MANAJEMEN JARINGAN

RENDIKA ADHA TANJUNG

(09011181419008)

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

TAHUN AJARAN 2017/2018

ANALISA *FCAPS* DENGAN LAPORAN KERJA PRAKTIK

PENERAPAN VLAN DENGAN DHCP SERVER DI PT. PUPUK SRIWIDJAJA PALEMBANG

	Problem	**Solution**	**Result**
Fault	Penggunanya tersebar di berbagai tempat.	Memperluas pada VLAN pada departemen lain	Pengguna dapat bekerja efektif
Configuration	Tidak optimalnya pelayanan jaringan	Metode Trunking	Mendukung pelayanan jaringan
Accounting	Akses layanan antar departemen yang terbatas dari pusat	Mengelola operasi peralatan seperti dengan melakukan backup dan sinkronisasi perangkat lunak	Efisiensi Biaya
Performance	Monitoring jaringan lebih sulit	Virtual LAN(VLAN)	Mengurangi beban jaringan pada setiap departemen.
Security	Akses dari VLAN tidak menggunakan nomor *MAC Address*	Akses dari VLAN menggunakan nomor *MAC Address*	Mencegah bocornya informasi sensitif

Analisa FCAPS

Fault :

Permasalahan juga timbul dengan jaringan yang penggunanya tersebar di berbagai tempat artinya tidak terletak dalam satu lokasi tertentu secara fisik. Maka, VLAN yang memberikan kebebasan terhadap batasan lokasi secara fisik dengan mengijinkan *workgroup* yang terpisah lokasinya atau berlainan gedung, atau tersebar untuk dapat terhubung secara logik ke jaringan meskipun hanya satu pengguna. Jika infrastuktur secara fisik telah terinstalasi, maka hal ini tidak menjadi masalah untuk menambah *port* bagi VLAN yang baru jika organisasi atau departemen diperluas dan tiap bagian dipindah.

Configuration:

Skenario konfigurasi ini membuat switch menjadi bagian dari suatu VTP management domain, setiap switch harus dikonfigurasi dalam satu dari tiga mode VTP yang dapat digunakan. Mode VTP yang digunakan pada switch akan menentukan bagaimana switch berinteraksi dengan switch VTP lainnya

dalam management domain tersebut. Mode VTP yang dapat digunakan pada switch Cisco adalah *mode server*, *mode client*, dan *mode transparent*.

Accounting :

VLAN memberikan mekanisme akuntansi secara efektif untuk mengontrol perubahan ini serta mengurangi banyak biaya untuk kebutuhan akan mengkonfigurasi ulang hub dan router. Pengguna VLAN dapat tetap berbagi dalam satu *network address* yang sama apabila ia tetap terhubung dalam satu swith *port* yang sama meskipun tidak dalam satu lokasi. Permasalahan dalam hal perubahan lokasi dapat diselesaikan dengan membuat komputer pengguna tergabung kedalam port pada VLAN tersebut dan mengkonfigurasikan switch pada VLAN tersebut.

P erformance:

Performa pada switch pula yang memungkinkan terjadinya segmentasi pada jaringan atau dengan kata lain switch-lah yang membentuk VLAN. Dengan adanya segmentasi yang membatasi jalur *broadcast* akan mengakibatkan suatu VLAN tidak dapat menerima dan mengirimkan jalur *broadcast* ke VLAN lainnya. Hal ini secara nyata akan mengurangi penggunaan jalur *broadcast* secara keseluruhan, mengurangi penggunaan *bandwidth* bagi pengguna, mengurangi kemungkinan terjadinya *broadcast storms* (badai siaran) yang dapat menyebabkan kemacetan total di jaringan komputer.

Administrator jaringan dapat dengan mudah mengontrol ukuran dari jalur *broadcast* dengan cara mengurangi besarnya *broadcast* secara keseluruhan, membatasi jumlah *port* switch yang digunakan dalam satu VLAN serta jumlah pengguna yang tergabung dalam suatu VLAN.

Security :

Dukungan Tingkat keamanan yang lebih baik dari LAN inilah yang dapat dijadikan suatu nilai tambah dari penggunaan VLAN sebagai sistem jaringan. Salah satu kelebihan yang diberikan oleh penggunaan VLAN adalah kontrol administrasi secara terpusat, artinya aplikasi dari manajemen VLAN dapat dikonfigurasikan, diatur dan diawasi secara terpusat, pengendalian *broadcast* jaringan, rencana perpindahan, penambahan, perubahan dan pengaturan akses khusus ke dalam jaringan serta mendapatkan media/data yang memiliki fungsi penting dalam perencanaan dan *administrasi* di dalam grup tersebut semuanya dapat dilakukan secara terpusat. Dengan adanya pengontrolan manajemen secara terpusat maka administrator jaringan juga dapat mengelompokkan grup-grup VLAN secara spesifik berdasarkan penggunadan port dari switch yang digunakan, mengatur tingkat keamanan, mengambil dan menyebar data melewati jalur yang ada, mengkonfigurasi komunikasi yang melewati switch, dan memonitor lalu lintas data serta penggunaan *bandwidth* dari VLAN saat melalui tempat-tempat yang rawan di dalam jaringan. Maka dari itu sebaiknya akses dari VLAN menggunakan nomor *MAC Address* agar antara pegawai dan pimpinan tidak dalam satu VLAN, ini mencegah bocornya informasi sensitif seperti password yang seharusnya hanya pejabat yang berwenang yang memilikinya bocor kepada pegawainya, keadaan ini bisa terjadi karena antara pagawai dan pimpinan dalam satu *broadcast address*.