PERANCANGAN *BLUE PRINT* JARINGAN MENGGUNAKAN *VIRTUAL LAN (VLAN)* DENGAN STUDI KASUS (PT. PLN PERSERO AREA KUDUS)

Faesol Puspito[1], Hj. Naniek Widyastutui[2], Joko Triyono[3]
[1]Teknik Informatika, FTI, IST AKPRIND, faisol.pito@gmail.com
[2]Teknik Informatika, FTI, IST AKPRIND, naniek_wid@yahoo.com
[3]Teknik Informatika, FTI, IST AKPRIND, zainjack@gmail.com

ABSTRACT

The development of computer network technology is growing rapidly as the current needs of people who use computer networks. It is seen from the number of companies or organizations that use computer networks. Thus the increasing needs and the increasing number of network users, the network also required the presence of forms that provide maximum results, both in terms of the efficiency of the network device, configuration and security.

Based on these conditions, conducted an analysis of the existing network, which includes the structure, network topology, network devices. From the analysis it made the design blueprint of the new network by using VLAN. Prior to implementation, the first blueprint for a VLAN network is simulated using Packet Tracert.

There are several advantages of a VLAN network, among others, can manage the switch manageable. In terms of flexibility, users on the same VLAN network is not dependent on the physical layout or location of the user is located. Moreover, in terms of availability. The use of VLANs also provide a higher level of security, since each user can not just go into the switch and dependent with other users.

Keyword : VLAN, blue print, switch.

INTISARI

Perkembangan teknologi jaringan komputer saat ini semakin pesat seiring kebutuhan masyarakat yang memanfaatkan jaringan komputer. Hal ini dilihat dari banyaknya perusahaan atau organisasi yang menggunakan jaringan komputer. Dengan demikian meningkatnya kebutuhan dan semakin banyaknya pengguna jaringan, maka dituntut pula adanya bentuk jaringan yang memberikan hasil maksimal, baik dari segi efisiensi perangkat jaringan, konfigurasi maupun keamanan.

Berdasarkan pada hal tersebut maka dilakukan analisis terhadap jaringan *existing*, yang meliputi struktur, topologi jaringan, perangkat jaringan. Dari hasil analisis maka dibuatlah perancangan *blue print* jaringan yang baru dengan menggunakan teknik VLAN. Sebelum diimplementasikan, terlebih dahulu *blue print* jaringan VLAN disimulasikan menggunakan *Packet Tracert.*

Ada beberapa keunggulan jaringan VLAN, antara lain dapat mengelola *switch managable*. Dari segi *flexibility*, *user* pada jaringan VLAN yang sama tidak bergantung pada letak fisik atau lokasi *user* berada. Selain itu, dari segi *availability*. Penggunaan VLAN juga memberikan tingkat keamanan yang lebih tinggi, karena setiap *user* tidak bisa begitu saja masuk ke dalam *switch* dan bergantung dengan *user* lain.

Kata kunci : VLAN, *blue print, switch.*

PENDAHULUAN

Perkembangan teknologi jaringan komputer dewasa ini semakin pesat seiring dengan kebutuhan masyarakat akan layanan yang memanfaatkan jaringan komputer. Hal ini bisa dilihat semakin banyaknya organisasi atau perusahaan yang menggunakan jaringan komputer untuk melancarkan arus informasi didalam perusahaan tersebut. Kebutuhan atas penggunaan

bersama *resources* yang ada dalam jaringan, baik *hardware* maupun *software* telah mengakibatkan timbulnya pengembangan teknologi jaringan itu sendiri.

PT. PLN (Persero) Area Kudus salah satu perusahaan yang sudah memanfaatkan jaringan komputer sebagai salah satu pendukung kegiatan operasional perusahaan. Seluruh bagian yang ada diperusahaan tersebut saling terhubung oleh jaringan LAN sehingga bisa saling bertukar data dan informasi, serta berbagi sumber daya, seperti *printer sharing*.

Masalah yang muncul di PT. PLN (Persero) Area Kudus saat ini adalah tidak adanya pembagian jaringan antar bagian, sehingga seluruh bagian berada dalam satu alamat jaringan yang sama. Penggunaan satu alamat jaringan untuk semua bagian menimbulkan *traffic* jaringan yang semakin padat. Dengan terhubungnya seluruh perangkat jaringan pada satu *broadcast domain* yang sama juga menyebabkan jaringan yang ada menjadi tidak *reliable*,bukan hanya karena *broadcast* yang menggangu namun juga semakin mudah dalam penyebaran virus.

Guna mengatasi permasalahan tersebut maka perlu dilakukan perancangan *blue print* jaringan baru yang memiliki kemampuan lebih baik. Dengan melalukan pembagian alamat jaringan, teknik *redundancy* serta penggantian *hardware* yang lebih baik maka dibangun jaringan *Virtual* LAN (VLAN) yang diharapkan mampu meningkatkan performa jaringan tersebut.

TINJAUAN PUSTAKA

Dalam laporan ini diambil beberapa referensi dari penelitian sebelumnya diantaranya adalah adalah (Dewi, 2009) dengan mengambil judul "*Simulasi Dynamic Routing Protocols, Access List Dan VLAN Pada Jaringan Komputer*". Kekurangan penelitian terebut adalah terlalu luasnya pokok bahasan yang dibahas, sehingga pembahasan yang mengenai jaringan VLAN hanya sekilas saja dan kurang detail mengenai pembahasan jaringan VLAN.

Penelitian yang lain (Susanti, 2010) dengan judul *"Perancangan Dan Simulasi Jaringan Berbasis Virtual Local Area Network (VLAN) Menggunakan Cisco Catalyst".* Kekurangan dari penelitian ini adalah perlunya perencanaan pengembangan infrastruktur yang lebih detail, komplek, dan kebutuhan *bandwidth* terhadapat jaringan.

Penelitian yang lain adalah (Dwiningsih, 2011) dengan mengambil judul "*Simulasi Virtual LAN (VLAN) Menggunakan Packet Tracert 5.3. Sebagai Pengembangan Jaringan Di PT. MekarArmada Jaya Magelang*". Dalam penelitian ini kekurangannya adalah tidak adanya penggunaan *firewall* dalam mengamankan jaringan tersebut.

PEMBAHASAN

Sebelum dilakukan perancangan *blue print* jaringan VLAN, terlebih dahulu mengklarifikasi perbedaan antara LAN, VLAN, VTP, VPN untuk memudahkan dalam merancang *blue print* jaringan VLAN yaitu LAN (*Local Area Network*) dari bentuk jaringan LAN sangat bergantung pada letak atau fisik dari *workstation*. Penggunaan *switch* pada LAN, menggunakan *switch* hanya digunakan untuk satu jaringan saja.

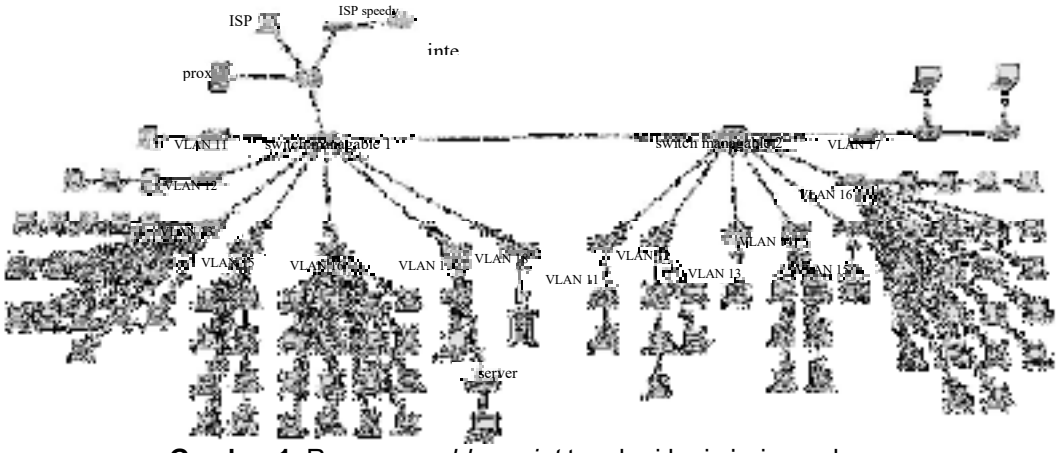
VLAN (*Virtual Local Area Network*) dari bentuk jaringan VLAN tiap-tiap *workstation* atau *user* yang tergabung dalam satu bagian (organisasi) dapat tetap saling berhubungan walaupun terpisah secara fisik. Penggunaan *switch* pada VLAN, menggunakan *switch managable* yang dapat digunakan untuk jaringan yang berbeda.

VTP (*Virtual Trunking Protocol*) digunakan untuk jaringan VLAN yang bersifat jaringan lokal sehingga dapat dilalui banyak jaringan VLAN yang berbda.

VPN (*Virtual Private Network*) digunakan untuk jaringan dengan komunikasi publik (*Internet*) dengan menggunakan *tunnelling protocol*. Dengan memakai jaringan publik, biaya yang dikeluarkan relatif lebih murah dari pada harus membangun sebuah jaringan internasional yang bersifat *private*.

Skema Jaringan Baru

Pada gambar 1. menunujukkan perancangan *blue print* jaringan yang baru yaitu jaringan topologi logis VLAN yang dibuat dengan percobaan menggunakan *packet tracert*. Dimana *switch managale* diletakkan pada lantai 1 dan lantai 2 yang masing-masing *swtich* dan antara *router* dengan *switch* yang terhubung *trunk link* menggunkan *port GigabitEthernet* yang memiliki kecepatan transfer data hingga 1.000 Mbps.

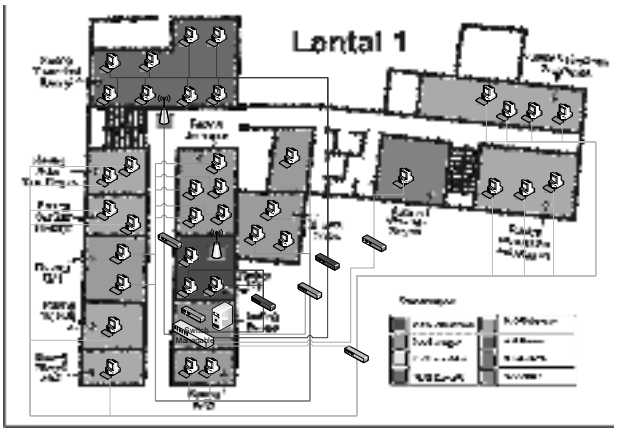


Gambar 1. Rancangan *blue print* topologi logis jaringan baru

Pada gambar 1 terdapat 2 buah *switch manageable* yang berfungsi untuk koneksi VLAN. VLAN mensegmentasi jaringan menjadi beberapa sub VLAN dalam kasus ini dikelompokkan menjadi VLAN manajer, VLAN perencanaan, VLAN jaringan, VLAN konstruksi, VLAN transaksi, VLAN pelayanan, VLAN *wireless*. Berikut merupakan rancangan pengalamatan jaringan yang akan disimulasikan:

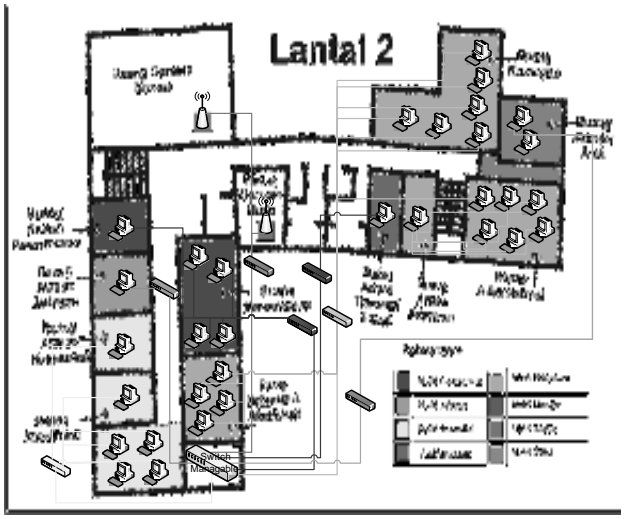
Tabel 1. Rancangan VLAN ID

No.	VLAN ID	VLAN *Name*	*Network Address*	*Gateway*	Jumlah
1.	11	vlan_manajer	192.168.11.0/29	192.168.11.1	3 PC
2.	12	vlan_perencanaan	192.168.12.0/28	192.168.12.1	8 PC
3.	13	vlan_jaringan	192.168.13.0/27	192.168.13.1	14 PC
4.	14	vlan_konstruksi	192.168.14.0/28	192.168.14.1	6 PC
5.	15	vlan_transaksi	192.168.15.0/28	192.168.15.1	9 PC
6.	16	vlan_pelayanan	192.168.16.0/26	192.168.16.1	26 PC
7.	17	vlan_*wireless*	192.168.17.0/26	192.168.17.1	2 AP
8.	18	vlan_*server*	192.168.18.0/29	192.168.18.1	1 PC



Gambar 2. Denah Lantai 1

Pada Gambar 2. di atas, penempatan *access point* terletak di atas alat mesin absen dan di ruang STI. *Switch manageable* terletak di Ruang *server*. Dari *switch managable* lantai 1 ke *switch managable* lantai 2 dihubungkan menggunakan *mode trunk*. Semua s*witch* yang menghubungkan ke VLAN-VLAN berada di ruang *server* yang terkoneksi dengan *switch manageable* yang berada di lantai 1.



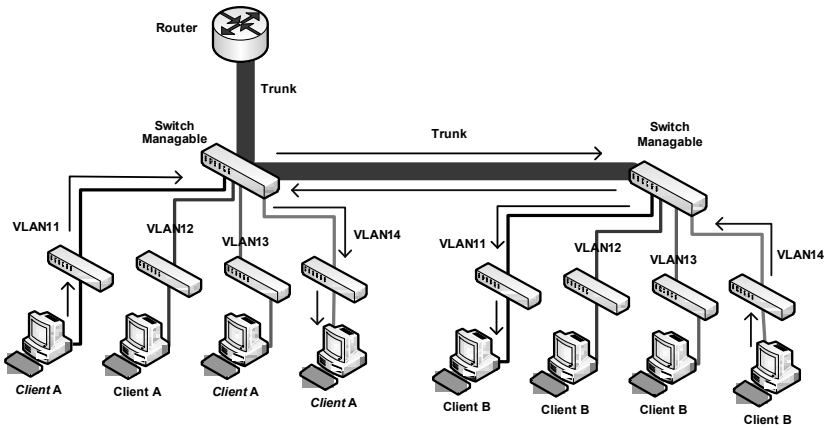
Gambar 3. Denah Lantai 2

Pada Gambar 3 di atas, peletakan *access point* di ruang rapat Menara dan di ruang rapat Muria. Sedangkan s*witch manageable* terletak di ruang gudang area. Seluruh s*witch* yang menghubungkan ke VLAN-VLAN berada di ruang gudang administrasi dan pelayanan yang terkoneksi dengan *switch manageable* yang berada di lantai 2.

Pengujian Sistem

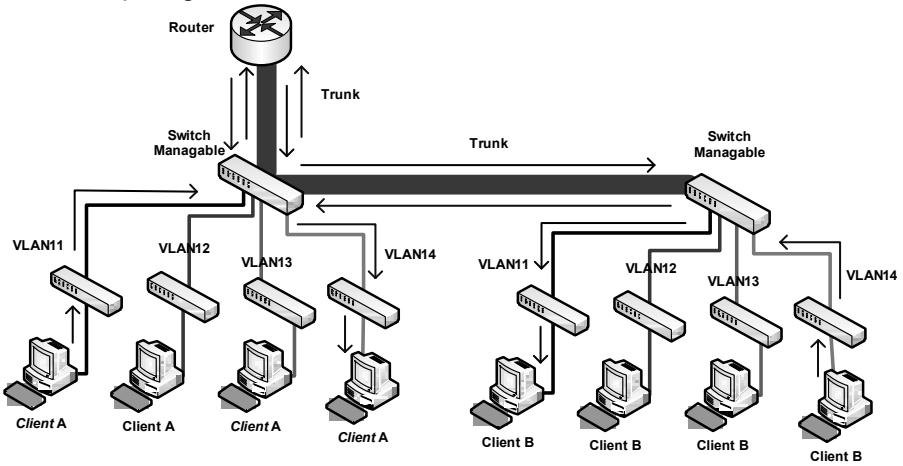
Pada penelitian ini pengujian dilakukan menggunakan 2 jenis pengujian sistem jaringan yaitu menggunakan simulator Cisco Packet Tracer untuk simulasi jaringan VLAN dan pengujian jaringan *VLAN* menggunakan 2 unit *notebook* dimana salah satu *notebook* tersebut berperan sebagai VLAN 12 dan yang lain berperan sebagai VLAN 13.

Pengujian VTP (VLAN *Trunking Protocol*)



Gambar 4. Pengujian VTP sesama VLAN yang sama

Pada gambar 4. dapat dilihat pengujian sesama VLAN yaitu dari VLAN 11 *client* A mengirimkan paket ke VLAN 11 *client* B akan melalui *trunk* yang sudah ditentukan pada switch mangable yaitu *interface* eth24. Begitu juga pada VLAN 14 *client* B mengirimkan paket ke VLAN 14 *client* A akan melalui *trunk* yang sama dengan VLAN 11 dalam hal ini karena penggunaan kabel secara bersama-sama dengan VLAN yang lain. jika pengiriman paket melakukan pengiriman antar VLAN yang berbeda maka dalam pengiriman tersebut akan melewati *router* seperti gambar 5.



Gambar 5. Pengujian VTP antar VLAN yang berbeda

Pengujian jaringan vlan pada mikrotik

Dalam pengujian yang dilakukan menggunakan aplikasi *ping* pada masing-masing komputer *client*. Pada pengujian ke-1 dengan menggunakan MikroTik menunjukkan hasil *ping* dari sesama komputer anggota VLAN 12 yaitu vlan_perencanaan dengan alamat IP 192.168.12.2 ke IP 192.168.12.1 menerima paket ICMP, berikut ini adalah hasil dari pengujian *ping* dari IP 192.168.12.2 ke IP 192.168.12.1:

```
C:\Users\User>ping 192.168.12.1
Pinging 192.168.12.1 with 32 bytes of data:
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64
Reply from 192.168.12.1: bytes=32 time<1ms TTL=64
```

Reply from 192.168.12.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.12.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Pada pengujian ke-2 dengan menggunakan MikroTik menunjukkan hasil dari *ping* komputer *client* yang berbeda VLAN yaitu vlan_perencanaan yang memiliki alamat IP 192.168.12.2 ke vlan_jaringan yang memiliki alamat IP 192.168.13.1, vlan_jaringan tersebut menirima paket ICMP dari vlan_perencanaan, berikut ini adalah hasil dari pengujian *ping* dari IP 192.168.12.2 ke IP 192.168.13.1:

C:\Users\User>ping 192.168.13.1
Pinging 192.168.13.1 with 32 bytes of data:
Reply from 192.168.13.1: bytes=32 time=1ms TTL=64
Reply from 192.168.13.1: bytes=32 time<1ms TTL=64
Reply from 192.168.13.1: bytes=32 time<1ms TTL=64
Reply from 192.168.13.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.13.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

Pada pengujian ke-3 menunjukkan hasil dari *ping* dari komputer *client* ke internet, karena *router* melewatkan paket ICMP ke internet untuk diterima, berikut ini adalah hasil dari pengujian *ping* 192.168.12.2 ke google.com :

C:\Users\User>ping google.com
Pinging google.com [202.67.41.187] with 32 bytes of data:
Reply from 202.67.41.187: bytes=32 time=47ms TTL=58
Reply from 202.67.41.187: bytes=32 time=50ms TTL=58
Reply from 202.67.41.187: bytes=32 time=56ms TTL=58
Reply from 202.67.41.187: bytes=32 time=61ms TTL=58
Ping statistics for 202.67.41.187:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 47ms, Maximum = 61ms, Average = 53ms

Pada pengujian ke-4 menunjukkan hasil dari komputer *client* melakukan *ping* dari vlan_*wireless* dengan alamat IP 192.168.17.2 ke vlan_perencanaan dengan alamat IP 192.168.12.1, pada paket ICMP di-*reject* karena vlan_*wireless* jika melakukan *ping* maka paket ICMP akan ditolak sehingga muncul pesan *Destination net uncreachable*, berikut ini adalah hasil dari pengujian *ping* dari IP 192.168.17.2 ke IP 192.168.12.1:

C:\Users\User>ping 192.168.12.1
Pinging 192.168.12.1 with 32 bytes of data:
Reply from 192.168.12.1: Destination net unreachable.
Reply from 192.168.12.1: Destination net unreachable.
Reply from 192.168.12.1: Destination net unreachable.
Reply from 192.168.12.1: Destination net unreachable.
Ping statistics for 192.168.12.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Pada pengujian ke-5 menunjukkan hasil dari komputer *client* melakukan *ping* dari vlan_perencanaan dengan alamat IP 192.168.12.2 ke vlan_*server* dengan alamat IP 192.168.18.1, paket ICMP tersebut dihapus karena semua komputer *client* VLAN tidah boleh melakukan *ping* terhadap *server* sehingga muncul pesan *Request timed out*, berikut ini adalah hasil dari pengujian *ping* dari IP 192.168.12.2 ke IP 192.168.18.1 :

```
C:\Users\User>ping 192.168.18.1
Pinging 192.168.18.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.18.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Pada pengujian ke-6 adalah hasil komputer *client* melakukan *scanning port* dengan menggunakan aplikasi Nmap yaitu dari komputer *client* vlan_perencanaan dengan alamat IP 192.168.12.2 ke *gateway router* Mikrotik dengan alamat IP 192.168.12.1, sehingga hanya muncul *port* yang terbuka saja oleh *router* Mikrotik, berikut adalah hasil dari pengujian *scanning port* dari IP 192.168.12.2 ke IP 192.168.12.1:

```
C:\Users\User>nmap -sS 192.168.12.1
Starting Nmap 6.40 ( http://nmap.org ) at 2013-12-16 16:00 SE Asia Standard Time
Nmap scan report for 192.168.12.1
Host is up (0.00077s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
8080/tcp open   http-proxy
8291/tcp open   unknown
MAC Address: D4:CA:6D:7F:25:A5 (Routerboard.com)
Nmap done: 1 IP address (1 host up) scanned in 11.43 seconds
```

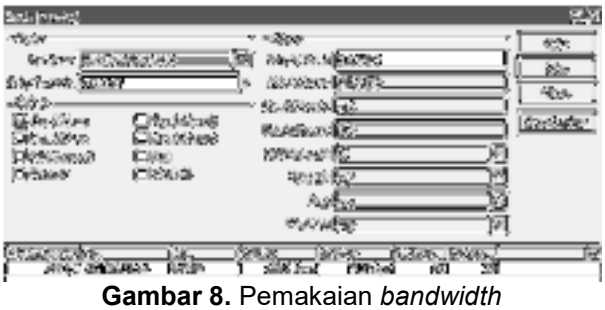
Pada gambar 6. menunjukkan komputer *client* dapat mengakses internet karena router mengizinkan semua komputer *client* VLAN dapat mengakses internet karena telah di-*filter* oleh *router* sebelum dapat mengakses internet.

Gambar 6. Komputer *Client browsing* ke internet

Pada gambar 7. menunjukkan komputer *client* tidak dapat mengakses www.youtube.com dikarenakan pada jam kerja yaitu mulai dari jam 8.00 situs tersebut tidak diizinkan untuk diakses oleh komputer *client*.

Gambar 7. Pemblokiran situs saat jam kerja

Pada gambar 8. menunjukkan komputer *client* termonitoring oleh *router* MikroTik dan menggunakan *bandwidth* yang terkoneksi ke jaringan VLAN ada 1 yaitu vlan_perencanaan dengan alamat IP 192.168.12.13, komputer *client* tersebut dapat menggunakan semua *bandwidth* yang ada.



Gambar 8. Pemakaian *bandwidth*

Analisis Dan Pembahasan

Dalam penggunaan VTP maka dalam pembuatan jaringan VLAN dapat menghemat pemakaian dalam penggunaan kabel karena kesemua VLAN telah menjadi satu, karena keterbatasan alat *switch managable* maka menggunakan alat MikroTik untuk mendukung dalam pembuatan jaringan VLAN tanpa *switch managable*.

Dalam konfigurasi MikroTik harus membuat VLAN ID untuk setiap *client*. Agar komputer *client* dapat terkoneksi dengan jaringan maka pada komputer *client* masing-masing diberi VLAN ID sesui bidangnya, karena tidak adanya *switch managable*.

Dalam menggunakan jaringan VLAN memudahkan seorang *administrator* untuk memonitoring jaringan VLAN tersebut karena dibaginya beberapa jaringan berdasarkan VLAN ID. *Broadcast domain* pada jaringan VLAN terjadi pada VLAN ID saja sehingga tidak menggangu jaringan VLAN yang lain.

Pada pengujian jaringan VLAN, terlihat pengujian ke-1 dan pengujian ke-2 pada *router* MikroTik dapat dilihat hasil *ping* menunjukkan *reply* yang berarti komputer yang dituju (*destination address*) dapat merespon paket ICMP dengan baik karena *router* mengizinkan selain VLAN 17 dapat mengirim paket ICMP.

Pada pengujian ke-3 dapat dilihat hasil dari *ping* menunjukkan *reply* yang berarti komputer *client* menuju (*destination address*) yaitu internet dengan situs google.com dapat merespon paket ICMP karena *router* MikroTik telah mengizinkan komputer *client* untuk dapat melakukan *ping* ke internet.

Pada pengujian ke-6 dapat dilihat bahwa komputer *client* VLAN 17 yaitu *wireless* dengan alamat IP 192.168.17.0/29 tidak dapat melakukan *ping* ke VLAN 11, VLAN 12, VLAN 13, VLAN 14, VLAN 15, dan VLAN 16. Dikarenakan berada dijaringan VLAN yang berbeda untuk

menajaga keamanan jaringan jika komputer *client* VLAN 17 melakukan *ping* ke VLAN 13 paket ICMP akan di-*reject* sehingga muncul pesan *Destination net uncreachable* karena *router* tidak mengizinkan paket ICMP untuk diteruskan dan *router* MikroTik akan me-*reject* paket ICMP tersebut.

Pada pengujian ke-7 dapat dilihat bahwa semua komputer *client* VLAN tidak dapat melakukan pengiriman paket ICMP ke VLAN 18 yaitu *server* karena *router* MikroTik tidak mengizinkan untuk melakukan pengiriman paket ICMP ke *server* sehingga muncul pesan *Request timed out* tetapi semua komputer *client* VLAN dapat mengakses *server* melalui *port* 80.

Pada pengujian ke-8 dapat dilihat bahwa jika ada komputer *client* yang melakukan aktifitas *scnning port* maka yang akan terlihat adalah beberapa *port* yang terbuka karena selain *port* 22, 80, 8080, dan 8291 akan dihapus karena demi keamanan *router* MikroTik agar komputer *client* tidak sembarangan menggunakan *port-port* yang lain.

Jika komputer *client* melakukan *browsing*, setiap paket yang melintas akan diperiksa oleh *router* MikroTik untuk diperksa dan router MikroTik berhak untuk menentukan apakah sebuah paket diizinkan atau tidaknya sebuah paket yang melintas. Seperti gambar 4. komputer *client* dapat melakukan *browsing* ke internet karena *router* MikroTik telah mengizinkan port 80, 443, 53, 21 untuk dilewatkan.

Pada saat jam kerja komputer *client* tidak diperbolehkan mengakses seperti facebook, twitter, dan youtube, agar tidak menurunkan kinerja karyawan maka situs tersebut akan diblok sementara dari jam 8.00 sampai jam 12.00, seperti yang terlihat pada gambar 5. Dalam pengeblokkan situs, *router* MikroTik telah dikonfigurasi untuk memblok *port* 80 pada youtube.com karena youtube masih menggunakan HTTP, *port* 443 untuk facebook.com dan twitter.com karena facebook dan twitter menggunakan port 443 yaitu HTTPS.

Dalam penggunaan manajemen *bandwidth* hanya membagi berdasarkan dari komputer *client* yang terkoneksi ke jaringan VLAN, *bandwidth* yang disediakan oleh ISP (*Internet Service Provider*) untuk *download* sebesar 1 Mbps dan untuk *upload* sebesar 512 kbps. Jika hanya ada satu *user* yang menggunakan jaringan dan melakukan *download* maka sepenuhnya *bandwidth* akan dipakai oleh 1 *user* yaitu sebesar 1 Mbps, apabila ternyata ada 9 komputer *client* lagi yang terkoneksi ke jaringan maka *bandwidth* akan dibagi menjadi 10 yaitu masing-masing komputer *client* mendapat *bandwidth* sebesar 102 kbps. Seperti pada gambar 6. adalah komputer *client* yang terkoneksi ke jaringan VLAN dan mendapatkan semua *bandwidth* yang ada

KESIMPULAN

Berdasarkan penelitian di atas, maka dapat mengambil beberapa kesimpulan antara lain yaitu :

a). Pada perancangan *blue print* jaringan VLAN dapat dijadikan alternatif untuk membangun jaringan yang baik sehingga memudahkan seorang *administrator* jaringan untuk menentukan kebijakan yang diterapkan kepada *client*.
b). Kelebihan menggunakan jaringan VLAN, jaringan menjadi aman karena dalam pengiriman segmennya terpisah secara *logic* untuk mengiriman data serta dapat mengurangi terjadinya *broadcast domain*.
c). Dalam mendistribusikan jaringan lebih termanajemen karena menggunakan jaringan berbasis VLAN.
d). Dalam penggunaan VTP pada VLAN dapat menghemat dalam penggunaan kabel jaringan.

Untuk pengembangan selanjutnya, dapat dibahas mengenai manajemen *bandwidth* dengan metode yang lain yaitu dengan memanajemen *bandwidth* berdasarkan *group* VLAN. Dalam pemblokiran situs saat jam kerja yakni situs HTTPS pada www.facebook.com tidak dilakukan pemblokiran karena keterbatasan penggunaan aplikasi pada MikroTik, diharapkan

kedepannya dapat memblokir situs-situs yang dirasa tidak penting dalam bekerja dengan memanfaatkan eksternal *proxy*.

DAFTAR PUSTAKA

Dewi, R. P. (2009). *Simulasi Dynamic Routing Protocols, Access List Dan VLAN Pada Jaringan Komputer.* Yogyakarta: Skripsi Universitas Gajah Mada.

Dwiningsih. (2011). *Simulasi Virtual LAN (VLAN) Menggunakan Packet Tracert 5.3. Sebagai Pengembangan Jaringan Di PT. MekarArmada Jaya Magelang.* Yogyakarta: Skripsi IST AKPRIND.

Mochammad, L. H., & Azis, C. (2008). *Menguasai Router Masa Depan Menggunakan Mikrotik RouterOS.* Yogyakarta: ANDI.

Sofana, I. (2012). *CISCO CCNA & Jaringan Komputer.* Bandung: INFORMATIKA.

Sofana, I. (2012). *CISCO CCNP & Jaringan Komputer.* Bandung: INFORMATIKA.

Susanti, I. (2010). *Perancangan Dan Simulasi Jaringan Berbasis Virtual Local Area Network (VLAN) Menggunakan Cisco Catalyst.* Yogyakarta: Skripsi IST AKPRIND.

Towidjojo, R. (2013). *Mikrotik Kung Fu Kitab 1.* Jakarta: JASAKOM.

Towidjojo, R. (2013). *Mikrotik Kung Fu Kitab 2.* Jakarta: JASAKOM.