DAFTAR PUSTAKA

Arif, Teuku Yuniar, dkk. (2007). Studi Protokol Autentikasi pada Layanan Internet Service Provider (ISP). Jurnal Rekayasa Elektrika Vol. 6 (1).

Anonim, (2006). Cisco IOS Security Configuration http://www.cisco.com/en/US/tech/tk59/technologiestechnote09186a0080094e99 (29 Mei 2015)

Akhmad, F. (2015). *Implementasi (AAA) Authentication Authorization dan Accounting Pada Jaringan Wireless InterVLAN.* Politeknik Negeri Jember: Teknik Komputer.

Handika, R. (2014). *Rancang Bangun Keamanan dan Sistem Remote Access Berbasis Authentication RADIUS Server Pada Jaringan InterVLAN.* Politeknik Negeri Jember: Teknik Komputer.

Pakpahan, M. (2011). Perbandingan TACACS+ Server Dan RADIUS Server.

Prasetyawan, A. (2011). Metode Autorisasi Dan Accounting Pada TACACS+ Server.

Rahaman, R. (2013). *Mahir Administrasi Server Dan Router dengan Linux Ubuntu 12.04 LTS.* Bekasi .

Sofana, I. (2012). *CISCO CCNA dan Jaringan Komputer.* Bandung: Informatika.

Sofana, I. (2012). *CISCO CCNP dan Jaringan Komputer.* Bandung: Informatika.

Sofana, I. (2013). *Membangun Jaringan Komputer.* Bandung: Informatika.

LAMPIRAN

Lampiran 1. File *souce code tac_plus.conf*

```
# Created by Henry-Nicolas Tourneur(henry.nicolas@tourneur.be)
# See man(5) tac_plus.conf for more details
# Define where to log accounting data, this is the default.
accounting file = /var/log/tac_plus.acct
# This is the key that clients have to use to access Tacacs+
key = testing123
# Use /etc/passwd file to do authentication
#default authentication = file /etc/passwd
# You can use feature like per host key with different enable
passwords
#host = 127.0.0.1 {
#        key = test
#        type = cisco
#        enable = <des|cleartext> enablepass
#        prompt = "Welcome XXX ISP Access Router \n\nUsername:"
#}
# We also can define local users and specify a file where data is
stored.
# That file may be filled using tac_pwd
#user = test1 {
#    name = "Test User"
#    member = staff
#    login = file /etc/tacacs/tacacs_passwords
#}
user = fitroh {
   member = network_admin
   login = cleartext @jk!23
   enable = cleartext tkk2013
}

user = faruq {
    login = cleartext p0l!j3
    enable = cleartext tkk2013
    member = sys_admin
}
user = all {
        login = cleartext ajk
        enable = cleartext cisco
        member = sys_admin
}

# We can also specify rules valid per group of users.
#group = group1 {
```

```
#       cmd = conf {
#               deny
#       }
#}
 group = network_admin {
      default service = permit
      login = file /etc/passwd
      enable = file /etc/passwd
      service = exec {
      priv-level = 15
      }
}
group = sys_admin {
default service = deny
service = exec {
priv-lvl = 0
}
cmd = enable {
permit .*
}
cmd = show {
permit .*
}
cmd = exit {
permit .*
}
cmd = configure {
permit .*
}
cmd = interface {
permit Ethernet.*
permit FastEthernet.*
permit GigabitEthernet.*
}
cmd = switchport {
permit "access vlan.*"
permit "trunk encapsulation.*"
permit "mode.*"
permit "trunk allowed vlan.*"
}
cmd = description {
permit .*
}
cmd = no {
permit shutdown
}
}
# Another example : forbid configure command for some hosts
# for a define range of clients
```

```
#group = group1 {
#       login = PAM
#       service = ppp
#       protocol = ip {
#               addr = 10.10.0.0/24
#       }
#       cmd = conf {
#               deny .*
#       }
#}
user = DEFAULT {
        login = PAM
        service = ppp protocol = ip {}
}
# Much more features are availables, like ACL, more service
compatibilities,
# commands authorization, scripting authorization.
# See the man page for those features.
```