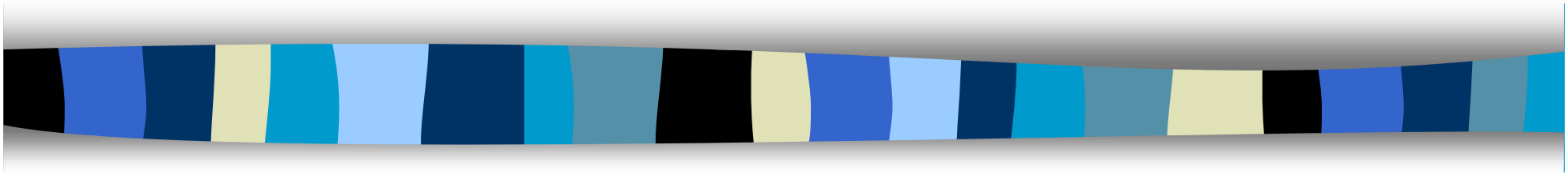
เอกสารประกอบการอบรมหลักสูตร Linux-SIS



วันที่ 3

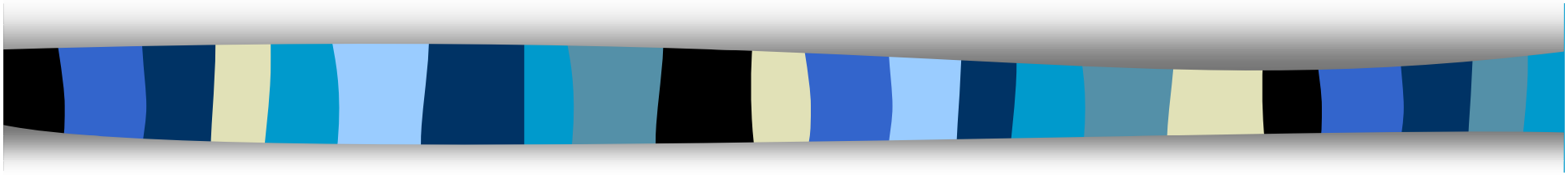
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ต้นฉบับที่ http://www.school.net.th/linux-sis/training/

ลิขสิทธิ์

- เอกสารชุดนี้สงวนลิขสิทธิ์โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ภายใต้ลิขสิทธิ์แบบ GNU Public License (GPL) รายละเอียดของลิขสิทธิ์แบบ GPL สามารถดูได้ที่
  - http://www.gnu.org/copyleft/gpl.html
  - http://linux.thai.net/gpl-th.html
- สามารถสรุปจุดที่สำคัญๆ ได้ดังนี้
  - อนุญาตให้นำไปใช้, เผยแพร่ต่อ, แก้ไข, แก้ไขฉบับที่เผยแพร่ต่อได้
  - เอกสารฉบับที่ถูกเผยแพร่ต่อจะต้องมีแสดงเงื่อนไขลิขสิทธิ์หน้านี้อย่างชัดเจน
  - เอกสารฉบับที่ท่านได้ทำการแก้ไขและเผยแพร่ต่อ จะต้องสงวนลิขสิทธิ์ภายใต้ลิขสิทธิ์ GPL เช่นเดียวกับเอกสารฉบับนี้
- หากที่ได้ทำการแก้ไขและพัฒนาเอกสารฉบับนี้ให้ดีขึ้น โปรดส่งต่อฉบับที่แก้ไขนั้นกลับมาที่ sis-master@nectec.or.th เพื่อที่จะได้ปรับปรุงตัวต้นฉบับให้ดีขึ้นต่อไป
- ทางศูนย์สงวนสิทธิ์ที่จะเปลี่ยนแปลง แก้ไขเงื่อนไขต่างๆ เพื่อรักษาผลประโยชน์ของทางศูนย์และส่วนรวม

การติดตั้งและใช้งาน Internet Server (ต่อ)



WWW Server (Apache)

- Apache Web Server จัดว่าเป็น Web Server ที่มีส่วนแบ่งตลาดมากที่สุดในโลก
- ปกติทำงานที่ port 80
- Apache สามารถทำงานร่วมกับ Module เช่น PHP module (คล้าย Microsoft ASP), Perl Module, SSL Module
- สามารถทำงานในโหมด SSL (Port 443)

Configuration File

- /usr/local/etc/httpd/conf/httpd.conf
  - Server Type, Port
  - ScriptAlias
  - Addhandler
  - Directory
  - Accessfile
  - Virtualhost
- /usr/local/etc/httpd/conf/mime.types

WWW Server ใน Linux-SIS

- /usr/local/etc/httpd
  - bin/httpd.org — httpd ตัวปกติ
  - bin/httpd.php — httpd ตัวที่สนับสนุนภาษา PHP
  - htdocs/ — เก็บเนื้อหา HTML
  - cgi-bin/ — เก็บไฟล์ CGI script
- /usr/local/etc/httpsd — Web Server ทำงานในโหมด SSL
- /usr/local/etc/webadmintool — Web Admin Tool

การควบคุมการเข้าดู web ด้วย .htaccess

- แก้ไข httpd.conf เพิ่ม AllowOverride All แล้ว restart httpd
- ในไดเรกทอรีที่ต้องการจะควบคุมให้ใส่ไฟล์ .htaccess และ .htpasswd ไว้ ดูตัวอย่างได้จากใน
  - /usr/local/etc/webadmin/htdocs/TMP/
- ใช้คำสั่ง /usr/local/etc/webadmin/bin/htpasswd .htpasswd <user> เพื่อตั้งรหัสผ่าน
- ระวัง Permission ของ .htaccess และ .htpasswd จะต้องให้ nobody อ่านได้

ทดลองใช้งาน CGI

- ไปที่ /usr/local/etc/httpd/
  - cd cgi-bin
  - cp examples/date .
- ทดลองเรียกไปยัง Web Site http://linux.intranet/cgi-bin/date
- ลองเข้าไปดูที่ http://linux.intranet/ และศึกษา script ที่ใช้ในส่วน Addressbook

ทดลองใช้งาน PHP3

- การใช้ CGI จำเป็นต้องมีหลายไฟล์ ถ้าเป็น PHP3 สามารถฝังเนื้อหาของ Script ไว้ในไฟล์ html ได้เลย
- ไฟล์ที่มี script PHP อยู่ ให้มีนามสกุลเป็น .php3
- ดูตัวอย่างไฟล์ในไดเรกทอรี htdocs/php_examples/
- ศึกษาการเขียน PHP ใน http://linux.intranet/news

แบบฝึกหัด

- สร้าง WWW Directory http://linux.intranet/training/ ขึ้นมาโดยจะต้องป้อนรหัสผู้ใช้ manager และรหัสผ่านก่อนเท่านั้น จึงจะเข้าได้ และเมื่อเข้าไปให้แสดงวันและเวลาในขณะนั้น

Web-based E-mail: Roxen+IMHO

- บางทีการใช้งาน E-mail ผ่าน Mail Reader มีความยุ่งยาก
- ใน Linux-SIS 3.1 จะมีการติดตั้ง Web-based E-mail ตัวที่ชื่อ IMHO ซึ่งทำงานบน Web Server ที่ชื่อ Roxen
- สามารถกำหนดให้ทำงานในตอนติดตั้ง หรือสั่ง chmod +x /etc/rc.d/rc.roxen
- ใช้งานเรียกไปที่ http://linux.intranet/ แล้ว Click ตรง Web-based E-mail

แบบฝึกหัด

- ทดลองใช้งาน Web-based E-mail ลองส่งจดหมายภาษาไทย และลอง attached ไฟล์ถึงกัน

Proxy/Cache Server

- Proxy/Cache คืออะไร
- ความสัมพันธ์ Parent/Sibling
- Hit/Miss
- ประหยัด Bandwidth ได้ถึง 30-40 % สำหรับ Cache Level ที่ 1 และ 20-25% สำหรับ Level ที่ 2

Squid

- Free/Open Source Cache Proxy Server
- http://squid.nlanr.net/
- ประสิทธิภาพดี
- ปัจจุบันเป็นเวอร์ชั่น 2
- บน Linux สามารถทำงานในโหมด Transparent Proxy ได้ (ผู้ใช้ไม่จำเป็นต้อง set ค่าใดๆ)

Squid Configuration

- Add user ชื่อ squid
- สร้างไดเรกทอรีสำหรับเก็บ cache และเก็บ log file ให้มี owner เป็น squid ใน Linux-SIS จะเป็น
  - /usr/local/etc/squid/cache เป็น link ไปที่ /data/cache/
  - /usr/local/etc/squid/logs เป็น links ไปที่ /var/adm/squid_logs/
- รายละเอียดการทำงานต่างๆ จะอยู่ในไดเรกทอรีที่เก็บ log file
- เรียกใช้งานครั้งแรกต้อง Initialize Cache Space ก่อน (squid -z)
- ใน Linux-SIS ได้ทำสิ่งที่กล่าวมาให้หมดแล้ว

Squid Configuration File

- มีไฟล์เดียว /usr/local/etc/squid/etc/squid.conf
- เพิ่มเติม parent และ sibling สำหรับหน่วยงานของท่าน
  - *cache_peer hostname type http_port icp_port options*
- กำหนด Access Control List เพื่อควบคุมการใช้งาน
  - *acl computer_room src 203.150.154.0-203.150.154.255/255.255.255.0*
  - *http_access allow computer_room*
  - *icp_access allow computer_room*

- ใช้งานกับเครือข่ายที่มีการปิด port 80 (default setting)
  - acl local-servers dstdomain schoolname.ac.th
  - never_direct deny local-servers
  - never_direct allow all
- กรณีที่ใช้ Transparent Proxy ต้องเพิ่ม
  - httpd_accel_uses_host_header on

การเรียกใช้งาน Squid

- รันไฟล์ /usr/local/etc/squid/bin/squid & หรือเรียก /etc/rc.d/rc.squid
- ดูรายละเอียดการทำงานได้ที่
  - /var/adm/squid_logs/cache.log
- ดูรายละเอียดการใช้งานจากตัวลูกได้ที่
  - /var/adm/squid_logs/access.log

การป้องกันไม่ให้เข้าไป Web Site ที่ไม่เหมาะสม

- ใช้โปรแกรม Redirector เวอร์ชั่น 1.1 ของคุณ Ian Lee
- สำหรับ Linux-SIS 3.1 ให้เพิ่ม URL ที่ต้องการ block ลงใน /usr/local/etc/squid/etc/acl-url.conf
- Restart Squid

แบบฝึกหัด

- ติดตั้ง Squid Cache Server ให้อนุญาตเฉพาะ client ที่มี IP 192.168.1.199 เท่านั้นที่ใช้งานได้ และไม่อนุญาตให้เรียกไป Web Site http://www.hotmail.com/ (เพื่อการทดสอบ)

DNS Server: bind

- DNS Server เป็น Server ที่จำเป็นที่สุดในเครือข่ายอินเทอร์เน็ต ?
- ซอฟต์แวร์ bind จัดเป็นซอฟต์แวร์ DNS Server ที่แพร่หลายที่สุด
- ใน Linux-SIS จะมีการติดตั้ง bind (process ชื่อ named) ให้ทำงานอยู่แล้ว โดยทำงานเป็น DNS Cache Server

Configuration File

- ไฟล์หลัก /etc/named.conf
- ที่เหลือจะอยู่ใน /var/named/

DNS Cache Server

- ใน /etc/named.conf

```
zone "." in {
        type hint;
        file "root.cache";
};
```

- สร้างไฟล์ root.cache
  - dig @rs.internic.net . ns > /var/named/root.cache

Secondary DNS Server

- ใน /etc/named.conf

```
zone “thai.net” in {
        type slave;
        file “slave/thai.net”;
        masters { 202.44.202.2; };
};
```

- ให้แน่ใจว่ามีไดเรกทอรี /var/named/slave อยู่

Primary DNS Server - Forward

- ใน /etc/named.conf
  - zone “schoolname.ac.th.” in {
    - type master;
    - file “master/schoolname.ac.th”
  - };
- สร้างไฟล์ /var/named/master/schoolname.ac.th ไว้เก็บฐานข้อมูลชื่อเครื่องและ IP Address ดูตัวอย่างในหนังสือหน้า 188-189

Primary DNS Server - Reverse

- ในไฟล์ /etc/named.conf

```
zone "1.168.192.in-addr.arpa" in {
        type master;
        file "master/192.168.1";
};
```

- และให้สร้างไฟล์ /var/named/master/192.168.1 ตามตัวอย่างในหนังสือหน้า 189-190

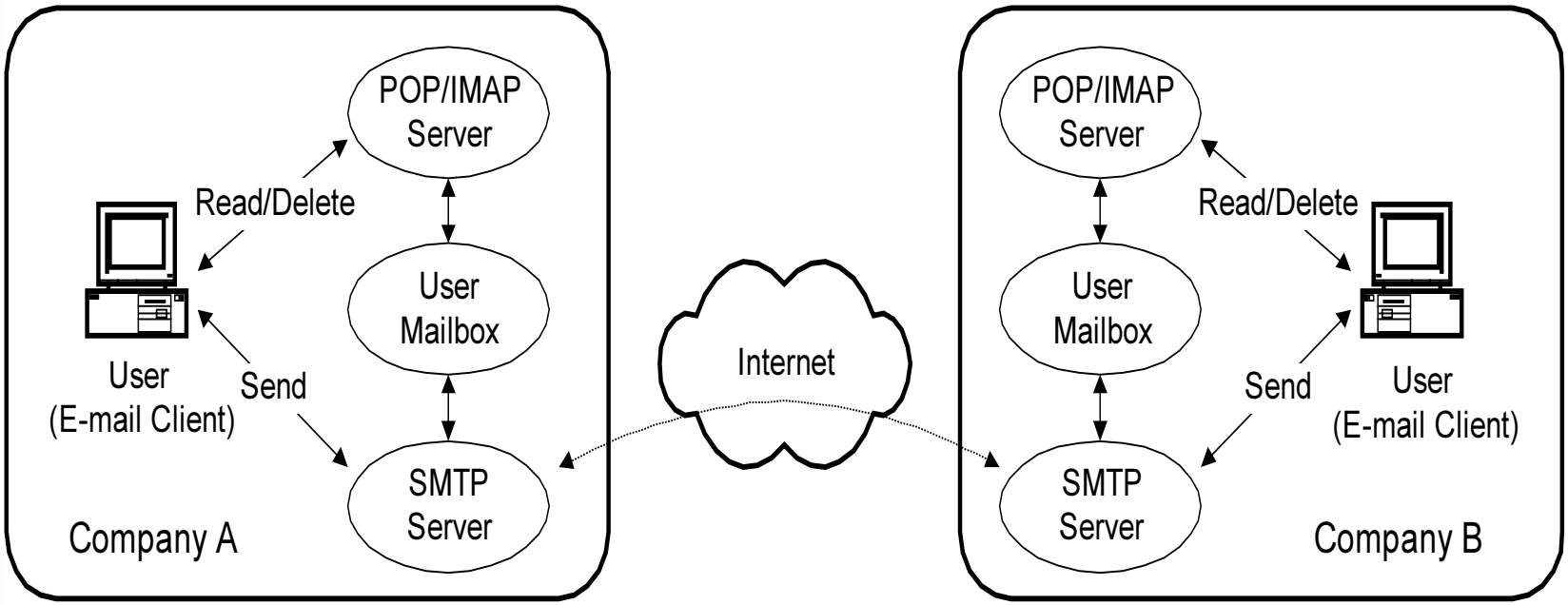
แบบฝึกหัด

- ศึกษา Configuration default ที่มากับ Linux-SIS 3.1 ใช้คำสั่ง host และ nslookup ช่วยในการวิเคราะห์ และให้ลองเพิ่มชื่อ host news.intranet ให้มี IP 192.168.1.9 เข้าไป (ทั้ง Reverse และ Forward)

SMTP Server Sendmail

- SMTP Server จะถูกใช้ในการรับและส่ง E-mail (แต่ไม่ใช่การอ่าน) ที่ใช้กันบนเครือข่ายอินเทอร์เน็ต
- ในบาง E-mail Client จะเรียกเป็น Outgoing E-mail Server

การรับ/ส่ง/อ่านจดหมายอิเล็กทรอนิกส์



MX DNS Record

- DNS MX Record จะเป็นตัวบอกว่า E-mail จะถูกส่งไปยัง SMTP Server ปลายทางตัวไหน เช่น ส่งจดหมายไปถึง ott@school.net.th SMTP Server ด้านส่ง ก็จะทำการตรวจสอบว่า DNS MX Record ของ school.net.th เป็นเครื่องไหน (user.school.net.th) จากนั้น ก็จะส่งต่อไปยังเครื่อง user.school.net.th
- ที่เครื่อง user.school.net.th ก็ต้องมี SMTP Server ทำงานอยู่
- วิธีตรวจสอบ DNS MX Record: host -t mx school.net.th
- หากไม่มี MX Record จะ check ว่าเป็นชื่อเครื่องหรือไม่ ถ้าใช่ก็ส่งไป ถ้าไม่ใช่ก็ error กลับมาหาผู้ส่ง

SMTP Server ในบทบาทหน้าที่ส่ง E-mail

- รับ E-mail จากโปรแกรมของผู้ใช้ และดูว่า E-mail Address ปลายทางเป็นที่ใด และส่งต่อไปยัง SMTP Server ปลายทาง
- การติดตั้ง
  - ต้องระบุค่า IP Range ของ Client ที่จะสามารถใช้เราเป็นตัว SMTP Server ขาส่งได้
    - /etc/mail/relays-domains

SMTP Server ในบทบาทตัวรับ E-mail

- รับ connection จาก SMTP Server ขาส่ง
- ตรวจสอบว่าจดหมายนั้นต้องการจะส่งถึงผู้ใช้ในความรับผิดชอบของเราหรือไม่ ถ้าใช่ก็รับไว้ ถ้าไม่ใช่ก็ Reject
- บาง SMTP Server ถูก set ไว้อย่างหละหลวม ใช่ไม่ใช่ก็รับหมด เป็นเหยื่อของพวกชอบส่ง spam E-mail
- การติดตั้ง: ระบุว่าโดเมนอะไรบ้างที่เป็นของผู้ใช้ในหน่วยงานเราเอง
  - /etc/sendmail.cw

Configuration เพิ่มเติม

- /etc/aliases
  - สร้าง alias รวมทั้ง mailing list อย่างง่าย
  - ตัวอย่างเนื้อหา
    - postmaster: root
    - user1: user1@school.net.th
    - user2: \user2, user2@cnn.com
    - list1: :include:/etc/mail/list1
  - แก้ไขแล้วให้สั่ง newaliases

/etc/access

- เก็บชื่อผู้ใช้, โดเมน ที่เราไม่ต้องการรับจดหมายได้ (เช่น พวกชอบส่ง Spam E-mail มา)
- ตัวอย่างเนื้อหา
  - /etc/mail/access
    - spammer@aol.com REJECT
    - cyberspammer.com REJECT
    - 206.117.147 REJECT
- แก้ไขแล้วให้สั่งดังนี้ และ restart sendmail
  - cd /etc/mail ; makemap hash access < access

/etc/mail/domaintable

- ต้องการให้เครื่องเดียวเป็น SMTP Server ของหลายๆ โดเมน
- Forward ทั้งโดเมน
  - domain1.co.th domain2.co.th
- แก้ไขแล้ว
  - cd mail ; makemap hash domaintable < domaintable
  - restart sendmail

/etc/virtusertable

- ส่งต่อจดหมายผู้ใช้ไปยังอีก E-mail หนึ่ง สามารถระบุได้เป็นรายคน ไม่ใช่ทั้งโดเมน
- ตัวอย่างเนื้อหา
  - ott@domain1.co.th pattara@domain2.co.th
- แก้ไขแล้ว
  - cd /etc/mail ; makemap hash virtusertable < virtusertable
  - restart sendmail

วิธีการทดสอบ Sendmail

- Telnet เข้า port 25
  - ดูวิธีตามตัวอย่างในหนังสือหน้า 203-204
- เรียกใช้ sendmail -bt
  - ดูวิธีตามตัวอย่างในหนังสือหน้า 204-205

แบบฝึกหัด

- ทดลองแก้ไฟล์ /etc/mail/relay-domains ให้ไม่มี IP ของเครื่อง Client PC ปรากฏอยู่ จากนั้น ทดสอบจากเครื่อง PC ว่ายังสามารถส่งจดหมายอิเล็กทรอนิกส์ออกได้อีกหรือไม่
- ทดลองแก้ไขไฟล์ /etc/mail/virtusertable ให้ทำการ forward E-mail ที่จะส่งไปถึง user1@linux.intranet ให้ไปยัง user2@linux.intranet แทน แล้วทดสอบด้วยวิธี sendmail -bt

POP/IMAP Server

- มีไว้อำนวยความสะดวกกับผู้ใช้ในการอ่านจดหมายอิเล็กทรอนิกส์
- POP จะมีวิธีการทำงานที่ง่ายกว่า แต่จะเลือกได้แค่จะดาวน์โหลด mail มาหรือไม่ จะลบบน Server ทิ้งไปเลยหรือไม่
- IMAP จะมีคุณสมบัติต่างๆ ที่ซับซ้อนมากกว่า สามารถดูเฉพาะ header ของ E-mail ก่อนได้ เลือกลบได้ สร้างแฟ้มใหม่บน Server ได้

การติดตั้ง

- แทบทุก Linux Version ในปัจจุบันจะมีการติดตั้ง POP/IMAP Server มาให้อยู่แล้ว
- ตรวจสอบใน /etc/inetd.conf ว่าบรรทัดของ pop และ imap ไม่ได้ถูก comment ไว้
- ทดสอบการใช้งานด้วยวิธี telnet เข้า port 110 (pop), 143 (imap)
  - ดูวิธีการตามหน้า 207-208 ในหนังสือ

แบบฝึกหัด

- ทดลองอ่านและส่ง E-mail ด้วยวิธี POP และ IMAP ผ่าน Linux-SIS Server ลองเปรียบเทียบว่าแตกต่างกันอย่างไร แบบไหนที่เหมาะกับการใช้งานของท่าน

Radius Server

- RADIUS = Remote Authentication Dial In User Service
- ระบบการโทรเข้าใช้งานจากอินเทอร์เน็ตในอดีต
  - ใช้วิธี Add User ที่ Terminal Server (ยุ่งยาก มีฐานข้อมูลหลายที่)
  - ใช้ Slirp (การโทรเข้ายุ่งยาก ต้องมีการ telnet, ไม่มี IP จริง โหลดเครื่อง Server)
- RADIUS
  - ฐานข้อมูลอยู่ที่ RADIUS Server ที่เดียว
  - Terminal Server ที่รับโทรศัพท์จะทำหน้าที่เป็น RADIUS Client

Radius Client

- อุปกรณ์ Terminal Server, Access Server ในปัจจุบัน จะสนับสนุน RADIUS Protocol หมด
- การติดตั้ง จะต้องใส่ชื่อของ RADIUS Server

RADIUS Server

- ต้นกำเนิดมาจากซอฟต์แวร์ Livingston Radius ของบริษัท Livingston (ปัจจุบัน Lucent)
- ปัจจุบันแตกสายย่อยออกเป็นจำนวนมาก
- Server -> Authentication Server, Accounting Server
- คุณสมบัติพิเศษ
  - เชื่อมต่อกับฐานข้อมูล
  - ตั้งค่าของ User ได้หลากหลาย
  - RADIUS Proxy

Free Radius Software

- http://www.livingston.com/tech/docs/radius/
- http://www.freeradius.org/
- http://www.miquels.cistron.nl/radius/
- ftp://ftp.cheapnet.net/pub/icradius/
- http://www.xtradius.com/

Common Configuration Files

- Radius DB: /etc/raddb , /usr/local/etc/raddb
  - clients — เก็บชื่อ Radius Client
  - dictionary — เก็บ ความหมายของ Code ต่างๆ
  - users — เก็บฐานข้อมูลผู้ใช้

วิธีตรวจสอบการทำงานของ Radius Server

- Radpwtst
  - radpwtst -I <client IP> -d “/etc/raddb” -s <radius-server-ip> -w “password” username

- ชมการสาธิตวิธีการดาวน์โหลดและติดตั้ง Radius Server