner motd $ Authorized Users Only! $
S2(config)# banner motd $ Authorized Users Only! $

Fungsinya: Menampilkan pesan peringatan saat seseorang mengakses perangkat.

i. Konfigurasikan alamat IP yang tercantum dalam Tabel Pengalamatan untuk VLAN 1 pada sakelar

S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S2(config)# interface vlan 1
S2(config-if)# ip address 192.168.1.12 255.255.255.0
S2(config-if)# no shutdown
S2(config-if)# exit

Fungsinya: Masuk ke antarmuka virtual VLAN 1, Memberikan alamat IP pada VLAN untuk keperluan manajemen switch, Mengaktifkan antarmuka VLAN, Kembali ke mode sebelumnya.

j. Matikan semua antarmuka yang tidak akan digunakan

S1(config)# interface range f0/2-5, f0/7-24, g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S1(config)# exit
S2(config)# interface range f0/2-17, f0/19-24, g0/1-2
S2(config-if-range)# shutdown
S2(config-if-range)# exit
S2(config)# exit

Fungsinya: Memilih beberapa port sekaligus, Menonaktifkan port agar aman dari serangan (best practice keamanan).

k. Atur jam pada setiap sakelar

S1# clock set 16:45:00 23 November 2025
S2# clock set 16:45:00 23 November 2025

Fungsinya: Mengatur tanggal dan waktu internal pada switch.

l. Simpan konfigurasi yang sedang berjalan ke berkas konfigurasi startup

S1# copy running-config startup-config
S2# copy running-config startup-config

Fungsinya: Menyimpan konfigurasi aktif ke NVRAM sehingga tidak hilang saat reboot.

Langkah 3: Konfigurasikan host PC

Dari tab Desktop pada setiap PC , klik Konfigurasi IP dan masukkan informasi pengalamatan seperti yang ditampilkan dalam Tabel Pengalamatan.

Langkah 4: Uji konektivitas

Uji konektivitas jaringan dengan mencoba melakukan ping antara setiap perangkat berkabel.

Bisakah PC-A melakukan ping ke PC-B? **Ya**

Bisakah PC-A melakukan ping ke S1? **Tidak**

Bisakah PC-B melakukan ping ke S2? **Tidak**

Bisakah S1 melakukan ping ke S2? **Ya**

Jika Anda menjawab tidak untuk pertanyaan di atas, mengapa ping tidak berhasil?

Ping tidak berhasil ketika mencoba ping ke perangkat di subnet yang berbeda. Agar ping tersebut berhasil, gateway default harus ada untuk merutekan lalu lintas dari satu subnet ke subnet lainnya.

Bagian 2: Membuat VLAN dan Menetapkan Port Switch

Langkah 1: Buat VLAN pada switch

Dari Tab Desktop di setiap PC , gunakan Terminal untuk melanjutkan konfigurasi kedua sakelar jaringan.

a. Buat VLAN pada **S1**

S1(config)# vlan 10
S1(config-vlan)# name Operations
S1(config-vlan)# vlan 20
S1(config-vlan)# name Parking_Lot
S1(config-vlan)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# vlan 1000
S1(config-vlan)# name Native
S1(config-vlan)# end

Fungsinya: Membuat VLAN baru di basis data VLAN, Memberikan nama VLAN agar mudah dikenali.

b. Buat VLAN yang sama pada S2

S2(config)# vlan 10
S2(config-vlan)# name Operations
S2(config-vlan)# vlan 20
S2(config-vlan)# name Parking_Lot
S2(config-vlan)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# vlan 1000
S2(config-vlan)# name Native
S2(config-vlan)# end

Fungsinya: Membuat VLAN baru di basis data VLAN, Memberikan nama VLAN agar mudah dikenali.

c. Keluarkan perintah **show vlan brief** untuk melihat daftar VLAN pada **S1**

S1# show vlan brief

Fungsinya: Melihat daftar semua VLAN dan port yang terkait

Apa VLAN defaultnya?

VLAN 1.

Port apa saja yang ditetapkan ke VLAN default?

Semua port switch ditetapkan ke VLAN 1 secara default.

Langkah 2: Tetapkan VLAN ke antarmuka sakelar yang benar

a. Tetapkan VLAN ke antarmuka di **S1**

1.) Tetapkan PC-A ke VLAN Operasi

S1(config)# interface f0/6
S1(config-if)# switchport mode access

S1(config-if)# switchport access vlan 10

Fungsinya: Memilih port individu, Mengatur port menjadi access mode, hanya membawa satu VLAN, Menetapkan port tersebut ke VLAN 10.

2.) Dari VLAN 1, hapus alamat IP manajemen dan konfigurasikan pada VLAN 99

S1(config)# interface vlan 1
S1(config-if)# no ip address
S1(config-if)# interface vlan 99
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# end

Fungsinya: Masuk VLAN 1, Menghapus IP dari VLAN 1, Masuk ke VLAN 99, Menetapkan IP manajemen baru.

b. Keluarkan perintah show vlan brief dan verifikasi bahwa VLAN ditetapkan ke antarmuka yang benar

S1#show vlan brief

Fungsinya: Melihat daftar semua VLAN dan port yang terkait.

c. Keluarkan perintah **show ip interface brief**

S1# show ip interface brief

Fungsinya: Menampilkan ringkasan seluruh antarmuka dan statusnya.

Bagaimana status VLAN 99? Jelaskan!

Status VLAN 99 adalah naik/turun, naik karena VLAN tersebut ada di basis data, tetapi turun karena VLAN tersebut belum ditetapkan ke port aktif.

d. Tetapkan **PC-B** ke VLAN Operasional di **S2**

S2(config)# interface f0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 10

Fungsinya: Memilih port individu, Mengatur port menjadi access mode, hanya membawa satu VLAN, Menetapkan port tersebut ke VLAN 10.

e. Dari VLAN 1, hapus alamat IP manajemen dan konfigurasikan pada VLAN 99 sesuai dengan Tabel Pengalamatan

S2(config)# interface vlan 1
S2(config-if)# no ip address
S2(config-if)# interface vlan 99
S2(config-if)# ip address 192.168.1.12 255.255.255.0

Fungsinya: Masuk VLAN 1, Menghapus IP dari VLAN 1, Masuk ke VLAN 99, Menetapkan IP manajemen baru.

f. Gunakan perintah **show vlan brief** untuk memverifikasi bahwa VLAN ditetapkan ke antarmuka yang benar

S2# show vlan brief

Fungsinya: Melihat daftar semua VLAN dan port yang terkait.

Apakah S1 bisa melakukan ping ke S2? Jelaskan!

Tidak. Alamat IP untuk switch sekarang berada di VLAN 99. Lalu lintas VLAN 99 tidak akan dikirim melalui antarmuka F0/1.

Apakah PC-A dapat melakukan ping ke PC-B? Jelaskan!

Tidak. Antarmuka F0/1 tidak ditetapkan ke VLAN 10, sehingga lalu lintas VLAN 10 tidak akan dikirimkan melaluinya.

Bagian 3: Pertahankan Penugasan Port VLAN dan Basis Data VLAN

Langkah 1: Tetapkan VLAN ke beberapa antarmuka

Dari Tab Desktop di setiap PC , gunakan Terminal untuk melanjutkan konfigurasi kedua sakelar jaringan

a. Pada S1, tetapkan antarmuka F0/11 – 24 ke VLAN99

S1(config)# interface range f0/11-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# end

Fungsinya: Memilih banyak port sekaligus, Menempatkan semua port ke VLAN 99.

b. Keluarkan perintah show vlan brief untuk memverifikasi penugasan VLAN

S1# show vlan brief

Fungsinya: Melihat daftar semua VLAN dan port yang terkait.

c. Tetapkan kembali F0/11 dan F0/21 ke VLAN 10

S1(config)# interface range f0/11, f0/21

S1(config-if-range)# switchport access vlan 10
S1(config-if-range)# end

Fungsinya: Memilih banyak port sekaligus, Mengganti VLAN port menjadi VLAN 10.

d. Verifikasi bahwa penugasan VLAN sudah benar

S1# show vlan brief

Fungsinya: Melihat daftar semua VLAN dan port yang terkait.

Langkah 2: Hapus penugasan VLAN dari suatu antarmuka

a. Gunakan perintah **no switchport access vlan** untuk menghapus penugasan VLAN 99 ke F0/24

S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end

Fungsinya: Memilih port individu, Menghapus VLAN dari port sehingga kembali ke VLAN default (1).

b. Verifikasi bahwa perubahan VLAN telah dilakukan

S1# show vlan brief

Fungsinya: Melihat daftar semua VLAN dan port yang terkait.

VLAN mana yang sekarang dikaitkan dengan F0/24?

VLAN 1, VLAN default

Langkah 3: Hapus ID VLAN dari basis data VLAN

a. Tambahkan VLAN 30 ke antarmuka F0/24 tanpa mengeluarkan perintah VLAN global

S1(config)# interface f0/24
S1(config-if)# switchport access vlan 30

Fungsinya: Memilih port individu, Menetapkan VLAN ke port (meskipun VLAN belum dibuat).

b. Verifikasi bahwa VLAN baru ditampilkan di tabel VLAN

S1# show vlan brief

Fungsinya: Melihat daftar semua VLAN dan port yang terkait.

Apa nama default VLAN 30?

VLAN0030.

c. Gunakan perintah **no vlan 30** untuk menghapus VLAN 30 dari basis data VLAN

S1(config)# no vlan 30
S1(config)# end

Fungsinya: Menghapus VLAN 30 dari basis data VLAN.

d. Jalankan perintah **show vlan brief** . F0/24 ditetapkan ke VLAN 30

S1# show vlan brief

Fungsinya: Melihat daftar semua VLAN dan port yang terkait.

Setelah menghapus VLAN 30 dari basis data VLAN, mengapa F0/24 tidak lagi ditampilkan pada keluaran perintah "show vlan brief" ? Port F0/24 sekarang ditetapkan ke VLAN apa? Apa yang terjadi pada lalu lintas yang ditujukan ke host yang terhubung ke F0/24?

Ketika Anda menghapus sebuah VLAN, semua port yang ditetapkan ke VLAN tersebut menjadi tidak aktif. Port F0/24 masih terhubung ke VLAN 30 tetapi tidak lagi ditampilkan pada keluaran. VLAN 30 sekarang tidak aktif karena tidak ada dalam basis data VLAN. Port apa pun yang terhubung dengan VLAN 30 tidak akan mentransfer lalu lintas apa pun.

e. Pada antarmuka F0/24, jalankan perintah **no switchport access vlan**

S1(config)# interface f0/24
S1(config-if)# no switchport access vlan
S1(config-if)# end

Fungsinya: Memilih port individu, Menghapus VLAN dari port sehingga kembali ke VLAN default (1).

f. Keluarkan perintah **show vlan brief** untuk menentukan penugasan VLAN untuk F0/24

S1# show vlan brief

Fungsinya: Melihat daftar semua VLAN dan port yang terkait.

VLAN mana yang ditetapkan untuk F0/24?

VLAN default, VLAN 1.

Mengapa Anda harus menetapkan ulang port ke VLAN lain sebelum menghapus VLAN tersebut dari basis data VLAN?

Antarmuka yang ditetapkan ke VLAN yang dihapus dari basis data VLAN menjadi tidak aktif dan tidak dapat digunakan hingga ditetapkan ulang ke VLAN lain. Hal ini bisa menjadi masalah yang rumit karena antarmuka yang di-trunk juga tidak muncul dalam daftar port

Bagian 4: Konfigurasikan Trunk 802.1Q Antar Switch

Langkah 1: Gunakan DTP untuk memulai trunking pada F0/1

a. Pada **S1** , atur F0/1 untuk menegosiasikan mode trunk

   S1(config)# interface f0/1
   S1(config-if)# switchport mode dynamic desirable

   Fungsinya: Memilih port individu, Port mencoba membentuk trunk secara aktif dengan DTP.

b. Pada **S1** dan **S2** , jalankan perintah **show vlan brief** . Antarmuka F0/1 tidak lagi ditetapkan ke VLAN 1. Antarmuka trunking tidak tercantum dalam tabel VLAN

   S1# show vlan brief

   Fungsinya: Melihat daftar semua VLAN dan port yang terkait.

c. Jalankan perintah " **show interfaces trunk"** untuk melihat antarmuka trunk. Perhatikan bahwa mode pada **S1** diatur ke "diinginkan", dan mode pada **S2** diatur ke "otomatis"

   S1# show interfaces trunk

   S2# show interfaces trunk

   Fungsinya: Menampilkan antarmuka yang berjalan dalam mode trunk.

d. Verifikasi bahwa lalu lintas VLAN berjalan melalui antarmuka trunk F0/1

   Bisakah S1 melakukan ping ke S2? **Ya**

   Bisakah PC-A melakukan ping ke PC-B? **Ya**

   Bisakah PC-A melakukan ping ke S1? **Tidak**

   Bisakah PC-B melakukan ping ke S2? **Tidak**

   Jika Anda menjawab tidak untuk salah satu pertanyaan di atas, jelaskan di bawah ini.

Switch berada di VLAN 99 dan PC berada di VLAN 10; oleh karena itu, ping antar VLAN tidak berhasil.

Langkah 2: Konfigurasikan antarmuka trunk F0/1 secara manual

a. Pada antarmuka F0/1, ubah mode switchport untuk memaksa trunking. Pastikan untuk melakukan ini pada kedua switch

   S1(config)# interface f0/1
   S1(config-if)# switchport mode trunk
   S2(config)# interface f0/1
   S2(config-if)# switchport mode trunk

   Fungsinya: Memilih port individu, Mengubah port menjadi trunk tanpa negosiasi.

b. Jalankan perintah **"show interfaces trunk"** untuk melihat mode trunk. Perhatikan bahwa mode berubah dari **yang diinginkan** menjadi **aktif**

   S1# show interfaces trunk

   Fungsinya: Menampilkan antarmuka yang berjalan dalam mode trunk.

c. Ubah konfigurasi trunk pada kedua switch dengan mengubah VLAN asli dari VLAN 1 ke VLAN 1000

   S1(config)# interface f0/1
   S1(config-if)# switchport trunk native vlan 1000
   S2(config)# interface f0/1
   S2(config-if)# switchport trunk native vlan 1000

   Fungsinya: Memilih port individu, Menetapkan VLAN 1000 sebagai native VLAN, menggantikan default VLAN 1.

d. Jalankan perintah **show interfaces trunk** untuk melihat trunk. Perhatikan bahwa informasi VLAN Asli telah diperbarui

   S2# show interfaces trunk

   Fungsinya: Menampilkan antarmuka yang berjalan dalam mode trunk.

   Mengapa Anda mungkin ingin mengonfigurasi antarmuka secara manual ke mode trunk, alih-alih menggunakan DTP?

   Tidak semua peralatan menggunakan DTP. DTP merupakan hak milik Cisco, dan penggunaan perintah switchport mode trunk memastikan

bahwa port tersebut akan menjadi trunk, apa pun jenis peralatan yang terhubung ke ujung tautan lainnya.

Mengapa Anda perlu mengubah VLAN asli pada trunk?

Menggunakan VLAN 1, VLAN default, sebagai VLAN asli, merupakan risiko keamanan. Semua protokol kontrol berbeda yang dipertukarkan antar switch dipertukarkan melalui VLAN 1 asli tanpa tag, dan informasi tersebut dapat terekspos jika pengaturan default digunakan pada port yang terhubung dengan pengguna.

Pertanyaan Refleksi

1. Apa yang dibutuhkan agar host di VLAN 10 dapat berkomunikasi dengan host di VLAN 99?

   Jawabannya akan beragam, tetapi untuk memungkinkan perutean antar-VLAN, diperlukan perangkat Layer 3 untuk merutekan lalu lintas antar-VLAN.

2. Apa saja manfaat utama yang dapat diperoleh organisasi melalui penggunaan VLAN yang efektif?

   Jawabannya akan beragam, tetapi manfaat VLAN meliputi: keamanan yang lebih baik, penghematan biaya (penggunaan bandwidth dan uplink yang efisien), kinerja yang lebih tinggi (domain siaran yang lebih kecil), mitigasi badai siaran, peningkatan efisiensi staf TI, serta manajemen proyek dan aplikasi yang lebih sederhana.