VIRTUAL LAN (VLAN)

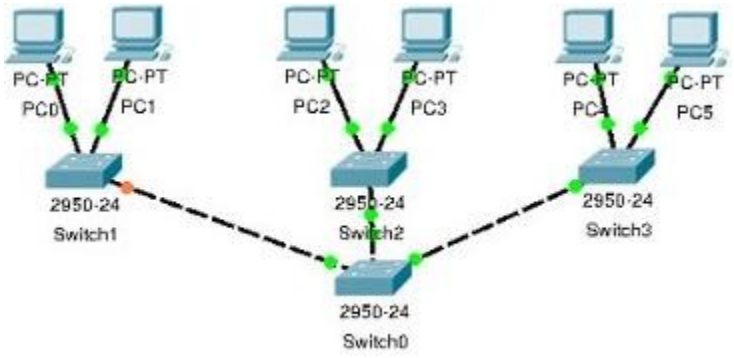
Irfan Akbar, site : http://laluirfan.web.ugm.ac.id

PENDAHULUAN

Rancangan network pada masa kini sangat berbeda jauh dengan rancangan network dimasa lalu, rancangan network di masa lalu berdasarkan pada *colapsed backbone* yaitu struktur network dimana semua alat menuju ke sebuah backbone yang sama. Rancangan network masa kini dicirikan dengan sebuah arsitektur yang lebih datar berkat adanya switch. Pertanyaannya adalah bagaimana membagi broadcast domain dalam sebuah internetwork switch yang murni? Caranya adalah dengan menciptakan sebuah Virtual Local Area Network (VLAN). Sebauah VLAN adalah pengelompokan logikal dari 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 subnetwork yang berbeda pula. Sebuah VLAN diperlakukan seperti subnet atau broadcast domainnya sendiri, yang berarti frame-frame yang dibroadcast pada sebuah network hanya di switch atau dialihkan diantara 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.

DASAR-DASAR VLAN

Seperti tampak pada Gambar1, network-network switch layer 2 biasanya dirancang 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. Jika PC 0 mengirimkan sebuah frame maka tersebut akan diforward ke semua end device (PC0-PC5)



Gambar 1

Secara defaul, router membolehkan broadcast hanya di dalam network di mana paket broadcast itu

berasal, tetapi switch-switch 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. Jika pada gambar 1 diterapkan sebuah network swithch layer 2 maka frame hanya akan di forward kan ke host tujuan sehingga frame tidak akan terlihat oelh host lain dalam jaringan. Jadi keuntungan terbesar yang diperoleh dengan memiliki network switch layer 2 adalah ia menciptakan sebuah *coallision domain* sendiri-sendiri untuk setiap alat yang terhubung ke setiap port pada switch tersebut. Skenario ini membebaskan kita dari keterbatasan jarak ethernet sehingga sebuah wan yang lebih besar dapat dibuat. Tetapi setiap kemajuan baru biasanya akan diikuti dengan masalah baru juga, semakin besar jumlah user dan alat, semakin banyak broadcasr dan paket yang harus di tangani oleh sebuah switch, dan masalah yang lain nya adalah *security* atau keamanan.

Keamanan menjadi faktor yang sangat penting karena di dalam internetwork switch layer 2, semua user secara default dapat melihat semua alat di network tersebut, dan kita tidak bisa menghentikan alat-alat tersebut untuk melakukan broadcasting atau menghentikan user untuk melakukan respon terhadap broadcast. Jika kondisinya seperti demikian maka pilihan keamanan hanya terrbatas pada menempatkan password pada server dan alat-alat di network.

Tetapi akan berbeda jika kita menciptakan sebuah Virtula LAN (VLAN), 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.

Mengapa Menggunakan VLAN?

1. **Kontrol Terhadap Broadcast**

   Broadcast terjadi di semua protokol, tetapi seberapa sering terjadinya tergantung pada tiga hal berikut :

   - Jenis protokol
   - Aplikasi yang berkerja di internetwork
   - Bagaimana layanan-layanan network digunakan

   Aplikasi-aplikasi pada dewasa ini semakin banyak membutuhkan bandwith, terutama aplikasi-aplikasi multimedia yang menggunakan broadcast dan multicast secara ekstensif. Memastikan agar network disegmentasi atau dipisahkan dengan baik, untuk mengisolasi masalah di satu segmen dan menghindari penyebarannya ke network

lain atau internetwork adalah sebuah keharusan. Cara melakukan ini adalah dengan strategi switching dan routing yang baik, yaitu dengan network switch murni dan lingkungan VLAN.

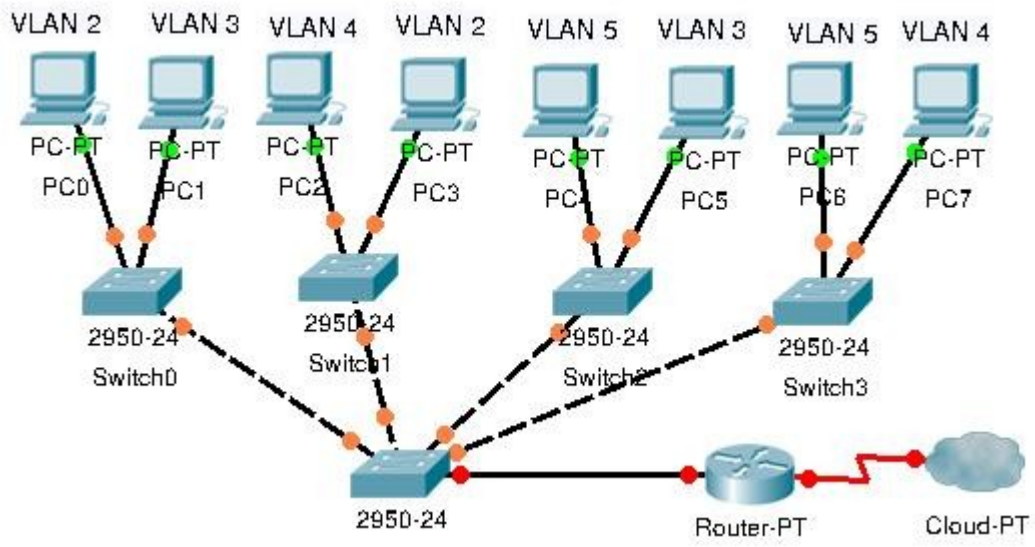
Semua peralatan di sebuah VLAN adalah anggota dari broadcast domain yang sama dan menerima semua broadcast. Secara default, broadcast tidak akan dilewatkan pada pada port dari sebuah switch yang bukan merupakan anggota VLAN yang sama.

2. **Keamanan**

Administrator akan dapat memiliki kontrol ternhadap setiap port dan user dengan cara membuat VLAN dan menciptakan banyak kelompok broadcast, dengan demikian user tidak akan bisa lagi dengan leluasa untuk menghubungkan work station mereka ke sembarang port pada swich dan memperoleh akses ke sumber daya network. Vlan juga dapat dibuat sesuai dengan kebutuhan sumber daya nework dari user, switch-switch dapat dikonfigurasi untuk memberikan informasi ke sebuah stasiun managemen network jika ada akses-akses yang tidak diizinkan ke sumber daya network

3. **Fleksibilitas dan Skalabilitas**

Apakah perbedaan router dengan switch? Secara default switch membagi coallision domain sedangkan router membagi broadcast domain.



Gambar 2

Vlan2 Marketing	192.168.10.0/24
Vlan3 Finance	192.168.20.0/24
Vlan4 Sales	192.168.30.0/24
Vlan5 Engineering	192.168.40.0/24

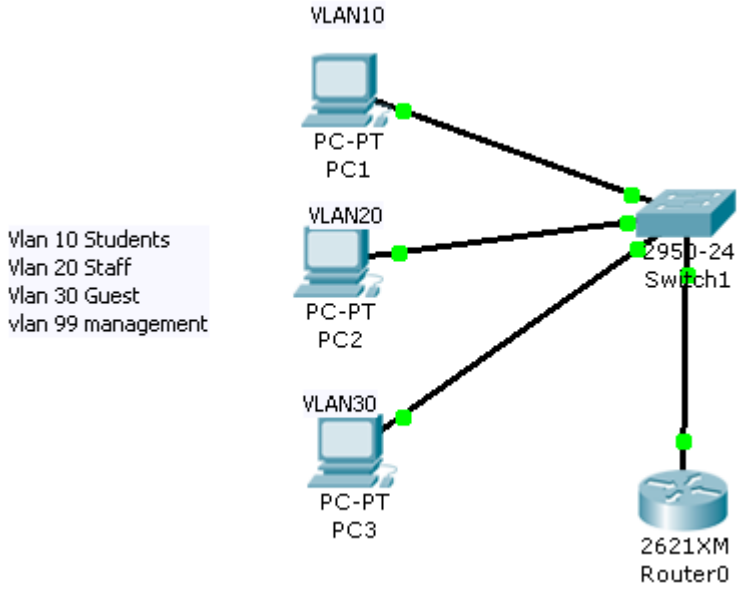
Gambar 2 memperlihatkan bagaimana sebuah switch-switch yang menerapkan VLAN

menghilangkan batasan-batasan fisikal. Gambar diatas menunjukkan bagaimana 4 buah VLAN digunakan untuk menciptakan sebuah broadcast domain untuk setiap departmen dalam perusahaan. Setiap port dari switch kemudian secara administratif ditempatkan sebagai sebuah anggota dari sebuah VLAN.

Jika seorang user untuk Marketing (VLAN2) perlu ditambahkan, maka port yang digunakan untuk user tersebut dapat dibuat menjadi anggota VLAN2 tidak bergantung dari lokasi fisikal dari port atau lokasi user baru tersebut.

Mengapa VLAN di mulai dengan no 2, nomor ini tidak lah penting tetapi mengapa tidak dimulai dengan VLAN1? Karena VLAN1 adalah sebuah VLAN administratif dan cisco merekomendasikannya untuk tujuan administratif saja. Secara default semua port dalam sebuah switch adalah anggota dari VLAN1 sebelum port tersebut di masukkan menjadi anggota VLAN yang lain, dan VLAN1 ini tidak dapat dihapus ataupun diubah dari switch.

CONTOH MENGKONFIGURASI VLAN



subneting tidak dibahas pada contoh ini.

1. konfigurasi pc

2. konfigurasi dasar pada switch 1

Switch>ena

Switch#conf

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname S1

S1(config)#enable secret class

S1(config)#no ip domain-lookup

S1(config)#line console 0

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#exit

S1(config)#line vty 0 15

S1(config-line)#password cisco

S1(config-line)#login

S1(config-line)#exit

S1(config)#ip default-gateway 172.20.29.1

S1(config)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy r
S1#copy running-config s
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

3. configure VTP pada sw 1

S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab3
Changing VTP domain name from NULL to Lab3
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

4. Enable kan port pada s1 dalam acces mode

S1(config)#int fa0/1
S1(config-if)#switchport mode access
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#int fa0/2
S1(config-if)#switchport mode access
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#int fa0/3
S1(config-if)#switchport mode access
S1(config-if)#no shutdown
S1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

5. buat trungking port sw1 pada device Fa0/4

S1(config)#int fa0/4
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#end

6. Buat vlan pada vtp server (sw1)

S1(config)#vlan 99
S1(config-vlan)#name Management&Native
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name Students
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name Staff
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name Guest
S1(config-vlan)#exit
S1(config)#end

7. verifikasi vlan yang sudah dibuat

8. masukkan port2 ke dalam vlan

S1(config)#int vlan 99
%LINK-5-CHANGED: Interface Vlan99, changed state to upS1(config-if)#
S1(config-if)#ip address 172.20.28.2 255.255.255.240
S1(config-if)#exit
S1(config)#int fa0/1
S1(config-if)#switchport access vlan 10
S1(config-if)#exit

S1(config)#int fa0/2
S1(config-if)#switchport access vlan 20
S1(config-if)#exit
S1(config)#int fa0/3
S1(config-if)#switchport access vlan 30
S1(config-if)#end

9. konfigurasi router 1

Router(config)#hostname R1
R1(config)#ena
R1(config)#enable s
R1(config)#enable secret clas
R1(config)#enable secret class
R1(config)#no ip domain-lookup
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#end

10. konfigurasi trunking interface (sub interface) pada Router 1

R1(config)#int fa0/0
R1(config-if)#no sh
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config-if)#exit
R1(config)#int fa0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip ad
R1(config-subif)#ip address 172.20.8.1 255.255.248.0
R1(config-subif)#exit
R1(config)#int fa0/0.20
%LINK-5-CHANGED: Interface FastEthernet0/0.20, changed state to up
R1(config-subif)#encapsulation d
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 172.20.16.1 255.255.248.0
R1(config-subif)#exit
R1(config)#int fa0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 172.20.24.1 255.255.254.0
R1(config-subif)#exit
R1(config)#int fa0/0.99
R1(config-subif)#encapsulation dot1Q 99 native
R1(config-subif)#ip address 172.20.29.1 255.255.255.240
R1(config-subif)#end
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]

Referensi

Lammle,T. CCNA Cicso Certified Networking Associate
Materi CNA TE-UGM