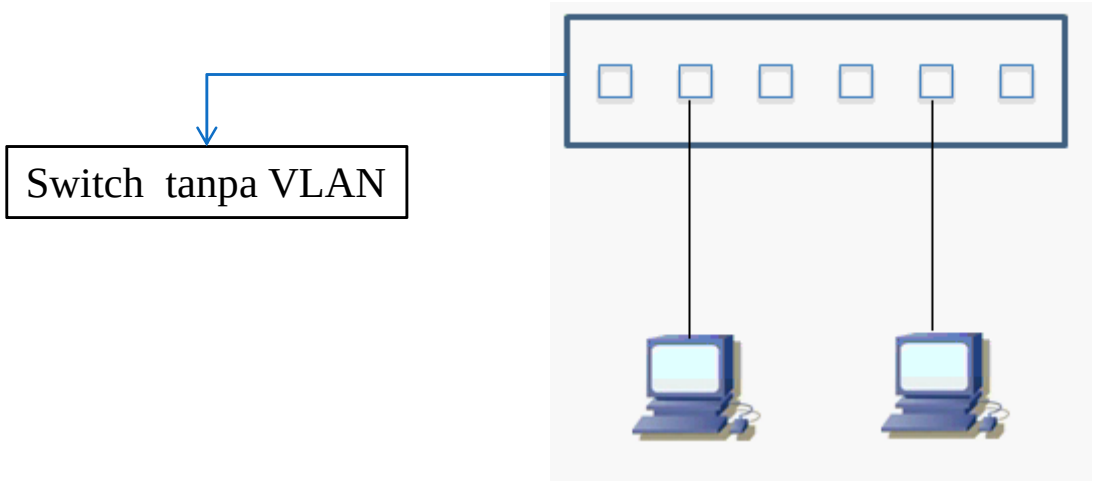
Virtual LAN

Oleh : Akhmad Mukhammad

Objektif

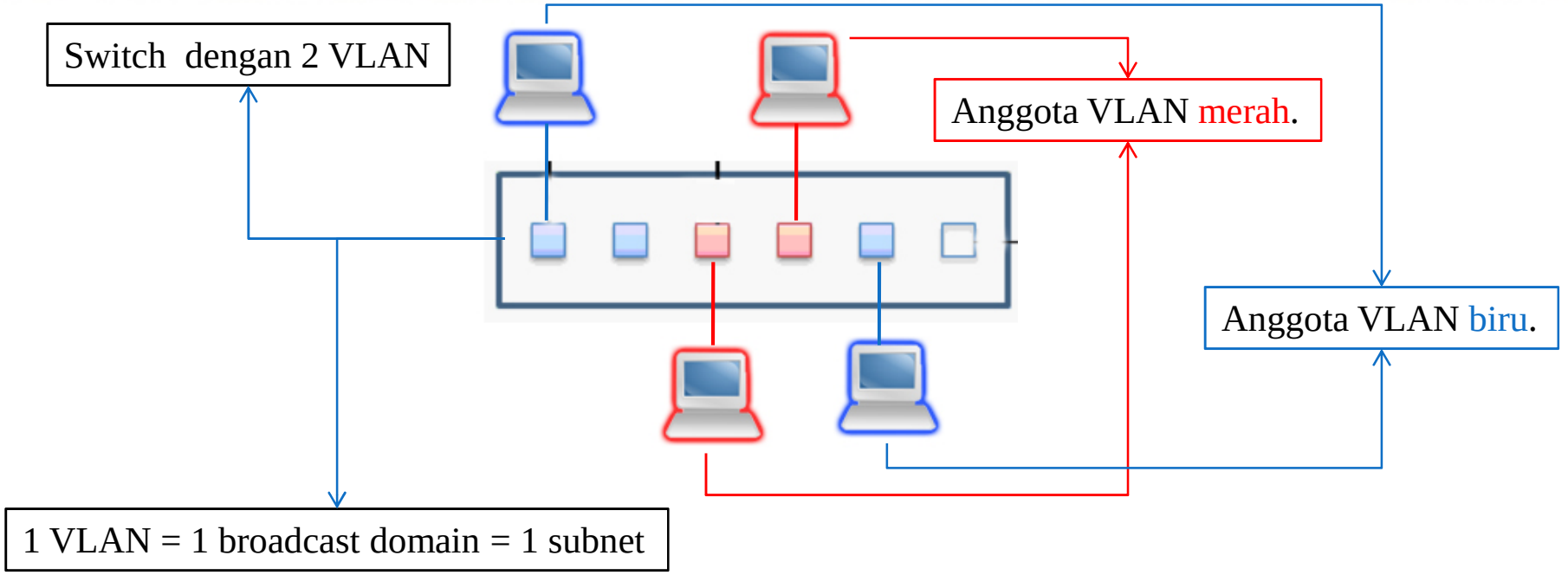
- Memahami peran VLAN dalam network
- Memahami peran VLAN trunking dalam network
- Mengkonfigurasi VLAN dalam switch sesuai dengan topologi network.
- Troubleshoot masalah-masalah yang biasa timbul dalam konfigurasi VLAN dalam switch.

Overview



- 1 collision domain / port.
- Semua port anggota 1 broadcast domain.
  - Paket broadcast akan dikirim ke semua port.
- Semua port berada dalam 1 LAN network (subnet) yang sama.
- Setiap host yang terhubung ke switch bisa berkomunikasi secara langsung dengan host-host lain.

Overview



- Ada 2 broadcast domain.
- Paket broadcast dari VLAN merah hanya akan dikirim ke port-port anggota VLAN merah.
- Setiap VLAN merupakan sebuah LAN network (subnet) tersendiri.
- Sekarang, host pada VLAN merah tidak bisa secara langsung berkomunikasi dengan host pada VLAN biru.
  - Dibutuhkan device layer 3 (Router) sebagai perantara.

VLAN

- VLAN adalah *pengelompokan logik* device-device network yang terhubung pada port switch seakan-akan berada pada network tersendiri.
- VLAN dapat diberi nama.
- Pada switch :
  - Konfigur VLAN.
  - Assign port-port ke VLAN yang diinginkan.
- Pada PC :
  - Assign IP address yang sesuai dengan subnet dalam VLAN.

VLAN -> Keuntungan

- Security
  - Sekelompok device yang memiliki data-data sensitif dapat ditaruh dalam 1 VLAN tersendiri terpisah dari user lain.
- Hemat biaya
  - Untuk membuat network (subnet) tidak perlu switch tersendiri.
- Performa meningkat
  - Memecah broadcast domain dapat mengurangi trafik yang tidak penting.
  - Mencegah broadcast storm.
- Efisiensi meningkat
  - User-user dengan kepentingan yang sama dapat ditaruh dalam 1 VLAN tanpa harus membeli switch baru.
- Flexibility
  - Anggota VLAN tidak harus berada dalam 1 switch dan 1 tempat.

VLAN -> Karakteristik

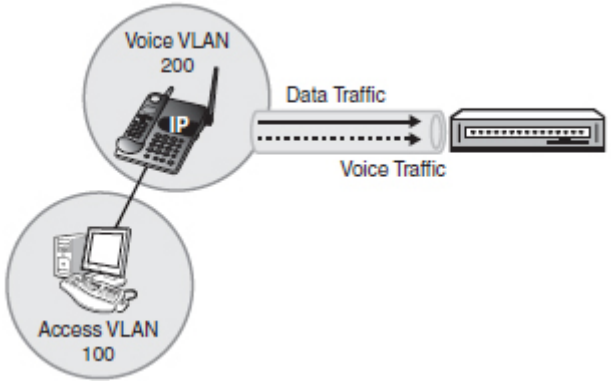
```
2950sw2#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

- VLAN normal-range ID
  - 1 – 1005
  - 1002 – 1005 digunakan untuk VLAN Token Ring dan FDDI
  - VLAN 1, 1002 – 1005 sudah otomatis ada dan tidak bisa di hapus.
  - Konfigurasi VLAN disimpan di file vlan.dat dalam flash.
- VLAN extended-range ID
  - 1006 – 4094
  - Biasanya dipakai oleh service provider
  - Disimpan dalam file running configuration

VLAN -> Tipe-tipe

- VLAN data
  - VLAN yang membawa trafik data dari end-user.
- VLAN default
  - Tanpa di konfigurasi, secara default semua port switch merupakan anggota dari VLAN 1.
  - VLAN 1 tidak bisa dihapus atau di rename.
  - Dianjurkan untuk tidak menggunakan VLAN 1, konfigurasi semua port sebagai anggota dari VLAN selain VLAN 1.
- VLAN management
  - VLAN yang digunakan untuk me-manage device-device network.
  - Secara default menggunakan VLAN 1, sebaiknya diubah.
  - Konfigure IP address switch-switch agar berada dalam 1 subnet VLAN management yang sama.

VLAN -> Voice VLAN



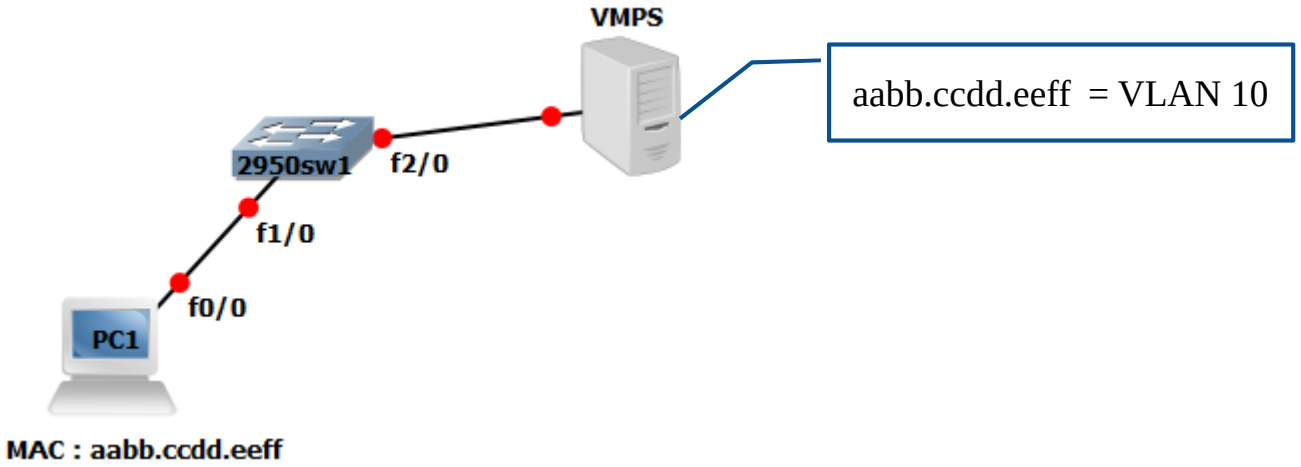
Misal Voice VLAN berada pada VLAN 200, gunakan perintah switchport voice vlan agar port switch mendukung voice.	2950sw1(config-if)#switchport mode access 2950sw1(config-if)#switchport access vlan 150 2950sw1(config-if)#switchport voice vlan 200
Memberikan prioritas pada trafik voice.	2950sw1(config-if)#mls qos trust cos

- Trafik voice sebaiknya dipisahkan dalam VLAN tersendiri.
  - Trafik voice harus diperlakukan secara istimewa.
- Trafik voice membutuhkan
  - Jaminan bandwidth untuk kualitas voice.
  - Prioritas transmisi yang lebih tinggi dari trafik data.
  - Jaminan transmisi meski trafik dalam network sedang padat
  - Delay transmisi kurang dari 150 milisecond.

VLAN -> Voice VLAN

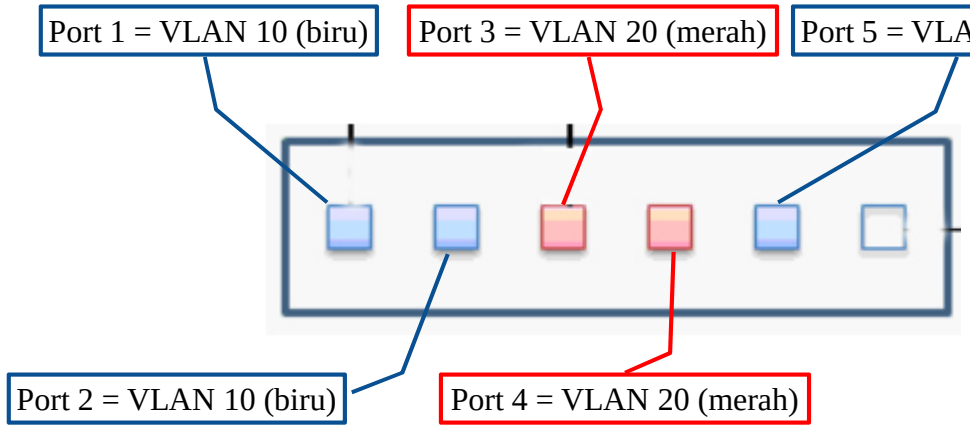
```
2950sw1#show interfaces f0/8 switchport
Name: Fa0/8
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 150 (VLAN0150)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 200 (SUARA)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

VLAN -> Membership



- Dinamik
  - Keanggotaan port-port switch dalam sebuah VLAN ditentukan oleh sebuah server VMPS (VLAN Membership Policy Server).
  - Keanggotaan berdasarkan MAC address device yang terhubung.
  - User / device terhubung ke port manapun tetap berada pada VLAN yang sama.
  - Sudah jarang digunakan pada network production.

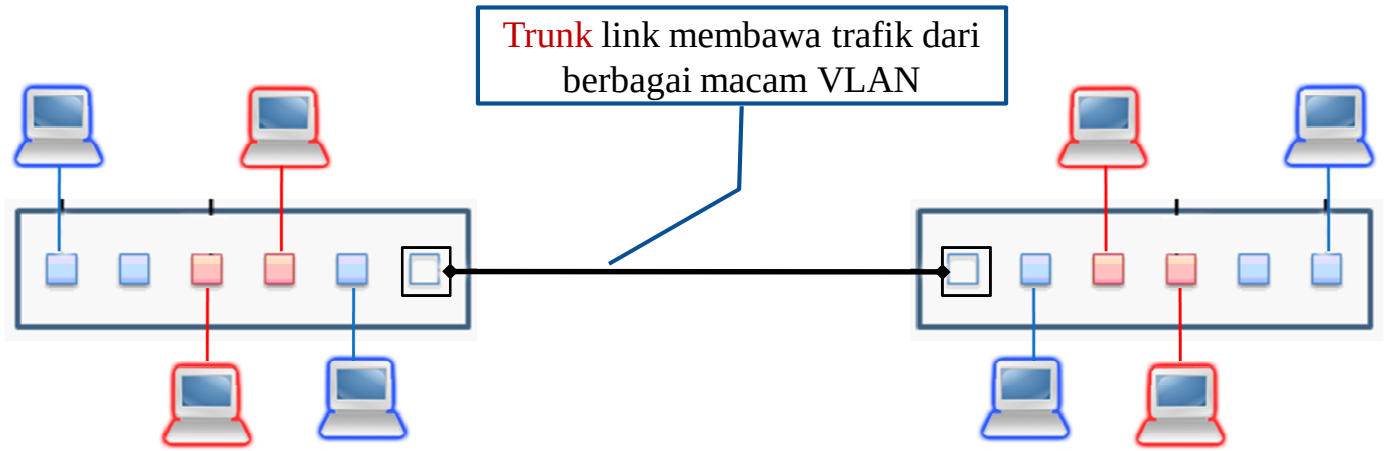
VLAN -> Membership



Siapapun yang terhubung ke port1 akan menjadi anggota dari VLAN 10

- Static
  - Port-port pada switch di konfigurasi secara manual sebagai anggota sebuah VLAN tertentu.
  - Kongurasi dan monitoring lebih mudah.
  - Lebih dianjurkan untuk digunakan.

VLAN -> Trunk

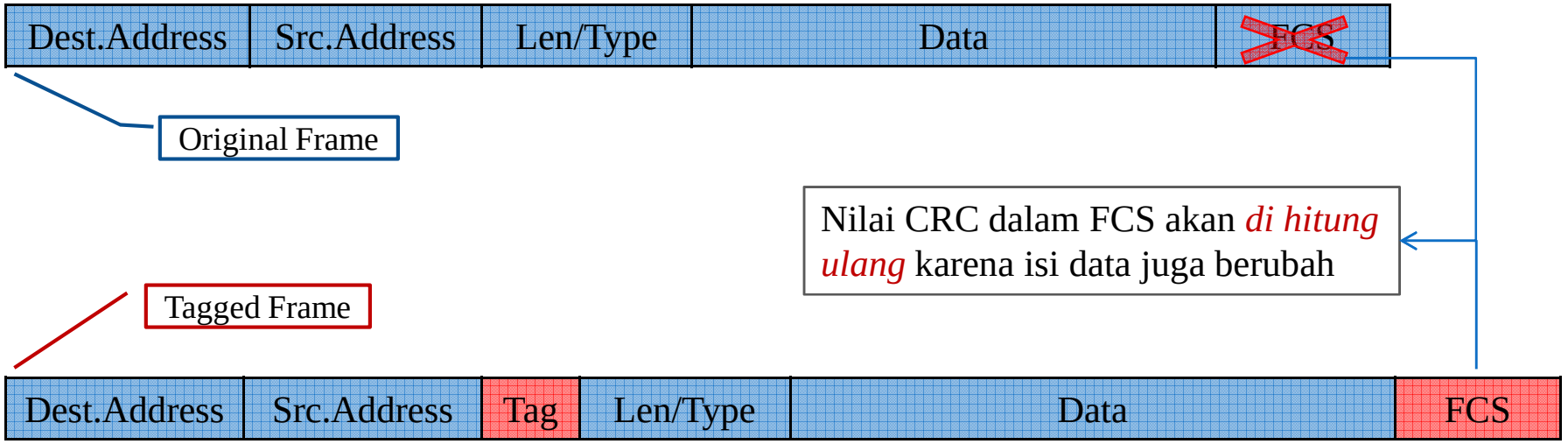


- Link antara :
  - Switch dan switch.
  - Switch dan router.
- Trunk memperluas jangkauan VLAN melebihi satu switch.
- Trunk link membawa trafik data dari berbagai macam VLAN.
- Setiap frame yang lewat akan diberi informasi VLAN (tagging)
  - ISL
  - 802.1Q
- Feature layer 2

VLAN -> Trunk -> ISL

- Protokol Cisco Proprietary.
  - Hanya dapat digunakan oleh produk-produk Cisco.
- Frame di enkapsulasi kedalam frame yang baru.
  - Header (26 bytes)
  - Trailer (CRC 4 bytes)
- Tidak menggunakan native VLAN
  - Frame yang tidak di enkapsulasi akan di drop.

VLAN -> Trunk -> 802.1Q



- Open Standar IEEE.
  - Dapat di implementasikan pada vendor apapun.
- Menyelipkan sebuah Tag kedalam frame original.
  - 4 byte tag
- Menggunakan native VLAN
  - Frame dari host anggota native VLAN tidak akan di tag.
  - Frame yang tidak di tag di anggap anggota native VLAN.

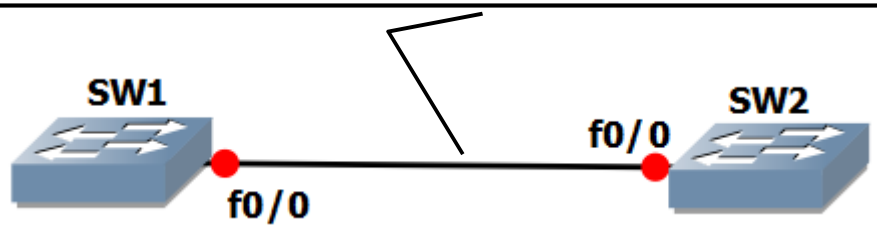
VLAN -> Trunk -> Switchport Mode

Mode	Fungsi
Dynamic Auto	1. Membentuk Trunk tergantung dari request DTP switch seberang. 2. Tidak mengirimkan request DTP.
Dynamic Desirable	1. Mengirimkan request DTP untuk menjadi Trunk. 2. Menjadi trunk jika port switch seberang mode Trunk / Desirable.
Trunk	Mengaktifkan Trunk pada port , terlepas dari status port dari switch seberang ataupun ada tidaknya request DTP dari switch seberang.
Access	Mendisable Trunk pada port, terlepas dari status port dari switch seberang ataupun ada tidaknya request DTP dari switch seberang.
Nonegotiate	Mencegah interface mengirimkan request DTP.

DTP, *Dynamic Trunking Protokol*, merupakan protokol proprietary Cisco, berfungsi mengatur negosiasi trunk dengan port switch seberang.

VLAN -> Trunk -> Switchport Mode

Link hasil interaksi antara 2 port switch yang terhubung



f0/0 vs f0/0	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Acces
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Tidak dianjurkan
Access	Access	Access	Tidak dianjurkan	Access

- Access
  - Gunakan mode access ketika port switch terhubung ke end-device.
  - Port mode access merupakan anggota sebuah VLAN.
- Trunk
  - Gunakan mode trunk ketika port switch terhubung dengan switch lain (atau router).
  - Port mode trunk membawa traffik dari semua VLAN (default).

VLAN -> Config -> Create

Membuat VLAN

Masuk ke mode *global configuration*.	2950sw1#configure terminal
Buat sebuah VLAN dengan syntax vlan <vlan id>.	2950sw1(config)#vlan 10
(optional) beri nama pada vlan tersebut, syntax yang dipakai adalah name <nama vlan>.	2950sw1(config-vlan)#name students
Konfigurasi vlan tidak akan disimpan dalam vlan.dat sampai sesi konfigurasi di akhiri	2950sw1(config-vlan)#end

```
2950sw1#
2950sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
10   students                         active
100  MANAGEMENT                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
2950sw1#
```

VLAN -> Config -> Membership

Meng-assign sebuah port menjadi anggota VLAN

Masuk ke mode interface configuration untuk port yang akan di konfigurasi keanggotaan VLANnya.	2950sw1(config)#interface f0/4
Set port ke mode access. Untuk alasan security, setiap port yang terhubung ke end-user sebaiknya di set ke mode access.	2950sw1(config-if)#switchport mode access
Set port sebagai anggota sebuah VLAN	2950sw1(config-if)#switchport access vlan 10

```
2950sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24
10   students                         active    Fa0/4
100  MANAGEMENT                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Port f0/4 sudah menjadi anggota vlan 10

By default, semua port termasuk anggota VLAN default (VLAN 1)

VLAN -> Config -> Membership

Menghapus keanggotaan sebuah port dari VLAN

Masuk ke mode interface configuration untuk port yang akan di konfigurasi keanggotaan VLANnya.	2950sw1(config)#interface f0/4
Menghapus keanggotaan port dari VLAN.	2950sw1(config-if)#no switchport access vlan

```
2950sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
10   students                         active
100  MANAGEMENT                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Port f0/4 akan kembali menjadi anggota VLAN default.

VLAN -> Config -> Membership

Re-assign keanggotaan sebuah port dari VLAN ke VLAN lain

Masuk ke mode interface configuration untuk port yang akan di konfigurasi keanggotaan VLANnya.	2950sw1(config)#interface f0/4
Set port sebagai anggota VLAN 10.	2950sw1(config-if)#switchport access vlan 10
Re-assign port sebagai anggota VLAN 20.	2950sw1(config-if)#switchport access vlan 20

```
2950sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24
10   students                         active
20   dosen                            active    Fa0/4
100  MANAGEMENT                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Port akan menjadi anggota VLAN yang terakhir di assign (VLAN 20).

VLAN -> Config -> Delete

Menghapus VLAN

Masuk ke mode interface configuration untuk port yang akan di konfigurasi keanggotaan VLANnya.	2950sw1(config)#interface f0/4
Menghapus vlan 20	2950sw1(config)#no vlan 20

```
2950sw1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                 Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                 Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24
10   students                          active
100  MANAGEMENT                        active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Port f0/4 tidak ditemukan di anggota VLAN manapun.

User yang terhubung ke Port f0/4 tidak bisa melakukan koneksi kemanapun

- Sebelum menghapus sebuah VLAN, pastikan untuk meng-assign port-port anggota VLAN tersebut menjadi anggota VLAN lain.
- Alternatif :
  - Gunakan delete flash:/vlan.dat , kemudian reload switch untuk menghapus semua konfigurasi VLAN.

VLAN -> Config -> Verifikasi

```
2950sw1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/5, Fa0/6, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24
10   students                         active
20   DOSEN                            active    Fa0/4
100  MANAGEMENT                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

show vlan brief

Menampilkan informasi semua VLAN dan port-port yang menjadi anggotanya.

```
2950sw1#show vlan summary
Number of existing VLANs            : 8
 Number of existing VTP VLANs       : 8
 Number of existing extended VLANs  : 0
```

show vlan summary

Menampilkan statistik konfigurasi VLAN

VLAN -> Config -> Verifikasi

Port trunk bisa dilalui trafik VLAN apapun termasuk VLAN 20.

Port anggota bisa dilalui trafik VLAN 20.

```
2950sw1#show vlan id 20

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
20   DOSEN                            active    Fa0/2, Fa0/3, Fa0/4

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

show vlan id <id>

Menampilkan informasi VLAN tertentu dan port-port yang bisa dilalui.

VLAN -> Config -> Verifikasi

```
2950sw1#show interfaces f0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (DOSEN)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
2950sw1#
```

Port di konfigurasi sebagai mode access secara statik (switchport mode access)

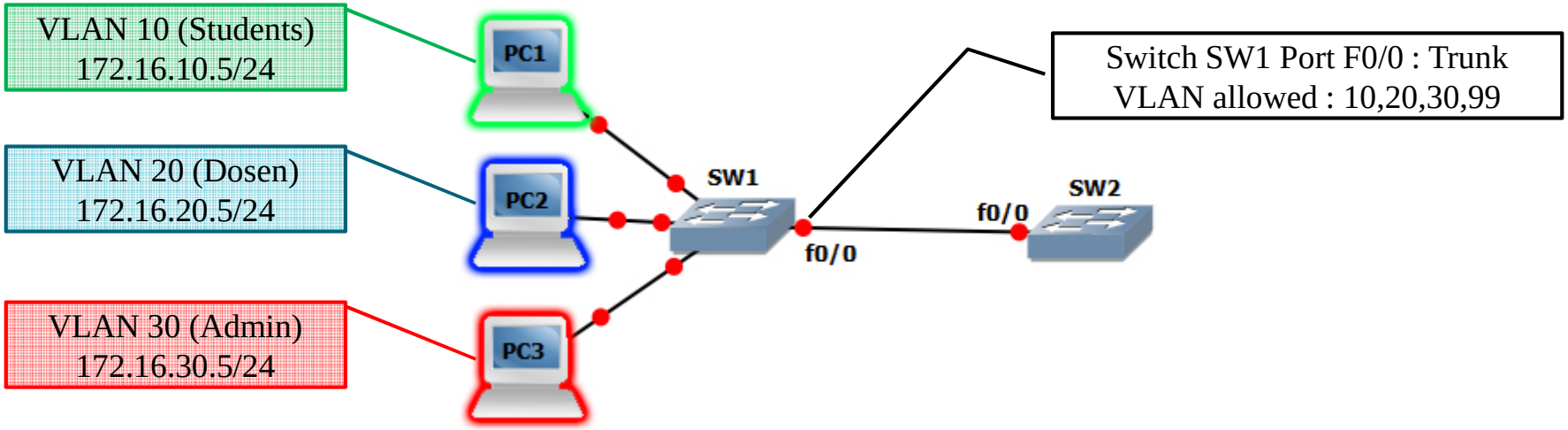
Port berada pada mode access, dan termasuk anggota VLAN 20

VLAN -> Config -> Switchport Mode

2950sw1(config)#interface f0/4
Masuk ke mode interface configuration untuk port yang akan di konfigurasi keanggotaan VLANnya.
2950sw1(config-if)#switchport mode trunk
Mengkonfigurasi port sebagai mode trunk
2950sw1(config-if)#switchport mode access
Mengkonfigurasi port sebagai mode access
2950sw1(config-if)#switchport mode dynamic desirable
Mengkonfigurasi port sebagai mode dynamic desirable, tidak bisa di kombinasikan dengan nonegotiate.
2950sw1(config-if)#switchport mode dynamic auto
Mengkonfigurasi port sebagai mode dynamic auto, tidak bisa di kombinasikan dengan nonegotiate.
2950sw1(config-if)#switchport nonegotiate
Mengkonfigurasi port agar men-disable fitur DTP (tidak mengirimkan paket request DTP).

- Port switch terhubung ke switch lain
  - Set mode Trunk : switchport mode trunk
  - Set nonegotiate : switchport nonegotiate
- Port switch terhubung ke end-device (user client, server)
  - Set mode access : switchport mode access

VLAN -> Config -> Trunking



2950sw1(config-if)#switchport mode trunk
Konfigurasi port sebagai mode trunk
2950sw1(config-if)#switchport trunk encapsulation dot1q
Tentukan metode tagging yang digunakan, dot1q (802.1q) atau ISL.
2950sw1(config-if)#switchport trunk native vlan 100
Tentukan VLAN yang digunakan sebagai native VLAN untuk trunking menggunakan 802.1q
2950sw1(config-if)#switchport trunk allowed vlan add 10,20
Tentukan VLAN-VLAN yang diijinkan untuk melewati link trunk ini (secara default trafik semua VLAN bisa melewati link Trunk).

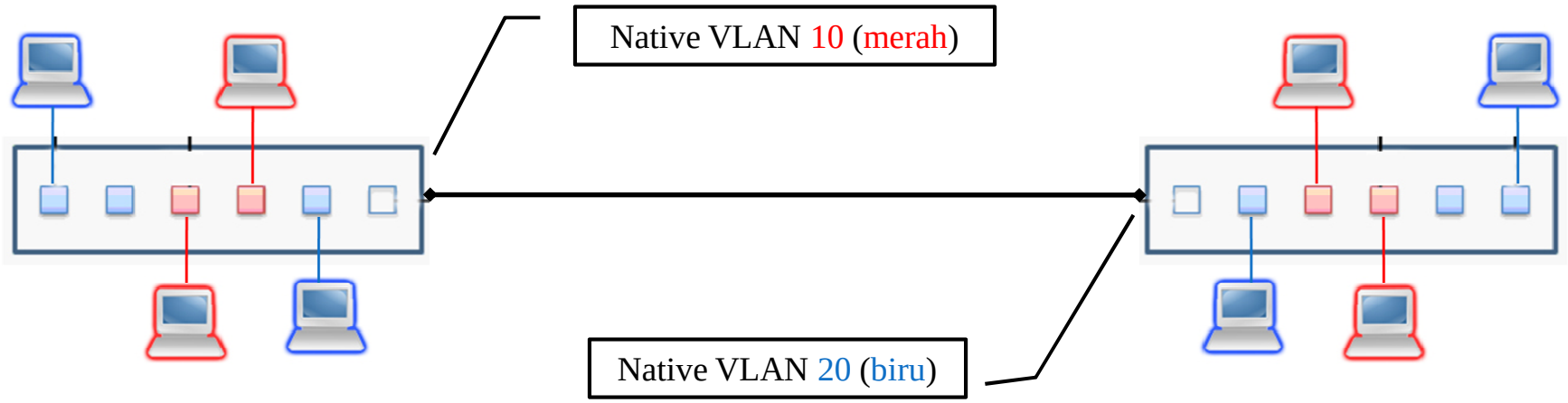
VLAN -> Config -> Trunking

```
2950sw1#show interfaces f0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (DOSEN)
Trunking Native Mode VLAN: 100 (MANAGEMENT)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
```

Port di konfigurasi sebagai mode trunk secara statik (switchport mode trunk)

Native VLAN adalah VLAN 100. default native VLAN adalah VLAN 1

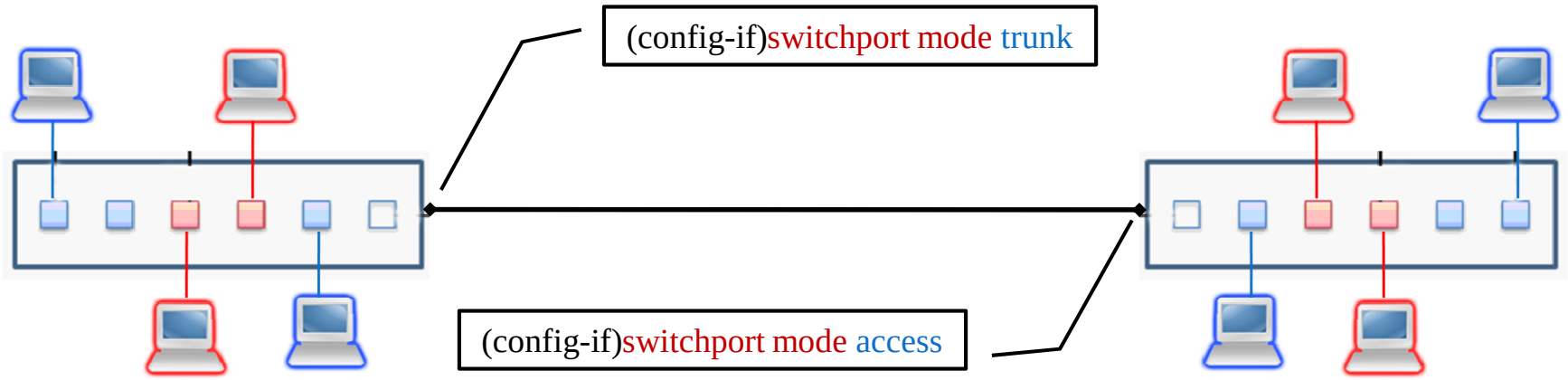
VLAN -> Masalah Umum



Native VLAN mismatch, dapat menimbulkan resiko keamanan, network merah di sebelah kiri seolah-olah berada dalam 1 network dengan network biru di sebelah kanan.

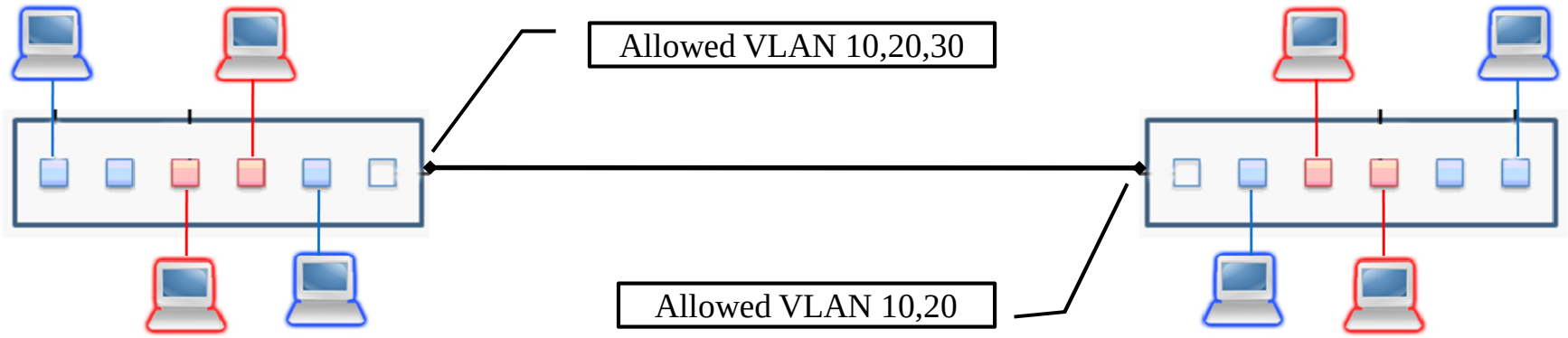
Terjadi pada metode tagging 802.1q, ISL tidak ada fitur native VLAN

VLAN -> Masalah Umum



Mode Trunk Mismatch, dapat menimbulkan masalah koneksi putus, misal satu port di konfigurasi sebagai trunk sementara port switch seberangnya di konfigurasi sebagai access

VLAN -> Masalah Umum



Allowed VLAN Mismatch, dapat menimbulkan masalah koneksi, dalam contoh di atas, VLAN 30 di sebelah kiri tidak bisa menghubungi VLAN 30 di kanan dan sebaliknya.

Terima Kasih