Penerapan Virtual Local Area Network Menggunakan OVS pada Jaringan Virtual Machine Berbasis Promiscuous Mode

Dinda Yunafril, Huda Ubaya*, Rido Zulfahmi
Program Studi Teknik Komputer, Diploma Komputer,
Fakultas Ilmu Komputer, Universitas Sriwijaya
Email: huda_ubaya@yahoo.com

***Abstract*—Penerapan sistem jaringan Virtual Local Area Network (VLAN) pada saat ini banyak dimanfaatkan oleh instansi pendidikan, ditempat umum, dan juga perkantoran. Pemanfaatan sistem jaringan ini memungkinkan untuk membagi suatu koneksi fisik pada sebuah LAN menjadi beberapa koneksi logika. Pada penelitian ini menggunakan virtual machine, maka untuk mendukung penerapan VLAN ini menggunakan OVS. OVS merupakan suatu software switch virtual yang berfungsi menghubungkan perangkat pada suatu sistem jaringan. Untuk sebuah jaringan komputer yang dibangun menggunakan virtual machine terdapat kontroler antarmuka yaitu promiscuous mode yang berfungsi untuk mengijinkan dan mencegat paket data yang masuk ke jaringan. Penelitian ini menggunakan metode observasi pada setiap pengerjaan dan pengujian, juga metode litelatur untuk memperoleh informasi. Hasil penelitian ini adalah perangkat virtual yang dihubungkan menggunakan OVS pada jaringan virtual machine pada sistem jaringan VLAN yang dapat menghubungkan jaringan dan mesin virtual dengan promiscuous mode.**

***Keywords*—VLAN, OVS, Virtual Machine, Promiscuous Mode**

I. PENDAHULUAN

Cloud Computing adalah teknologi informasi yang tengah digemari pada beberapa tahun terakhir, karena dapat meminimalkan infrastruktur teknologi informasi. Teknologi utama yang digunakan dalam pembangunan *Cloud Computing* adalah Virtualisasi. Virtualisasi adalah proses pembuatan suatu yang bersifat fisik, misalnya operating system (OS),perangkat penyimpanan atau penyimpanan data dan sumber daya jaringan. Dimana virtual machine (VM) bertanggung jawab untuk menjalankan OS tersebut seperti menggunakan mesin sesungguhnya [1].

Virtualisasi jaringan (network virtualization) bertujuan untuk menghubungkan setiap VM yang dibangun tersebut ke sebuah port switch virtual. Walaupun virtualisasi membuat implementasi semakin sederhana, perlu ada administrasi jaringan diantara virtual machine (VM). Administrasi jaringan tersebut dilakukan oleh software hypervisor. Namun, hypervisor hanya berfungsi sebagai bridge. Open virtual switch (OVS) sebagai alternatif virtual switch yang cukup populer di kalangan pengembang cloud, dapat menjadi solusi untuk mengelola trafik antar VM dengan komunikasi dari luar.

Virtualisasi dapat di implementasikan kedalam berbagai bentuk, misal nya Network Virtualization yaitu VLAN. Dimana VLAN masuk ke dalam teknik untuk transmisi data pada data link layer. Permodelan data link layer adalah permodelan layer yang dapat dimanfaatkan pada pengembangan cloud computing. Data link layer menghubungkan host dengan host lain sehingga dapat melakukan kegiatan apa saja yang telah diatur pada sistem dan memungkinkan host tersebut bisa mengatur segala aktifitas pada host lain namun tetap dapat saling terhubung antar keduanya.Pada sebuah jaringan komputer yang dibangun menggunakan virtual machineterdapat mode kontroler antarmuka jaringan pada setiap jaringan yaitu Promiscious mode, Promiscuous mode adalah sebuah mode yang mengijinkan dan juga mencegat setiap paket data yang masuk dalam sebuah jaringan tersebut [2].

Dalam penulisan penelitian ini penulis akan mencoba melakukan konfigurasi Virtual Local Area Network (VLAN) menggunakan OVS pada jaringanvirtual machine dengan menerapkan promiscuous mode. Dimana promiscuous mode ini berfungsi untuk menerima dan memproses data yang datang dari VLAN.

II. MATERIAL DAN METODE

A. Jaringan Komputer

Jaringan Komputer adalah kumpulan dari beberapa komputer dengan perangkat lain pendukung komputer yang saling terhubung, dirancangdalam satu kesatuan untuk bekerja sama dalam berbagai tujuan dan manfaat seperti bertukar informasi dan berkomunikasi data. Media yang digunakan jaringan komputer dapat melewati kabel atau tanpa kabel yang mengijinkan pengguna jaringan komputer dapat melakukan aktifitas seperti bertukar informasi, dokumen dan data, juga perangkat keras (hardware) dan perangkat lunak (*software*) yang terhubung dengan jaringan.

Tujuan dan manfaat dibangunnya jaringan komputer adalah untuk komunikasi data yang dilakukan antara pengirim (transmitter) dan penerima (receiver) lebih akurat dan cepat, resource sharing adalah kegiatan yang dilakukan bersama-sama bertujuan untuk meningkatkan layanan dalam melakukan komunikasi data antar pengguna komputer, Saving Money adalah penghematan biaya dalam pembelian hardware untuk pembangunan jaringan komputer, Dan High reability (kehandalan tinggi) maksudnya adalah dari segi kehandalan, manajemen sistem dan keamanan data yang akurat dapat diterapkan pada jaringan komputer karena setiap komputer client dapat dikendalikan dari suatu tempat [3].

B. Virtualisasi dan Cloud Computing

Virtualisasi adalah komponen penting dari cloud computing. Pada cloud environment, sumber daya (umumnya berbentuk fisik/hardware) divirtualisasi sehingga dapat dikelola lebih efisien. Dari sudut pandang komputasi, virtualisasi dapat diasumsikan alih-alih menggunakan perangkat fisik (real environment), perangkat virtual (virtual environment) digunakan untuk menjalankan sebuah serangkaian program yang sesuai kebutuhan Virtualisasi merupakan salah satu cara untuk mengelola komputer dalam berbagai lingkungan yang dibagi pada saat yang sama.

Cloud Computing merupakan kata kunci dari virtualisasi. *Cloud Computing* merupakan sistem komputerisasi yang menggunakan jaringan/internet yang menyediakan sumber daya, software, informasi dan aplikasi yang dbutuhkan oleh pengguna. *Cloud Computing* menggunakan internet dan remote server pusat sebagai teknik untuk menjaga data dan aplikasi. Cloud computingmemudahkan konsumen dan pebisnis dalam menggunakan aplikasi tanpa harus instalasi dan mengakses file di komputer pribadi [1]. Sistem *Cloud Computing* ini memudahkan untuk sistem komputasi yang jauh lebih mudah dengan menyatukan penyimpanan data, mengatur dan bandwidth. Jadi, *Cloud Computing* bisa diartikan sebagai sistem komputerisasi berbasis komputer yang saling terhubung.

Cloud Computing biasa disebut sebagai virtualisasi yang telah dikembangkan. Karena *Cloud Computing* merupakan salah satu teknologi untuk menyatukan sistem virtualisasi dan grid computing. Karena, terdapat proses virtualisasi juga grid computing, dimana proses komputasi yang dilakukan ke berbagai server akan diteruskan dan saling terhubung di dalam cloud, sehingga proses yang dilakukan akan lebih mudah[4]. Virtualisai dapat diterapkan kedalam berbagai bentuk diantara nya yaitu Network Virtualization.

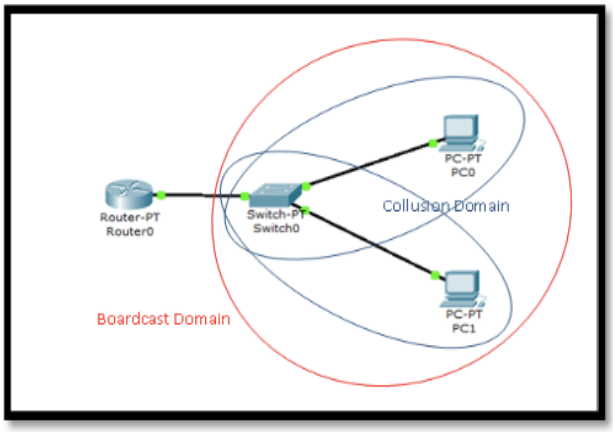
C. Network Virtualization (Virtualisasi Jaringan)

Network virtualization (virtualisasi jaringan) adalah sebuah network environment di mana beberapa jaringan virtual dibangun di atas jaringan fisik sebenarnya. Setiap jaringan virtual pada virtualized environment adalah kumpulan dari virtual node dan virtual link. Pada jaringan tersebut kita dapat membuat dan mengelola beberapa jaringan virtual pada level software tanpa mengganggu satu sama lain. Jaringan inilah yang umumnya dipakai penyedia jasa untuk melayani user pengguna layanan. Network virtualization diimplementasikan pada jaringan VLAN [1].

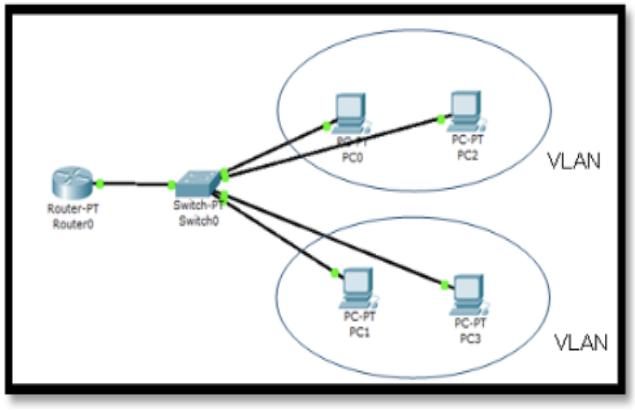
D. Virtual Local Area Network (VLAN)

VLAN (Virtual Local Area Network) merupakan salah satu cara untuk membagi koneksi fisik menjadi beberapa koneksi logika sebuah LAN. Biasanya pada LAN setiap worktation tersambung pada suatu hub atau repeater. Bila terdapat dua workstation yang melakukan pengiriman data di waktu yang sama, akan terjadi tubrukan (collosion) dan data yang dikirimkan akan hilang. Untuk menghindari terjadinya tubrukan, maka dalam jaringan ditambah perangkat switch. Workstation dan hub masuk dalam sebuah segmen LAN. Segmen LAN dapat dikatakan collosion domain karena collosion terjadi pada sebuah segmen. Wilayah dimana terdapat broadcast disebut dengan broadcast domain. Ilustrasi LAN dapat dilihat pada gambar 1.

VLAN bisa membuat sebuah segmen LAN menjadi banyak broadcast domain. Sebab VLAN membuat segmen LAN memakai koneksi logika, maksudya setiap workstation dapat ditempatkan secara terpisah yang tidak harus diletakkan pada lokasi yang sama. Contoh pada satu gedung yang memiliki banyak lantai. Sebab broadcast pada suatu VLAN tidak bisa dihubungkan ke VLAN lainnya, Untuk dapat meneruskan paket data dari VLAN ke VLAN lainnya harus menggunakan perangkat router sebagai penghubung antara VLAN yang berbeda[8]. Ilustrasi fisik VLAN dapat dilihat pada gambar 2.



Gambar 1. Ilustrasi LAN



Gambar 2. Topologi Fisik VLAN

VLAN dikelola berdasarkan metode untuk mengelolanya, dalam mengatur VLAN terdapat beberapa metode yaitu menggunakan port, MAC address, dan lain- lain. Ketika VLAN disetting berdasarkan port maka data yang tersimpan dalam database merupakan port-port yang digunakan untuk VLAN, pengonfigurasian VLAN diatur pada switch yang nantinya switch ini lah yang bertanggung jawab untuk menyimpan data atau yang mengatur jalan nya pengiriman data yang melewati metode dalam mengklasifikasikan VLAN.

Jika switch mendapat data dari suatu komputer, switch bisa mengenali VLAN ID mana yang mengirim data tersebut. VLAN ID dapat dikenali menggunakan port pengirim, alamat Media Access Controll (MAC Address) dari pengirim dan alamat jaringan [5].

Dalam melakukan transfer data VLAN mempunyai 2 jalur yaitu Tradisional yang artinya VLAN memiliki banyak jalur. Kemudian, VLAN Trunking maksudnya VLAN yang mempunyai 1 jalur mempunyai teks yang

mengidentifikasikan beberapa VLAN atau jalurnya mempunyai banyak jalur logikadalam 1 fisik.

Trunk beroperasi pada layer 2 switching, sementara di ethernet frame tersebut tidak ada field untuk VLAN. Jika ada traffic yang masuk ke sebuah switch dan akan dilewatkan ke trunk port, untuk mengetahui VLAN yang akan dituju maka yang digunakan adalah trunk encapsulation. Ada 2 trunk encapsulation yang digunakan di swtich Cisco yaitu ISL (Inter Switch Link) namun encapsulation jenis ini sudah tidak di pakai karena bit nya yang terlalu besar dan IEEE 802.1q (open standard) adalah jenis encapsukation default yang digunakan switch Cisco [5].

E. Open Virtual Switch

Dalam artikel Open vSwitch In Your Network [6], dijelaskan bahwa open virtual switch didesain berbasis Apache 2.0. Open vSwitch ini dirancang untuk memungkinkan otomatisasi jaringan besar melalui ekstentensi terprogram, sambil tetap mendukung antarmuka dan protokol manajemen standar. Open vSwitch mampu menjalankan enkapsulasi paket VLAN. Open virtual Switch dirancang untuk mendukung distribusi di beberapa server fisik yang mirip dengan Vmware yang didistribusikan Vswitch atau Nexus 1000V dari Cisco. Open virtual switch dapat beroperasi baik sebagai switch jaringan berbasis perangkat lunak yang berjalan dalam mesin virtual (VM) hypervisor. Open virtual switch juga telah diintegrasikan ke dalam berbagai platform *Cloud Computing* software dan sistem manajemen virtualisasi.

Open vSwitch digunakan dalam banyak produk dan berjalan dibanyak lingkungan produksi besar. Open vSwitch merupakan software multilayer yang didesain untuk digunakan sebagai virtual switch dalam lingkungan virtual server. Open vSwitch berfungsi sebagai virtual switch dalam lingkungan virtual machine yang dirancang untuk mendukung distribusi di beberapa server fisik.

Open vSwitch menggunaan berbagai jenis flow untuk tujuan yang berbeda yaitu :

- OpenFlow flow , adalah jenis aliran yang paling penting. Pengontrol OpenFlow menggunakan aliran ini untuk menentukan kebijakan switch. Arus OpenFlow ini mendukung wildcard, prioritas, dan banyak tabel. Ketika control in-band sedang digunakan Open vSwitch membuat bebrapa aliran tersembunyi dengan prioritas lebih tinggi dari controller atau pengguna dapat mengkonfigurasi yang tidak terlihat melalui OpenFlow.
- Implementasi software Open vSwitch menggunakan aliran jenis kedua secara internal. Aliran ini disebut datapath atau kernel yang tidak mendukung prioritas dan hanya terdiri dari satu tabel membuat aliran ini cocok untuk penyimpanan cache. Arus OpenFlow dan arus datapath juga mendukung tindakan yang berbeda dan nomor port yang berbeda. Aliran datapath adalah detail implementasi Oen vSiwtch yang dapat dikembangkan dimasa yang akan datang. Bahkan saat ini implementasi datapath pada open vSwitch menggunakan perangkat keras.

F. Promiscuous Mode

Promiscuous mode merupakan salah satu mode/ port dalam penerapan VLAN pada sebuah jaringan. Dimana umumnya ada dua jenis mode/port yang bisa diterapkan pada VLAN yaitu:

- Promiscuous port (P-Port)

  Pada Promiscuous port/ mode ini port switch terhubung ke router, firewall atau perangkat gateway yang lainnya. Kemudian, Promiscuous port/ mode dapat berkomunikasi dengan perangkat lain yang terhubung ke VLAN utama atau sekunder. Oleh karena itu port/ mode jenis ini adalah jenis port yang diizinkan untuk mengirim dan menerima data dari port lain pada VLAN.

- Host Ports, dibagi menjadi 2 yaitu :
  - Isolated Port (I-Port)

    Isolated port ini berfungsi untuk menghubungkan ke host biasa yang berada di VLAN terisolasi. Port ini hanya berkomunikasi dengan P-Ports.

  - Community Port (C-Port)

    Sedangkan community port berfungsi untuk menghubungkan ke host biasa yang berada di komunitas VLAN. Port ini berkomunikasi dengan promiscuous port dan port pada komunitas VLAN yang sama. Dengan kata lain, Promiscuous mode adalah sebuah mode dimana setiap paket data yang dikirim dapat diterima dan dibaca oleh adapter jaringan (LAN Card). Promiscuous mode diartikan sebagai kemampuan menerima (dalam hal ini paket) dari sumber lain yang tidak diminta. Atau dalam bahasa lainnya ‘distributed or applied without order’ Artinya ketika network card sudah diatur sebagai promiscuous mode, maka komputer atau laptop akan memiliki kemampuan menerima paket yang tidak hanya ditujukan pada IP Address [5].

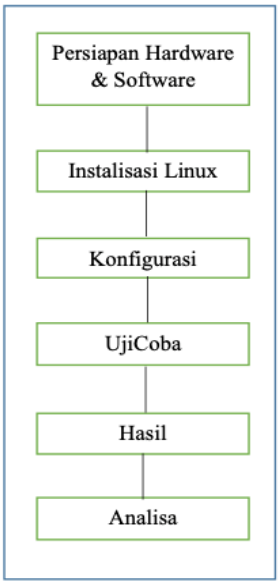
III. PERANCANGAN SISTEM

A. Perancangan

Perancangan Sistem meliputi :

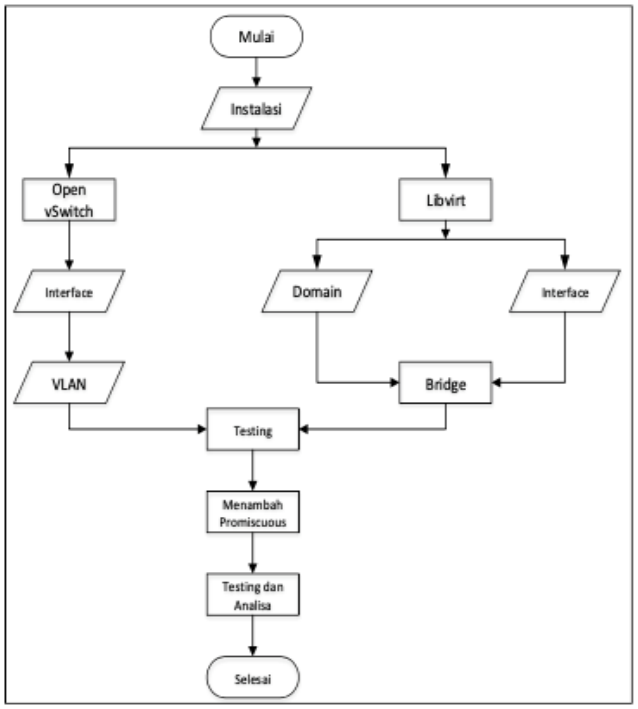
- Perancangan proses kebutuhan yang dibutuhkan dalam membangun *Cloud Computing* dengan system operasi Linux.
- Mengaktifkan promiscuous mode pada salah satu port Virtual Local Area Network.

Tahap awal yang dilakukan adalah mempersiapkan software & hardware yang akan digunakan pada sistem yang akan dibuat. Melakukan instalasi Linux Ubuntu, dimana pada penerapan sistem kali ini menggunakan Open vSwitch dan Libvirt. Kemudian mengkonfigurasi system yaitu network, open vswitch, libvirt, dan VLAN. Pada tahap akhir penerapan system melakukan uji coba untuk menentukan apakah sistem yang dibuat berhasil atau tidak. Apabila percobaan tersebut berhasil, maka tahap selanjutnya adalah mengumpulkan seluruh data untuk dianalisa. Mekanisme penerapan sistem dapat dilihat dari gambar 3.

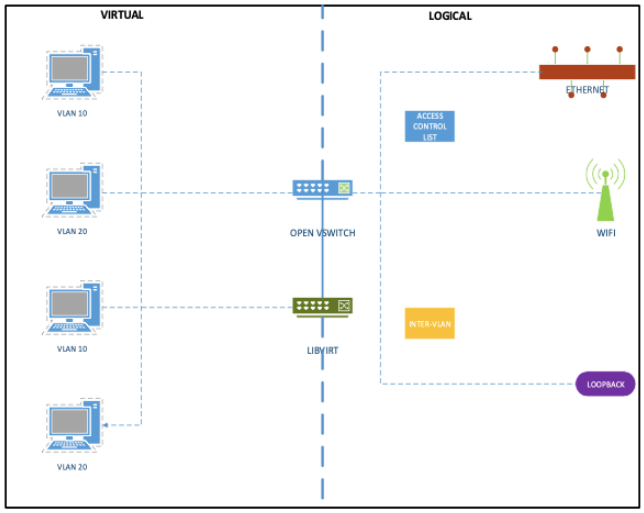


Gambar 3. Mekanisme Penerapan Sistem

Pada gambar 4 menjelaskan tentang alur pengerjaan sistem, pertama melakukan instalasi program yaitu Linux Ubuntu, software Open vSwitch dan Libvirt. Pada Libvirt terdapat domain yaitu ovs-network dan interface vnet0-vnet3yang kemudian di Bridge. Sedangkan pada Open vSwitch terdapat interface yaitu ovsbr0 yang kemudian di konfigurasikan untuk VLAN. Tahap selanjutnya yaitu tes ping antara VLAN dan Bridge untuk mengetahui apakah konfigurasi VLAN tersebut benar atau salah. Langkah selanjutnya yang dilakukan adalah menambah konfigurasi prmosicuous mode pada salah satu interface, dan penulis mensetting promiscuous mode pada interface vnet0 yaitu pc0 pada virtual machine. Terakhir, melakukan Tes ping dan analisa setelah dilakukan konfigurasi promiscuous mode pada vnet0 tersebut.



Gambar 4. Flowchart Sistem



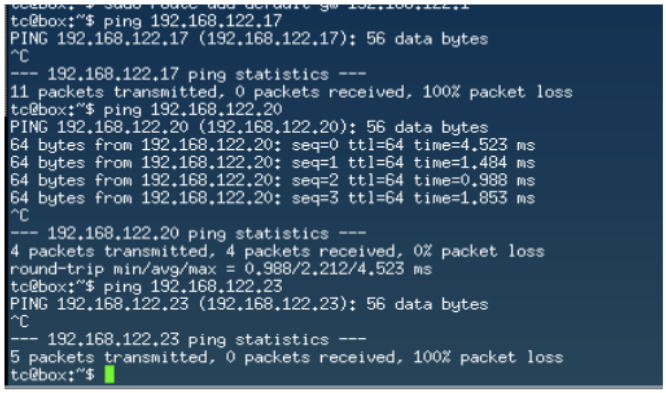
Gambar 5. Topologi Virtualisasi

IV. HASIL DAN PEMBAHASAN

Dari hasil pembuatan rancangan bangun sistem *Cloud Computing* menggunakan Open vSwitch pada sistem operasi Linux. Dimana pada project ini Open vSwitch yang berfungsi sebagai virtual switch untuk mengkoneksikan empat virtual machine, dimana empat virtual machine tersebut berada pada satu network yang sama dengan gateway 192.168.122.1. Pada pengujian ini dibuat dua buah tag VLAN yang berbeda diantara virtual machine yang telah dibangun yaitu tag 10 dan tag 20.

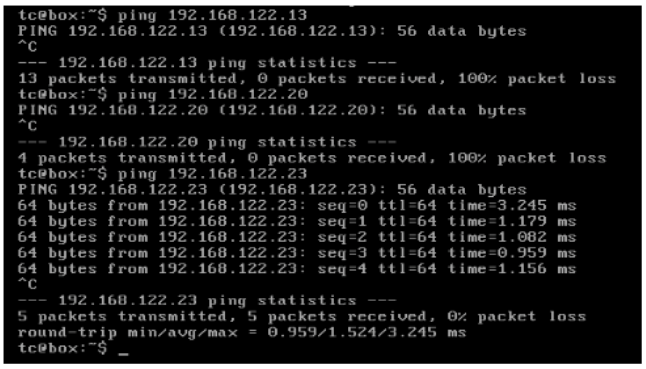
Maka, dihasilkan suatu penerapan Virtual Local Area Network (VLAN) menggunakan Open vSwitch pada jaringan virtual machine yang kemudian akan dilakukan pengujian tes ping pada setiap virtual machine untuk membuktikan apakah konfigurasi Virtual Local Area Network (VLAN) dengan Open vSwitch telah berhasil atau tidak..

Pada gambar 6 diatas menjelaskan tentang pc0 yang merupakan anggota dari VLAN10 melakukan uji tes ping ke pc1, pc2, dan pc3. Dimana pc1 dan pc3 merupakan anggota dari VLAN yang berbeda dengan pc0 yaitu VLAN20. IP pc1 adalah 192.168.122.17 dan IP pc3 yaitu 192.168.122.23. Maka hasil tes ping yang dilakukan pc0 terhadap kedua pc tersebut tidak berhasil. Sedangkan, pada pc2 yang merupakan anggota dari VLAN yang sama dengan pc0 yaitu VLAN10 dengan IP 192.168.122.20 uji tes ping berhasil dilakukan.



Gambar 6. Test ping ke PC 1, PC 2, dan PC 3

Hasil tes ping yang dilakukan pc1 ke pc0, pc2, dan pc3 seperti pada gambar 7 menjelaskan bahwa tes ping berhasil dilakukan pada pc yang berada di anggota VLAN yang sama yaitu pc1 dengan IP 192.168.122.17 dan pc3 dengan IP 192.168.122.23. Dimana, pc1 dan pc3 merupakan anggota dari VLAN20. Namun, uji tes ping tidak berhasil dilakukan pada pc yang berbeda VLAN seperti tes ping pc1 ke pc0 dengan IP 192.168.122.13 dan pc2 dengan IP 192.168.122.20, karena pc0 dan pc2 merupakan anggota VLAN10.



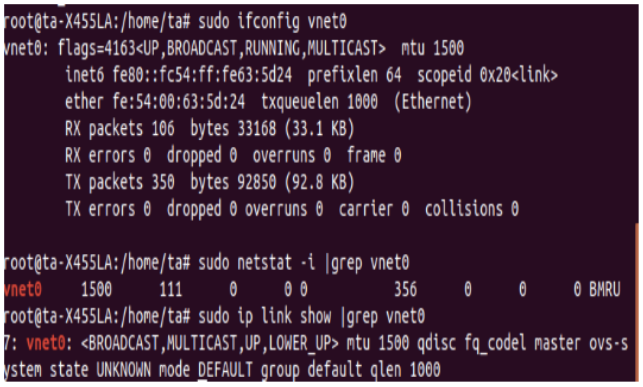
Gambar 7 Tes PING pc1 ke pc0, pc2, dan pc3

Setelah melakukan konfigurasi Virtual Local Area Network (VLAN) pada sistem ini penulis mengaktifkan promiscuous mode pada port vnet0 atau pc0 pada virtual machine dengan IP 192.168.122.13 yang merupakan anggota dari VLAN10. Kemudian masing-masing pc virtual yaitu pc1 dan pc2 akan melakukan ping terhadap pc0 yang nanti nya promiscuous mode tersebut berfungsi untuk mengijinkan setiap paket-paket data yang masuk ke port pc0. Dimana pc1 merupakan anggota yang berbeda dari pc0 yaitu VLAN20, yang pada umumnya VLAN yang berbeda tidak dapat saling terhubung. Selanjutnya pc2 yang merupakan anggota VLAN yang sama dengan pc0 yaitu VLAN10. Dimana pc yang berada pada VLAN yang sama dapat saling terhubung satu sama lain. Dengan adanya promiscuous mode paket data yang berasal dari pc yang berbeda maupun yang sama VLAN dapat dibaca oleh port yang telah diatur promiscuous mode nya.

Selanjutnya hasil tesping pada masing-masing pc yaitu pc1, pc2, dan pc3 terhadap pc0 tersebut akan dapat dibaca oleh promiscuous mode dan ditampilkan menggunakan software tcpdump. Setelah melakukan konfigurasi Virtual Local Area Network (VLAN) pada sistem ini penulis mengaktifkan promiscuous mode pada port vnet0 atau pc0 pada virtual machine dengan IP 192.168.122.13 yang merupakan anggota dari VLAN10. Kemudian masing-masing pc virtual yaitu pc1 dan pc2 akan melakukan ping terhadap pc0 yang nanti nya promiscuous mode tersebut berfungsi untuk mengijinkan setiap paket-paket data yang masuk ke port pc0. Dimana pc1 merupakan anggota yang berbeda dari pc0 yaitu VLAN20, yang pada umumnya VLAN yang berbeda tidak dapat saling terhubung. Selanjutnya pc2 yang merupakan anggota VLAN yang sama dengan pc0 yaitu VLAN10. Dimana pc yang berada pada VLAN yang sama dapat saling terhubung satu sama lain. Dengan adanya promiscuous mode paket data yang berasal dari pc yang berbeda maupun yang sama VLAN dapat dibaca oleh port yang telah diatur promiscuous mode nya.

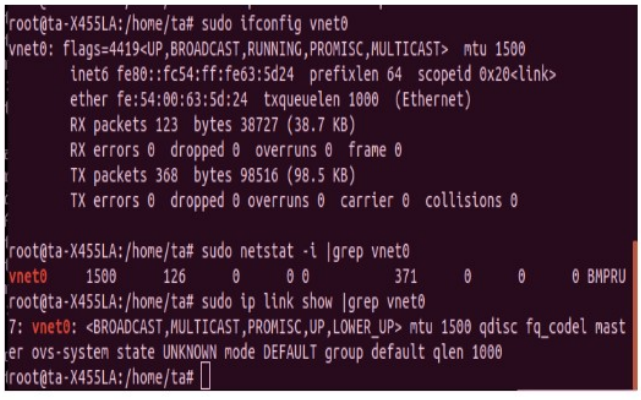
Selanjutnya hasil tesping pada masing-masing pc yaitu pc1, pc2, dan pc3 terhadap pc0 tersebut akan dapat dibaca oleh promiscuous mode dan ditampilkan menggunakan software tcpdump.

Pada gambar 8 menjelaskan tentang port vnet0 yang belum diaktifkan promiscuous mode nya. Terdapat 3 perintah yang pertama yatu ifconfig vnet0 yang bertujuan untuk menampilkan infromasi terkait dengan informasi penting mengenai network interface pada vnet0 dan hasil ifconfig tersebut terdapat flags Up, Broadcast, Running, dan Multicast . Kedua, perintah netstat –i |grep vnet0 maksud nya adalah menampilkan antar muka yang berada pada vnet0 terdapat juga flag BMRU yang artinya Broadcast, Multicast, Running, dan UP. Dan Ketiga yaitu perintah ip link show |grep vnet0 yang digunakan untuk membaca link status pada vnet0 dan hasil nya juga terdapat flag Broadcast, Multicast, Up, dan Lower Up.



Gambar 8 vnet0 yang belum diaktifkan promiscuous mode nya

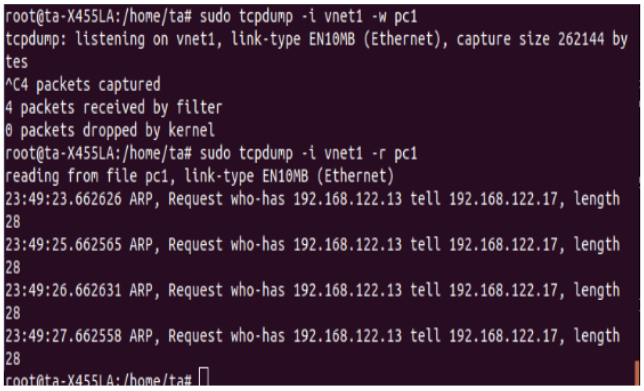
Gambar 9 menjelaskan tentang hasil setelah konfigurasi promiscuous mode pada port vnet0. Sama dengan penjelasan pada Gambar 4.5 terdapat 3 perintah yaitu ifconfig vnte0, netstat –i |grep vnet0, dan ip link show |grep vnet0. Dimana ketiga perintah diatas memiliki tujuan yang sama yaitu bertujuan menampilkan informasi dari port vnet0. Pada hasil dari masing- masing perintah tersebut terdapat nilai baru pada flag yaitu PROMISC yang berarti promiscuous mode pada vnet0 telah aktif dan konfigurasi promiscuous mode yang dilakukan benar.



Gambar 9. Hasil Setelah Konfigurasi Promiscuous Mode

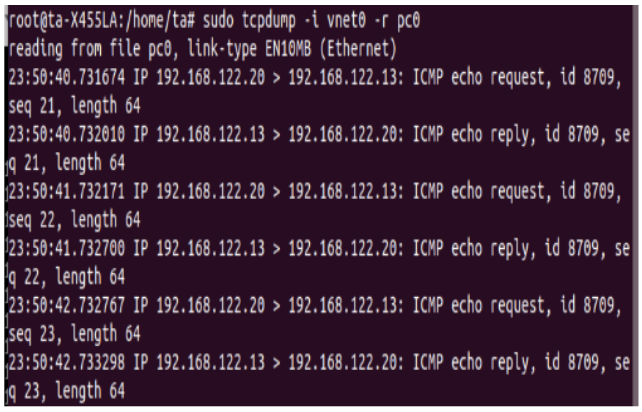
Pada gambar 10 menjelaskan tentang hasil ping dari vnet1 atau pc1 pada virtual machine terhadap vnet0. Dimana kedua

port tersebut berada pada vlan yang berbeda. Maka hasil paket data yang dibaca oleh tcpdump yaitu pc1 dengan IP 192.168.122.17 mengirim ARP request yang ditunjukkan ke pc0 dengan IP 192.168.122.13. Namun ARP dari pc1 tidak di reply oleh pc0 karena kedua pc tersebut berada pada VLAN berbeda.



Gambar 10 hasil ping dari pc1 ke VM terhadap vnet0

Gambar 11 menjelaskan tentang hasil ping vnet2 ke vnet0 dimana kedua port tersebut saling terhubung karena berada pada VLAN yang sama yaitu VLAN10. Hasil paket data yang dapat dibaca oleh tcpdump adalah vnet2 atau pc2 pada virtual machine dengan IP 192.168.122.20 mengirim ICMP echo request ke vnet0 atau pc0 dengan IP 192.168.122.13. Kemudian pc0 IP 192.168.122.13 menerima ICMP echo request dari pc2 dengan memberikan ICMP reply ke pc2 dengan IP 192.168.122.20.



Gambar 11. Hasil ping vnet2 ke vnet0 dimana kedua port tersebut saling terhubung karena berada pada VLAN10

V. KESIMPULAN

Dari pembuatan penelitian ini, penulis dapat mengambil kesimpulan bahwa hasil dari penerapan Virtual Local Area Network (VLAN) menggunakan Open vSwitch pada jaringan virtual machine berbasis promiscuous mode ini adalah sebagi berikut :

- Open vSwitch mampu beroperasi dengan baik sebagai switch pada perangkat lunak yang berjalan dalam virtual machine. Pada sistem yang dibangun oleh penulis Open vSwitch berperan sebagai penghubung antara sistem operasi Linux dengan Libvirt. Dimana Libvirt ini berfungsi untuk menjalankan dan mengelola virtual machine.
- Sistem jaringan Virtual Local Area Network (VLAN) yang penulis bangun berhasil diterapkan menggunakan Open vSwitch sebagai penghubung antar virtual machinedengan IP gateway 192.168.122.1 dan netmask 255.255.255.0 pada sistem operasi Linux Ubuntu.
- Penulis berhasil mengaktifkan promiscuous mode pada sistem jaringan Virtual Local Area Network (VLAN) dan melakukan uji coba ping dari masing-masing VLAN pada pc virtual, yang kemudian dapat dibaca dengan menggunakan software tcpdump.

DAFTAR PUSTAKA

[1] M. G. U. P. K. Utomo, R. Munadi, and L. V. Yovita, "Perancangan Dan Analisis Performansi Open Vswitch Untuk Jaringan Virtual," *eProceedings Eng.*, vol. 2, no. 2, 2015.

[2] L. A. N. DI JARINGAN, "DAMPAK SNIFFING PADA KEAMANAN DATA."

[3] A. H. Oktaviani and M. Nelisa, "Pembuatan Pangkalan Data Arsip Menggunakan Microsoft Access Pada Seksi Pemberitaan Di LPP RRI Bukittinggi," *Ilmu Inf. Perpust. dan Kearsipan*, vol. 4, no. 1, pp. 1–8, 2015.

[4] P. Simanjuntak, C. Sugianto, and I. Asyarie, "ANALISIS PENGGUNAAN JARINGAN LAN PADA PT USDA SEROJA KOTA BATAM," *Comput. Based Inf. Syst. J.*, vol. 6, no. 1, p. 23, 2018.

[5] E. Prasetyo, "Perancangan VLAN (Virtual Local Area Network) untuk Manajemen IP Address pada Politeknik Sekayu," *J. TIPS J. Teknol. Inf. dan Komput. Politek. Sekayu*, vol. 1, no. 1, pp. 10–23, 2014.

[6] E. J. Jackson *et al.*, "Softflow: A middlebox architecture for open vswitch," in *2016 ${$USENIX$}$ Annual Technical Conference (${$USENIX$}${ATC}$ 16)*, 2016, pp. 15–28.