Perancangan Sistem Keamanan Jaringan TCP/IP Berbasis *Virtual* LAN dan *Access Control List*

Muhammad Ariq Istiqlal*, Linna Oktaviana Sari, Irsan Taufik Ali****
*Teknik Elektro Universitas Riau **Jurusan Teknik Elektro Universitas Riau
Kampus Binawidya Km 12,5 Simpang Baru Panam, Pekanbaru 28293
Jurusan Teknik Elektro Universitas Riau
Email: ariq.iq@gmail.com

ABSTRACT

Internet network that has been developed at this time is a network architecture based on TCP / IP. Each layer of the TCP / IP on the Internet provides an opportunity for a security hole. One of many ways of closing the security hole is to set the Access Control List (ACL) on the Internetwork layer. ACL is used to permit or deny the package from the host towards a specific purpose. ACL consists of rules and conditions that determine and define the process network traffic at the router whether the package will be passed or not. Methods ACL is created on an existing VLAN network, thus increasing the security of the network. Results of this research is with implement an ACL can block internet sites that can not be accessed by the user in a network. Then by applying ACL on VLAN, the access rights of a user on the network can be segmented, thus reducing the chance of spreading "a network virus" which can make a network busy.

Kata kunci : *TCP/IP Security, Virtual LAN, DHCP Server, Access Control List*

I. PENDAHULUAN

Penggunaan jaringan internet disegala bidang terus berkembang sangat pesat. Internet telah menjadi bagian yang tidak bisa dipisahkan dalam kegiatan masyarakat. Melalui internet banyak informasi yang dipertukarkan dengan cepat. Jaringan internet yang telah berkembang saat ini, adalah jaringan yang berdasarkan arsitektur protokol TCP/IP. Jaringan internet berbasis TCP/IP ini dibagi dalam 4 lapisan yang memiliki fungsi-fungsi tertentu sesuai dengan protokol yang bekerja pada lapisan tersebut, lapisan tersebut yaitu lapisan *Aplication, Transport, Internetwork, dan Network Access*. Setiap lapisan TCP/IP pada jaringan internet memberikan peluang adanya lubang keamanan (*security hole*).

Supaya dapat mengamankan dan mencegah jaringan TCP/IP dari berbagai ancaman (*threats*) diperlukan beberapa solusi perancangan suatu sistem keamanan atau *multiple layers of security* yang dapat bekerja pada lapisan-lapisan jaringan TCP/IP. Pada *Network Access Layer* dapat dirancang sistem keamanan dengan melakukan segmentasi *Virtual* LAN (VLAN).

Penelitian mengenai ACL sudah banyak dilakukan oleh berbagai peneliti dari berbagai kalangan dengan berbagai keperluan. Begitu pula dengan penelitian mengenai perancangan keamanan jaringan menggunakan ACL. Hikmaturokhman, dkk (2010) dalam tesisnya menerapkan *Extended Access List* pada jaringan akan membantu menentukan alamat sumber dan tujuan serta *protocol* dan nomer *port* yang mengidentifikasikan aplikasi. Sedangkan Dinata (2013) meningkatkan dan mengoptimalkan kinerja jaringan menggunakan *access list*. Dengan memblokir *traffic* paket data dari sebuah situs tertentu yang tidak bermanfaat bahkan mengandung unsur asusila dan pornografi, serta memblokir *traffic* paket data virus yang menyebar secara terus menerus (*broadcast*) dalam sebuah jaringan. Kemudian Simamora, dkk (2011) membuktikan proses *filtering* dan selektivitas permintaan panggilan/sambungan dalam

keamanan akses jaringan ke internet pada infrastruktur sebuah LAN (Local Area Network) dengan cara terpusat, dengan menyediakan metode filtering berbasiskan Access Control List, serta model jaringan intranet berbasis Access Control List yang telah dapat menyaring identifikasi perangkat berdasar IP-Address dan MAC-Address serta selektivitas permintaan layanan data berdasarkan URL yang dikunjungi. Riswanto (2011) mengkaji bagaimana penerapan konfigurasi kontrol keamanan jaringan komputer menggunakan metode *Access Control List* (ACLs) dengan program simulasi Packet Tracer 5.1.

Penelitian ini merujuk pada penelitian yang dilakukan oleh Yuniar (2014) yaitu dengan penerapan Access Control List (ACL) dapat menentukan paket data mana yang ditolak dan diteruskan dalam jaringan VLAN sehingga jalur lalu lintas data akan lancar. Jadi, pada penelitian ini merancang ACL pada jaringan VLAN yang sudah ada sehingga dapat meningkatkan keamanan pada jaringan tersebut.

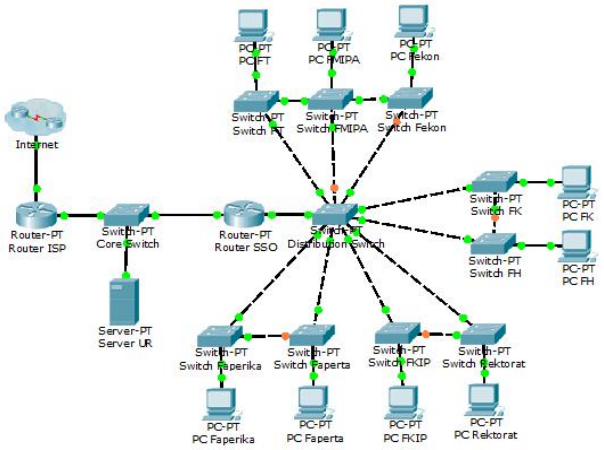
II. METODE PENELITIAN

2.1 Perancangan Jaringan

Adapun hal-hal yang perlu dirancang pada jaringan di kampus Universitas Riau adalah:

1. Menerapkan VTP (VLAN *Trunking Protocol*) pada VLAN yang sudah ada, sehingga mempermudah administrator memperbaharui VLAN apabila terdapat *update* VLAN sewaktu-waktu.
2. Menambahkan jalur redundan pada perancangan, sehingga menerapkan *Rapid Spanning Tree Protocol* yang berfungsi untuk mempercepat perpindahan jalur akses ke jalur lain apabila jalur utama terputus.
3. Menerapkan ACL (*Access Control List*) pada VLAN yang sudah ada, guna membatasi hak akses masing-masing VLAN ataupun user.
4. Menerapkan ACL (*Access Control List*) pada *firewall*, guna membatasi akses dari luar jaringan lokal (internet) untuk mengacaukan jaringan lokal.

Untuk merancang keamanan jaringan, perlu diketahui kondisi jaringan yang akan di atur yaitu topologi jaringan UR.



Gambar 1. Rancangan Topologi UR

Gambar diatas merupakan hasil rancangan topologi yang telah penulis rancang pada jaringan komputer di Universitas Riau, dimana penulis menambahkan jalur redundan pada fakultas dan rektorat yang berdekatan dan menerapkan topologi star-bus agar apabila jalur utama terputus maka ada jalur alternatif yang bisa di pakai. Disini penulis menggunakan aplikasi simulator yaitu packet tracer 5.3.3.

Pada rancangan topologi diatas, penulis sedikit meng-upgrade dan membuat asumsi pada topologi jaringan UR yaitu:

1. Pada *subinterface* fakultas dan rektorat yang berdekatan diberikan jalur redundan (FT, FMIPA dan FEKON; Rektorat dan FKIP; Faperika dan Faperta; FK dan FH).
2. Diasumsikan tiap *subinterface* fakultas dan rektorat hanya terdapat satu user untuk pengujian.
3. Diasumsikan tiap *subinterface* fakultas dan rektorat hanya terdapat satu VLAN untuk pengujian.
4. Diasumsikan terdapat server Situs X pada Internet dengan IP *Address* (192.168.1.5).
5. Konfigurasi SSO (*Single Sign On*) pada Router SSO tidak dilakukan, namun tetap melakukan konfigurasi IP DHCP Pool.

Selain pada asumsi dan pembaharuan diatas, penulis tetap mempertahankan topologi jaringan UR yang ada.

Tabel 1 Pemetaan IP *Address* dan VLAN

Switch	VLAN	*Range IP Address*	*Gateway*	*Network*
Rektorat	6	172.16.6.1 s.d. 172.16.6.254	172.16.6.1	172.16.6.0/24
FT	9	172.16.9.1 s.d. 172.16.9.254	172.16.9.1	172.16.9.0/24
FMIPA	10	172.16.10.1 s.d. 172.16.10.254	172.16.10.1	172.16.10.0/24
Fekon	11	172.16.11.1 s.d. 172.16.11.254	172.16.11.1	172.16.11.0/24
Faperika	12	172.16.12.1 s.d. 172.16.12.254	172.16.12.1	172.16.12.0/24
Faperta	13	172.16.13.1 s.d. 172.16.13.254	172.16.13.1	172.16.13.0/24
FKIP	14	172.16.14.1 s.d. 172.16.14.254	172.16.14.1	172.16.14.0/24
FH	17	172.16.17.1 s.d. 172.16.17.254	172.16.17.1	172.16.17.0/24
FK	18	172.16.18.1 s.d. 172.16.18.254	172.16.18.1	172.16.18.0/24

Dibawah ini merupakan tabel hak akses yang akan digunakan dan dikonfigurasi pada *router cisco* untuk masing-masing VLAN.

Tabel 2 Hak akses masing-masing VLAN

VLAN	*Ping* ke *server* UR	*Akses* ke Situs X	*Telnet* ke Router	Akses ke VLAN lain
Rektorat	V	X	V	V
FT	X	X	X	X
FMIPA	X	X	X	X
Fekon	X	X	X	X
Faperika	X	X	X	X
Faperta	X	X	X	X
FKIP	X	X	X	X
FH	X	X	X	X
FK	X	X	X	X

Keterangan: (V) Diizinkan/*Permit*
(X) Tidak diizinkan/*Deny*

1. Untuk mengurangi kemungkinan terjadinya serangan *traffic flooding* yang dapat menghambat kinerja pada server maka user di semua fakultas tidak diizinkan ping ke server UR namun masih dapat mengakses server UR.
2. Untuk membatasi user dalam mengakses situs-situs tertentu di internet, maka user di semua fakultas dan rektorat tidak diizinkan akses ke situs X.
3. Untuk meningkatkan keamanan Router agar tidak diakses sembarangan oleh user maka user di semua fakultas tidak diizinkan telnet ke Router kecuali user di Rektorat.
4. User di semua Fakultas tidak diizinkan untuk saling berkomunikasi kecuali komunikasi user di Rektorat karena user di Rektorat digunakan oleh dosen dan pihak-pihak yang berkepentingan, kemudian untuk mengurangi kemungkinan penyebaran virus melaui jaringan.

2.2 Konfigurasi Jaringan

2.2.1 Konfigurasi VLAN Pada *Distribution Switch*

Distribution Switch merupakan switch yang menghubungkan Router SSO dengan switch-switch pada fakultas dan rektorat di jaringan UR. Switch ini merupakan pusat dari seluruh jaringan di UR, apabila switch ini mati maka seluruh user pada jaringan lokal tidak dapat mengakses server UR maupun jaringan internet. Konfigurasi pada *Distribution Switch* adalah VTP *server*, VLAN ID, *Trunk Link* dan *Rapid Spanning Tree Protocol*.

```
Dis_Switch>en
Dis_Switch#conf t
Dis_Switch(config)#vtp mode server
```

```
Device mode already VTP SERVER.
Dis_Switch(config)#vtp version 2
Dis_Switch(config)#vtp domain UR
Changing VTP domain name from NULL to UR
Dis_Switch(config)#vtp password ur12345
Setting device VLAN database password to
ur12345
Dis_Switch(config)#vlan 6
Dis_Switch(config-vlan)#name Rektorat
Dis_Switch(config-vlan)#vlan 9
Dis_Switch(config-vlan)#name FT
Dis_Switch(config-vlan)#vlan 10
Dis_Switch(config-vlan)#name FMIPA
Dis_Switch(config-vlan)#vlan 11
Dis_Switch(config-vlan)#name Fekon
Dis_Switch(config-vlan)#vlan 12
Dis_Switch(config-vlan)#name Faperika
Dis_Switch(config-vlan)#vlan 13
Dis_Switch(config-vlan)#name Faperta
Dis_Switch(config-vlan)#vlan 14
Dis_Switch(config-vlan)#name FKIP
Dis_Switch(config-vlan)#vlan 17
Dis_Switch(config-vlan)#name FH
Dis_Switch(config-vlan)#vlan 18
Dis_Switch(config-vlan)#name FK
Dis_Switch(config-vlan)#exit
Dis_Switch(config)#int range fa1/1, fa2/1,
fa3/1, fa4/1, fa5/1, fa6/1, fa7/1, fa8/1,
fa9/1
Dis_Switch(config-if-range)#switchport mode
trunk
Dis_Switch(config-if-range)#exit
Dis_Switch(config)#spanning-tree mode rapid-
pvst
Dis_Switch(config)#spanning-tree vlan 1,6,9-
14,17-18 priority 4096
Dis_Switch(config)#end
Dis_Switch#
%SYS-5-CONFIG_I: Configured from console by
console

Dis_Switch#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Dis_Switch#
```

2.2.2 Konfigurasi VLAN Pada *Access Switch*

Access Switch pada jaringan UR terdiri dari 9 switch yaitu switch Rektorat, switch FT, switch FMIPA, switch Fekon, switch Faperika, switch Faperta, switch FKIP, switch FH dan switch FK. Adapun konfigurasi pada tiap *access switch* berupa konfigurasi VTP *client*, *Access Link* dan *Rapid Spanning Tree Protocol.*

1. Konfigurasi VLAN pada switch Rektorat

```
Switch_Rek(config)>en
Switch_Rek(config)#conf t
Switch_Rek(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch_Rek(config)#vtp domain UR
Domain name already set to UR.
Switch_Rek(config)#vtp password ur12345
Setting device VLAN database password to
ur12345
Switch_Rek(config)#interface range fa0/1,
fa1/1
Switch_Rek(config-if-range)#switchport
mode trunk
Switch_Rek(config-if-range)#exit
Switch_Rek(config)#interface fa2/1
Switch_Rek(config-if)#switchport mode
access
Switch_Rek(config-if)#switchport access
vlan 6
Switch_Rek(config-if)#exit
Switch_Rek(config)#spanning-tree mode
rapid-pvst
Switch_Rek(config)#end
Switch_Rek#
%SYS-5-CONFIG_I: Configured from console
by console

Switch_Rek#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch_Rek#
```

2. Konfigurasi VLAN pada switch FT

```
Switch_FT(config)>en
Switch_FT(config)#conf t
Switch_FT(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch_FT(config)#vtp domain UR
Changing VTP domain name from NULL to UR
Switch_FT(config)#vtp password ur12345
Setting device VLAN database password to
ur12345
Switch_FT(config)#interface range fa0/1,
fa1/1
Switch_FT(config-if-range)#switchport mode
trunk
Switch_FT(config-if-range)#exit
Switch_FT(config)#interface fa3/1
Switch_FT(config-if)#switchport mode
access
Switch_FT(config-if)#switchport access
vlan 9
Switch_FT(config-if)#exit
Switch_FT(config)#spanning-tree mode
rapid-pvst
Switch_FT(config)#end
Switch_FT#
%SYS-5-CONFIG_I: Configured from console
by console

Switch_FT#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch_FT#
```

3. Konfigurasi VLAN pada switch FMIPA

```
Switch_FMIPA(config)>en
Switch_FMIPA(config)#conf t
Switch_FMIPA(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch_FMIPA(config)#vtp domain UR
Domain name already set to UR.
Switch_FMIPA(config)#vtp password ur12345
Setting device VLAN database password to
ur12345
Switch_FMIPA(config)#interface range
fa0/1, fa1/1, fa2/1
Switch_FMIPA(config-if-range)#switchport
mode trunk
```

```
Switch_FMIPA(config-if-range)#exit
Switch_FMIPA(config-if)#interface fa3/1
Switch_FMIPA(config-if)#switchport mode
access
Switch_FMIPA(config-if)#switchport access
vlan 10
Switch_FMIPA(config-if)#exit
Switch_FMIPA(config)#spanning-tree mode
rapid-pvst
Switch_FMIPA(config)#end
Switch_FMIPA#
%SYS-5-CONFIG_I: Configured from console
by console

Switch_FMIPA#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch_FMIPA#
```

4. Konfigurasi VLAN pada switch Fekon

```
Switch_Fekon>en
Switch_Fekon#conf t
Switch_Fekon(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch_Fekon(config)#vtp domain UR
Domain name already set to UR.
Switch_Fekon(config)#vtp password ur12345
Setting device VLAN database password to
ur12345
Switch_Fekon(config)#interface range
fa0/1, fa1/1
Switch_Fekon(config-if-range)#switchport
mode trunk
Switch_Fekon(config-if-range)#exit
Switch_Fekon(config)#interface fa3/1
Switch_Fekon(config-if)#switchport mode
access
Switch_Fekon(config-if)#switchport access
vlan 11
Switch_Fekon(config-if)#exit
Switch_Fekon(config)#spanning-tree mode
rapid-pvst
Switch_Fekon(config)#end
Switch_Fekon#
%SYS-5-CONFIG_I: Configured from console
by console

Switch_Fekon#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch_Fekon#
```

5. Konfigurasi VLAN pada switch Faperika

```
Switch_Faperika>en
Switch_Faperika#conf t
Switch_Faperika(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch_Faperika(config)#vtp domain UR
Changing VTP domain name from NULL to UR
Switch_Faperika(config)#vtp password
ur12345
Setting device VLAN database password to
ur12345
Switch_Faperika(config)#interface range
fa0/1, fa1/1
Switch_Faperika(config-if-
range)#switchport mode trunk
Switch_Faperika(config-if-range)#exit
Switch_Faperika(config)#interface fa2/1
Switch_Faperika(config-if)#switchport
access vlan 12
Switch_Faperika(config-if)#exit
Switch_Faperika(config)#spanning-tree mode
rapid-pvst
Switch_Faperika(config)#end
Switch_Faperika#
%SYS-5-CONFIG_I: Configured from console
by console

Switch_Faperika#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch_Faperika#
```

6. Konfigurasi VLAN pada switch Faperta

```
Switch_Faperta>en
Switch_Faperta#conf t
Switch_Faperta(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch_Faperta(config)#vtp domain UR
Domain name already set to UR.
Switch_Faperta(config)#vtp password
ur12345
Setting device VLAN database password to
ur12345
Switch_Faperta(config)#interface range
fa0/1, fa1/1
Switch_Faperta(config-if-range)#switchport
mode trunk
Switch_Faperta(config-if-range)#exit
Switch_Faperta(config)#interface fa2/1
Switch_Faperta(config-if)#switchport mode
access
Switch_Faperta(config-if)#switchport
access vlan 13
Switch_Faperta(config-if)#exit
Switch_Faperta(config)#spanning-tree mode
rapid-pvst
Switch_Faperta(config)#end
Switch_Faperta#
%SYS-5-CONFIG_I: Configured from console
by console

Switch_Faperta#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch_Faperta#
```

7. Konfigurasi VLAN pada switch FKIP

```
Switch_FKIP>en
Switch_FKIP#conf t
Switch_FKIP(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch_FKIP(config)#vtp domain UR
Domain name already set to UR.
Switch_FKIP(config)#vtp password ur12345
Setting device VLAN database password to
ur12345
Switch_FKIP(config)#interface range fa0/1,
fa1/1
Switch_FKIP(config-if-range)#switchport
mode trunk
Switch_FKIP(config-if-range)#exit
Switch_FKIP(config)#interface fa2/1
Switch_FKIP(config-if)#switchport mode
access
Switch_FKIP(config-if)#switchport access
vlan 14
Switch_FKIP(config-if)#exit
```

```
Switch_FKIP(config)#spanning-tree mode
rapid-pvst
Switch_FKIP(config)#end
Switch_FKIP#
%SYS-5-CONFIG_I: Configured from console
by console

Switch_FKIP#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch_FKIP#
```

8. Konfigurasi VLAN pada switch FH

```
Switch_FH>en
Switch_FH#conf t
Switch_FH(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch_FH(config)#vtp domain UR
Domain name already set to UR.
Switch_FH(config)#vtp password ur12345
Setting device VLAN database password to
ur12345
Switch_FH(config)#interface range fa0/1,
fa1/1
Switch_FH(config-if-range)#switchport mode
trunk
Switch_FH(config-if-range)#exit
Switch_FH(config)#interface fa2/1
Switch_FH(config-if)#switchport mode
access
Switch_FH(config-if)#switchport access
vlan 17
Switch_FH(config-if)#exit
Switch_FH(config)#spanning-tree mode
rapid-pvst
Switch_FH(config)#end
Switch_FH#
%SYS-5-CONFIG_I: Configured from console
by console

Switch_FH#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch_FH#
```

9. Konfigurasi VLAN pada switch FK

```
Switch_FK>en
Switch_FK#conf t
Switch_FK(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch_FK(config)#vtp domain UR
Domain name already set to UR.
Switch_FK(config)#vtp password ur12345
Setting device VLAN database password to
ur12345
Switch_FK(config)#interface range fa0/1,
fa1/1
Switch_FK(config-if-range)#switchport mode
trunk
Switch_FK(config-if-range)#exit
Switch_FK(config)#interface fa2/1
Switch_FK(config-if)#switchport mode
access
Switch_FK(config-if)#switchport access
vlan 18
Switch_FK(config-if)#exit
Switch_FK(config)#spanning-tree mode
rapid-pvst
Switch_FK(config)#end
Switch_FK#
%SYS-5-CONFIG_I: Configured from console
by console

Switch_FK#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Switch_FK#
```

2.2.3 Konfigurasi DHCP *Pool* dan *Inter*-VLAN *Routing* pada Router SSO

Router SSO dikonfigurasi untuk dapat memperikan IP *Address* secara DHCP kepada *client.* Kemudian *Inter*-VLAN *Routing* dikonfigurasi agar antar VLAN dapat saling terhubung.

```
Router_SSO>en
Router_SSO#conf t
Router_SSO(config)#int fa1/0.6
Router_SSO(config-subif)#encapsulation
dot1Q 6
Router_SSO(config-subif)#ip address
172.16.6.1 255.255.255.0
Router_SSO(config-subif)#exit
Router_SSO(config)#int fa1/0.9
Router_SSO(config-subif)#encapsulation
dot1Q 9
Router_SSO(config-subif)#ip address
172.16.9.1 255.255.255.0
Router_SSO(config-subif)#exit
Router_SSO(config)#int fa1/0.10
Router_SSO(config-subif)#encapsulation
dot1Q 10
Router_SSO(config-subif)#ip address
172.16.10.1 255.255.255.0
Router_SSO(config-subif)#exit
Router_SSO(config)#int fa1/0.11
Router_SSO(config-subif)#encapsulation
dot1Q 11
Router_SSO(config-subif)#ip address
172.16.11.1 255.255.255.0
Router_SSO(config-subif)#exit
Router_SSO(config)#int fa1/0.12
Router_SSO(config-subif)#encapsulation
dot1Q 12
Router_SSO(config-subif)#ip address
172.16.12.1 255.255.255.0
Router_SSO(config-subif)#exit
Router_SSO(config)#int fa1/0.13
Router_SSO(config-subif)#encapsulation
dot1Q 13
Router_SSO(config-subif)#ip address
172.16.13.1 255.255.255.0
Router_SSO(config-subif)#exit
Router_SSO(config)#int fa1/0.14
Router_SSO(config-subif)#encapsulation
dot1Q 14
Router_SSO(config-subif)#ip address
172.16.14.1 255.255.255.0
Router_SSO(config-subif)#exit
Router_SSO(config)#int fa1/0.17
Router_SSO(config-subif)#encapsulation
dot1Q 17
Router_SSO(config-subif)#ip address
172.16.17.1 255.255.255.0
Router_SSO(config-subif)#exit
Router_SSO(config)#int fa1/0.18
Router_SSO(config-subif)#encapsulation
dot1Q 18
```

```
Router_SSO(config-subif)#ip address
172.16.18.1 255.255.255.0
Router_SSO(config-subif)#exit
Router_SSO(config)#ip dhcp pool VLAN6
Router_SSO(dhcp-config)#network 172.16.6.0
255.255.255.0
Router_SSO(dhcp-config)#default-router
172.16.6.1
Router_SSO(dhcp-config)#exit
Router_SSO(config)#ip dhcp pool VLAN9
Router_SSO(dhcp-config)#network 172.16.9.0
255.255.255.0
Router_SSO(dhcp-config)#default-router
172.16.9.1
Router_SSO(dhcp-config)#exit
Router_SSO(config)#ip dhcp pool VLAN10
Router_SSO(dhcp-config)#network
172.16.10.0 255.255.255.0
Router_SSO(dhcp-config)#default-router
172.16.10.1
Router_SSO(dhcp-config)#exit
Router_SSO(config)#ip dhcp pool VLAN11
Router_SSO(dhcp-config)#network
172.16.11.0 255.255.255.0
Router_SSO(dhcp-config)#default-router
172.16.11.1
Router_SSO(dhcp-config)#exit
Router_SSO(config)#ip dhcp pool VLAN12
Router_SSO(dhcp-config)#network
172.16.12.0 255.255.255.0
Router_SSO(dhcp-config)#default-router
172.16.12.1
Router_SSO(dhcp-config)#exit
Router_SSO(config)#ip dhcp pool VLAN13
Router_SSO(dhcp-config)#network
172.16.13.0 255.255.255.0
Router_SSO(dhcp-config)#default-router
172.16.13.1
Router_SSO(dhcp-config)#exit
Router_SSO(config)#ip dhcp pool VLAN14
Router_SSO(dhcp-config)#network
172.16.14.0 255.255.255.0
Router_SSO(dhcp-config)#default-router
172.16.14.1
Router_SSO(dhcp-config)#exit
Router_SSO(config)#ip dhcp pool VLAN17
Router_SSO(dhcp-config)#network
172.16.17.0 255.255.255.0
Router_SSO(dhcp-config)#default-router
172.16.17.1
Router_SSO(dhcp-config)#exit
Router_SSO(config)#ip dhcp pool VLAN18
Router_SSO(dhcp-config)#network
172.16.18.0 255.255.255.0
Router_SSO(dhcp-config)#default-router
172.16.18.1
Router_SSO(dhcp-config)#exit
Router_SSO(config)#
```

2.2.4 Konfigurasi *Routing* Pada Router

Pada jaringan Universitas Riau memiliki dua router yaitu router SSO dan router ISP. Pertama adalah router SSO yang menghubungkan server UR dengan jaringan lokal UR, kemudian yang kedua adalah router ISP yang menghubungkan seluruh jaringan UR baik itu jaringan LAN dan server UR dengan jaringan luar (internet). Konfigurasi *routing* pada router tersebut adalah sebagai berikut:

1. Pada Router SSO

```
Router_SSO>en
Router_SSO#conf t
Router_SSO(config)#ip route 0.0.0.0
0.0.0.0 103.10.169.1
Router_SSO(config)#
```

2. Pada Router ISP

```
Router_ISP>en
Router_ISP#conf t
Router_ISP(config)#ip route 172.16.6.0
255.255.255.0 103.10.169.3
Router_ISP(config)#ip route 172.16.9.0
255.255.255.0 103.10.169.3
Router_ISP(config)#ip route 172.16.10.0
255.255.255.0 103.10.169.3
Router_ISP(config)#ip route 172.16.11.0
255.255.255.0 103.10.169.3
Router_ISP(config)#ip route 172.16.12.0
255.255.255.0 103.10.169.3
Router_ISP(config)#ip route 172.16.13.0
255.255.255.0 103.10.169.3
Router_ISP(config)#ip route 172.16.14.0
255.255.255.0 103.10.169.3
Router_ISP(config)#ip route 172.16.17.0
255.255.255.0 103.10.169.3
Router_ISP(config)#ip route 172.16.18.0
255.255.255.0 103.10.169.3
Router_ISP(config)#
```

2.2.5 Konfigurasi ACL pada Router SSO

Pada konfigurasi ACL di router SSO, penulis menggunakan *standard* ACL dan juga *extended* ACL dimana ACL nomor 10 untuk interface telnet, nomor 20 dan 110 untuk subinterface di semua fakultas, dan 100 untuk subinterface ruangan server.

1. Konfigurasi ACL pada *Telnet* di Router SSO

   ACL pada *telnet* ini hanya mengizinkan user pada Rektorat untuk mengakses telnet router sedangkan user di semua fakultas tidak diizinkan.

```
Router_SSO(config)#access-list 10 permit
172.16.6.0 0.0.0.255
Router_SSO(config)#access-list 10 deny any
Router_SSO(config)#line vty 0 4
Router_SSO(config-line)#access-class 10 in
Router_SSO(config-line)#exit
Router_SSO(config)#username ur password
ur1234
Router_SSO(config)#enable secret ur12345
Router_SSO(config)#line vty 0 4
Router_SSO(config-line)#login local
Router_SSO(config-line)#exit
```

2. Konfigurasi ACL pada *subinterface* antar VLAN

ACL disini membatasi akses antar VLAN pada semua user di fakultas kecuali pada user di Rektorat.

```
Router_SSO(config)#access-list 20 permit
172.16.6.0 0.0.0.255
Router_SSO(config)#access-list 20 deny
172.16.0.0 0.0.255.255
Router_SSO(config)#access-list 20 permit
any
Router_SSO(config)#interface range
fa1/0.9-fa1/0.18
Router_SSO(config-if-range)#ip access-
group 20 out
Router_SSO(config-if-range)#exit
Router_SSO(config)#
```

3. Konfigurasi ACL pada *subinterface* untuk Server UR dan Situs X
   Pada perintah dibawah ini menggunakan *extended* ACL yang mana hanya mengizinkan user di Rektorat yang dapat Ping ke Server UR. Namun sesuai perintah ACL dibawah yang di *deny* adalah ICMP (ping), user di semua Fakultas masih dapat akses situs Universitas Riau ke Server UR. Kemudian pada baris ketiga dikonfigurasi seluruh user di Fakultas dan Rektorat tidak dapat mengakses situs X.

```
Router_SSO(config)#access-list 102 permit
icmp 172.16.6.0 0.0.0.255 103.10.169.5
0.0.0.0
Router_SSO(config)#access-list 102 deny
icmp 172.16.0.0 0.0.255.255 103.10.169.5
0.0.0.0
Router_SSO(config)#access-list 102 deny
tcp any 192.168.1.5 0.0.0.0 eq www
Router_SSO(config)#access-list 102 permit
ip any any
Router_SSO(config)#interface fa0/0
Router_SSO(config-if)#ip acc 102 out
```

2.3 Pengujian Hasil Rancangan

Disini penulis melakukan pengujian dari rancangan keamanan jaringan VLAN dan ACL yang telah dilakukan, yaitu dengan cara:

1. *Ping* ke server UR
2. Mengakses situs UR
3. Akses ke masing-masing Fakultas dan Rektorat
4. Mengakses situs X
5. *Telnet* ke router SSO

III. KESIMPULAN DAN SARAN

4.1 Kesimpulan

1. Perancangan model jaringan berhasil dilakukan berdasarkan pada jaringan existing tanpa merubah topologi jaringan, sehingga rancangan dapat langsung diimplementasikan.
2. VLAN pada jaringan UR dapat mensegmentasi suatu jaringan yang fungsinya apabila terjadi kesalahan pada suatu titik (node), maka akan mudah mengetahui letak kesalahan tersebut tanpa mengganggu segmen lain.
3. Dengan menerapkan ACL pada VLAN, maka hak akses user pada jaringan dapat tersegmentasi, sehingga mengurangi kemungkinan penyebaran virus jaringan yang dapat membuat jaringan sibuk.
4. ACL berhasil digunakan untuk mengatur hak akses masing-masing VLAN. Selain itu, ACL berhasil digunakan sebagai firewall sehingga tidak ada akses dari luar yang dapat masuk ke jaringan.

4.2 Saran

Sebelum menerapkan perancangan ACL berbasis Web Address, diperlukan data lengkap IP Address suatu situs untuk diterapkan dalam ACL.

Untuk mendapatkan performansi keamanan jaringan TCP/IP yang paling aman, dibutuhkan konfigurasi keamanan pada layer-layer lain. Hal ini dapat dijadikan judul penelitian selanjutnya untuk mendapatkan sistem keamanan yang terbaik.

DAFTAR PUSTAKA

Cisco, 2014. *Cisco Packet Tracer.* https://www.netacad.com/web/about-us/cisco-packet-tracer, diakses pada 26 Juni 2015, Pkl. 20.05 WIB.

Dinata, S.K. (2013). *Monitoring* aktfitas jarngan dan simulasi *Access Control List* pada STMIK PalComTech berbasis Cisco Router. Jurnal Teknologi dan Informatika, 3, 27-53.

Hikmaturokhman, A., dkk. 2010, Analisis perancangan dan implementasi *firewall* dan *traffic filtering* menggunakan Cisco Router. Tesis Pasca Sarjana, Teknik

Informatika, IT Telkom Bandung, Indonesia.
Riswanto. 2011, Simulasi Konfigurasi Kontrol Keamanan Jaringan Komputer Berbasis *Access List* Menggunakan Cisco Router. Tesis Pasca Sarjana, Teknik Elektro, Universitas Gunadarma, Indonesia.
Roestam, Rusdianto. 2011, Analisis dan pengembangan jaringan pada PT. Natrindo Telepon Seluler. Skripsi Sarjana, Teknik Informatika, Binus University, Indonesia.
Simamora, dkk. (2011). Metode *Access Control List* sebagai Solusi Alternatif Seleksi Permintaan Layanan Data pada Koneksi Internet. Jurnal Teknologi dan Informasi Politeknik Telkom, 1, 15-19.
Sutarno, dkk. 2013, Analisa dan Perancangan sistem keamanan jaringan menggunakan teknik ACL (Access Control List). Skripsi Sarjana, Teknik Informatika, Universitas Muhammadiyah Surakarta, Indonesia.
Sutomo, E. (2010). Jaringan Komputer & Pengamanannya. Surabaya: STIKom Surabaya.
Todd, L. (2005). CCNA Cisco Certified Network Associate Study Guide. Jakarta, Elex Media Komputindo.
Yuniar, A. 2014, Penerapan Access Control List (ACL) pada Jaringan VLAN di PT Goodyear Indonesia Tbk. Tugas Akhir, Teknik Komputer, Institut Pertanian Bogor, Indonesia.