การทำ Wireless LAN Controller ด้วย Chillispot แบบ web login + freeradius + mysql + transparent proxy

Written by วิบูลย์

Saturday, 01 December 2007

Wireless LAN Controller Chillispot web login + freeradius + mysql + transparent proxy

เขียนโดย วิบูลย์ วราสิทธิชัย นักวิชาการคอมพิวเตอร์ ศูนย์คอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์ (wiboon.w (at) psu.ac.th)

เอกสารอ้างอิง
แหล่งข้อมูลต้นฉบับ chillispot คือ http://www.chillispot.info
ขอขอบคุณ คุณวิภัทร ศรุติพรหม ให้ความรู้ linux server ที่เวบไซต์ http://www.opensource.psu.ac.th เมนู ทำง่าย-ใช้เป็น
ขอขอบคุณ คุณ ลน ร.ร.จุฬาภรณราชวิทยาลัย ปทุมธานี ให้ตัวอย่าง radius attribute

ประวัติการปรับปรุง

เขียนครั้งแรก 16-01-2550 โดย: วิบูลย์ วราสิทธิชัย
เฉพาะเนื้อหาของตอนที่ 1
ครั้งที่ 1 1-12-2550 โดย: วิบูลย์ วราสิทธิชัย
รวบรวมจากบทความหลาย ๆ เรื่องใน chillispot wifi ที่เขียนไว้นำมารวมใหม่
ครั้งที่ 2 14-12-2550 โดย: วิบูลย์ วราสิทธิชัย
เพิ่มคำอธิบายเรื่อง cache_peer ในบทที่ 3 เพราะบางคนเข้าใจผิด คิดว่าต้องทำตาม
ครั้งที่ 3 8-2-2551 โดย: วิบูลย์ วราสิทธิชัย
แก้ไขเลขเวอร์ชั่นของ freeradius ในเอกสาร
ครั้งที่ 4 13-2-2551 โดย วิบูลย์ วราสิทธิชัย
แก้ไข /etc/firewall.iptables ป้องกันการแฮคเซ็ตพร็อกซี่ตรง ๆ
ครั้งที่ 5 24-9-2551 โดย วิบูลย์ วราสิทธิชัย
แก้ไขเอกสาร ให้ใส่เครื่องหมาย # หน้าคำว่า files ใน section authorize {} ด้วย

เอกสารนี้ใช้เพื่อ

เป็นคำแนะนำในการติดตั้งและปรับแต่ง Linux server ให้เป็น Wireless LAN Access Point Controller ด้วยโปรแกรม chillispot
เลือกวิธีการ authentication แบบ web login โดยตรวจสอบ username ที่ freeradius ที่ใช้ mysql เป็น database
รวมทั้งติดตั้ง proxy server ด้วยโปรแกรม squid แบบ transparent proxy เพื่อให้เครื่องไคลเอนต์ (โน้ตบุ๊ค) ที่ไม่เซ็ตค่าพร็อกซี่ก็สามารถใช้งานอินเทอร์เน็ตได้ทันทีภายหลังจากที่ตรวจสอบ username ผ่านแล้ว

เอกสารนี้แบ่งออกเป็น 3 ตอน

ตอนที่ 1

การติดตั้ง Linux server
การติดตั้งโปรแกรม Apache web server
การติดตั้งโปรแกรม Freeradius
ทดสอบ authentication โดยใช้ username/password ของ Unix
การติดตั้งโปรแกรม Chillispot แบบ Web login

ตอนที่ 2

การติดตั้งโปรแกรม Mysql
ตัวอย่าง radius attribute
Max-All-Session
Max-Daily-Session
Max-Monthly-Session
Session-Timeout
WISPr-Bandwidth-Max-Down
WISPr-Bandwidth-Max-Up
Simultaneous-Use
ทดสอบ authentication โดยใช้ username/password ของ Mysql
การติดตั้งโปรแกรม radiusContext เพื่อทำรายงานการใช้งาน Freeradius

ตอนที่ 3

การติดตั้งโปรแกรม squid
การทำ Transparent proxy ด้วย iptables
การตั้งเวลาเก็บ access.log ทุกคืน

ตอนที่ 4

รออาสาสมัครที่สามารถใช้ php + mysql เขียนโปรแกรมจัดการบัญชีผู้ใช้ chillispot ด้วย php + mysql

รูปภาพการติดตั้ง

ข้อมูลเครือข่าย
eth0 คือ แลนการ์ดใบที่ 1 ต่อกับอินเทอร์เน็ต ได้รับแจก ip จาก dhcp server ในอินเทอร์เน็ต
eth1 คือ แลนการ์ดใบที่ 2 ต่อกับแอคเซสพอยต์ ได้รับแจก ip จาก chillispot server
แอคเซสพอยต์ได้รับแจก ip จาก chillispot server
ไคลเอนต์ที่มาต่อกับแอคเซสพอยต์ได้รับแจก ip จาก chillispot server ส่งต่อโดยแอคเซสพอยต์
chillispot server 1 เครื่อง ติดตั้งโปรแกรมดังนี้
Linux fedora core 6
freeradius 1.1.* (rpm) (ทดสอบแล้ว 1.1.3 - 1.1.7)
apache 2.2.* (rpm) (ทดสอบแล้ว 2.2.3 - 2.2.6)
chillispot 1.1.0 (rpm)
[Day 1]

ตอนที่ 1

1.1 การติดตั้ง Linux server

คำแนะนำการติดตั้ง
ในขั้นตอนที่ติดตั้งจากแผ่นซีดี ให้เลือก Package selection เป็น Software Development
ในขั้นตอนที่ติดตั้งจากแผ่นซีดีครบแล้ว เมื่อรีบูตกลับมาให้ปิด SeLinux โดยเปลี่ยนจาก enforcing เป็น disabled
คำแนะนำการใช้งาน
การคอนฟิกระบบจะง่ายขึ้น ให้ใช้วิธีการ copy และ paste คำสั่งหรือข้อความจากเอกสารที่กำลังอ่านอยู่นี้
หากภายหลังการติดตั้งได้รับหน้าจอเป็น text mode ให้เปลี่ยนเป็นกราฟฟิคโหมด ด้วยคำสั่ง startx
เปิดวินโดวชื่อ terminal เพื่อใช้ในการปรับแต่งและรันคำสั่ง ดังนี้ คลิก Application, Accessories, Terminal
โปรแกรม editor ที่ใช้ในการแก้ไขค่าคือ gedit เป็น full screen editor ใช้เมาส์คลิกวางตำแหน่ง cursor ได้
จบด้วยคลิกปุ่ม Save และคลิก X เพื่อปิดโปรแกรม

1.1.1 การปรับแต่งระบบลินุกซ์

(ดัดแปลงจาก การปรับแต่งระบบลินุกซ์หลังการติดตั้ง (28-9-2550) วิภัทร ศรุติพรหม http://rd.cc.psu.ac.th/content/view/14/46/)

1. ตรวจสอบการ์ดแลนพร้อมใช้งานด้วยคำสั่ง
ifconfig -a

ผลลัพธ์

```
[root@dhcp160 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:60:97:A5:38:6F
          inet addr:192.168.2.220  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: 2001:3c8:9009:300:260:97ff:fea5:386f/64 Scope:Global
          inet6 addr: fe80::260:97ff:fea5:386f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:126 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
```

```
        RX bytes:9430 (9.2 KiB)  TX bytes:8450 (8.2 KiB)
        Interrupt:9 Base address:0x2080

eth1      Link encap:Ethernet  HWaddr 00:01:03:18:BA:59
        BROADCAST MULTICAST  MTU:1500  Metric:1
        RX packets:431699 errors:0 dropped:0 overruns:520 frame:0
        TX packets:858 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:32878596 (31.3 MiB)  TX bytes:88551 (86.4 KiB)
        Interrupt:5

lo        Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:34660 errors:0 dropped:0 overruns:0 frame:0
        TX packets:34660 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:9917351 (9.4 MiB)  TX bytes:9917351 (9.4 MiB)
```

2. หากต้องการเปลี่ยนรหัสผ่านของ root ทำด้วยคำสั่ง
passwd

ผลลัพธ์

```
[root@dhcp160 ~]# passwd
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

3. ยกเลิกการตั้งค่า update อัตโนมัติ ด้วยคำสั่งดังนี้คือ
service yum-updatesd stop
chkconfig yum-updatesd off

ผลลัพธ์

```
[root@dhcp160 ~]# service yum-updatesd stop
Stopping yum-updatesd:                                     [  OK  ]
[root@dhcp160 ~]# chkconfig yum-updatesd off
[root@dhcp160 ~]#
```

4. ตั้งเวลาให้ตรงกับสากลด้วยคำสั่ง /usr/sbin/ntpdate -u <ชื่อเซิร์ฟเวอร์>
โดยที่
pool.ntp.org เป็น ntp server ที่เป็นสากลโดยตรง
time.psu.ac.th เป็น ntp server ภายใน ม.อ.
ใช้คำสั่ง
/usr/sbin/ntpdate -u pool.ntp.org

ผลลัพธ์

```
[root@dhcp160 ~]# /usr/sbin/ntpdate -u pool.ntp.org
27 Nov 17:20:45 ntpdate[22639]: step time server 61.19.242.42 offset -130.874347 sec
```

ต้องการให้ทุกครั้งที่บูทเครื่องมีการตั้งเวลาใหม่ ให้แก้ไขแฟ้ม /etc/rc.local ใช้คำสั่ง
gedit /etc/rc.local

เพิ่มบรรทัดข้อความว่า
/usr/sbin/ntpdate -u pool.ntp.org

บันทึกและปิดหน้าต่าง gedit

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /etc/rc.local
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.
```

```
touch /var/lock/subsys/local
/usr/sbin/ntpdate -u pool.ntp.org
```

ตั้งเวลาให้ตรงกับสากลทุกวัน ให้สร้างแฟ้มข้อมูลชื่อ /etc/cron.daily/ntp.cron ใช้คำสั่ง
gedit /etc/cron.daily/ntp.cron

มีข้อมูลดังนี้
#!/bin/sh
/usr/sbin/ntpdate -u pool.ntp.org

และเปลี่ยนโหมดของแฟ้มเป็น execute ด้วยคำสั่ง
chmod +x /etc/cron.daily/ntp.cron

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /etc/cron.daily/ntp.cron
#!/bin/sh
/usr/sbin/ntpdate -u pool.ntp.org
[root@dhcp160 ~]# chmod +x /etc/cron.daily/ntp.cron
[root@dhcp160 ~]#
```

5. เกี่ยวกับ SeLinux อาจทำให้การใช้งานบางอย่างยากขึ้น ให้เปลี่ยนจาก enforcing เป็น disabled โดยแก้ไขแฟ้ม /etc/selinux/config ใช้คำสั่ง
gedit /etc/selinux/config

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /etc/selinux/config
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced. (default)
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - SELinux is fully disabled.
SELINUX=disabled
# SELINUXTYPE= type of policy in use. Possible values are:
#       targeted - Only targeted network daemons are protected.
#       strict - Full SELinux protection.
SELINUXTYPE=targeted
```

1.1.2 การ update packages linux fedora core 6 ให้ทันสมัย

(ดัดแปลงจาก การ update packages ด้วยโปรแกรม Yum สำหรับมหาวิทยาลัยสงขลานครินทร์ (01-03-2550)
วิภัทร ศรุตพรหม http://rd.cc.psu.ac.th/content/view/52/46/)

กรณีที่เครื่องอยู่ในมหาวิทยาลัยสงขลานครินทร์

แก้ไขให้ชี้ update server มาอยู่ที่ repository server ที่ตั้งอยู่ภายในมหาวิทยาลัย ด้วยวิธีการคือ
ลบข้อมูลเดิมใน cache ทิ้งก่อนด้วยคำสั่ง
rm -rf /var/cache/yum/*

สำรองต้นฉบับ yum.repos.d เก็บไว้ก่อน เผื่อใช้ในอนาคต
cp -r /etc/yum.repos.d/ /etc/yum.repos.d.save

ลบแฟ้มใน directory /etc/yum.repos.d ทิ้งทั้งหมด
เพราะต้นฉบับ yum ที่ติดตั้งมีข้อมูลระบุให้ชี้ไปที่ server ต่างประเทศ ด้วยคำสั่ง
rm -f /etc/yum.repos.d/*

แล้วสร้างแฟ้ม 3 แฟ้มขึ้นมาใหม่ โดยระบุ repository server เป็น ftp.psu.ac.th
สร้างแฟ้ม /etc/yum.repos.d/psu-fedora.repo ให้มีข้อมูลดังนี้
[base]
name=Fedora Core $releasever - $basearch - Base
baseurl=ftp://ftp.psu.ac.th/pub/yum/fedora/core/6/base
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora

สร้างแฟ้ม /etc/yum.repos.d/psu-fedora-extras.repo ให้มีข้อมูลดังนี้
[extras]

name=Fedora Extras $releasever - $basearch
baseurl=ftp://ftp.psu.ac.th/pub/yum/fedora/core/6/extras
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-extras
gpgcheck=1

สร้างแฟ้ม /etc/yum.repos.d/psu-fedora-updates.repo ให้มีข้อมูลดังนี้
[updates]
name=Fedora Updates $releasever - $basearch
baseurl=ftp://ftp.psu.ac.th/pub/yum/fedora/updates/6/i386
enabled=1
gpgcheck=0

ผลลัพธ์

```
[root@dhcp160 ~]# rm  -rf  /var/cache/yum/*
[root@dhcp160 ~]# cp -r /etc/yum.repos.d/ /etc/yum.repos.d.save
[root@dhcp160 ~]# rm -f /etc/yum.repos.d/*
```

```
[root@dhcp160 ~]# gedit /etc/yum.repos.d/psu-fedora.repo
```

```
[base]
name=Fedora Core $releasever - $basearch - Base
baseurl=ftp://ftp.psu.ac.th/pub/yum/fedora/core/6/base
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora
```

```
[root@dhcp160 ~]# gedit /etc/yum.repos.d/psu-fedora-extras.repo
```

```
[extras]
name=Fedora Extras $releasever - $basearch
baseurl=ftp://ftp.psu.ac.th/pub/yum/fedora/core/6/extras
enabled=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-extras
gpgcheck=1
```

```
[root@dhcp160 ~]# gedit /etc/yum.repos.d/psu-fedora-updates.repo
```

```
[updates]
name=Fedora Updates $releasever - $basearch
baseurl=ftp://ftp.psu.ac.th/pub/yum/fedora/updates/6/i386
enabled=1
gpgcheck=0
```

กรณีที่เครื่องตั้งอยู่นอกมหาวิทยาลัยสงขลานครินทร์

ให้เริ่มทำเฉพาะ 2 คำสั่งข้างล่างนี้เลย

สั่งปรับปรุงรายชื่อ package ให้ทันสมัยตามแหล่งข้อมูลต้นทาง
yum check-update

สั่งปรับปรุง/ติดตั้ง package ให้ทันสมัย
yum update

ผลลัพธ์

```
[root@dhcp160 ~]# yum check-update
Loading "installonlyn" plugin
Setting up repositories
extras                  100% |=========================| 1.1 kB    00:00
updates                 100% |=========================| 1.2 kB    00:00
base                    100% |=========================|  951 B    00:00
Reading repository metadata in from local files
primary.xml.gz          100% |=========================| 1.7 MB    00:00
...

[root@dhcp160 ~]# yum update
Loading "installonlyn" plugin
Setting up Update Process
Setting up repositories
Reading repository metadata in from local files

Transaction Summary
```

```
================================================================================
Install     11 Package(s)
Update     329 Package(s)
Remove       0 Package(s)

Total download size: 524 M
Is this ok [y/N]:y
... more lines...
[root@dhcp160 ~]#
```

1.2 การติดตั้งโปรแกรม Apache web server

ชื่อแฟ้มที่เกี่ยวข้องเมื่อติดตั้งเสร็จแล้ว
/var/log/httpd/access.log
/etc/httpd/conf/httpd.conf
/etc/httpd/conf.d/

1. ติดตั้งโปรแกรม httpd พร้อมคู่มือ ด้วยคำสั่ง
yum install httpd
yum install httpd-manual
yum install mod_ssl

ผลลัพธ์

```
[root@dhcp160 ~]# yum install httpd
================================================================================
 Package              Arch      Version         Repository       Size
================================================================================
Updating:
 httpd                i386      2.2.6-1.fc6     updates          1.0 M

Transaction Summary
================================================================================
...
Complete!
[root@dhcp160 ~]# yum install httpd-manual
================================================================================
 Package              Arch      Version         Repository       Size
================================================================================
Installing:
 httpd-manual         i386      2.2.6-1.fc6     updates          812 k

Transaction Summary
================================================================================
...
Complete!
[root@dhcp160 ~]# yum install mod_ssl
================================================================================
 Package              Arch      Version         Repository       Size
================================================================================
Installing:
 mod_ssl              i386      1:2.2.6-1.fc6   updates          84 k
Installing for dependencies:
 distcache            i386      1.4.5-14.1      base             120 k

Transaction Summary
================================================================================
...
Complete!
[root@dhcp160 ~]#
```

2. แก้ไขให้ทำงานทุกครั้งที่บูทเครื่อง
chkconfig httpd on

ผลลัพธ์

```
[root@dhcp160 ~]# chkconfig httpd on
[root@dhcp160 ~]#
```

3. สั่งให้ทำงานด้วยคำสั่งว่า

service httpd start

ผลลัพธ์

```
[root@dhcp160 ~]# service httpd start
Starting httpd:                                [  OK  ]
[root@dhcp160 ~]#
```

1.3 การติดตั้งโปรแกรม Freeradius

ชื่อแฟ้มที่เกี่ยวข้องเมื่อติดตั้งเสร็จแล้ว
/var/log/radius/radius.log
/etc/raddb/radiusd.conf
/etc/raddb/clients.conf

1. ติดตั้งโปรแกรม freeradius ด้วยคำสั่ง
yum install freeradius

แก้ไขให้ทำงานทุกครั้งที่บูทเครื่อง
chkconfig radiusd on

สั่งให้ทำงานด้วยคำสั่งว่า
service radiusd start

ผลลัพธ์

```
[root@dhcp160 ~]# yum install freeradius
================================================================================
 Package                Arch       Version          Repository       Size
================================================================================
Installing:
 freeradius             i386       1.1.7-3.1.fc6    updates          1.2 M
Installing for dependencies:
 lm_sensors             i386       2.10.1-1.fc6     updates          506 k
 net-snmp               i386       1:5.3.1-15.fc6   updates          695 k
 net-snmp-utils         i386       1:5.3.1-15.fc6   updates          179 k
 perl-DBI               i386       1.52-1.fc6       base             605 k

Transaction Summary
================================================================================
Install      5 Package(s)
Update       0 Package(s)
Remove       0 Package(s)

Total download size: 3.1 M
Is this ok [y/N]: y
Downloading Packages:
...
Complete!
[root@dhcp160 ~]# chkconfig radiusd on
[root@dhcp160 ~]# service radiusd start
radiusd is stopped
Starting RADIUS server:                        [  OK  ]
[root@dhcp160 ~]#
```

1.4 ทดสอบ authentication โดยใช้ username/password ของ Unix

1. (หากยังไม่มี) ให้เตรียม username ที่จะใช้ทดสอบชื่อ chilli มีรหัสผ่านเป็น abcd1234 ด้วยคำสั่งดังนี้
adduser chilli
passwd chilli

ผลลัพธ์

```
[root@dhcp160 ~]# adduser chilli
[root@dhcp160 ~]# passwd chilli
Changing password for user chilli.
New UNIX password:
BAD PASSWORD: it is too simplistic/systematic
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@dhcp160 ~]#
```

2. เมื่อให้ radiusd ทำงานแล้ว เริ่มขั้นตอนทดสอบระบบโดยป้อนตัวอย่างคำสั่งดังนี้
radtest chilli abcd1234 localhost 0 testing123

จะมีการแจ้งว่า Access-Reject
เป็นสาเหตุเนื่องจากไม่มีสิทธิในการอ่านแฟ้ม /etc/shadow ของระบบ

ผลลัพธ์

```
[root@dhcp160 ~]# radtest chilli abcd1234 localhost 0 testing123
Sending Access-Request of id 232 to 127.0.0.1 port 1812
        User-Name = "chilli"
        User-Password = "abcd1234"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
Re-sending Access-Request of id 232 to 127.0.0.1 port 1812
        User-Name = "chilli"
        User-Password = "abcd1234"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
rad_recv: Access-Reject packet from host 127.0.0.1:1812, id=232, length=20
[root@dhcp160 ~]#
```

หมายเหตุ คำว่า localhost คือ ชื่อโดเมนของไอพีแอดเดรส 127.0.0.1 ก็คือ ตัวเครื่องเซิร์ฟเวอร์เอง
ซึ่งต้องมีระบุไว้ในแฟ้ม /etc/hosts ใช้คำสั่งดูข้อมูลข้างในแฟ้มดังนี้
cat /etc/hosts

```
[root@dhcp160 ~]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1       localhost.localdomain localhost
::1             localhost.localdomain localhost
[root@dhcp160 ~]#
```

3. แก้ไขให้อ่านแฟ้ม /etc/shadow ได้ โดยแก้ไขแฟ้ม /etc/raddb/radiusd.conf
3.1 ให้ทำการสำรองแฟ้มต้นฉบับเก็บไว้ก่อน ด้วยคำสั่ง
cp /etc/raddb/radiusd.conf /etc/raddb/radiusd.conf.save

ผลลัพธ์

```
[root@dhcp160 ~]# cp /etc/raddb/radiusd.conf /etc/raddb/radiusd.conf.save
[root@dhcp160 ~]#
```

3.2 แก้ไขแฟ้ม /etc/raddb/radiusd.conf เพื่อทำการ comment ยกเลิกบรรทัดข้อความจากเดิม
user = radiusd
group = radiusd
ให้เป็น
#user = radiusd
#group = radiusd

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /etc/raddb/radiusd.conf
```

```
Line 114
#user = radiusd
#group = radiusd
```

3.3 เสร็จแล้วให้ restart ระบบ radiusd ใหม่ด้วยคำสั่ง
service radiusd restart

ผลลัพธ์

```
[root@dhcp160 ~]# service radiusd restart
radiusd (pid 23004) is running...
radiusd (pid 23004) is running...
Stopping RADIUS server:                                    [  OK  ]
radiusd is stopped
Starting RADIUS server:                                    [  OK  ]
[root@dhcp160 ~]#
```

3.4 ต่อไปลองป้อนตัวอย่างคำสั่งเดิมเพื่อทดสอบดังนี้
radtest chilli abcd1234 localhost 0 testing123

จะมีการแจ้งว่า Access-Accept ถูกต้องตามต้องการ
ผลลัพธ์

```
[root@dhcp160 ~]# radtest chilli abcd1234 localhost 0 testing123
Sending Access-Request of id 39 to 127.0.0.1 port 1812
      User-Name = "chilli"
      User-Password = "abcd1234"
      NAS-IP-Address = 255.255.255.255
      NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=39, length=20
[root@dhcp160 ~]#
```

3.5 ในการนำไปใช้งานจริง ขอให้แก้ไข secret ใหม่ ตัวอย่างเช่น ตั้งใหม่เป็น mytestkey
ให้แก้ไขแฟ้ม /etc/raddb/clients.conf ของโปรแกรม freeradius ให้มีค่าดังตัวอย่างนี้
client 127.0.0.1 {
...
บรรทัดที่ 35 เดิม secret = testing123
แก้ไขเป็น secret = mytestkey
...
}
เสร็จแล้วให้ restart ระบบ radiusd ใหม่ด้วยคำสั่ง
service radiusd restart
ทดสอบ radius อีกครั้งด้วย secret อันใหม่ ดังนี้
radtest chilli abcd1234 localhost 0 mytestkey

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /etc/raddb/clients.conf
```

```
Line 35
        secret          = mytestkey
```

```
[root@dhcp160 ~]# service radiusd restart
radiusd (pid 23068) is running...
radiusd (pid 23068) is running...
Stopping RADIUS server:                                    [  OK  ]
radiusd is stopped
Starting RADIUS server:                                    [  OK  ]

[root@dhcp160 ~]# radtest chilli abcd1234 localhost 0 mytestkey
Sending Access-Request of id 166 to 127.0.0.1 port 1812
        User-Name = "chilli"
        User-Password = "abcd1234"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=166, length=20
[root@dhcp160 ~]#
```

1.5 การติดตั้งโปรแกรม Chillispot แบบ Web login

ชื่อแฟ้มที่เกี่ยวข้องเมื่อติดตั้งเสร็จแล้ว

/etc/chilli.conf
/var/www/cgi-bin/hotspotlogin.cgi
/var/www/html/welcome.html
/etc/firewall.iptables

โปรดตรวจสอบ
เนื่องจาก chillispot จะเป็น dhcp server เอง
กรณีที่นำเครื่องเดิมมาติดตั้ง chillispot เพิ่ม จะต้องเช็คว่าในเครื่องไม่มี dhcp server รันอยู่ ถ้ามีอยู่ก็หยุดดังนี้
service dhcpd stop
chkconfig dhcpd off

---

1. เราต้องทำให้เครื่องนี้ทำหน้าที่เป็นเราเตอร์เพื่อ forward packet ทุกครั้งที่รีบูตเครื่อง
ให้แก้ไขแฟ้ม /etc/sysctl.conf ให้มีค่าดังตัวอย่างนี้
บรรทัดที่ 7 เดิม net.ipv4.ip_forward = 0
แก้ไขเป็น net.ipv4.ip_forward = 1

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /etc/sysctl.conf
```

```
# Controls IP packet forwarding
net.ipv4.ip_forward = 1
```

2. เพื่อให้มีผลทันทีในขณะนี้ ให้เครื่อง forward packet
รันคำสั่ง echo "1" > /proc/sys/net/ipv4/ip_forward

ผลลัพธ์

```
[root@dhcp160 ~]# echo "1" > /proc/sys/net/ipv4/ip_forward
[root@dhcp160 ~]#
```

3. เพื่อให้การ์ดแลน eth1 ไม่รับ dhcp ตอนรีบูตเครื่อง
ให้แก้ไขแฟ้ม /etc/sysconfig/network-scripts/ifcfg-eth1 ให้มีค่าดังตัวอย่างนี้
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=none

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /etc/sysconfig/network-scripts/ifcfg-eth1
```

```
# 3Com Corporation 3c905C-TX/TX-M [Tornado]
DEVICE=eth1
BOOTPROTO=none
HWADDR=00:01:03:18:BA:59
ONBOOT=yes
```

4. ดาวน์โหลดโปรแกรม chillispot จากเครื่องเอฟทีพีของม.อ. ด้วยคำสั่ง wget ดังนี้
wget ftp://ftp.psu.ac.th/pub/chillispot/chillispot-1.1.0.i386.rpm

ผลลัพธ์

```
[root@dhcp160 ~]# wget ftp://ftp.psu.ac.th/pub/chillispot/chillispot-1.1.0.i386.rpm
--20:25:02--  ftp://ftp.psu.ac.th/pub/chillispot/chillispot-1.1.0.i386.rpm
        => `chillispot-1.1.0.i386.rpm'
Resolving ftp.psu.ac.th... 192.168.100.101
Connecting to ftp.psu.ac.th|192.168.100.101|:21... connected.
Logging in as anonymous ... Logged in!
==> SYST ... done.    ==> PWD ... done.
==> TYPE I ... done.  ==> CWD /pub/chillispot ... done.
==> SIZE chillispot-1.1.0.i386.rpm ... 88761
==> PASV ... done.    ==> RETR chillispot-1.1.0.i386.rpm ... done.
Length: 88761 (87K)

100%[======================================>] 88,761      --.-K/s   in 0.04s

20:25:03 (2.00 MB/s) - `chillispot-1.1.0.i386.rpm' saved [88761]
[root@dhcp160 ~]#
```

หรือดาวน์โหลดจากเว็บต้นฉบับที่ http://www.chillispot.info/download.html

```
http://www.chillispot.info/download.html
Suitable for Redhat 9, Fedora (FC1, FC2 and FC3 and FC4).
http://www.chillispot.info/download/chillispot-1.1.0.i386.rpm
Or other linux distro.
http://www.chillispot.info/download/chillispot-1.1.0.tar.gz
```

5. แล้วติดตั้ง package rpm ด้วยคำสั่งดังนี้
rpm -Uvh chillispot-1.1.0.i386.rpm

ผลลัพธ์

```
[root@dhcp160 ~]# rpm -Uvh chillispot-1.1.0.i386.rpm
Preparing...                ########################################### [100%]
   1:chillispot             ########################################### [100%]
[root@dhcp160 ~]#
```

6. แก้ไขแฟ้ม /etc/chilli.conf ให้มีค่าดังตัวอย่างนี้
[หัวข้อ TUN parameters]

บรรทัดที่ 38 เดิม net 192.168.182.0/24
แก้ไขเป็น net 10.0.1.0/24

[หัวข้อ Radius parameters]
บรรทัดที่ 113 เดิม radiusserver1 rad01.chillispot.org
แก้ไขเป็น radiusserver1 127.0.0.1

บรรทัดที่ 120 เดิม radiusserver2 rad02.chillispot.org
แก้ไขเป็น radiusserver2 127.0.0.1

บรรทัดที่ 139 เดิม #radiussecret testing123
แก้ไขเป็น radiussecret mytestkey
(ตรงกับ radius secret ในแฟ้ม /etc/raddb/clients.conf ของ freeradius)

[หัวข้อ Universal access method (UAM) parameters]
บรรทัดที่ 237 เดิม #uamserver https://radius.chillispot.org/hotspotlogin
แก้ไขเป็น uamserver https://10.0.1.1/cgi-bin/hotspotlogin.cgi

บรรทัดที่ 244 เดิม #uamhomepage http://192.168.182.1/welcome.html
แก้ไขเป็น uamhomepage http://10.0.1.1/welcome.html

บรรทัดที่ 248 เดิม #uamsecret ht2eb8ej6s4et3rg1ulp
แก้ไขโดยให้เอาเครื่องหมาย# ออก เป็น uamsecret ht2eb8ej6s4et3rg1ulp
(หรือแก้ไขเป็นรหัสใหม่ แต่ต้องเหมือนกับในแฟ้ม hotspotlogin.cgi ในข้อถัดไป)

บรรทัดที่ 253 เดิม #uamlisten 192.168.182.1
แก้ไขเป็น uamlisten 10.0.1.1

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /etc/chilli.conf
```

```
Line 38
net 10.0.1.0/24
radiusserver1 127.0.0.1
radiusserver2 127.0.0.1
radiussecret mytestkey
uamserver https://10.0.1.1/cgi-bin/hotspotlogin.cgi
uamhomepage http://10.0.1.1/welcome.html
uamsecret ht2eb8ej6s4et3rg1ulp
uamlisten 10.0.1.1
```

7. ให้คัดลอกแฟ้ม firewall.iptables ด้วยคำสั่ง
cp /usr/share/doc/chillispot-1.1.0/firewall.iptables /etc

ให้คัดลอกแฟ้ม hotspotlogin.cgi ด้วยคำสั่ง
cp /usr/share/doc/chillispot-1.1.0/hotspotlogin.cgi /var/www/cgi-bin/

ผลลัพธ์

```
[root@dhcp160 ~]# cp /usr/share/doc/chillispot-1.1.0/firewall.iptables /etc
[root@dhcp160 ~]# cp /usr/share/doc/chillispot-1.1.0/hotspotlogin.cgi /var/www/cgi-bin/
[root@dhcp160 ~]#
```

8. แก้ไขแฟ้ม /var/www/cgi-bin/hotspotlogin.cgi ให้มีค่าดังตัวอย่างนี้
บรรทัดที่ 27 เดิม #$uamsecret = "ht2eb8ej6s4et3rg1ulp";
แก้ไขโดยให้เอาเครื่องหมาย# ออก เป็น $uamsecret = "ht2eb8ej6s4et3rg1ulp";

บรรทัดที่ 31 เดิม #$userpassword=1;
แก้ไขโดยให้เอาเครื่องหมาย# ออก เป็น $userpassword=1;

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /var/www/cgi-bin/hotspotlogin.cgi
```

```
Line 27
$uamsecret = "ht2eb8ej6s4et3rg1ulp";

# Uncomment the following line if you want to use ordinary user-password
# for radius authentication. Must be used together with $uamsecret.
$userpassword=1;
```

9. สร้างแฟ้ม /var/www/html/welcome.html ให้มีค่าดังตัวอย่างนี้

Welcome to Our Hotspot, Wireless Network.

You are connected to an authentication and restricted network access point.

Click here to login

Enjoy.

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /var/www/html/welcome.html
```

```
<html>
<head>
<title>Welcome to Our Hotspot, Wireless Network.</title>
</head>
<body>
<center>
<H1><font color="red">TESTING ONLY</font></H1>
<img src="chillispot.png" mce_src="chillispot.png">
<H3><font color="blue">Welcome to Our Hotspot, Wireless Network.</font></H3>
<p>You are connected to an authentication and restricted network access point.
<H3><a href="http://10.0.1.1:3990/prelogin" mce_href="http://10.0.1.1:3990/prelogin">Click here to login</a></H3>
<p>
<p>Enjoy.
</center>
</body>
</html>
```

10. ถ้าต้องการรูป chillispot.png ให้ดาวน์โหลดได้ที่นี่
wget http://mamboeasy.psu.ac.th/~wiboon.w/images/stories/chillispot/chillispot.png

แล้วคัดลอกแฟ้มนี้ไปไว้ใน /var/www/html ด้วยคำสั่งดังนี้
cp chillispot.png /var/www/html

ผลลัพธ์

```
[root@dhcp160 ~]# wget http://mamboeasy.psu.ac.th/~wiboon.w/images/stories/
chillispot/chillispot.png
[root@dhcp160 ~]# cp chillispot.png /var/www/html
[root@dhcp160 ~]#
```

11. ก่อนที่จะสตาร์ท chillispot ให้ไปทำการคอนฟิกแอคเซสพอยน์/ไวร์เลสเราเตอร์ ให้พร้อมใช้งาน โดยทำตามเอกสารของแต่ละรุ่น
ความต้องการคือ ให้ทำ factory defaults แล้วกำหนดให้มันจะต้องรับ dhcp ip จาก chillispot และตัวมันเองจะต้องไม่ทำหน้าที่แจก ip
รวมทั้งควรแก้ไข ESSID ตั้งชื่อใหม่ด้วย เพื่อให้รู้ว่าตัวไหนของเรา ดูตัวอย่างบางรุ่นในเว็บนี้ได้

หมายเหตุ Linksys WRT54GL ที่ผมนำมา upgrade firmware เป็น DD-WRT แล้ว
ผมพบว่า ต้อง Enable DHCP server ให้กับ port LAN 1-4 ของเราเตอร์ด้วย
มันยังคงแจกไอพีให้กับ เครื่องที่ต่อ port LAN 1-4 แต่มันไม่แจกไอพีให้ไวร์เลส

12. เปิดใช้งาน iptables เพื่อทำเป็น firewall ด้วยคำสั่ง
sh /etc/firewall.iptables

ผลลัพธ์

```
[root@dhcp160 ~]# sh /etc/firewall.iptables
[root@dhcp160 ~]#
```

13. สั่งให้ chillispot ทำงานด้วยคำสั่ง
service chilli start

ผลลัพธ์

```
[root@dhcp160 ~]# service chilli start
Starting chilli:                                           [  OK  ]
```

14. ตรวจสอบการทำงานของ chiilispot ว่าสร้างอินเทอร์เฟส tun0 พร้อมใช้งานและมีเลข IP เป็น 10.0.1.1 โดยที่อินเทอร์เฟส eth1 จะไม่มี IP ใด ๆ ส่วน eth0 ก็เป็นเลข IP ที่รับจากเน็ตที่เซิร์ฟเวอร์นี้ต่ออยู่เหมือนเดิม ด้วยคำสั่ง ifconfig ดังตัวอย่าง

ผลลัพธ์

```
[root@dhcp160 ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:60:97:A5:38:6F
          inet addr:192.168.2.220  Bcast:192.168.2.255  Mask:255.255.255.0
...

eth1      Link encap:Ethernet  HWaddr 00:01:03:18:BA:59
          inet6 addr: fe80::201:3ff:fe18:ba59/64 Scope:Link
          UP BROADCAST RUNNING  MTU:1500  Metric:1
...

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
...

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.0.1.1  P-t-P:10.0.1.1  Mask:255.255.255.0
          UP POINTOPOINT RUNNING  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:116 (116.0 b)  TX bytes:240 (240.0 b)
[root@dhcp160 ~]#
```

15. ให้จดเลข Mac address ของโน้ตบุ๊คที่จะนำมาทดสอบการเชื่อมต่อกับ chillispot และรันคำสั่งตรวจสอบว่าโน้ตบุ๊คได้ IP Address จาก chillispot ดังนี้
tail -f /var/log/messages
จะได้ผลลัพธ์แสดงคล้าย ๆ ดังอย่างข้างล่างนี้

ผลลัพธ์

```
[root@dhcp160 ~]# tail -f /var/log/messages
Nov 27 20:05:18 dhcp160 Installed: httpd-manual.i386 2.2.6-1.fc6
Nov 27 20:06:54 dhcp160 Installed: distcache.i386 1.4.5-14.1
Nov 27 20:06:57 dhcp160 Installed: mod_ssl.i386 1:2.2.6-1.fc6
Nov 27 20:57:57 dhcp160 chillispot[23328]: ChilliSpot 1.1.0.
Copyright 2002-2005 Mondru AB. Licensed under GPL.
See http://www.chillispot.org for credits.
Nov 27 20:57:57 dhcp160 kernel: tun: Universal TUN/TAP device driver, 1.6
Nov 27 20:57:57 dhcp160 kernel: tun: (C) 1999-2004 Max Krasnyansky <
maxk@qualcomm.com

>
Nov 27 20:57:57 dhcp160 kernel: ADDRCONF(NETDEV_CHANGE): tun0: link becomes ready
Nov 27 20:57:57 dhcp160 kernel: eth1:  setting full-duplex.
Nov 27 20:58:00 dhcp160 chillispot[23328]: chilli.c: 3509:
New DHCP request from MAC=00-1D-7E-27-C3-18
Nov 27 20:58:00 dhcp160 chillispot[23328]: chilli.c: 3479:
Client MAC=00-1D-7E-27-C3-18 assigned IP 10.0.1.2
Nov 27 21:16:55 dhcp160 chillispot[23328]: chilli.c: 3509:
New DHCP request from MAC=00-13-02-69-41-FA
Nov 27 21:16:55 dhcp160 chillispot[23328]: chilli.c: 3479:
Client MAC=00-13-02-69-41-FA assigned IP 10.0.1.3
Nov 27 21:20:32 dhcp160 chillispot[23328]: chilli.c: 3759:
Successful UAM login from username=chilli IP=10.0.1.3
Ctrl-C break
```

โดยที่ 10.0.1.2 จะเป็น IP ของแอคเซสพอยน์ และ 10.0.1.3 จะเป็น IP ของโน้ตบุ๊คตัวแรกที่เชื่อมต่อ

16. เริ่มขั้นตอนทดสอบระบบที่เครื่องโน้ตบุคดังนี้

เริ่มทำการคอนเนค W-IFI
คลิกที่นี่เพื่อดูรูป

ที่บราวเซอร์ให้ยกเลิกการเซ็ตพร็อกซี่เซิร์ฟเวอร์

ที่บราวเซอร์ที่มีการเซ็ตหน้าโฮมเพจไว้ จะถูก redirect ไปยัง welcome.html ทันทีเมื่อเรียกโปรแกรม คลิกที่นี่เพื่อดูรูป

คลิกที่ข้อความ Click here to login แล้วจะมีหน้าต่างเพื่อให้ใส่ username และ password
คลิกที่นี่เพื่อดูรูป

เมื่อ login เข้าได้สำเร็จจะมีหน้าต่าง logged in พร้อมเวลาเริ่มนับ และเอาไว้ใช้สำหรับ logout
คลิกที่นี่เพื่อดูรูป

17. แก้ไขแฟ้ม /etc/rc.local เพื่อให้ firewall.iptables และ chilli มีผลทำงานด้วยเมื่อรีบูตเครื่องใหม่
เพิ่มบรรทัด 2 บรรทัดนี้ต่อท้าย
sh /etc/firewall.iptables
service chilli start

ผลลัพธ์

```
[root@dhcp160 ~]# gedit /etc/rc.local
```

```
#!/bin/sh
#
# This script will be executed *after* all the other init scripts.
# You can put your own initialization stuff in here if you don't
# want to do the full Sys V style init stuff.

touch /var/lock/subsys/local
/usr/sbin/ntpdate -u pool.ntp.org
sh /etc/firewall.iptables
service chilli start
```

18. รีบูตเครื่องเซิร์ฟเวอร์ 1 ครั้ง

19. ถึงขั้นตอนนี้เป็นอันเปิดใช้ระบบ chillispot แบบ web login ได้แล้ว

[Day 2]

ตอนที่ 2

2.1 การติดตั้งโปรแกรม Mysql

1. ติดตั้งโปรแกรม mysql ด้วยคำสั่งดังนี้
yum install mysql
yum install mysql-server

ผลลัพธ์

```
[root@dhcp220 ~]# yum install mysql
================================================================================
 Package              Arch      Version         Repository       Size
================================================================================
Installing:
 mysql                i386      5.0.27-1.fc6    updates          3.3 M

Transaction Summary
================================================================================
...
Complete!

[root@dhcp220 ~]# yum install mysql-server
================================================================================
 Package              Arch      Version         Repository       Size
================================================================================
Installing:
 mysql-server         i386      5.0.27-1.fc6    updates          10 M
Installing for dependencies:
 perl-DBD-MySQL       i386      3.0007-1.fc6    base             147 k

Transaction Summary
================================================================================
```

```
...
Complete!
[root@dhcp220 ~]#
```

2. สั่งให้รันทุกครั้งที่รีบูตเครื่อง ด้วยคำสั่งดังนี้
chkconfig mysqld on

ผลลัพธ์

```
[root@dhcp220 ~]# chkconfig mysqld on
[root@dhcp220 ~]#
```

3. รัน mysqld ด้วยคำสั่ง
service mysqld start

ผลลัพธ์

```
[root@dhcp220 ~]# service mysqld start
Initializing MySQL database:  Installing all prepared tables
Fill help tables

To start mysqld at boot time you have to copy support-files/mysql.server
to the right place for your system

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:
/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h dhcp220.cc.psu.ac.th password 'new-password'
See the manual for more instructions.

You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &

You can test the MySQL daemon with the benchmarks in the 'sql-bench' directory:
cd sql-bench ; perl run-all-tests

Please report any problems with the /usr/bin/mysqlbug script!

The latest information about MySQL is available on the web at
http://www.mysql.com
Support MySQL by buying support/licenses at http://shop.mysql.com
                                           [  OK  ]
Starting MySQL:                            [  OK  ]
[root@dhcp220 ~]#
```

4. เปลี่ยนรหัสผ่านให้กับ admin ของ mysql ด้วยคำสั่งดังนี้
/usr/bin/mysqladmin -u root password 'abcd1234'

ผลลัพธ์

```
[root@dhcp220 ~]# /usr/bin/mysqladmin -u root password 'abcd1234'
[root@dhcp220 ~]#
```

5. เข้าไปสร้าง database และ user ชื่อ radius เพื่อให้ freeradius ใช้ฐานข้อมูลที่เกี่ยวข้องในการ authentication ได้ ดังนี้
mysql -uroot -pabcd1234

สร้าง database ชื่อ radius ดังนี้
CREATE DATABASE radius;

สร้าง user ที่มีสิทธิใน database ดังนี้
GRANT ALL PRIVILEGES ON radius.* to 'radius'@'localhost' IDENTIFIED BY 'abcd1234';
FLUSH PRIVILEGES;

ออกจาก mysql ด้วยคำสั่ง
quit

ผลลัพธ์

```
[root@dhcp220 ~]# mysql -uroot -pabcd1234
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 3 to server version: 5.0.27
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
mysql> CREATE DATABASE radius;
Query OK, 1 row affected (0.00 sec)

mysql> GRANT ALL PRIVILEGES ON radius.* to 'radius'@'localhost'
IDENTIFIED BY 'abcd1234';
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)
mysql> quit
Bye
[root@dhcp220 ~]#
```

6. ใส่ database schema ด้วยคำสั่งดังนี้ (ตรวจสอบเลขเวอร์ชั่นก่อน)
mysql -uroot -pabcd1234 radius < /usr/share/doc/freeradius-?.?.?/examples/mysql.sql

ผลลัพธ์

```
[root@dhcp220 ~]# mysql -uroot -pabcd1234 radius < /usr/share/doc/freeradius-1.1.*/
examples/mysql.sql
[root@dhcp220 ~]#
```

7. เข้าไปใน mysql อีกครั้งด้วยคำสั่ง
mysql -uroot -pabcd1234

เปิดใช้ฐานข้อมูลชื่อ radius
use radius;

แล้วใส่ข้อมูลตัวอย่าง

บัญชีผู้ใช้ fredf จะได้รับสิทธิ 3 ชั่วโมงต่อวัน (10800 วินาที) ใช้ได้สูงสุด 90 ชั่วโมง (324000 วินาที)
ถูกกำหนดให้ใช้งานได้ (session) 1 ชั่วโมงต่อครั้ง (3600 วินาที) และสามารถดาวน์โหลดได้ที่ 56K และอัปโหลดได้ที่ 33.4K

บัญชีผู้ใช้ barney จะได้รับสิทธิ 3 ชั่วโมงต่อวัน (10800 วินาที) และถูกกำหนดให้ใช้งานได้ 1 ชั่วโมงต่อครั้ง

บัญชีผู้ใช้ dialrouter จะได้รับสิทธิเดือนละ 90 ชั่วโมง (324000 วินาที) และถูกกำหนดให้ใช้งานได้ 30 นาทีต่อครั้ง

```
INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('fredf', 'Password', '==', 'wilma');
INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('fredf', 'Max-Daily-Session', ':=', '10800');
INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('fredf', 'Max-All-Session', ':=', '324000');
INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('barney', 'Password', '==', 'betty');
INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('barney', 'Max-Daily-Session', ':=', '10800');
INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('dialrouter', 'Password', '==', 'dialup');
INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES ('dialrouter', 'Max-Monthly-Session', ':=', '324000');

INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('fredf', 'Idle-Timeout', ':=', '1800');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('fredf', 'Session-Timeout', ':=', '3600');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('fredf', 'WISPr-Bandwidth-Max-Down', ':=', '56000');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('fredf', 'WISPr-Bandwidth-Max-Up', ':=', '33400');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('barney', 'Idle-Timeout', ':=', '1800');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('barney', 'Session-Timeout', ':=', '3600');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('dialrouter', 'Idle-Timeout', ':=', '900');
INSERT INTO radreply (UserName, Attribute, Op, Value) VALUES ('dialrouter', 'Session-Timeout', ':=', '1800');

INSERT INTO usergroup (UserName, GroupName) VALUES ('fredf', 'dynamic');
INSERT INTO usergroup (UserName, GroupName) VALUES ('barney', 'static');
INSERT INTO usergroup (UserName, GroupName) VALUES ('dialrouter', 'netdial');

INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('dynamic', 'Auth-Type', ':=', 'Local');
INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('dynamic', 'Simultaneous-Use', ':=', '1');
INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('static', 'Auth-Type', ':=', 'Local');
INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('static', 'Simultaneous-Use', ':=', '1');
INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('netdial', 'Auth-Type', ':=', 'Local');
INSERT INTO radgroupcheck (GroupName, Attribute, Op, Value) VALUES ('netdial', 'Simultaneous-Use', ':=', '1');
```

```
INSERT INTO radgroupreply (GroupName, Attribute, Op, Value) VALUES ('dynamic', 'Service-Type', ':=', 'Login-User');
INSERT INTO radgroupreply (GroupName, Attribute, Op, Value) VALUES ('static', 'Service-Type', ':=', 'Login-User');
INSERT INTO radgroupreply (GroupName, Attribute, Op, Value) VALUES ('netdial', 'Service-Type', ':=', 'Login-User');
```

คำสั่งที่ใช้แสดงข้อมูลเรคคอร์ดใน table

```
show tables;
select * from radcheck;
select * from radreply;
select * from usergroup;
select * from radgroupcheck;
select * from radgroupreply;
```

แล้วออกจาก mysql

ผลลัพธ์

```
[root@dhcp220 ~]# mysql -uroot -pabcd1234
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5 to server version: 5.0.27

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
mysql> use radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> INSERT INTO radcheck (UserName, Attribute, Op, Value) VALUES
('fredf', 'Password', '==', 'wilma');
Query OK, 1 row affected (0.00 sec)

...

mysql> INSERT INTO radgroupreply (GroupName, Attribute, Op, Value) VALUES
('netdial', 'Service-Type', ':=', 'Login-User');
Query OK, 1 row affected (0.00 sec)

mysql> show tables;
+------------------+
| Tables_in_radius |
+------------------+
| nas              |
| radacct          |
| radcheck         |
| radgroupcheck    |
| radgroupreply    |
| radippool        |
| radpostauth      |
| radreply         |
| usergroup        |
+------------------+
9 rows in set (0.00 sec)

mysql> select * from radcheck;
+----+------------+---------------------+----+--------+
| id | UserName   | Attribute           | op | Value  |
+----+------------+---------------------+----+--------+
|  1 | fredf      | Password            | == | wilma  |
|  2 | fredf      | Max-Daily-Session   | := | 10800  |
|  3 | fredf      | Max-All-Session     | := | 324000 |
|  4 | barney     | Password            | == | betty  |
|  5 | barney     | Max-Daily-Session   | := | 10800  |
|  6 | dialrouter | Password            | == | dialup |
|  7 | dialrouter | Max-Monthly-Session | := | 324000 |
+----+------------+---------------------+----+--------+
7 rows in set (0.02 sec)

mysql> select * from radreply;
+----+------------+--------------------------+----+-------+
| id | UserName   | Attribute                | op | Value |
+----+------------+--------------------------+----+-------+
```

```
|  1 | fredf      | Idle-Timeout             | := | 1800  |
|  2 | fredf      | Session-Timeout          | := | 3600  |
|  3 | fredf      | WISPr-Bandwidth-Max-Down | := | 56000 |
|  4 | fredf      | WISPr-Bandwidth-Max-Up   | := | 33400 |
|  5 | barney     | Idle-Timeout             | := | 1800  |
|  6 | barney     | Session-Timeout          | := | 3600  |
|  7 | dialrouter | Idle-Timeout             | := | 900   |
|  8 | dialrouter | Session-Timeout          | := | 1800  |
+----+------------+--------------------------+----+-------+
8 rows in set (0.00 sec)

mysql> select * from usergroup;
+------------+-----------+----------+
| UserName   | GroupName | priority |
+------------+-----------+----------+
| fredf      | dynamic   |        1 |
| barney     | static    |        1 |
| dialrouter | netdial   |        1 |
+------------+-----------+----------+
3 rows in set (0.01 sec)

mysql> select * from radgroupcheck;
+----+------------+------------------+----+-------+
| id | GroupName | Attribute        | op | Value |
+----+------------+------------------+----+-------+
|  1 | dynamic   | Auth-Type        | := | Local |
|  2 | dynamic   | Simultaneous-Use | := | 1     |
|  3 | static    | Auth-Type        | := | Local |
|  4 | static    | Simultaneous-Use | := | 1     |
|  5 | netdial   | Auth-Type        | := | Local |
|  6 | netdial   | Simultaneous-Use | := | 1     |
+----+------------+------------------+----+-------+
6 rows in set (0.00 sec)

mysql> select * from radgroupreply;
+----+------------+--------------+----+------------+
| id | GroupName | Attribute    | op | Value      |
+----+------------+--------------+----+------------+
|  1 | dynamic   | Service-Type | := | Login-User |
|  2 | static    | Service-Type | := | Login-User |
|  3 | netdial   | Service-Type | := | Login-User |
+----+------------+--------------+----+------------+
3 rows in set (0.00 sec)
mysql> quit
Bye
[root@dhcp220 ~]#
```

8. ติดตั้งโปรแกรมเพิ่มเพื่อให้ mysql ทำงานร่วมกับ freeradius ได้
yum install freeradius-mysql

ผลลัพธ์

```
[root@dhcp220 ~]# yum install freeradius-mysql
================================================================================
 Package              Arch      Version         Repository       Size
================================================================================
Installing:
 freeradius-mysql     i386      1.1.7-3.1.fc6   updates          17 k

Transaction Summary
================================================================================
...
Complete!
[root@dhcp220 ~]#
```

9. แก้ไขไฟล์ /etc/raddb/sql.conf
บรรทัดที่ 21 แก้ไขให้เป็น
login = "radius"

password = "abcd1234"
radius_db = "radius"

ผลลัพธ์

```
[root@dhcp220 ~]# gedit /etc/raddb/sql.conf
        # Connect info
        server = "localhost"
        login = "radius"
        password = "abcd1234"

        # Database table configuration
        radius_db = "radius"
```

10. แก้ไขไฟล์ /etc/raddb/radiusd.conf
ใน section module {}
บรรทัดที่ 1261 เดิม # $INCLUDE ${confdir}/sql.conf
แก้ไขโดยการเอาคอมเมนต์ออก เป็น $INCLUDE ${confdir}/sql.conf
ใน section authorize {}
บรรทัดที่ 1858 เดิม files
แก้ไขโดยการใส่คอมเมนต์ เป็น #files
บรรทัดที่ 1865 เดิม #sql
แก้ไขโดยการเอาคอมเมนต์ออก เป็น sql
ใน section accounting {}
บรรทัดที่ 2028 เดิม #sql
แก้ไขโดยการเอาคอมเมนต์ออก เป็น sql

ผลลัพธ์

```
[root@dhcp220 ~]# gedit /etc/raddb/radiusd.conf
Line 1261
        #  Include another file that has the SQL-related configuration.
        #  This is another file only because it tends to be big.
        #
        #  The following configuration file is for use with MySQL.
        #
        #  For Postgresql, use:         ${confdir}/postgresql.conf
        #  For MS-SQL, use:             ${confdir}/mssql.conf
        #  For Oracle, use:             ${confdir}/oraclesql.conf
        #
        $INCLUDE  ${confdir}/sql.conf
Line 1858
                #files



Line 1865
        #
        #  Look in an SQL database.  The schema of the database
        #  is meant to mirror the "users" file.
        #
        #  See "Authorization Queries" in sql.conf
        sql

Line 2028
        #
        #  Log traffic to an SQL database.
        #
        #  See "Accounting queries" in sql.conf
        sql
```

11. สั่งรีสตาร์ท radius ใหม่ ด้วยคำสั่ง
service radiusd restart

ผลลัพธ์

```
[root@dhcp220 ~]# service radiusd restart
radiusd (pid 2062) is running...
radiusd (pid 2062) is running...
Stopping RADIUS server:                    [  OK  ]
```

```
radiusd is stopped
Starting RADIUS server: Wed Nov 28 09:55:07 2007 : Info: Starting - reading configur
ation files ...
                                        [ OK ]
[root@dhcp220 ~]#
```

12. ทดสอบการเข้าใช้งาน ดังนี้
radtest fredf wilma localhost 0 mytestkey

ผลลัพธ์

```
[root@dhcp220 ~]# radtest fredf wilma localhost 0 mytestkey
Sending Access-Request of id 124 to 127.0.0.1 port 1812
        User-Name = "fredf"
        User-Password = "wilma"
        NAS-IP-Address = 255.255.255.255
        NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1:1812, id=124, length=62
        Idle-Timeout = 1800
        Session-Timeout = 3600
        WISPr-Bandwidth-Max-Down = 56000
        WISPr-Bandwidth-Max-Up = 33400
        Service-Type = Login-User
[root@dhcp220 ~]#
```

13. ตรวจสอบข้อผิดพลาดได้ที่ /var/log/radius/radius.log และ /var/log/radius/radius.log

ผลลัพธ์

```
[root@dhcp220 ~]# tail -f /var/log/radius/radius.log
...
Wed Nov 28 09:55:08 2007 : Info: rlm_sql_mysql: Starting connect to MySQL server for #0
Wed Nov 28 09:55:08 2007 : Info: rlm_sql_mysql: Starting connect to MySQL server for #1
Wed Nov 28 09:55:08 2007 : Info: rlm_sql_mysql: Starting connect to MySQL server for #2
Wed Nov 28 09:55:08 2007 : Info: rlm_sql_mysql: Starting connect to MySQL server for #3
Wed Nov 28 09:55:08 2007 : Info: rlm_sql_mysql: Starting connect to MySQL server for #4
Wed Nov 28 09:55:08 2007 : Info: Ready to process requests.
[root@dhcp220 ~]#
[root@dhcp220 ~]# tail -f /var/log/mysqld.log
...
InnoDB: Creating foreign key constraint system tables
InnoDB: Foreign key constraint system tables created
071128  9:16:14  InnoDB: Started; log sequence number 0 0
071128  9:16:14 [Note] /usr/libexec/mysqld: ready for connections.
Version: '5.0.27'  socket: '/var/lib/mysql/mysql.sock'  port: 3306  Source distribution
[root@dhcp220 ~]#
```

14. ตรวจสอบดูข้อมูลของการ login ของผู้ใช้งาน freeradius จะเก็บไว้ที่ไดเรกทอรี
/var/log/radius/radacct/127.0.0.1/

ผลลัพธ์

```
[root@dhcp220 ~]# more  /var/log/radius/radacct/127.0.0.1/detail-20071128
Wed Nov 28 10:11:04 2007
        Acct-Status-Type = Start
        User-Name = "fredf"
        Calling-Station-Id = "00-13-02-69-41-FA"
        Called-Station-Id = "00-01-03-18-BA-59"
        NAS-Port-Type = Wireless-802.11
        NAS-Port = 0
        NAS-Port-Id = "00000000"
        NAS-IP-Address = 0.0.0.0
        NAS-Identifier = "nas01"
        Framed-IP-Address = 10.0.1.2
        Acct-Session-Id = "474cdc1f00000000"
        Client-IP-Address = 127.0.0.1
        Acct-Unique-Session-Id = "0db96d0b6e7fdf38"
        Timestamp = 1196219464

Wed Nov 28 10:13:39 2007
        Acct-Status-Type = Stop
```

```
        User-Name = "fredf"
        Calling-Station-Id = "00-13-02-69-41-FA"
        Called-Station-Id = "00-01-03-18-BA-59"
        NAS-Port-Type = Wireless-802.11
        NAS-Port = 0
        NAS-Port-Id = "00000000"
        NAS-IP-Address = 0.0.0.0
        NAS-Identifier = "nas01"
        Framed-IP-Address = 10.0.1.2
        Acct-Session-Id = "474cdc1f00000000"
        Acct-Input-Octets = 3061
        Acct-Output-Octets = 4948
        Acct-Input-Gigawords = 0
        Acct-Output-Gigawords = 0
        Acct-Input-Packets = 19
        Acct-Output-Packets = 23
        Acct-Session-Time = 155
        Acct-Terminate-Cause = User-Request
        Client-IP-Address = 127.0.0.1
        Acct-Unique-Session-Id = "0db96d0b6e7fdf38"
        Timestamp = 1196219619
[root@dhcp220 ~]#
```

คำแนะนำเพิ่มเติม

การเซ็ตค่า sqlcounter

ใน freeradius เวอร์ชั่น 1.1.7 จะมี modules sqlcounter ให้แล้ว เราเพียงแต่เพิ่ม
noresetcounter
dailycounter
monthlycounter
ใน section ชื่อ authorize แค่นั้นเอง จะทำให้สามารถใช้งาน session-timeout และ อื่น ๆ ได้

ความหมาย
noresetcounter
the counter that never resets, can be used for real session-time cumulation

dailycounter
the counter that resets everyday, can be used for limiting daily access time (eg. 3 hours a day)

monthlycounter
the counter that resets monthly, can be used for limiting monthly access time (eg. 50 hours per month)

ใน freeradius เวอร์ชั่นต่ำกว่า 1.1.7 อาจจำเป็นต้องสร้าง sqlcounter.sql ให้อ่านคำแนะนำเพิ่มเติมได้จากเว็บไซต์
http://wiki.freeradius.org/index.php?title=Rlm_sqlcounter&printable=yes

---

15. แก้ไขแฟ้ม /etc/raddb/radiusd.conf เพื่อเพิ่ม sqlcounter name ทั้ง 3 ชื่อใน section authorize { ... }

ผลลัพธ์

```
[root@dhcp220 ~]# gedit /etc/raddb/radiusd.conf
```

```
        authorize {

            ...some entries here...
        # Append at last line in this section by wiboon
            noresetcounter
            dailycounter
            monthlycounter

        }
```

16. เพิ่ม sqlcounter name ชื่อ noresetcounter พร้อมรายละเอียด เนื่องจากขาดหายไปจากในแฟ้ม /etc/raddb/radiusd.conf
ให้แทรกไว้ใกล้ ๆ กับ sqlcounter name ชื่อ dailycounter

ผลลัพธ์

```
[root@dhcp220 ~]# gedit /etc/raddb/radiusd.conf
```

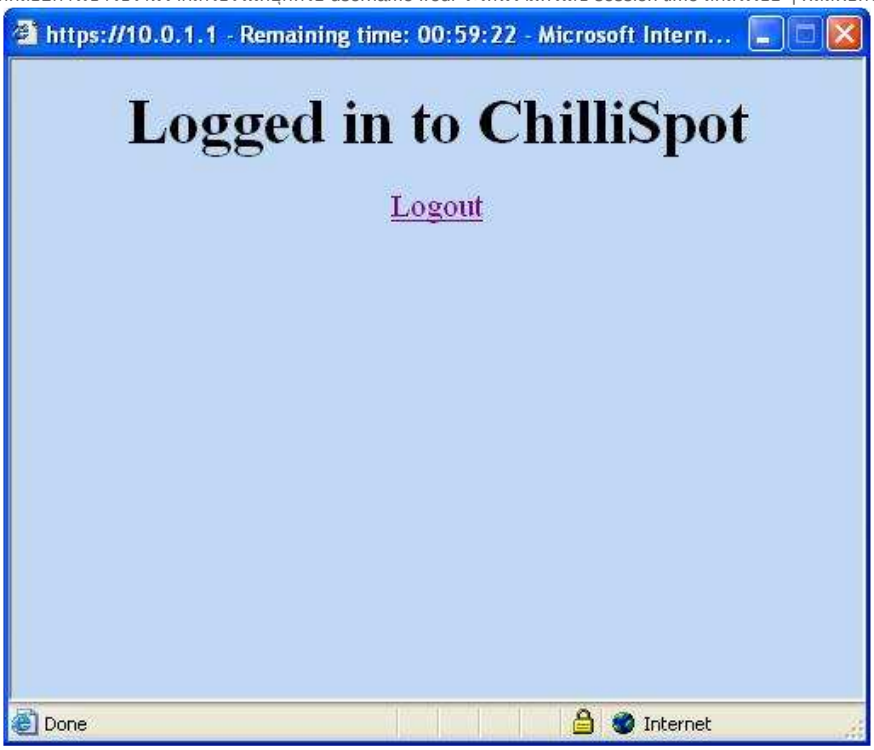
```
sqlcounter noresetcounter {

    counter-name = Max-All-Session-Time
    check-name = Max-All-Session
    sqlmod-inst = sql
    key = User-Name
    reset = never
    query = "SELECT SUM(AcctSessionTime) FROM radacct WHERE UserName='%{%k}'"

}
```

2.1 ทดสอบ authentication โดยใช้ username/password ของ Mysql

1. ทดสอบการเข้าใช้งานจากเครื่องโน้ตบุ๊คด้วย username fredf จะเห็นว่ามีตัวเลข session time ลดลงเรื่อย ๆ ผลลัพธ์ดังรูป



2. ทดสอบการเข้าใช้งานเมื่อ username fredf ใช้งานครบ 3 ชั่วโมงใน 1 วันแล้ว ผลลัพธ์ดังรูป

3. ทดสอบการเข้าใช้งานของ username fredf เป็นครั้งที่ 2 ในขณะที่กำลังใช้งานอยู่อีกเครื่อง ผลลัพธ์ดังรูป

คำแนะนำเพิ่มเติม

กรณีที่ต้องการลบฐานข้อมูล ชื่อ radius และสร้างใหม่ทำได้ดังนี้
เข้า mysql ด้วยคำสั่งดังนี้
mysql -uroot -pabcd1234

ใช้คำสั่ง
DROP DATABASE radius;
CREATE DATABASE radius;
GRANT ALL PRIVILEGES ON radius.* to 'radius'@'localhost' IDENTIFIED BY 'abcd1234';
FLUSH PRIVILEGES;

เปิดฐานข้อมูล
use radius;

สร้าง schema โดยใช้คำสั่งนำเข้าคือ \. (โปรดระวังเลขเวอร์ชั่นของ freeradius อาจเปลี่ยนไป)
\. /usr/share/doc/freeradius-1.1.?/examples/mysql.sql

นำเข้าเรคคอร์ดจากแฟ้ม (คัดลอกข้อมูลตัวอย่างมาเก็บไว้ /root/chilli-sql-example.sql)
\. /root/chilli-sql-example.sql

ออก
quit

2.3 การติดตั้งโปรแกรม radiusContext เพื่อทำรายงานการใช้งาน Freeradius

---

คัดลอกจาก การติดตั้ง radius server ด้วยโปรแกรม freeradius (18-01-2550)
http://rd.cc.psu.ac.th/content/view/35/46/

การแสดงผลรายงานจำเป็นต้องหาโปรแกรมมาต่างหาก
ขอแนะนำตัวอย่างโปรแกรมแสดงผลรายงาน

* ต้นแหล่งข้อมูลคือ http://www.tummy.com/radiusContext/
สามารถได้ดาวน์โหลดโปรแกรมได้ที่
ftp://ftp.psu.ac.th/pub/freeradius/radiusContext-1.93.tar.gz

* ให้ดาวน์โหลดมาแล้วขยายแฟ้มเก็บไว้ที่ /root ด้วยตัวอย่างคำสั่ง
tar -C /root -zxvf radiusContext-1.93.tar.gz

* สร้าง directory สำหรับแสดงผลบนเวบ ดังตัวอย่างคือ
mkdir /var/www/html/radius-report
จะแสดงผลบนโฮมพจ http://x.x.x.x/radius-report

* ตัวอย่าง ขั้นตอนที่ใช้สำหรับประมวลผลรวมข้อมูลจาก

/var/log/radius/radacct ไปเก็บไว้เพื่อแสดงผลที่ /var/www/html/radius-report
*** ภายใน /var/log/radius/radacct จะแยกเก็บข้อมูลเป็น directory ของ
แต่ละหมายเลข ip ทำให้อาจยุ่งยากต่อการรวบรวมข้อมูล

/root/radiusContext-1.93/raddetail /var/log/radius/radacct/*/*
/root/radiusContext-1.93/stdreport -D /var/www/html/radius-report

*** ต้องใช้คำสั่งเหล่านี้ทุกครั้งเพื่อปรับปรุงผลรายงาน

* ทดสอบผลรายงานได้เลยที่ http://x.x.x.x/radius-report
---

1. ติดตั้งโปรแกรมตามคำแนะนำข้างบนนี้

ผลลัพธ์

```
[root@dhcp220 ~]# wget ftp://ftp.psu.ac.th/pub/freeradius/radiusContext-1.93.tar.gz
[root@dhcp220 ~]# tar -C /root -zxvf radiusContext-1.93.tar.gz
[root@dhcp220 ~]# mkdir /var/www/html/radius-report
[root@dhcp220 ~]# /root/radiusContext-1.93/raddetail /var/log/radius/radacct/*/*
[root@dhcp220 ~]# /root/radiusContext-1.93/stdreport -D /var/www/html/radius-report
[root@dhcp220 ~]#
```

2. เข้าโปรแกรม Mozilla แล้วไปที่ http://127.0.0.1/radius-report/ จะเห็นรายงานการใช้งาน

3. สั่งให้ linux ทำการจัดทำรายงานใหม่ทุกชั่วโมง โดยใช้ crontab
ใช้คำสั่ง more ตรวจสอบดูแฟ้ม /etc/crontab

ผลลัพธ์

```
[root@dhcp220 ~]# more /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
[root@dhcp220 ~]#
```

4. สร้างแฟ้มเก็บคำสั่งจัดทำรายงาน ตั้งชื่อว่า radius-report ด้วยคำสั่ง
gedit /etc/cron.hourly/radius-report

ใส่ข้อความ 2 บรรทัดนี้
/root/radiusContext-1.93/raddetail /var/log/radius/radacct/*/*
/root/radiusContext-1.93/stdreport -D /var/www/html/radius-report

แล้วเปลี่ยนโหมดของแฟ้มเป็น execute ด้วยคำสั่ง
chmod +x /etc/cron.hourly/radius-report

ผลลัพธ์

```
[root@dhcp220 ~]# gedit /etc/cron.hourly/radius-report
```

```
/root/radiusContext-1.93/raddetail /var/log/radius/radacct/*/*
/root/radiusContext-1.93/stdreport -D /var/www/html/radius-report
```

```
[root@dhcp220 ~]# chmod +x /etc/cron.hourly/radius-report
[root@dhcp220 ~]#
```

[Day 3]

ตอนที่ 3

3.1 การติดตั้งโปรแกรม squid

โปรแกรม squid คือโปรแกรมที่ทำงานเป็น proxy / webcache server เพื่อใช้อินเทอร์เน็ตผ่านพร็อกซี่

1. ติดตั้งโปรแกรม squid ด้วยคำสั่ง
yum install squid

ผลลัพธ์

```
[root@dhcp220 ~]# yum install squid
================================================================================
 Package                 Arch       Version          Repository        Size
================================================================================
Installing:
 squid                   i386       7:2.6.STABLE13-1.fc6  updates           1.2 M
Installing for dependencies:
 perl-URI                noarch     1.35-3           base              116 k

Transaction Summary
================================================================================
...
Complete!
[root@dhcp220 ~]#
```

2. สั่งให้โปรแกรม squid ทำงานในการรีบูตเครื่องในครั้งต่อไป ด้วยคำสั่ง
chkconfig squid on

ผลลัพธ์

```
[root@dhcp220 ~]# chkconfig squid on
[root@dhcp220 ~]#
```

3. สร้างไดเรกทอรีเพื่อเก็บข้อมูลเว็บแคช ด้วยคำสั่ง
squid -z

ผลลัพธ์

```
[root@dhcp220 ~]# squid -z
2007/11/29 10:44:51| Creating Swap Directories
[root@dhcp220 ~]#
```

4. ปรับแต่งแฟ้มคอนฟิก /etc/squid/squid.conf ให้เหมาะสมดังนี้
ทำเป็น tranparent proxy
http_port 3128 transparent

ใช้ parent cache ในการออกอินเทอร์เน็ต (cache.your.domain คือชื่อ parent proxy ของหน่วยงานคุณ)
โดยที่ parent cache ตั้งใจเปิด port 8080 แทน 3128
cache_peer cache.your.domain parent 8080 0 no-query
(ถ้าไม่มี parent cache หรือ ไม่รู้ว่า parent cache คืออะไร cache_peer ไม่ต้องเซ็ตครับ)

ไม่เก็บ log ชนิด dump memory
cache_store_log none

กำหนดไอพีแอดเดรสเครือข่ายที่อนุญาตให้ใช้งาน proxy server นี้ได้
ตัวอย่างอนุญาตเฉพาะ net ของไวร์เลส
สามารถเพิ่มรายการ our_networks บรรทัดที่ 2,3,... ได้เองจากที่ผมทำไว้ให้
acl our_networks src 10.0.1.0/24 192.168.2.0/24
http_access allow our_networks

กำหนดให้มีแฟ้มเก็บ access.log 2 แฟ้มหมุนเวียนแบบเขียนทับ คือ access.log และ access.log.0
logfile_rotate 1

กำหนดให้ใช้งานผ่าน parent cache เท่านั้น จะไม่มีการ direct port 80 ไปอินเทอร์เน็ตเอง
never_direct allow all
(ถ้าไม่มี parent cache หรือ ไม่รู้ว่า parent cache คืออะไร never_direct ไม่ต้องเซ็ตครับ)

กำหนดให้ไปยังเว็บอินทราเน็ตโดยไม่ต้องใช้ proxy ของเรา เพื่อลดเวลาตอบสนอง
สามารถเพิ่มรายการ intranet_server ได้เองจากที่ผมทำไว้ให้
acl intranet_server dst 192.168.0.0/255.255.0.0
acl intranet_server dst 172.16.0.0/255.240.0.0
acl intranet_server dst 10.0.0.0/255.0.0.0
always_direct allow intranet_server

ผลลัพธ์

```
[root@dhcp220 ~]# gedit /etc/squid/squid.conf
```

```
Line 89
http_port 3128 transparent

Line 583
cache_peer cache.your.domain parent 8080 0 no-query

Line 1123
cache_store_log none

Line 2548
acl our_networks src 10.0.1.0/24 192.168.2.0/24
http_access allow our_networks

Line 2987
logfile_rotate 1

Line 3400
never_direct allow all

Line 3366
acl intranet_server dst 192.168.0.0/255.255.0.0
acl intranet_server dst 172.16.0.0/255.240.0.0
acl intranet_server dst 10.0.0.0/255.0.0.0
always_direct allow intranet_server
```

5. สั่งให้โปรแกรม squid ทำงาน ด้วยคำสั่ง
service squid start

ผลลัพธ์

```
[root@dhcp220 ~]# service squid start
Starting squid: .                                          [  OK  ]
[root@dhcp220 ~]#
```

3.2 การทำ Transparent proxy ด้วย iptables

1. แก้ไขแฟ้ม /etc/firewall.iptables โดยเพิ่มบรรทัด
##Allow transparent proxy (wiboon 1/2)
$IPTABLES -A INPUT -p tcp -m tcp --dport 3128 --syn -j ACCEPT
และ
##Allow transparent proxy (wiboon 2/2)
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp --dport 3128 --syn -j DROP
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp -d 192.168.0.0/16 --dport 80 -j RETURN
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp -d 172.16.0.0/12 --dport 80 -j RETURN
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp -d 10.0.0.0/8 --dport 80 -j RETURN
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 3128

ผลลัพธ์

```
[root@dhcp220 ~]# gedit /etc/firewall.iptables
```

```
IPTABLES="/sbin/iptables"
EXTIF="eth0"
INTIF="eth1"

#Flush all rules
$IPTABLES -F
$IPTABLES -F -t nat
$IPTABLES -F -t mangle

#Set default behaviour
$IPTABLES -P INPUT DROP
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -P OUTPUT ACCEPT

#Allow related and established on all interfaces (input)
$IPTABLES -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

#Allow releated, established and ssh on $EXTIF. Reject everything else.
```

```
$IPTABLES -A INPUT -i $EXTIF -p tcp -m tcp --dport 22 --syn -j ACCEPT
$IPTABLES -A INPUT -i $EXTIF -j REJECT

#Allow related and established from $INTIF. Drop everything else.
$IPTABLES -A INPUT -i $INTIF -j DROP

#Allow http and https on other interfaces (input).
#This is only needed if authentication server is on same server as chilli
$IPTABLES -A INPUT -p tcp -m tcp --dport 80 --syn -j ACCEPT
$IPTABLES -A INPUT -p tcp -m tcp --dport 443 --syn -j ACCEPT

#Allow 3990 on other interfaces (input).
$IPTABLES -A INPUT -p tcp -m tcp --dport 3990 --syn -j ACCEPT
##Allow transparent proxy (wiboon 1/2)
$IPTABLES -A INPUT -p tcp -m tcp --dport 3128 --syn -j ACCEPT

#Allow ICMP echo on other interfaces (input).
$IPTABLES -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

#Allow everything on loopback interface.
$IPTABLES -A INPUT -i lo -j ACCEPT

##Allow transparent proxy (wiboon 2/2)
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp --dport 3128 --syn -j DROP
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp -d 192.168.0.0/16 --dport 80 \
-j RETURN
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp -d 172.16.0.0/12 --dport 80 \
-j RETURN
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp -d 10.0.0.0/8 --dport 80 \
-j RETURN
$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp --dport 80 \
-j REDIRECT --to-ports 3128

# Drop everything to and from $INTIF (forward)
# This means that access points can only be managed from ChilliSpot
$IPTABLES -A FORWARD -i $INTIF -j DROP
$IPTABLES -A FORWARD -o $INTIF -j DROP

#Enable NAT on output device
$IPTABLES -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE
```

หากต้องการเปิด port ด้าน eth0 ให้อนุญาต port 443 และ 10000 ให้เพิ่ม 2 บรรทัดข้างล่างนี้ต่อท้ายบรรทัดที่อนุญาต port 22
#Allow https to web account management (wiboon).
$IPTABLES -A INPUT -i $EXTIF -p tcp -m tcp --dport 443 --syn -j ACCEPT
#Allow any port i.e. 10000 to this server (wiboon).
$IPTABLES -A INPUT -i $EXTIF -p tcp -m tcp --dport 10000 --syn -j ACCEPT

---

2. สั่งให้ iptables ทำงานเป็น firewall ตามแฟ้ม /etc/firewall.iptables ด้วยคำสั่ง
sh /etc/firewall.iptables

ผลลัพธ์

```
[root@dhcp220 ~]# sh /etc/firewall.iptables
[root@dhcp220 ~]#
```

3. ทดสอบการใช้งานที่เครื่องไคลเอนต์ ลองไปยังเว็บไซต์ google
แล้วเช็คดูในแฟ้ม /var/log/squid/access.log

ผลลัพธ์

```
[root@dhcp220 ~]# tail -f /var/log/squid/access.log
1196309038.756   2449 10.0.1.4 TCP_MISS/200 2551 GET http://www.google.co.th/
- TIMEOUT_FIRST_UP_PARENT/cache.psu.ac.th text/html
1196309220.447 181690 10.0.1.4 TCP_MISS/504 1480 GET http://www.google.co.th/gen_204?
- DIRECT/72.14.235.104 text/html
ctrl-c break
```

3.3 การตั้งเวลาเก็บ access.log ทุกคืน

1. สร้างแฟ้ม shell script ใหม่ชื่อ rotate_and_keep_proxy_log
เพื่อเก็บบรรทัดคำสั่งที่ใช้ในการ rotate log และเก็บ log ในรูปแบบย่อ เพื่อให้อ่านง่ายและประหยัดเนื้อที่
โดยใช้คำสั่ง
gedit /etc/cron.daily/rotate_and_keep_proxy_log

แล้วเปลี่ยนโหมดของแฟ้มเป็น execute
chmod +x /etc/cron.daily/rotate_and_keep_proxy_log

ผลลัพธ์

```
[root@dhcp220 ~]# gedit /etc/cron.daily/rotate_and_keep_proxy_log
```

```
#!/bin/bash
day=`date '+%Y%m%d'`
if [ -f /root/logs/access.log.cache.${day} ]; then
    exit 0
fi
squid -k rotate
cat /var/log/squid/access.log.0 | awk '{print $1 " " $3 " " $6 " " $7}' | \
perl -pe 's/^\d+\.\d+/localtime($&)/e;' > /root/logs/access.log.cache.${day}
```

```
[root@dhcp220 ~]# chmod +x /etc/cron.daily/rotate_and_keep_proxy_log
[root@dhcp220 ~]#
```

2. หากเนื้อที่ดิสก์ไม่เพียงพอ จำเป็นจะต้องย้ายไปเก็บยังเซิร์ฟเวอร์ตัวอื่น ให้ใช้คำสั่ง scp คัดลอกแฟ้มไป
ต้องแก้ไข shell script อีกเล็กน้อย

จบซะที เฮ้อเหนื่อยจัง แล้วจะกลับมาต่อตอนที่ 4 โปรแกรมจัดการบัญชีผู้ใช้ chillispot ด้วย php + mysql

Last Updated (Thursday, 25 September 2008)

Close Window