# TUJUAN

**MODUL II**

**VLAN**

* 1. Mampu Mengetahui konsep dan konfigurasi VLAN pada *Switch Cisco.*
  2. Mengetahui implementasi VLAN pada sebuah jaringan computer.

# DASAR TEORI

* 1. VLAN

Sebuah VLAN adalah pengelompokan logikal dari *user* dan sumber daya *network* yang terhubung ke *port*-*port* yang telah ditentukan secara administratif pada sebuah *switch*. Ketika seorang administrator membentuk VLAN-VLAN, maka ia diberikan kemampuan untuk menciptakan *broadcast domain* yang lebih kecil di dalam *internetwork switch layer 2*. Dengan cara memilih *port*-*port* yang berbeda pada *switch* untuk *sub-network* yang berbeda pula. Sebuah VLAN diperlakukan seperti *subnet* atau *broadcast domain*-nya sendiri, yang berarti *frame*-*frame* yang di-*broadcast* pada sebua *network* hanya di-*switch* atau dialihkan di antara *port*-*port* yang dikelompokkan secara logikal di dalam VLAN yang sama.

Dalam kondisi seperti ini sebuah *router* dapat tidak diperlukan ataupun masih diperlukan tergantung dari apa yang ingin dilakukan. Secara *default* semua *host* dalam sebuah VLAN tertentu tidak dapat berkomunikasi dengan *host*-*host* yang merupakan anggota VLAN yang lain, jadi jika diinginkan komunikasi antar VLAN bisa dilakukan maka diperlukan sebuah *router* .[1]

* 1. Dasar-dasar VLAN

*Network*-*network* yang ada pada *switch layer* 2biasanya di rancang sebagai *network*-*network* yang *flat* atau datar setiap paket *broadcast* yang ditransmisikan akan terlihat oleh setiap alat di *network* tidak tergantung apakah alat itu membutuhkan atau tidak. Secara *default*, *Router* membolehkan *broadcast* hanya di dalam *network* dimana paket *broadcast* itu berasal, tetapi *switch*-*switch* dapat mem-*forward* paket-paket *broadcast* ke semua *segmen*. Alasan mengapa disebut *network* yang *flat* adalah karena *network*-*network* berada dalam satu *broadcast domain*, jadi bukan karena rancangan datar secara fisik.

banyak masalah yang bisa dipecahkan pada *switching layer 2* dengan VLAN. Ada beberapa cara VLAN dalam menyederhanakan *management network*:

* + 1. Penambahan, perpindahan, dan perubahan *network* dilakukan dengan mengkonfigurasi sebuah *port* ke VLAN yang sesuai.
    2. Sekelompok *user* yang memerlukan keamanan yang tinggi dapat ditempatkan pada sebuah VLAN sehingga tidak *user* di luar VLAN tersebut yang dapat berkomunikasi dengan mereka.
    3. Sebagai pengelompokan logikal *user* berdasarkan fungsi, VLAN dapat dianggap independen dari lokasi fisikal atau geografisnya.
    4. VLAN dapat meningkatkan keamanan *network*
    5. VLAN-VLAN meningkatkan jumlah *broadcast* domain dan pada saat yang sama memperkecil ukurannya sendiri.[3]
  1. Mekanisme VLAN

VLAN diciptakan melalui konfigurasi pada *switch* atau pada *server* eksternal dan direferensi oleh *switch*. Paket *broadcast* tidak akan mencapai VLAN lainnya karena tiap VLAN merupakan *broadcast domain* tersendiri. *Broadcast domain* merupakan pengelompokkan berdasarkan *layer* 3, oleh karena itu diperlukan *device layer* 3 seperti *router* untuk mem-*forward traffic* antar VLAN.

VLAN terdiri atas *device*-*device* yang berada dalam satu *bridging domain*. Untuk implementasi VLAN, setiap VLAN memerlukan *address (bridging)* tablemasing- masing. *Bridging table* ini di simpan pada *switch*. Jika suatu paket diterima oleh *port* VLAN tertentu maka hanya *address table* VLAN tersebut yang akan diperiksa.

*Default* VLAN untuk semua *port* pada *switch* adalah *management* VLAN yang selalu merupakan VLAN 1. VLAN 1 ini tidak bisa di hapus dan setidaknya satu *port* harus menjadi anggota *management* VLAN untuk mengatur *switch.* [1]

Menurut Tanenbaum, ada tiga metode yang digunakan untuk menerapkan VLAN yaitu:

* + 1. *Port*-*based*
       1. VLAN di bagi berdasarkan *port*.
       2. Metode konfigurasi yang paling banyak digunakan.
       3. *Port* ditugaskan secara individual, dalam grup, dalam baris, atau melewati dua *switch* atau lebih.
       4. Sederhana untuk digunakan.
       5. Sering di implementasikan dimana DHCP digunakan untuk memberikan alamat IP ke *host*.
    2. *MAC*-*based*
       1. VLAN dibagi berdasarkan *MAC address*.
       2. Saat ini jarang di implementasikan.
       3. Setiap alama harus dimasukkan ke dalam *switch* dan dikonfigurasi secara individual.
       4. Lebih berguna untuk pengguna.
       5. Sulit untuk di *manage* dan *troubleshoot*
    3. *Protocol*-*based*
       1. VLAN dibagi berdasarkan *protocol layer* 3 atau IP.
       2. Dikonfigurasi seperti *MAC address* tapi menggunakan alamat IP.
       3. Jarang digunakan.[2]
  1. Manfaat dalam menggunakan VLAN

Menurut *Cisco System Inc*., beberapa tujuan utama dari implementasi VLAN pada jaringan antara lain:

* + 1. *Security*

Implementasi VLAN dalam suatu perusahaan memungkinkan terkontrolnya keamanan data dalam tiap-tiap departemen karena berada dalam satu *broadcast domain* yang sama.

* + 1. *Cost Reduction*

Mengurangi biaya yang akan dikeluarkan apabila terdapat penambahan jaringan dan lebih efisien dalam pemakaian *bandwidth* dan *up-links.*

* + 1. *Higher Performance*

Memisahkan jaringan *layer* 2 ke dalam berbagai *logical workgroup* (*broadcast domain*) yang dapat mengurangi *traffic* data yang tidak diperlukan dan meningkatkan performance jaringan.

* + 1. *Broadcast Storm Mitigation*

Penerapan VLAN dapat mengurangi jumlah *device* yang turut serta dalam sebuah *broadcast storm*.

* + 1. *Improved IT Staff Efficiency*

Penerapan VLAN memudahkan pengaturan jaringan dan konfigurasi VLAN dapat langsung tersebar apabila ada sebuah switch baru yang terhubung ke dalam jaringan tersebut.[2]

Menurut Odom, secara keseluruhan VLAN memberikan keuntungan sebagai berikut :

1. Pemindahan, penambahan host, dan perubahan host menjadi lebih mudah.
2. Dengan menggunakan device *layer* 3 di antara VLAN, pengendalian administratif menjadi lebih mudah
3. Konsumsi *bandwidth* LAN lebih efisien jika dibandingkan konsumsi

*bandwidth* dalam suatu *broadcast domain* yang besar.

1. Penggunaan CPU lebih efisien karena lebih sedikit mem-*forward* paket *broadcast*.
   1. Keanggotaan VLAN

Keanggotaan sebuah *device* dalam sebuah VLAN dapat ditentukan dengan salah satu dari dua metode yaitu *static* dan *dynamic*. Apabila yang digunakan adalah *static* VLAN, maka setiap *port* dari sebuah *switch* harus di-*assign* secara manual dengan menggunakan perintah *Interface Subconfiguration*. VLAN yang diciptakan dengan menggunakan cara ini disebut juga dengan *port-based* VLAN.

Keanggotaan *dynamic* VLAN diciptakan dengan menggunakan aplikasi *network management* seperti *CiscoWorks* 2000. Keanggotaan *dynamic* VLAN memungkinkan penentuan *device* yang masuk ke dalam suatu VLAN berdasarkan *MAC address*. Pada saat suatu *device* masuk ke

dalam jaringan, jaringan tersebut akan mengecek *database* yang tersimpan dalam *switch* jaringan tersebut untuk menentukan keanggotaan dari *device* tersebut.

Informasi keanggotaan (*database*) pada *dynamic* VLAN disimpan pada suatu *switch* yang berfungsi sebagai *policy server* yang biasa disebut dengan VLAN *Membership Policy Server* (VPMS). Salah satu *switch* yang berada pada jaringan VLAN harus diatur menjadi *policy server*.

*Dynamic* VLAN mempunyai satu kelebihan dibandingkan *static* VLAN yaitu *plug and play movability*. Sebagai contoh jika sebuah PC hendak dipindahkan dari satu *port* ke *port* lainnya pada *switch* yang berbeda maka pengguna akan secara otomatis dialokasikan ke VLAN yang sesuai. Walaupun demikian di sisi lain ada satu keuntungan *static* VLAN dibandingkan *dynamic* VLAN. Proses konfigurasi pada *static* VLAN lebih mudah dan langsung. Sedangkan pada *dynamic* VLAN banyak persiapan

awal yang harus dilakukan dalam menghubungkan pengguna ke dalam VLAN.[4]

Selain *static* dan *dynamic*, keanggotan VLAN secara umum juga dapat dibedakan menjadi *End-To-End* VLAN dan geografi VLAN.

* + 1. Jaringan *End-To-End* memiliki karakteristik:

1. Keanggotaan VLAN suatu *user* tergantung dari departemen/bagian dalam suatu organisasi.
2. Semua anggota VLAN mempunyai pola *traffic flow* 80/20 (80% *traffic* berada pada VLAN *local* dan 20% keluar dari VLAN *local* yang sama).
3. Keanggotaan VLAN tidak berubah walaupun *user* berpindah lokasi secara geografis.
4. Setiap VLAN mempunyai sebuah set keamanan yang sama untuk setiap pengguna.
   * 1. Jaringan VLAN geografis memiliki karakteristik:
        1. Keanggotaan VLAN berdasarkan lokasi pengguna.
        2. Biasanya memiliki pola *traffic* flow 20/80 (20% *traffic* berada pada VLAN *local*, dan 80% keluar dari VLAN *local*) karena

biasanya perusahaan kini mulai melakukan sentralisasi sumber daya.

* 1. *Link* VLAN

VLAN dibangun menggunakan berbagai perangkat seperti *switch*, *router*, PC dan sebagainya. Tentunya diperlukan hubungan atau *link* di antara perangkat-perangkat tersebut. *Link* seringkali disebut sebagai *interface*.

Menurut Iwan Sofana, ada dua jenis *link* yang umum digunakan dalam VLAN yaitu:

* + 1. *Access link*

*Access link* merupakan tipe *link* yang umum dan dimiliki oleh hampir semua jenis *switch* VLAN. *Access link* lazimmnya digunakan untuk menghubungkan komputer dengan *switch*. *Access link* tidak lain merupakan *port switch* yang sudah terkonfigurasi. Selama proses transfer data, *switch* akan membuang informasi tentang VLAN. Anggota suatu VLAN tidak bisa berkomunikasi dengan anggota VLAN yang lain kecuali jika dihubungkan dengan device *layer* 3.

* + 1. *Trunk link*

Istilah *Trunk* diambil dari sistem telepon yang dapat mengangkut beberapa percakapan sekaligus (*multiple conversation*). *Trunk link* digunakan untuk menghubungkan *switch* dengan *switch* yang lain, *switch* dengan *router*, atau *switch* dengan *server*. Jadi, *port* telah dikonfigurasi untuk dilalui berbagai VLAN (tidak hanya sebuah VLAN). *Trunk link* hanya mendukung teknologi *Fast* (100 Mbps) atau Gigabit (1Gbps) *Ethernet*. Sebab *trunk link* lazimnya dihubungkan dengan *network backbone* berkecepatan tinggi. Wajar jika kebutuhannya lebih tinggi dibandingkan *access link*.

Selain kedua jenis *link* di atas, masih ada satu lagi jenis *link* yang merupakan gabungan dari *trunk* dan *access link* yaitu *hybrid link*. [1]

* 1. *Access* VLAN

Menurut *Cisco System Inc*., akses VLAN dibagi menjadi dua yaitu

normal *range* dan *extended range*.

* + 1. *Normal Range* VLAN
       1. Digunakan dalam jaringan skala kecil dan menengah. Rentang VLAN ID mulai dari 1 hingga 1005.
       2. ID antara 1002 sampai 1005 digunakan untuk *Token Ring* dan FDDI VLAN.
       3. ID 1 dan 1002 sampai 1005 secara otomatis akan dibuat dan tidak bisa dihapus. Konfigurasi ini disimpan dalam VLAN *database file* yang dinamakan *vlan.dat*. *File* ini terletak pada *flash memory switch*. VLAN *Trunking Protocol* (VTP) yang berfungsi untuk mengatur konfigurasi VLAN antar *switch* hanya bisa mengenali *normal range* ini dan menyimpannya dalam VLAN *database*.
    2. *Extended Range* VLAN
       1. Memungkinkan ISP untuk mengembangkan infrastrukturnya untuk mencukupi lebih banyak pelanggan.
       2. Rentang VLAN ID antara 1006 sampai 4094.
       3. Fitur VLAN yang dimiliki lebih sedikit dibanding VLAN yang termasuk *normal range*.
       4. Konfigurasinya disimpan dalam *running configuration*.
       5. VTP tidak dapat mengenali *extended range* VLAN ini.

# Tipe VLAN

Menurut *Cisco System Inc*., tipe-tipe VLAN dapat dibedakan menjadi :

* + 1. Data VLAN

VLAN yang dikonfigurasi hanya untuk *user* dan tidak memiliki kemampuan untuk mengirim *voice-based traffic*.

* + 1. *Default* VLAN

Ketika *switch* pertama kali dinyalakan maka semua *port* yang ada di- *switch* akan menjadi anggota *default* VLAN. *Default* VLAN dari *switch Cisco* adalah VLAN 1 dimana VLAN tersebut tidak dapat diganti namanya atau dihapus.

* + 1. *Native* VLAN

*Link* antara *switch* dengan *switch* atau *switch* dengan *router* menjadi

*native* VLAN. Jangan menjadikan VLAN 1 sebagai *native* VLAN.

*Native* VLAN berfungsi untuk *tagged*-*traffic* dan *untagged*- *traffic*. Tujuannya agar *switch non-Cisco* bisa terhubung dengan *device Cisco* yang lainnya.

* + 1. *Management* VLAN

VLAN yang dibuat untuk admin dalam mengatur kapabilitas dari *switch* atau VLAN yang dibuat untuk me-*manage device* yang terhubung.

* + 1. *Voice* VLAN

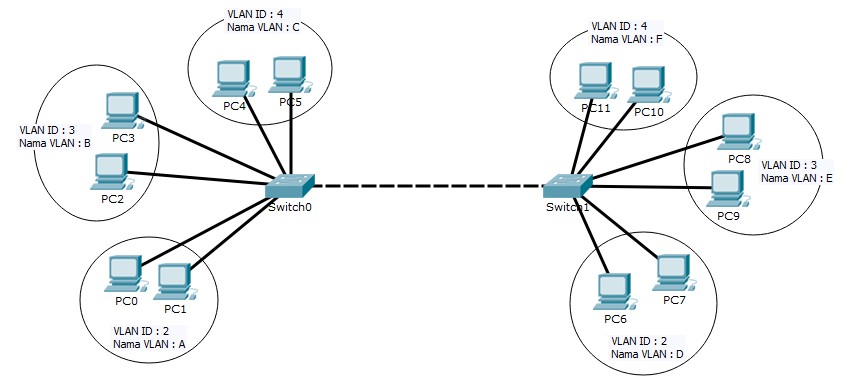
VLAN yang ditujukan hanya untuk *traffic voice*.[4]

# ALAT DAN BAHAN

* 1. Laptop/PC
  2. Software Packet Tracer

**D. PERMASALAHAN**

1. Membuat jaringan VLAN seperti gambar di bawah ini:



**Gambar 2.1** Jaringan VLAN

* 1. Mengatur akses VLAN seperti aturan berikut:

Tabel 2.1 Tabel akses VLAN pada setiap PC

|  |  |  |
| --- | --- | --- |
| **A ≠ B** | **D ≠ E** | **A = D** |
| **A ≠ C** | **D ≠ F** | **B = E** |
| **B ≠ C** | **E ≠ F** | **C = F** |

Konfigurasi IP Address:

Tabel 2.2 Tabel konfigurasi VLAN pada setiap PC

|  |  |  |  |
| --- | --- | --- | --- |
| **Switch** | **Nama VLAN** | **PC** | **IP Address** |
| **0** | **A** | **0** | **192.168.10.1** |
| **1** | **192.168.10.2** |
| **B** | **2** | **192.168.10.3** |
| **3** | **192.168.10.4** |
| **C** | **4** | **192.168.10.5** |
| **5** | **192.168.10.6** |
| **1** | **D** | **6** | **192.168.10.7** |
| **7** | **192.168.10.8** |
| **E** | **8** | **192.168.10.9** |
| **9** | **192.168.10.21** |
| **F** | **10** | **192.168.10.22** |
| **11** | **192.168.10.23** |

* 1. Catat hasil konfigurasi VLAN (daftar VLAN) pada tabel yang telah disediakan, lalu screenshot hasilnya.
  2. Lakukan tes koneksi antar PC pada VLAN yang sama maupun pada VLAN yang berbeda, catat hasilnya pada tabel yang telah disediakan, lalu screenshot hasilnya.

# LANGKAH PERCOBAAN

* 1. Membuat jaringan VLAN
     1. Langkah 1

Membuka aplikasi *Packet Tracer*.

* + 1. Langkah 2

Memasukkan dua buah *switch.*

* + 1. Langkah 3

Menghubungkan *Switch0* dengan *Switch1* dengan menggunakan kabel *Cross* – *Over* melalui *Port FastEthernet 0/7* pada masing-masing *switch*.

* + 1. Langkah 4

Memasukkan 6 buah PC untuk masing – masing *switch.*

* + 1. Langkah 5

Mengkonfigurasi IP *Address* masing – masing PC tersebut. Klik PC0, pindah ke *tab* *Desktop*, klik IP *configuration*, pilih *Static*, masukkan 192.168.8.1 untuk IP *Address* dan 255.255.255.0 untuk *Subnet* *Mask*.

* + 1. Langkah 6

Mengulangi langkah ke-5 untuk PC1sampai PC11. Namun IP *Address* yang dimasukkan berbeda, sedangkan *Subnet Mask*-nya sama. Berikut tabel IP *Address* dan *Subnet Mask* PC 1 sampai 11.

Tabel 2.3 Tabel daftar IP *address* dan *subnet* *mask* setiap PC

|  |  |  |
| --- | --- | --- |
| **PC** | **IP *Address*** | ***Subnet Mask*** |
| 0 | 192.168.10.1 | 255.255.255.0 |
| 1 | 192.168.10.2 | 255.255.255.0 |
| 2 | 192.168.10.3 | 255.255.255.0 |
| 3 | 192.168.10.4 | 255.255.255.0 |
| 4 | 192.168.10.5 | 255.255.255.0 |
| 5 | 192.168.10.6 | 255.255.255.0 |
| 6 | 192.168.10.7 | 255.255.255.0 |
| 7 | 192.168.10.8 | 255.255.255.0 |
| 8 | 192.168.10.9 | 255.255.255.0 |
| 9 | 192.168.10.21 | 255.255.255.0 |
| 10 | 192.168.10.22 | 255.255.255.0 |
| 11 | 192.168.10.23 | 255.255.255.0 |

* + 1. Langkah 7

Menghubungkan PC0, PC1, PC2, PC3, PC4, PC5ke *Switch0*menggunakan kabel *Straight*-*Through*. Di mana pada *Switch0*, untuk

PC0 menggunakan *Port* *FastEthernet0*/1

PC1 menggunakan *Port* *FastEthernet0*/2

PC2 menggunakan *Port* *FastEthernet0*/3

PC3 menggunakan *Port* *FastEthernet0*/4

PC4 menggunakan *Port* *FastEthernet0*/5

PC5 menggunakan *Port* *FastEthernet0*/6

* + 1. Langkah 8:

Menghubungkan PC6,PC7, PC8,PC9,PC10,PC11ke *Switch1*menggunakan kabel *Straight*-*Through*. Di mana pada *Switch1*, untuk

PC6 menggunakan *Port* *FastEthernet0*/1

PC7 menggunakan *Port* *FastEthernet0*/2

PC8 menggunakan *Port* *FastEthernet0*/3

PC9 menggunakan *Port* *FastEthernet0*/4

PC10 menggunakan *Port* *FastEthernet0*/5

PC11 menggunakan *Port* *FastEthernet0*/6

* 1. Mengatur akses VLAN
     1. Langkah 1

Mengkonfigurasi VLAN pada *Switch0*. Klik *Switch0*, pindah ke *tab* CLI, masukkan *command* di bawah ini:

|  |
| --- |
| Switch>enable  Switch#configure terminal  Switch(config)#interface FastEthernet 0/7  Switch(config-if)#switchport mode trunk  Switch(config-if)#exit  Switch(config)#vlan 2  Switch(config-vlan)#name A  Switch(config-vlan)#exit  Switch(config)#vlan 3  Switch(config-vlan)#name B  Switch(config-vlan)#exit  Switch(config)#vlan 4  Switch(config-vlan)#name C  Switch(config-vlan)#exit  Switch(config)#interface fa 0/1  Switch(config-if)#switchport access vlan 2  Switch(config-if)#exit  Switch(config)#interface fa 0/2  Switch(config-if)#switchport access vlan 2  Switch(config-if)#exit  Switch(config)#interface fa 0/3  Switch(config-if)#switchport access vlan 3  Switch(config-if)#exit  Switch(config)#interface fa 0/4  Switch(config-if)#switchport access vlan 3  Switch(config-if)#exit  Switch(config)#interface fa 0/5  Switch(config-if)#switchport access vlan 4  Switch(config-if)#exit  Switch(config)#interface fa 0/6  Switch(config-if)#switchport access vlan 4  Switch(config-if)#exit  Switch(config)#exit  Switch#  Switch#show vlan brief |

**Gambar 2.2** Konfigurasi *switch0*

* + 1. Langkah 2

Mengkonfigurasi VLAN pada *Switch1*. Klik *Switch1*, pindah ke *tab* CLI, masukkan *command* di bawah ini:

|  |
| --- |
| Switch>enable  Switch#configure terminal  Switch(config)#interface FastEthernet 0/7  Switch(config-if)#switchport mode trunk  Switch(config-if)#exit  Switch(config)#vlan 2  Switch(config-vlan)#name D  Switch(config-vlan)#exit  Switch(config)#vlan 3  Switch(config-vlan)#name B  Switch(config-vlan)#exit  Switch(config)#vlan 4  Switch(config-vlan)#name F  Switch(config-vlan)#exit  Switch(config)#interface fa 0/1  Switch(config-if)#switchport access vlan 2  Switch(config-if)#exit  Switch(config)#interface fa 0/2  Switch(config-if)#switchport access vlan 2  Switch(config-if)#exit  Switch(config)#interface fa 0/3  Switch(config-if)#switchport access vlan 3  Switch(config-if)#exit  Switch(config)#interface fa 0/4  Switch(config-if)#switchport access vlan 3  Switch(config-if)#exit  Switch(config)#interface fa 0/5  Switch(config-if)#switchport access vlan 4  Switch(config-if)#exit  Switch(config)#interface fa 0/6  Switch(config-if)#switchport access vlan 4  Switch(config-if)#exit  Switch(config)#exit  Switch#  Switch#show vlan brief |

**Gambar 2.3** Konfigurasi *switch1*

* + 1. Langkah 3: Tes koneksi dengan perintah *ping* dan *screenshot* hasilnya.
       1. PC VLAN A ke PC VLAN B.

Klik pada PC, pindah ke tab *Desktop*, klik *Command* *Prompt*, ketikkan : PING <IP *Address* tujuan>.

* + - 1. PC VLAN A ke PC VLAN E.

Klik pada PC, pindah ke tab *Desktop*, klik *Command* *Prompt*, ketikkan : PING <IP *Address* tujuan>.

* + - 1. PC VLAN A ke PC VLAN D.

Klik pada PC, pindah ke tab *Desktop*, klik *Command* *Prompt*, ketikkan : PING <IP *Address* tujuan>

* + - 1. PC VLAN B ke PC VLAN D.

Klik pada PC, pindah ke tab *Desktop*, klik *Command* *Prompt*, ketikkan : PING <IP *Address* tujuan>.

* + - 1. PC VLAN B ke PC VLAN C.

Klik pada PC, pindah ke tab *Desktop*, klik *Command* *Prompt*, ketikkan : PING <IP *Address* tujuan>.

* + - 1. PC VLAN B ke PC VLAN E.

Klik pada PC, pindah ke tab *Desktop*, klik *Command* *Prompt*, ketikkan : PING <IP *Address* tujuan>.

* + - 1. PC VLAN F ke PC VLAN D.

Klik pada PC, pindah ke tab *Desktop*, klik *Command* *Prompt*, ketikkan : PING <IP *Address* tujuan>.

* + - 1. PC VLAN F ke PC VLAN A.

Klik pada PC, pindah ke tab *Desktop*, klik *Command* *Prompt*, ketikkan : PING <IP *Address* tujuan>.

* + - 1. PC VLAN F ke PC VLAN C.

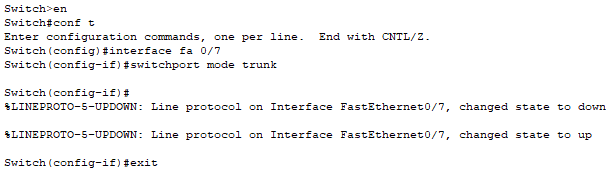
Klik pada PC, pindah ke tab *Desktop*, klik *Command* *Prompt*, ketikkan : PING <IP *Address* tujuan>.

# HASIL DAN PEMBAHASAN

* 1. Melalukan konfigurasi akses VLAN

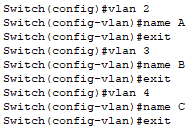
Langkah 1**:**

Mengkonfigurasi VLAN pada *Switch0.*

****

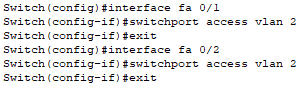
**Gambar 2.4** Tampilan konfigurasi VLAN pada *switch0.*

Pada **Gambar 2.4** merupakan tampilan konfigurasi pada *switch0*, dimana perintah “enable” digunakan untuk masuk ke mode EXEC dari *switch*, sedangkan perintah “configure terminal” digunakan untuk masuk ke mode konfigurasi melalui terminal. *Script* “Enter configuration commands, one per line. End with CNTL/Z.” merupakan pemberitahuan bahwa *user* sudah masuk ke konfigurasi “commands” yang artinya *user* sudah bias melakukan konfigurasi *switch* sesuai yang *user* inginkan. Perintah “FastEthernet 0/7” dengan mode “trunk” berguna agar dapat berkomunikasi dengan perangkat *switch* yang lain. Karena *port* ini akan dihubungkan dengan perangkat *Switch1*.

****

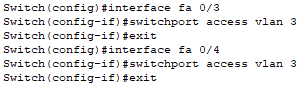
**Gambar 2.5** Perintah pembuatan VLAN pada *switch0*

Pada **Gambar 2.5** merupakan tampilan perintah untuk membuat VLAN, dimana perintah “vlan” digunakan untuk pembuatan VLAN yaitu perintah untuk membuat VLAN nomor 2 “vlan 2” dengan memberikan nama “A” “name A”, VLAN nomor 3 “vlan 3” dengan memberikan nama “B” “name B”, serta VLAN nomor 4 “vlan 4” dengan memberikan nama “C” “name C”.

****

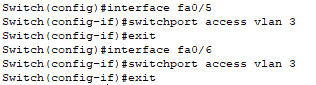
**Gambar 2.6** Proses konfigurasi *port* pada *switch0*

Pada **Gambar 2.6** merupakan perintah untuk mengkonfigurasi *port.* Dimana perintah “interface” digunakan untuk konfigurasi *interface* pada *port* “Fa 0/1” dan “Fa 0/2” dengan tipe “access” yang hanya dapat mengakses data dari VLAN 2.

****

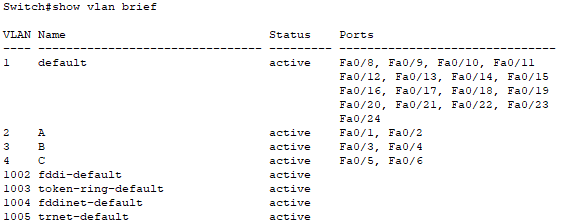
**Gambar 2.7** Proses konfigurasi *port* pada *switch0*

Pada **Gambar 2.7** merupakan perintah untuk mengkonfigurasi *port.* Dimana perintah “interface” digunakan untuk konfigurasi *interface* pada *port* “Fa 0/3” dan “Fa 0/4” dengan tipe “access” yang hanya dapat mengakses data dari VLAN 3.



**Gambar 2.8** Proses konfigurasi *port* pada *switch0*

Pada **Gambar 2.8** merupakan perintah untuk mengkonfigurasi *port.* Dimana perintah “interface” digunakan untuk konfigurasi *interface* pada *port* “Fa 0/5” dan “Fa 0/6” dengan tipe “access” yang hanya dapat mengakses data dari VLAN 4.

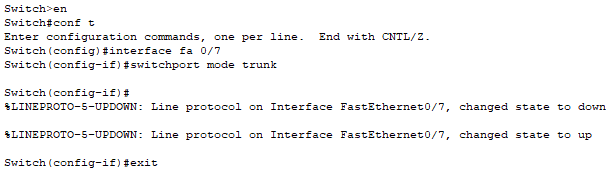


**Gambar 2.9** Hasil perintah yang dilakukan pada *switch0*

Pada **Gambar 2.9** merupakan perintah untuk melihat daftar VLAN yang telah dibuat, berdasarkan hasil penjalanan perintah didapat 4 buah VLAN yang berstatus aktif, yaitu *default* (VLAN 1), A (VLAN 2), B (VLAN 3) dan C (VLAN 4). Adapun *port* yang terhubung pada VLAN 2 adalah *port* “Fa 0/1” dan “Fa 0/2”, pada *port* “Fa 0/3” dan “Fa 0/4” terhubung dengan VLAN3, serta *port* “Fa 0/5” dan “Fa 0/6” terhubung dengan VLAN 4. Sisa dari *port* yang tidak tersambung, masih terhubung pada VLAN 1.

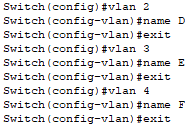
Langkah 2**:**

Mengkonfigurasi VLAN pada *Switch1.*

****

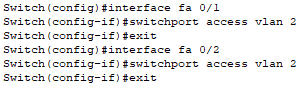
**Gambar 2.10** Tampilan konfigurasi VLAN pada *switch1.*

Pada **Gambar 2.10** merupakan tampilan konfigurasi pada *switch1*, dimana perintah “enable” digunakan untuk masuk ke mode EXEC dari *switch*, sedangkan perintah “configure terminal” digunakan untuk masuk ke mode konfigurasi melalui terminal. *Script* “Enter configuration commands, one per line. End with CNTL/Z.” merupakan pemberitahuan bahwa *user* sudah masuk ke konfigurasi “commands” yang artinya *user* sudah bias melakukan konfigurasi *switch* sesuai yang *user* inginkan. Perintah “FastEthernet 0/7” dengan mode “trunk” berguna agar dapat berkomunikasi dengan perangkat *switch* yang lain. Karena *port* ini akan dihubungkan dengan perangkat *Switch0*.



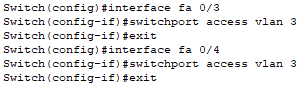
**Gambar 2.11** Perintah pembuatan VLAN pada *switch1*

Pada **Gambar 2.11** merupakan tampilan perintah untuk membuat VLAN, dimana perintah “vlan” digunakan untuk pembuatan VLAN yaitu perintah untuk membuat VLAN nomor 2 “vlan 2” dengan memberikan nama “D” “name D”, VLAN nomor 3 “vlan 3” dengan memberikan nama “E” “name E”, serta VLAN nomor 4 “vlan 4” dengan memberikan nama “F” “name F”.

****

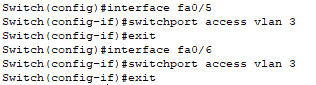
**Gambar 2.12** Proses konfigurasi *port* pada *switch1*

Pada **Gambar 2.12** merupakan perintah untuk mengkonfigurasi *port.* Dimana perintah “interface” digunakan untuk konfigurasi *interface* pada *port* “Fa 0/1” dan “Fa 0/2” dengan tipe “access” yang hanya dapat mengakses data dari VLAN 2.

****

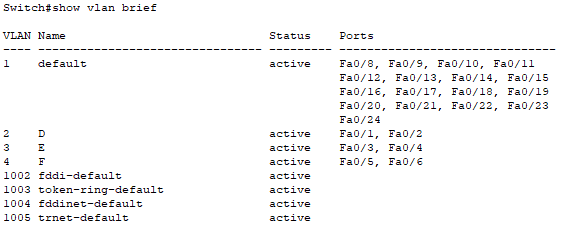
**Gambar 2.13** Proses konfigurasi *port* pada *switch1*

Pada **Gambar 2.13** merupakan perintah untuk mengkonfigurasi *port.* Dimana perintah “interface” digunakan untuk konfigurasi *interface* pada *port* “Fa 0/3” dan “Fa 0/4” dengan tipe “access” yang hanya dapat mengakses data dari VLAN 3.



**Gambar 2.14** Proses konfigurasi *port* pada *switch1*

Pada **Gambar 2.14** merupakan perintah untuk mengkonfigurasi *port.* Dimana perintah “interface” digunakan untuk konfigurasi *interface* pada *port* “Fa 0/5” dan “Fa 0/6” dengan tipe “access” yang hanya dapat mengakses data dari VLAN 4.



**Gambar 2.15** Hasil perintah yang dilakukan pada *switch1*

Pada **Gambar 2.15** merupakan perintah untuk melihat daftar VLAN yang telah dibuat, berdasarkan hasil penjalanan perintah didapat 4 buah VLAN yang berstatus aktif, yaitu *default* (VLAN 1), D (VLAN 2), E (VLAN 3) dan F (VLAN 4). Adapun *port* yang terhubung pada VLAN 2 adalah *port* “Fa 0/1” dan “Fa 0/2”, pada *port* “Fa 0/3” dan “Fa 0/4” terhubung dengan VLAN3, serta *port* “Fa 0/5” dan “Fa 0/6” terhubung dengan VLAN 4. Sisa dari *port* yang tidak tersambung, masih terhubung pada VLAN 1.

Berdasarkan percobaan dalam konfigurasi akses VLAN antara *Switch0* dan *Switch1*, berikut merupakan tabel daftar VLAN setelah melakukan konfigurasi tersebut :

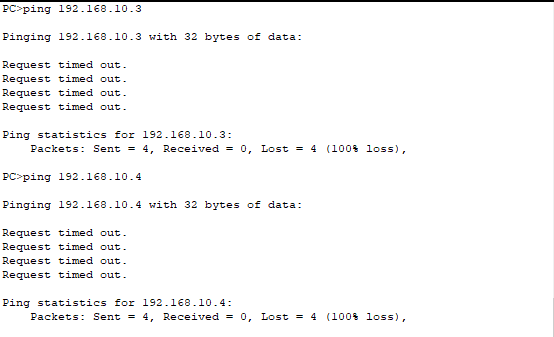
Tabel 2.4 Tabel daftar VLAN pada *Switch0* dan *Switch1.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Switch*** | **VLAN** | ***Name*** | **Status** | ***Port*** |
| 0 | 2 | A | *Active* | Fa 0/1, Fa 0/2 |
| 3 | B | *Active* | Fa 0/3, Fa 0/4 |
| 4 | C | *Active* | Fa 0/5, Fa 0/6 |
| 1 | 2 | D | *Active* | Fa 0/1, Fa 0/2 |
| 3 | E | *Active* | Fa 0/3, Fa 0/4 |
| 4 | F | *Active* | Fa 0/5, Fa 0/6 |

Langkah 3:

Tes koneksi dengan perintah *ping.*

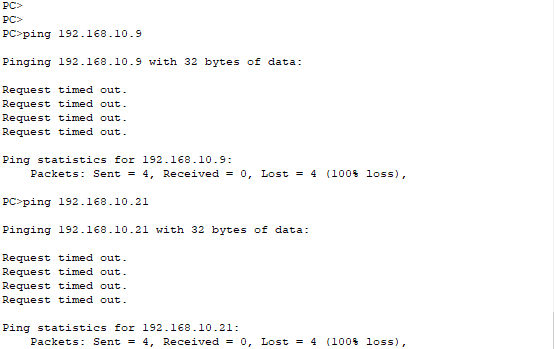
* + - * 1. PC VLAN A ke PC VLAN B



**Gambar 2.16** Perintah *ping* untuk melakukan tes koneksi dari VLAN A ke VLAN B

Pada **Gambar 2.16** merupakan perintah *ping* untuk melakukan tes koneksi antara VLAN A dengan VLAN B. Pada VLAN A menggunakan PC0 dengan IP *Address* 192.168.10.1 mencoba mengecekan dengan PC2 dan PC3 dengan IP *Address* 192.168.10.3 dan 192.168.10.4. Saat perintah dilakukan maka menghasilkan informasi “Request timed out.”. Hal itu dikarenakan PC0 tidak bisa berkoneksi dengan PC2 dan PC3, karena berbeda VLAN. Yang mana VLAN A merupakan VLAN dengan nomor 2 dan VLAN B merupakan VLAN bernomor 3.

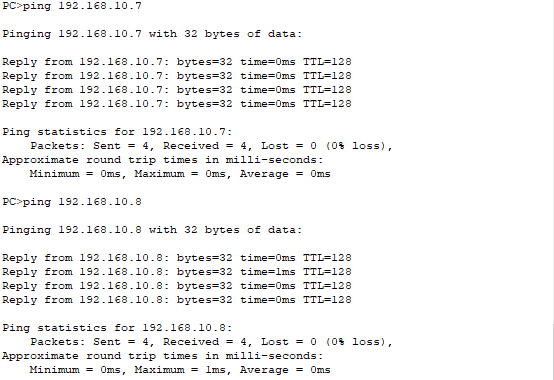
* + - * 1. PC VLAN A ke PC VLAN E



**Gambar 2.17** Perintah *ping* untuk melakukan tes koneksi dari VLAN A ke VLAN E

Pada **Gambar 2.17** merupakan perintah *ping* untuk melakukan tes koneksi antara VLAN A dengan VLAN E. Pada VLAN A menggunakan PC0 dengan IP *Address* 192.168.10.1 mencoba mengecekan dengan PC2 dan PC3 dengan IP *Address* 192.168.10.9 dan 192.168.10.21. Saat perintah dilakukan maka menghasilkan informasi “Request timed out.”. Hal itu dikarenakan PC0 tidak bisa berkoneksi dengan PC8 dan PC9, karena berbeda VLAN. Yang mana VLAN A merupakan VLAN dengan nomor 2 dan VLAN B merupakan VLAN bernomor 3.

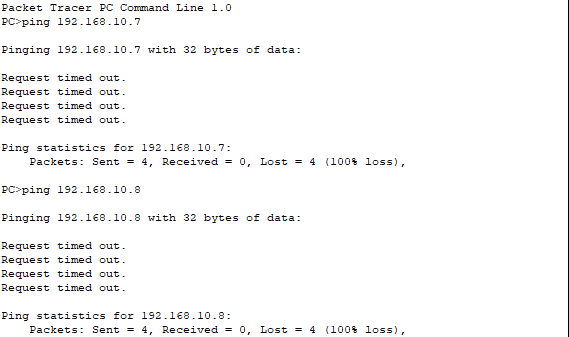
* + - * 1. PC VLAN A ke PC VLAN D



**Gambar 2.18** Perintah *ping* untuk melakukan tes koneksi dari VLAN A ke VLAN D

Pada **Gambar 2.18** merupakan perintah *ping* untuk melakukan tes koneksi antara VLAN A dengan VLAN D. Pada VLAN A menggunakan PC0 dengan IP *Address* 192.168.10.1 mencoba mengecekan dengan PC6 dan PC7 dengan IP *Address* 192.168.10.7 dan 192.168.10.8. Saat perintah dilakukan maka menghasilkan informasi “Reply from 192.168.10.7; bytes=32 time=1ms TTL=128”, dan “Reply from 192.168.10.8; bytes=32 time=0ms TTL=128”. Dapat dilihat dari tiap paket yang dikirimkan adalah sebesar 32 *byte* dalam waktu 1 ms. Sementara TTL (*Time To Live*) yaitu angka maksimum dari PC ketika me-*reply*. Paket ICMP disebut juga *latency/delay.* Secara *default* TTL *windows* adalah 128 . Hal itu dapat ditentukan bahwa antara PC0, PC6 dan PC7 dapat saling terhubung dikarenakan memiliki VLAN yang sama yaitu VLAN bernomor 2.

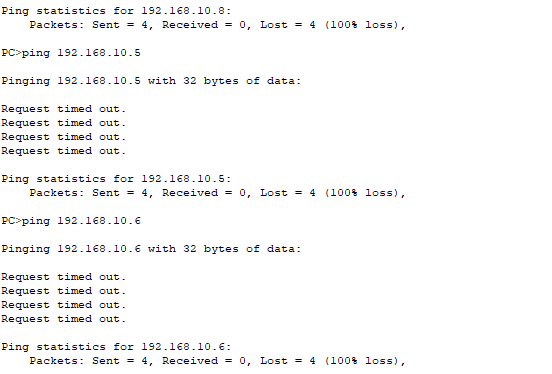
* + - * 1. PC VLAN B ke PC VLAN D



**Gambar 2.19** Perintah *ping* untuk melakukan tes koneksi dari VLAN B ke VLAN D

Pada **Gambar 2.19** merupakan perintah *ping* untuk melakukan tes koneksi antara VLAN B dengan VLAN D. Pada VLAN B menggunakan PC2 dengan IP *Address* 192.168.10.3 mencoba mengecekan dengan PC6 dan PC7 dengan IP *Address* 192.168.10.7 dan 192.168.10.8. Saat perintah dilakukan maka menghasilkan informasi “Request timed out.”. Hal itu dikarenakan PC2 tidak bisa berkoneksi dengan PC6 dan PC7, karena berbeda VLAN. Yang mana VLAN B merupakan VLAN dengan nomor 3 dan VLAN D merupakan VLAN bernomor 2.

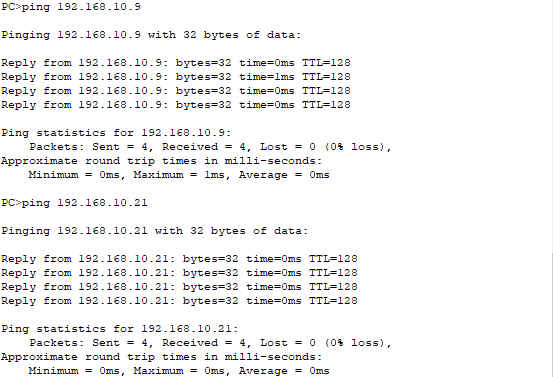
* + - * 1. PC VLAN B ke PC VLAN C



**Gambar 2.20** Perintah *ping* untuk melakukan tes koneksi dari VLAN B ke VLAN C

Pada **Gambar 2.20** merupakan perintah *ping* untuk melakukan tes koneksi antara VLAN B dengan VLAN C. Pada VLAN B menggunakan PC2 dengan IP *Address* 192.168.10.3 mencoba mengecekan dengan PC4 dan PC5 dengan IP *Address* 192.168.10.5 dan 192.168.10.6. Saat perintah dilakukan maka menghasilkan informasi “Request timed out.”. Hal itu dikarenakan PC2 tidak bisa berkoneksi dengan PC4 dan PC5, karena berbeda VLAN. Yang mana VLAN B merupakan VLAN dengan nomor 3 dan VLAN C merupakan VLAN bernomor 4.

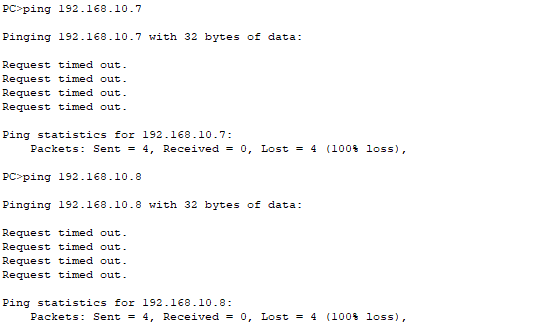
* + - * 1. PC VLAN B ke PC VLAN E



**Gambar 2.21** Perintah *ping* untuk melakukan tes koneksi dari VLAN B ke VLAN E

Pada **Gambar 2.21** merupakan perintah *ping* untuk melakukan tes koneksi antara VLAN B dengan VLAN E. Pada VLAN B menggunakan PC2 dengan IP *Address* 192.168.10.3 mencoba mengecekan dengan PC8 dan PC9 dengan IP *Address* 192.168.10.9 dan 192.168.10.21. Saat perintah dilakukan maka menghasilkan informasi “Reply from 192.168.10.9; bytes=32 time=1ms TTL=128”, dan “Reply from 192.168.10.9; bytes=32 time=0ms TTL=128”. Dapat dilihat dari tiap paket yang dikirimkan adalah sebesar 32 *byte* dalam waktu 1 ms. Sementara TTL (*Time To Live*) yaitu angka maksimum dari PC ketika me-*reply*. Paket ICMP disebut juga *latency/delay.* Secara *default* TTL *windows* adalah 128 . Hal itu dapat ditentukan bahwa antara PC2, PC8, dan PC9 dapat saling terhubung dikarenakan memiliki VLAN yang sama yaitu VLAN bernomor 3.

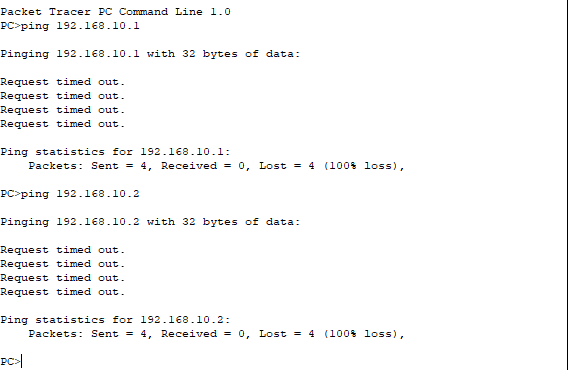
* + - * 1. PC VLAN F ke PC VLAN D



**Gambar 2.22** Perintah *ping* untuk melakukan tes koneksi dari VLAN F ke VLAN D

Pada **Gambar 2.22** merupakan perintah *ping* untuk melakukan tes koneksi antara VLAN F dengan VLAN D. Pada VLAN F menggunakan PC10 dengan IP *Address* 192.168.10.22 mencoba mengecekan dengan PC6 dan PC7 dengan IP *Address* 192.168.10.7 dan 192.168.10.8. Saat perintah dilakukan maka menghasilkan informasi “Request timed out.”. Hal itu dikarenakan PC10 tidak bisa berkoneksi dengan PC6 dan PC7, karena berbeda VLAN. Yang mana VLAN F merupakan VLAN dengan nomor 4 dan VLAN D merupakan VLAN bernomor 2.

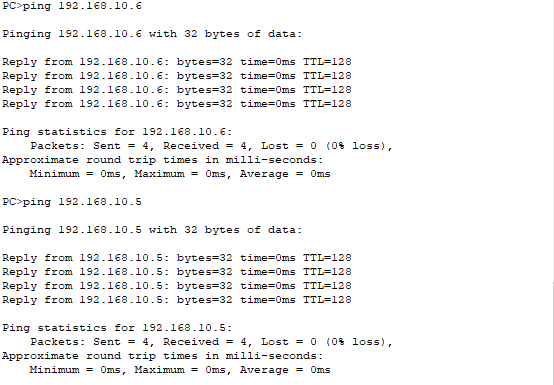
* + - * 1. PC VLAN F ke PC VLAN A



**Gambar 2.23** Perintah *ping* untuk melakukan tes koneksi dari VLAN F ke VLAN A

Pada **Gambar 2.23** merupakan perintah *ping* untuk melakukan tes koneksi antara VLAN F dengan VLAN A. Pada VLAN F menggunakan PC10 dengan IP *Address* 192.168.10.22 mencoba mengecekan dengan PC0 dan PC1 dengan IP *Address* 192.168.10.1 dan 192.168.10.2. Saat perintah dilakukan maka menghasilkan informasi “Request timed out.”. Hal itu dikarenakan PC10 tidak bisa berkoneksi dengan PC0 dan PC1, karena berbeda VLAN. Yang mana VLAN F merupakan VLAN dengan nomor 4 dan VLAN A merupakan VLAN bernomor 2.

* + - * 1. PC VLAN F ke PC VLAN C



**Gambar 2.24** Perintah *ping* untuk melakukan tes koneksi dari VLAN F ke VLAN C

Pada **Gambar 2.24** merupakan perintah *ping* untuk melakukan tes koneksi antara VLAN F dengan VLAN C. Pada VLAN F menggunakan PC10 dengan IP *Address* 192.168.10.22 mencoba mengecekan dengan PC4 dan PC5 dengan IP *Address* 192.168.10.5 dan 192.168.10.6. Saat perintah dilakukan maka menghasilkan informasi “Reply from 192.168.10.6; bytes=32 time=1ms TTL=128”, dan “Reply from 192.168.10.5; bytes=32 time=0ms TTL=128”. Dapat dilihat dari tiap paket yang dikirimkan adalah sebesar 32 *byte* dalam waktu 1 ms. Sementara TTL (*Time To Live*) yaitu angka maksimum dari PC ketika me-*reply*. Paket ICMP disebut juga *latency/delay.* Secara *default* TTL *windows* adalah 128 . Hal itu dapat ditentukan bahwa antara PC10, PC4, dan PC5 dapat saling terhubung dikarenakan memiliki VLAN yang sama yaitu VLAN bernomor 4.

Berdasarkan hasil tes koneksi antara satu VLAN ke VLAN lain, berikut ditampilkan tabel hasil tes koneksi melalui perintah *ping*:

Tabel 2.5 Tabel hasil tes koneksi dengan menggunakan perintah *ping.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VLAN Asal** | **PC Asal** | **VLAN** **Tujuan** | **PC Tujuan** | **Hasil** |
| **BISA / TIDAK** |
| A | PC0 | B | PC 2 | Tidak |
| PC 3 | Tidak |
| A | PC1 | E | PC 8 | Tidak |
| PC 9 | Tidak |
| A | PC0 | D | PC 6 | Bisa |
| PC 7 | Bisa |
| B | PC2 | D | PC 6 | Tidak |
| PC 7 | Tidak |
| B | PC3 | C | PC 4 | Tidak |
| PC 5 | Tidak |
| B | PC3 | E | PC 8 | Bisa |
| PC 9 | Bisa |
| F | PC10 | D | PC 6 | Tidak |
| PC 7 | Tidak |
| F | PC10 | A | PC 0 | Tidak |
| PC 1 | Tidak |
| F | PC11 | C | PC 4 | Bisa |
| PC 5 | Bisa |

1. **KESIMPULAN**

Berdasarkan praktikum modul 2 *Virtual* LAN (VLAN), dapat disimpulkan bahwa:

* + - 1. VLAN merupakan sekelompok jaringan yang dapat dikonfigurasi secara *virtual*. Konfigurasi pada VLAN dilakukan melalui CLI dengan menggunakan beberapa perintah dasar.
      2. Dalam pengimplementasian VLAN dapat digunakan pada sebuah jaringan komputer secara *virtual,* yang mana pada pengimplementasiannya harus terlebih dahulu membuat sebuah jaringan yang terdiri dari komputer dan *switch* yang saling berhubungan.

# DAFTAR PUSTAKA

1. Agustina, Harry. *Teknik VLAN.* Bandung: Penerbit PT.BisikTetangga. 2011.
2. Kurniawan, Wiharsono. *Jaringan Komputer.* Yogyakarta :Andi. 2007.
3. Nugroho, Bunafit. *Instalasidan Konfigurasi Jaringan Windows dan Linux.*Yogyakarta :Andi. 2005.
4. Pranata, Kadek Surya. *Sistem Operasi Jaringan untuk SMK/MAK Kelas*

*XI.* Jakarta :Kementrian Pendidikan dan Kebudayaan. 2013.