การติดตั้งอุปกรณ์ควบคุมแลนไร้สายด้วย ChilliSpot สำหรับการพิสูจน์ตัวจริงแบบเว็บล็อกอิน

Setting up a Wireless Lan Controller with ChilliSpot for Web Login Authentication

---

วิบูลย์ วราสิทธิชัย
นักวิชาการคอมพิวเตอร์ 6
ศูนย์คอมพิวเตอร์
มหาวิทยาลัยสงขลานครินทร์
2550

ชื่องานวิจัย การติดตั้งอุปกรณ์ควบคุมแลนไร้สายด้วย ChilliSpot สำหรับการพิสูจน์ตัวจริงแบบเว็บล็อกอิน

ผู้เขียน วิบูลย์ วราสิทธิชัย

ปีพ.ศ. 2550

บทคัดย่อ

เนื่องจากมีการนำอุปกรณ์แลนไร้สายราคาถูกมาใช้โดยไม่มีการจำกัดสิทธิเข้าใช้งาน การปล่อยให้ใครก็ได้เข้าใช้งานแลนไร้สายอาจเป็นช่องทางที่ผู้ไม่ประสงค์ดีหรือผู้บุกรกใช้ละเมิดสิทธิของผู้อื่นหรือเจาะระบบ/เซิร์ฟเวอร์ที่ต้องการได้ ChilliSpot ซึ่งเป็นซอฟต์แวร์โอเพ่นซอร์สสำหรับจัดการหรือควบคุมแอกเซสพอยต์แลนไร้สายจึงถูกนำมาใช้เพื่อให้มีการพิสูจน์ตัวจริงก่อนเข้าใช้งานของผู้ใช้ในรูปแบบเว็บล็อกอินซึ่งเป็นวิธีที่ได้รับความนิยมในการให้บริการ Wireless Hotspot ในปัจจุบัน งานวิจัยนี้เป็นการพัฒนาต้นแบบเซิร์ฟเวอร์ที่ใช้ ChilliSpot และซอฟต์แวร์โอเพ่นซอร์สที่เกี่ยวข้องในการพิสูจน์ตัวจริง

Title Setting up a Wireless LAN Controller with ChilliSpot for Web Login Authentication

Author Wiboon Warasittichai

Year 2007

Abstract

Since most of cheap wireless LAN network devices have been widely used without proper authentication process, a security breach in an organization information system is most likely to take place. To prevent such a case, an open source software, ChilliSpot, has been used to manage and control wireless LAN access points. ChilliSpot provides a web-based authentication which is popular among public hotspots. A prototype to set up a wireless LAN controller with ChilliSpot for web login has been developed and implemented in this research.

สารบัญ

ภาคผนวก

ขั้นตอนการติดตั้ง

การติดตั้งอุปกรณ์ควบคุมแลนไร้สายด้วย ChilliSpot สำหรับการพิสูจน์ตัวจริงแบบเว็บล็อกอิน

การติดตั้ง phpMyPrepaid 0.4b3 ใช้ร่วมกับ ChilliSpot

การเซตแอกเซสพอยต์ยี่ห้อ Linksys รุ่น WAP54G

การเซตแอกเซสพอยต์ยี่ห้อ 3Com รุ่น 3CRWE454G72

การเซตแอกเซสพอยต์ยี่ห้อ Cisco รุ่น Aironet1100 (802.11b)

การเซตไวร์เลสเร้าเตอร์ยี่ห้อ NETGEAR รุ่น DG834G

ไฟล์ firewall.iptables

ประวัติผู้เขียน

สารบัญภาพประกอบ

บทที่ 1

บทนำ

1.1 ความสำคัญและที่มาของงานวิจัย

ในขณะที่ทั่วโลกมีการใช้งานอินเทอร์เน็ตกันอย่างแพร่หลาย สถาบันการศึกษาอย่างมหาวิทยาลัยก็เช่นเดียวกัน อาจารย์ บุคลากร และนักศึกษาต่างก็มีความต้องการใช้งานอินเทอร์เน็ตในการติดต่อสื่อสารหรือค้นคว้าวิจัยเป็นอย่างมาก ทำให้เกิดการใช้เครือข่ายคอมพิวเตอร์ทั้งจากผู้ใช้งานที่ใช้เครื่องคอมพิวเตอร์ตามสำนักงานหรือห้องปฏิบัติการคอมพิวเตอร์ที่เชื่อมต่อเครือข่ายแบบใช้สายที่เรียกว่าแลน (Local Area Network: LAN) และผู้ใช้งานที่ใช้เครื่องคอมพิวเตอร์เช่น โน้ตบุ๊ค ที่เชื่อมต่อเครือข่ายแบบไร้สายที่เรียกว่าแลนไร้สาย (Wireless LAN)

ผู้วิจัยพบว่าภายในมหาวิทยาลัยสงขลานครินทร์นั้น มีการนำอุปกรณ์แลนไร้สายราคาถูก เช่น แอกเซสพอยต์ (Access Point) หรือไวร์เลสเร้าเตอร์ (Wireless Router) เป็นต้น มาใช้กันแล้วเป็นจำนวนมาก เพราะว่าอุปกรณ์ประเภทนี้หาซื้อได้ง่าย นำมาใช้โดยต่อเข้ากับแลนของอาคาร ส่วนใหญ่ไม่มีการจำกัดสิทธิเข้าใช้งานอุปกรณ์เหล่านี้ เครื่องคอมพิวเตอร์เครื่องใดก็ได้ที่เชื่อมต่อสัญญาณเครือข่ายได้แล้วก็มีสิทธิใช้งานทันที แต่การปล่อยให้ใครก็ได้เข้าใช้งานแลนไร้สายอาจเป็นช่องทางที่ผู้ไม่ประสงค์ดีหรือผู้บุกรุกใช้ละเมิดสิทธิของผู้อื่นหรือเจาะระบบ/เซิร์ฟเวอร์ที่ต้องการได้ แต่ก็มีอยู่บ้างที่มีการป้องกันการเข้าใช้โดยใช้วิธีการกำหนดรหัสผ่านให้กับอุปกรณ์และแจ้งรหัสผ่านให้กับผู้ต้องการใช้เป็นราย ๆ ไป

ส่วนอุปกรณ์ที่มีความสามารถมากขึ้น ซึ่งก็มักจะมีราคาสูงขึ้น จะมีความสามารถในการพิสูจน์ตัวจริง (Authentication) เช่น แอกเซสพอยต์บางรุ่น เป็นต้น กำหนดให้มีการพิสูจน์ตัวจริงกับ RADIUS Server ซึ่งเป็นวิธีที่จะต้องตั้งค่าที่ตัวอุปกรณ์นั้น หากมีหลายตัวก็จะต้องทำทุกตัว

บริษัทชั้นนำหลาย ๆ บริษัทที่ขายโซลูชันด้านระบบแลนไร้สาย จะมีอุปกรณ์ราคาสูงที่มีการรักษาความปลอดภัยให้เลือกใช้งานตั้งแต่ระดับพื้นฐานจนถึงระดับสูง หนึ่งในโซลูชันดังกล่าวคือระบบจัดการแลนไร้สายที่มีการป้องกันการเข้าใช้งานด้วยการให้มีการพิสูจน์ตัวจริงเมื่อมีการร้องขอใช้อินเทอร์เน็ตในรูปแบบที่เรียกว่าเว็บล็อกอิน (Web Login) ซึ่งเป็นวิธีที่ได้รับความนิยมในการให้บริการ Wireless Hotspot เพราะว่าแอกเซสพอยต์ทุกตัวจะถูกควบคุมด้วยอุปกรณ์ควบคุมแลนไร้สาย (Wireless LAN Controller) ระบบดังกล่าวถูกออกแบบมาให้ใช้งานได้ง่ายและสะดวกอย่างมาก

ระบบจัดการแลนไร้สายมีให้ใช้งานแบบโอเพ่นซอร์ส (Open Source) ด้วย โดยการติดตั้งซอฟต์แวร์จัดการแลนไร้สายในเครื่องคอมพิวเตอร์พร้อมทั้งตั้งค่าการทำงานที่เหมาะสมกับองค์กรหรือสถานที่ใช้งาน

งานวิจัยนี้นำเสนอการพัฒนาต้นแบบการรักษาความปลอดภัยแลนไร้สายสำหรับแอกเซสพอยต์ราคาถูกด้วยวิธีการพิสูจน์ตัวจริงแบบเว็บล็อกอินโดยใช้ซอฟต์แวร์โอเพ่นซอร์ส เพื่อติดตั้งให้บริการ Wireless Hotspot

1.2 การตรวจเอกสาร

ซอฟต์แวร์จัดการแลนไร้สายชนิดโอเพ่นซอร์สที่มีวิธีการพิสูจน์ตัวจริงเพื่อเข้าใช้งานแบบเว็บล็อกอินนั้นมีหลายตัว แต่ที่ใช้กับระบบปฏิบัติการ Linux มีดังต่อไปนี้

- ChilliSpot
- NoCat
- WiFiDog

ผู้วิจัยพบว่า ChilliSpot เป็นซอฟต์แวร์ที่มีการกล่าวถึงในเว็บไซต์และบล็อกต่าง ๆ เป็นจำนวนมาก แสดงให้เห็นได้ว่าเป็นซอฟต์แวร์ที่กำลังอยู่ในความสนใจของผู้บริหารข่ายงาน (Network Administrator) ทั่วโลก ในขณะที่มีเว็บไซต์ที่กล่าวถึง WiFiDog อยู่บ้าง ส่วน NoCat นั้นหยุดพัฒนาไปแล้วตั้งแต่ปี ค.ศ. 2004

เมื่อวิเคราะห์ดูระหว่าง ChilliSpot กับ WiFiDog พบข้อแตกต่างที่เป็นจุดเด่นของ ChilliSpot ก็คือ ChilliSpot มีการพิสูจน์ตัวจริงกับ RADIUS Server ซึ่งมีความยืดหยุ่นในการเลือกใช้ฐานข้อมูลใดก็ได้ เช่น Text File, LDAP หรือ MySQL เป็นต้น ในขณะที่ WiFiDog นั้นระบุว่าการพิสูจน์ตัวจริงใช้ฐานข้อมูล PostgreSQL ในการเก็บชื่อผู้ใช้และรหัสผ่านเท่านั้น

จากการศึกษารายละเอียดในเว็บไซต์ที่เป็นทางการของ ChilliSpot [1] มีคำอธิบายไว้ดังนี้ ChilliSpot คือซอฟต์แวร์โอเพ่นซอร์สประเภท Captive Portal หรือ Wireless LAN Access Point Controller ใช้สำหรับการพิสูจน์ตัวจริงเพื่อเข้าใช้งานแลนไร้สาย สนับสนุนวิธีเว็บล็อกอินซึ่งเป็นคุณสมบัติมาตรฐานที่จะต้องมีใน Hotspot สาธารณะในปัจจุบัน สามารถเลือกใช้ RADIUS Server ใด ๆ ในการพิสูจน์ตัวจริง การกำหนดสิทธิ การบันทึกการใช้งาน สิ่งที่ต้องใช้ในการสร้าง Wireless Hotspot มีดังต่อไปนี้

- Internet Connection
- Wireless LAN Access Point

- ChilliSpot
- RADIUS Server
- Web Server

จากการค้นหาเว็บไซต์ที่ให้คำแนะนำการติดตั้ง ChilliSpot ในอินเทอร์เน็ต พบว่ามีอยู่หลายเว็บไซต์ แต่ที่ตรงกับความต้องการในการทำวิจัย มีดังนี้

เว็บไซต์ WifiDocs/ChillispotHotspot – Community Ubuntu Documentation [2] มีคำอธิบายว่า ChilliSpot เป็นซอฟต์แวร์ที่ใช้ในการพิสูจน์ตัวจริงและจำกัดการเข้าถึงเครือข่ายของไคลเอนต์ที่จะใช้แลนไร้สาย พร้อมทั้งกล่าวถึงซอฟต์แวร์ที่จำเป็นในการติดตั้งเพิ่มเติมลงไปในเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Linux Ubuntu ดังนี้

- ChilliSpot 1.0
- FreeRADIUS 1.0.x
- Apache 2.x
- MySQL 4.1.x

และมีคำอธิบายคร่าว ๆ ถึงโปรแกรมชื่อ phpMyPrepaid ที่จะสามารถนำมาใช้ในการจัดการบัญชีผู้ใช้

เว็บไซต์ wireless: Chillispot Howto [3] อธิบายว่าวิธีที่กำลังทำอยู่นี้คือการติดตั้งเกตเวย์ (Gateway) ที่จะบังคับผู้ใช้ให้ลงบันทึกเข้าใช้งาน เกตเวย์จะมีอินเตอร์เฟสเชื่อมต่อเครือข่าย 2 อินเตอร์เฟส อินเตอร์เฟสแรก (eth0) จะเป็นแลนการ์ด (LAN Card) ที่ต่อกับอินเทอร์เน็ต ส่วนอีกอินเตอร์เฟส (eth1) ต่อกับเครือข่ายภายในซึ่งจะเป็นได้หลายอย่าง อาจเป็แลนการ์ดที่ต่อกับแลนสวิตช์ (LAN Switch) ที่มีเครื่องคอมพิวเตอร์หรือแอกเซสพอยต์จำนวนหนึ่ง หรืออาจเป็นแลนการ์ดไร้สาย (Wireless LAN Card) ที่ทำให้เกตเวย์นี้เป็นแอกเซสพอยต์ไปในตัว พร้อมทั้งกล่าวถึงซอฟต์แวร์ที่เลือกใช้ติดตั้งลงไปในระบบปฏิบัติการ Linux Ubuntu ดังนี้

- ChilliSpot
- FreeRADIUS
- Apache Web Server
- MySQL

เว็บไซต์ Authenticated Wireless Network w/ Open Source Tools [4] อธิบายว่ามีวิธีการรักษาความปลอดภัยแลนไร้สายอยู่หลายวิธี แต่ไม่ว่าจะเลือกใช้วิธีไหนก็จำเป็นต้องทำการตั้งค่าอย่างใดอย่างหนึ่งที่ไคลเอนต์ เช่น Shared Key หรือ Certificate เป็นต้น ซึ่งไม่สะดวกสำหรับบริการ Wireless Hotspot แต่การติดตั้งตามคำแนะนำในเว็บไซต์นี้จะเป็นวิธีที่ง่ายกว่ามาก มีความ

ปลอดภัย (เพราะรหัสผ่านถูกเข้ารหัส) และมีการพิสูจน์ตัวจริงกับ LDAP ซึ่งเป็นฐานข้อมูลที่ใช้งานจริง พร้อมทั้งแนะนำซอฟต์แวร์ที่ใช้ในการติดตั้งบนระบบปฏิบัติการ Linux RedHat ดังต่อไปนี้

- ChilliSpot 1.0
- FreeRADIUS 1.0.1
- IPTABLES (Linux Kernel 2.4.21-37)
- Squid Proxy Server 2.5.STABLE3

จากข้อมูลของเว็บไซต์ที่กล่าวไปแล้วข้างต้น สรุปได้ว่ามีผู้ที่ศึกษาใช้ ChilliSpot ในการพิสูจน์ตัวจริงเพื่อเข้าใช้งานกับ FreeRADIUS ซึ่งเป็นซอฟต์แวร์โอเพ่นซอร์ส แต่เลือกใช้ฐานข้อมูลที่แตกต่างกันคือ Text File, MySQL และ LDAP ซึ่งเป็นความสามารถของ FreeRADIUS ที่ให้ตั้งค่าการทำงานได้ตรงกับความต้องการใช้ฐานข้อมูล นอกจากนี้มีการนำโปรแกรม Squid มาติดตั้งเป็นพร็อกซี่เซิร์ฟเวอร์แบบ Tranparent Proxying และมีคำอธิบายคร่าว ๆ ถึงโปรแกรมชื่อ phpMyPrepaid ที่ใช้สร้างบัญชีผู้ใช้ลงในฐานข้อมูล MySQL เพื่อใช้งานร่วมกับ FreeRADIUS แต่เนื่องจากงานที่ศึกษาเหล่านี้อยู่กระจัดกระจายในหลายที่ และไม่มีรายระเอียดที่เพียงพอ ผู้วิจัยจึงค้นคว้าเพิ่มเติมจากเว็บไซต์อื่นๆ อีกหลายเว็บ แล้วนำมารวบรวมสร้างเป็นต้นแบบและเขียนคำแนะนำในฉบับภาษาไทยเพื่อให้ง่ายต่อการศึกษาค้นคว้าของผู้สนใจ

1.3 วัตถุประสงค์

1. เพื่อการรักษาความปลอดภัยแลนไร้สายสำหรับแอกเซสพอยต์ราคาถูกให้มีวิธีการพิสูจน์ตัวจริงเพื่อเข้าใช้งานในรูปแบบเว็บล็อกอินโดยใช้ซอฟต์แวร์โอเพ่นซอร์ส
2. เพื่อติดตั้งให้บริการ Wireless Hotspot อย่างง่าย
3. เพื่อเป็นแนวทางให้กับผู้บริหารข่ายงานและผู้ที่สนใจทั่วไป

1.4 ขอบเขตการดำเนินงาน

1. สร้างต้นแบบการรักษาความปลอดภัยแลนไร้สายสำหรับแอกเซสพอยต์ราคาถูกที่ใช้วิธีการพิสูจน์ตัวจริงแบบเว็บล็อกอินโดยใช้ซอฟต์แวร์โอเพ่นซอร์ส
2. ต้นแบบเป็นวิธีการที่เหมาะสมกับการให้บริการ Wireless Hotspot
3. จัดทำเว็บเพจเผยแพร่ความรู้ชนิด How To เพื่อเป็นแหล่งความรู้สำหรับผู้สนใจ

1.5 ขั้นตอนการดำเนินงานวิจัย

1. ศึกษาและค้นคว้าเอกสารที่เกี่ยวข้องกับงานวิจัย
2. รวบรวมแนวคิด และเลือกเทคโนโลยีสำหรับการพัฒนาต้นแบบ
3. พัฒนาต้นแบบจากแนวคิดที่ทำการศึกษา
4. ทดสอบการทำงานของต้นแบบ
5. สรุปผลการทดสอบ และจัดทำเอกสารประกอบการวิจัย

1.6 ระยะเวลาการดำเนินงาน

มกราคม - ธันวาคม พ.ศ. 2550

1.7 เครื่องมือและอุปกรณ์ที่ใช้ในงานวิจัย

ฮาร์ดแวร์

- เครื่องไมโครคอมพิวเตอร์ 1 เครื่อง
  - หน่วยประมวลผลกลาง Pentium III 667 MHz
  - หน่วยความจำ 512 MB
  - ฮาร์ดดิสก์ 20 GB
- แลนการ์ด 10/100 Mbps จำนวน 2 การ์ด
- แอกเซสพอยต์และไวร์เลสเร้าเตอร์จำนวนหนึ่ง
  - แอกเซสพอยต์ยี่ห้อ Linksys รุ่น WAP54G
  - แอกเซสพอยต์ยี่ห้อ 3Com รุ่น 3CRWE454G72
  - แอกเซสพอยต์ยี่ห้อ Cisco รุ่น Aironet1100
  - ไวร์เลสเร้าเตอร์ยี่ห้อ NETGEAR รุ่น DG834G

ซอฟต์แวร์

- ระบบปฏิบัติการ Linux Fedora Core 6
- ChilliSpot 1.1.0
- FreeRADIUS 1.1.3
- Apache 2.2.3

- MySQL 5.0.27
- Squid 2.6.STABLE13
- phpMyPrepaid 0.4 beta3

1.8 ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถนำแอกเซสพอยต์ราคาถูกมาใช้งานได้อย่างปลอดภัยเพราะมีการพิสูจน์ตัวจริงเพื่อเข้าใช้งาน
2. สามารถติดตั้งให้บริการ Wireless Hotspot ในสำนักงาน หรือสถานที่จัดประชุม/สัมมนาที่ยังไม่มีระบบจัดการแลนไร้สาย
3. สามารถนำเครื่องคอมพิวเตอร์ราคาถูกหรือที่เหลือใช้มาทำเป็นเซิร์ฟเวอร์สำหรับการพิสูจน์ตัวจริง
4. จัดอบรมให้ความรู้ในการติดตั้งเซิร์ฟเวอร์สำหรับการพิสูจน์ตัวจริงแก่ผู้บริหารข่ายงานของมหาวิทยาลัย
5. ผู้สนใจสามารถทำด้วยตนเองโดยศึกษาจากเว็บเพจเผยแพร่ความรู้ชนิด How TO ที่เขียนขึ้น

1.9 สรุปท้ายบท

เนื้อหาในบทแรกนี้ เป็นการนำเสนอความสำคัญและที่มาของงานวิจัย การตรวจเอกสารจากเว็บไซต์ต่าง ๆ ที่มีการทำในเรื่องนี้มาก่อน และกำหนดขอบเขตของการพัฒนาต้นแบบการรักษาความปลอดภัยแลนไร้สายสำหรับแอกเซสพอยต์ราคาถูกด้วยวิธีการพิสูจน์ตัวจริงแบบเว็บล็อกอินโดยใช้ซอฟต์แวร์โอเพ่นซอร์ส รายละเอียดของหลักการและเทคโนโลยีที่เกี่ยวข้องจะนำเสนอในบทที่ 2 สำหรับในบทที่ 3 นำเสนอแนวคิดในการสร้างต้นแบบ บทที่ 4 นำเสนอขั้นตอนการติดตั้ง และบทที่ 5 นำเสนอผลสรุปโครงงานพร้อมทั้งข้อเสนอแนะ

บทที่ 2

หลักการและเทคโนโลยีที่เกี่ยวข้อง

ในบทนี้นำเสนอหลักการพื้นฐานและเทคโนโลยีทางด้านเครือข่ายที่เกี่ยวข้องสำหรับงานวิจัยนี้

2.1 รูปแบบการใช้งานแลนไร้สายประเภทต่าง ๆ [5]

เพื่อให้สามารถออกแบบระบบแลนไร้สายให้มีลักษณะตรงตามความต้องการใช้งานของผู้ใช้แต่ละประเภท สามารถแบ่งออกเป็นประเภทต่าง ๆ ได้ดังต่อไปนี้

1. แลนไร้สายภายในบ้าน

ส่วนใหญ่จะเป็นการเชื่อมต่อโน้ตบุ๊คที่ซื้อมาใหม่กับเครื่องเดสก์ท็อปเข้าด้วยกันผ่าน Wireless ADSL Router อุปกรณ์นี้เป็นทั้ง ADSL Modem, Access Point และ Switch/Hub นั่นทำให้สามารถทั้งต่อคอมพิวเตอร์แบบมีสายและไร้สายเข้าด้วยกัน ใช้อินเทอร์เน็ตผ่าน ADSL Modem ได้ แลนไร้สายคลอบคลุมพื้นที่ทุก ๆ จุดในบ้านโดยใช้แอกเซสพอยต์จากอุปกรณ์นี้ อุปกรณ์ชนิดนี้ติดตั้งง่าย เสียบปลั๊กแล้วก็ใช้งานได้เลย

แนวทางในการออกแบบเครือข่ายในบ้านจึงเน้นด้านความสามารถในการเชื่อมต่อเป็นหลัก การกำหนดจุดติดตั้งเป็นเรื่องที่สำคัญมาก เพราะจะทำให้สามารถใช้งานแลนไร้สายได้ทั่วบ้าน ส่วนเรื่องการรักษาความปลอดภัยนั้นเป็นเรื่องรอง ไม่มากเท่าการใช้ในสำนักงาน เพราะในบ้านคงไม่มีข้อมูลที่สำคัญมากนัก แต่ก็เป็นสิ่งที่ละเลยไม่ได้เพราะอาจจะมีผู้ลักลอบเข้ามาใช้เครือข่ายได้ง่าย ๆ

2. แลนไร้สายในอาคารสำนักงาน

การใช้งานแลนไร้สายนี้จะเป็นการใช้อินเทอร์เน็ตเพื่อค้นหาข้อมูล ส่งอีเมลให้ลูกค้า รับส่งข้อมูลขนาดใหญ่ให้กับเพื่อนร่วมงานในองค์กร การพิมพ์งาน หรือการเข้าสู่ฐานข้อมูล

ปัญหาเรื่องความเร็วในการใช้งานเป็นปัญหาที่ละเลยไม่ได้ ควรติดตั้งแอกเซสพอยต์ไว้ในบริเวณที่มีผู้ใช้งานหนาแน่นและให้คลอบคลุมพื้นที่ของสำนักงาน แต่ปัญหาหลักของแลนไร้สายในอาคารสำนักงานก็คือเรื่องความปลอดภัย ต้องมั่นใจได้ว่าจะไม่มีผู้ใช้จากสำนักงานข้าง ๆ ลักลอบเข้ามาใช้เครือข่ายของคุณและไม่ถูกแฮคข้อมูลที่เป็นความลับทางการค้า ซึ่งการเลือกซื้อแอกเซสพอยต์หลายยี่ห้อและประสิทธิภาพที่ไม่เท่าเทียมกันจะทำให้ยากทั้งการ

จัดการและบริหารเครือข่าย ควรเลือกซื้ออุปกรณ์ยี่ห้อเดียวกันที่สามารถอัพเกรดระบบรักษาความปลอดภัยได้ มีเซิร์ฟเวอร์สำหรับตรวจสอบรหัสผ่านก่อนเข้าใช้งานแลนไร้สายด้วยก็จะเป็นการดีมาก

3. แลนไร้สายแบบ Hotspot ในร้านกาแฟ/ที่พักผู้โดยสารขาออก

เครือข่ายในจุด Hotspot ประเภทนี้ ลักษณะการวางเครือข่ายนั้นไม่ยากเพียงแค่ติดตั้ง ADSL Router ไว้ที่ร้านและเชื่อมต่อเข้ากับเซิร์ฟเวอร์ของผู้ให้บริการอินเทอร์เน็ตที่จะทำหน้าที่ตรวจสอบชื่อผู้ใช้และรหัสผ่านทุกครั้งที่ใช้งาน ส่วนปัญหาเรื่องพื้นที่การให้บริการนั้นเนื่องจากร้านเหล่านี้มีพื้นที่ขนาดเล็ก คลื่นจึงสามารถเดินทางไปได้ทั่วร้าน แต่ก็อาจมีปัญหาคลื่นรบกวนกันได้หากร้านกาแฟตั้งอยู่ในศูนย์การค้าที่มีผู้ให้บริการแลนไร้สายรายอื่นอยู่ด้วยจึงเป็นเรื่องหนึ่งที่ต้องคำนึงถึง

4. แลนไร้สายในสถานศึกษา

ลักษณะการใช้งานแลนไร้สายในมหาวิทยาลัยนี้ต้องใช้งบประมาณสูงมาก ๆ เพราะต้องติดตั้งแลนไร้สายในคณะต่าง ๆ หอประชุม ห้องเรียน ห้องสัมมนาต่าง ๆ มากมาย การบริหารเครือข่ายก็ทำได้ยากเช่นกัน เพราะจำนวนแอกเซสพอยต์ที่ต้องบริหารก็มีนับสิบถึงร้อยตัว นอกจากนี้ปริมาณการใช้งานในจุดต่าง ๆ ก็ต่างกันมาก ๆ เช่น หอประชุม บางครั้งก็มีผู้เข้าร่วมงานที่ต้องการใช้แลนไร้สายจำนวนมาก หรือบางครั้งก็ไม่มีเลย

การออกแบบแลนไร้สายของสถานศึกษาจะต้องคำนึงถึงเรื่องการบริหารความถี่ไม่ให้เกิดปัญหาคลื่นรบกวนกัน เลือกติดตั้งแอกเซสพอยต์ในจุดที่มีผู้ใช้งานมาก ๆ ส่วนปัญหาเรื่องการรักษาความปลอดภัยนั้นก็เป็นเรื่องที่ละเว้นไม่ได้คล้ายกับการวางเครือข่ายในสำนักงาน แต่แลนไร้สายของสถานศึกษาจะมีลักษณะคล้ายเครือข่ายสาธารณะที่มีการรักษาความปลอดภัย ระบบจะต้องเข้าใช้งานง่ายแต่จะต้องมีการรักษาความปลอดภัย

2.2 การรักษาความปลอดภัยแลนไร้สายด้วยคุณสมบัติของแอกเซสพอยต์ [5]

สืบเนื่องจากเครื่องคอมพิวเตอร์ไร้สายและอุปกรณ์ในแลนไร้สายใช้คลื่นวิทยุสื่อสารข้อมูลระหว่างกัน ซึ่งเราไม่สามารถมองเห็นการแพร่กระจายคลื่นวิทยุและขอบเขตพื้นที่ให้บริการได้ด้วยตาเปล่า ทำให้ยากแก่การป้องกันและตรวจสอบผู้บุกรุกเข้ามาโจรกรรมข้อมูลและลักลอบเข้าใช้งานเครือข่าย จริง ๆ แล้วแลนไร้สายเองมีโซลูชันความปลอดภัยให้เลือกใช้งานตั้งแต่ระดับพื้นฐานจนถึงระดับสูง ดังนี้

1. ควบคุมการเชื่อมโยงเข้าสู่เครือข่ายด้วย SSID (Service Set Identifier)

Service Set Identifier นอกจากจะใช้เป็นสื่ออ้างอิง Service Set ของแลนไร้สายแล้ว ยังสามารถใช้เป็นกลไกควบคุมการเชื่อมโยงเข้าสู่แลนไร้สายของเครื่องคอมพิวเตอร์ไร้สายแต่ละเครื่องได้อีกด้วย เครื่องคอมพิวเตอร์ไร้สายที่ต้องการเชื่อมโยงเข้าเครือข่ายจะต้องกำหนด SSID ของตนเองให้เป็นชื่อเดียวกันกับชื่อ SSID ของแอกเซสพอยต์ที่บริการในพื้นที่นั้น ๆ บุคคลภายนอกที่มีเครื่องคอมพิวเตอร์ไร้สายแต่ไม่ทราบ SSID ก็จะไม่สามารถเชื่อมโยงเข้าสู่แลนไร้สายได้

2. กลั่นกรองผู้ใช้งานด้วยการทำ MAC Address Filtering

MAC Address เป็นชุดตัวเลขฐานสิบหกขนาด 6 ไบต์ (Byte) ตัวอย่างเช่น 0C:14:3A:29:2F:AA ค่านี้ใช้สำหรับอ้างอิงที่อยู่กายภาพ (Physical Address) ของแลนการ์ดไร้สาย ซึ่งแลนการ์ดไร้สายที่ผลิตออกมาจำหน่ายจะมีค่า MAC Address ประจำตัวที่ไม่ซ้ำกัน เราจึงสามารถใช้วิธีตรวจสอบและกลั่นกรอง MAC Address ของแลนการ์ดไร้สายของเครื่องคอมพิวเตอร์ก่อนที่จะเชื่อมโยงเข้าสู่แลนไร้สาย

แอกเซสพอยต์จะทำหน้าที่เป็นผู้ตรวจสอบและกลั่นกรองเครื่องคอมพิวเตอร์ไร้สายว่ามีเครื่องใดบ้างที่อยู่ใน List ได้รับอนุญาต โดยการนำ MAC Address ของแลนการ์ดไร้สายบนเครื่องคอมพิวเตอร์ที่ต้องการเชื่อมโยงมาเปรียบเทียบกับค่า MAC Address ในฐานข้อมูลบนตัวแอกเซสพอยต์ หากค้นพบว่า MAC Address ตรงกับที่มีอยู่ในฐานข้อมูล แอกเซสพอยต์จะอนุญาตให้เครื่องคอมพิวเตอร์ไร้สายเครื่องนั้นสื่อสารข้อมูลผ่านตัวแอกเซสพอยต์ไปยังเครือข่าย

3. Wired Equivalency Privacy (WEP) เป็นวิธีป้องกันแบบเก่าซึ่งอาศัยการเข้ารหัส/ถอดรหัส ด้วยวิธี RC4

ข้อมูลที่สื่อสารกันระหว่างอุปกรณ์บนแลนไร้สาย มักจะอยู่ในรูปของข้อมูลที่ไม่มีการเข้ารหัส หรือเรียกว่า “Plain Text Message” หรือ “Clear Text” ทำให้ผู้บุกรุกสามารถโจรกรรมข้อมูลที่กำลังสื่อสาร โดยใช้โปรแกรมประเภท Packet Sniffer ดักจับข้อมูลที่แพร่กระจายออกมาในอากาศ

มาตรฐาน IEEE802.11 จึงได้มีการกำหนดเรื่องความปลอดภัยในการสื่อสารข้อมูลบนแลนไร้สายขึ้นมา เพื่อให้อุปกรณ์ไร้สายที่สนับสนุนมาตรฐาน IEEE802.11 สามารถใช้ WEP เพื่อการสร้างความปลอดภัยแก่ข้อมูลที่สื่อสารโดยอาศัยกลไกเข้ารหัส/ถอดรหัสแบบ RC4 ก่อนส่งและรับข้อมูล การใช้งาน WEP ผู้ใช้จะต้อง Enable ฟังก์ชัน WEP และกำหนดค่าคีย์ที่มีขนาด 64 บิต หรือ 128 บิต บนตัวอุปกรณ์แลนไร้สาย เช่น แอกเซสพอยต์และเครื่องคอมพิวเตอร์ไร้สาย เป็นต้น ซึ่งอุปกรณ์ทุกเครื่องบนเครือข่ายต้องกำหนดคีย์เป็นค่าเดียวกัน

4. พิสูจน์ตัวจริงเพื่อเข้าใช้งานแลนไร้สายด้วย RADIUS Server

การป้องกันผู้บุกรุกลักลอบเข้าใช้งานแลนไร้สายและโจรกรรมข้อมูลสำหรับองค์กรที่ต้องการความปลอดภัยข้อมูลในระดับสูง สามารถใช้การพิสูจน์ตัวจริงเพื่อเข้าใช้งานเครือข่ายตามมาตรฐาน IEEE802.1X เพื่อเสริมจุดอ่อนความปลอดภัยของแลนไร้สายที่ใช้ WEP ทุก ๆ ครั้งเมื่อผู้ใช้งานเครื่องคอมพิวเตอร์ไร้สายต้องการเชื่อมโยงเข้าสู่เครือข่ายผ่านแอกเซสพอยต์จะต้องถูกพิสูจน์ตัวจริงก่อนโดยอาศัย Remote Authentication Dial-In User Service (RADIUS) Server หรือที่เรียกว่า RADIUS Server ทำหน้าที่เป็นผู้ตรวจสอบและอนุญาตการเข้าใช้งาน ภายใน RADIUS Server จะมีฐานข้อมูลชื่อผู้ใช้และรหัสผ่านของผู้ใช้เก็บอยู่ ผู้ที่มีสิทธิเข้าใช้งานแลนไร้สายจะต้องมีบัญชีผู้ใช้อยู่ในฐานข้อมูลของ RADIUS Server เท่านั้น

ในกระบวนการพิสูจน์ตัวจริงตามมาตรฐาน IEEE802.1X เครื่องคอมพิวเตอร์ไร้สาย แอกเซสพอยต์ และ RADIUS Server สื่อสารข้อมูลกันด้วยโพรโทคอล EAP (Extensible Authentication Protocol) ได้มีการพัฒนาโพรโทคอลสำหรับการพิสูจน์ตัวจริงต่อยอดจาก EAP เป็น PEAP (Protected Extensible Authentication Protocol) เพื่อเพิ่มประสิทธิภาพในกระบวนการพิสูจน์ตัวจริงเพื่อเข้าใช้งานเครือข่ายด้วย Certificate

5. สร้าง Virtual Private Network (VPN) บนแลนไร้สาย

การเพิ่มความปลอดภัยให้กับข้อมูลที่กำลังสื่อสารบนแลนไร้สายจากการโจรกรรมข้อมูลของผู้บุกรุกมีอยู่อีกวิธีหนึ่งคือ Virtual Private Network กลไกของ VPN คือ สร้างอุโมงค์ หรือท่อ (VPN Tunnel) ขึ้นมาใช้เป็นช่องทางที่ปลอดภัยสำหรับการสื่อสารข้อมูลระหว่างเครื่องคอมพิวเตอร์ไร้สายกับเครือข่ายหลัก โดยผู้ใช้งานจะต้องติดตั้งโปรแกรม VPN Client ลงบนเครื่องคอมพิวเตอร์ไร้สายของตนเอง โปรแกรมดังกล่าวจะทำหน้าที่สร้าง VPN Tunnel ผ่านแอกเซสพอยต์ไปยัง VPN Server เพื่อเชื่อมเข้าสู่เครือข่ายหลักอีกที VPN Tunnel ที่สร้างขึ้นช่วยป้องกันไม่ให้ผู้บุกรุกดักจับข้อมูลที่กำลังสื่อสารบนแลนไร้สาย โดยที่แอกเซสพอยต์และเครื่องคอมพิวเตอร์ไร้สายไม่จำเป็นต้องใช้การเข้า/ถอดรหัส WEP เลย

6. Wi-Fi Protected Access (WPA) เป็นวิธีการป้องกันแบบใหม่ที่มีความปลอดภัยมากกว่า

Wi-Fi Protected Access (WPA) เป็นมาตรฐานความปลอดภัยข้อมูลที่พัฒนาขึ้นมาโดยองค์กร Wi-Fi Alliance (WECA) เพื่อแก้ไขจุดอ่อนของ WEP ในเรื่องการเข้ารหัสข้อมูล ถูกประกาศให้เป็นมาตรฐานในเดือนพฤศจิกายน ค.ศ. 2002 การพัฒนา WPA อยู่บนพื้นฐานเดียวกับมาตรฐาน IEEE802.11i ของสถาบันวิศวกรรมไฟฟ้าและอิเล็กทรอนิกส์ (IEEE) WPA จะถูกนำมาใช้แทน WEP เพื่อแก้ไขจุดอ่อนเรื่องการเข้ารหัส/ถอดรหัสข้อมูลด้วย WEP Key โดยการ

นำเอา Dynamic Key Distribution และการตรวจสอบและพิสูจน์ตัวจริง IEEE802.1X มารวมไว้เป็นกลไกของ WPA อุปกรณ์ไร้สายที่สนับสนุนมาตรฐาน WPA จะมีแบบวิธีให้เลือก 2 แบบวิธีดังนี้

- WPA Pre-Shared Key

แบบวิธี Pre-Shared Key ออกแบบมาสำหรับแลนไร้สายที่ใช้ภายในบ้านหรือในสำนักงานขนาดเล็ก (Home Office Small Office: SOHO) เพื่อสร้างความปลอดภัยให้แก่ข้อมูล เนื่องจากแบบวิธีนี้ไม่ต้องการ RADIUS Server สำหรับการตรวจสอบและพิสูจน์ตัวจริง Pre-Shared Key จะใช้กลไกการเข้า/ถอดรหัสข้อมูลสองแบบคือ แบบแรกใช้ TKIP (Temporal Key Integrity Protocol) ร่วมกับ MIC (Message Integrity Checking) และแบบที่สอง AES (Advanced Encryption Standard)

- WPA RADIUS/IEEE802.1X

โหมดการทำงานนี้จะคล้ายกับการใช้ WEP ร่วมกับ IEEE802.1X เพียงแต่เปลี่ยนกลไกการเข้ารหัส/ถอดรหัสข้อมูลจาก WEP เป็น TKIP หรือ AES เท่านั้น หลักการก็คือใช้ RADIUS Server ทำหน้าที่คอยตรวจสอบและพิสูจน์ตัวจริงก่อนการเชื่อมโยงเครื่องคอมพิวเตอร์ไร้สายเข้าสู่ระบบและในระหว่างการสื่อสารข้อมูลของแอกเซสพอยต์กับเครื่องคอมพิวเตอร์ไร้สาย ข้อมูลถูกเข้ารหัสด้วยคีย์ที่แตกต่างกันและคีย์เข้ารหัสจะถูกเปลี่ยนไปเรื่อย ๆ อัตโนมัติ ทำให้ผู้บุกรุกคาดเดาคีย์ได้ลำบากและยังต้องเจอการพิสูจน์ตัวจริงก่อนผ่านเข้าระบบอีกด้วย

7. จำกัดขอบเขตพื้นที่ให้บริการด้วยการควบคุมกำลังส่งของแอกเซสพอยต์

แอกเซสพอยต์บางยี่ห้อออกแบบมาให้มีฟังก์ชันปรับเปลี่ยนกำลังส่งคลื่น ทำให้ผู้ดูแลระบบสามารถกำหนดขนาดขอบเขตพื้นที่ให้บริการแลนไร้สายให้แคบลง เพื่อตนเองสามารถเฝ้าระวังสอดส่องผู้ใช้งานในพื้นที่นั้นได้อย่างทั่วถึงโดยการลดกำลังส่งคลื่น

2.3 Wireless LAN Controller

เว็บไซต์ Understanding Wireless LAN Switching for Wi-Fi Wireless LAN Centralized Control and Management [6] ได้อธิบายถึง Wireless LAN Switch โดยเน้นให้เห็นว่าอุปกรณ์ประเภทนี้ถูกออกแบบมาเพื่อมุ่งเน้นในการควบคุมคลื่นวิทยุของแอกเซสพอยต์ทุกตัวโดยกระทำจากส่วนกลาง และมีความสามารถในการป้องกันรักษาความปลอดภัย ทำให้สามารถเรียกได้อีกอย่างว่า Wireless LAN Controller ดังนี้

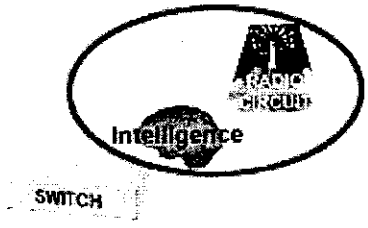
Wireless LAN Switch คือ อุปกรณ์ที่มีความฉลาดในการควบคุมและจัดการตัวรับสัญญาณคลื่นวิทยุทุก ๆ ตัวได้อย่างพร้อมกัน ตัวรับสัญญาณนี้จะทำตัวคล้ายกับว่ามันเป็นแอกเซสพอยต์ทั่วไปตามมาตรฐาน IEEE802.11

การตั้งค่าการทำงานต่าง ๆ ของแอกเซสพอยต์ที่ออกแบบเฉพาะที่เรียกว่า "Thin" กระทำผ่าน Controller ขีดความสามารถของแต่ละผลิตภัณฑ์จะแตกต่างกันไป โดยส่วนใหญ่ของ Wireless LAN Switch จะมีกลไกในการจัดการสัญญาณคลื่น มักจะมีเครื่องมือที่จัดการกำลังส่งคลื่นไปครอบคลุมพื้นที่ตามต้องการ ตรวจสอบพื้นที่ที่มีปัญหาได้ และใช้ในการอัปเกรดเวอร์ชันผ่านเครือข่าย ในระบบเครือข่ายที่ใช้ Wireless LAN Switch เมื่อมีแอกเซสพอยต์ใหม่ติดตั้งเข้าในเครือข่าย แอกเซสพอยต์ที่อยู่โดยรอบจะมีการปรับกำลังส่งโดยอัตโนมัติเพื่อลดการรบกวนกันและเพื่อให้เกิดประสิทธิภาพสูงสุด ยิ่งไปกว่านั้น Controller ซึ่งรู้จักแอกเซสพอยต์ทุกตัวของมันอยู่แล้วจะสามารถจับได้อย่างรวดเร็วว่ามีแอกเซสพอยต์แปลกปลอมติดตั้งโดยผู้ใช้ นอกจากจัดการเรื่องสัญญาณคลื่นวิทยุแล้ว Wireless LAN Switch สามารถบริหารความปลอดภัยและบันทึกการเข้าใช้โดย Controller นี้ด้วย และจัดเป็นโซลูชันที่บริษัทขนาดใหญ่นำไปใช้เพิ่มขึ้นเรื่อย ๆ

บริษัทชั้นนำที่เป็นที่รู้จักในการเสนอขายผลิตภัฑณ์ประเภทนี้คือ บริษัท Cisco, Airespace, 3Com, Trapeze Network และ Aruba Networks เป็นต้น

ข้อแตกต่างระหว่าง Stand-Alone Access Point System กับ Wireless LAN Switching

Stand-Alone Access Point



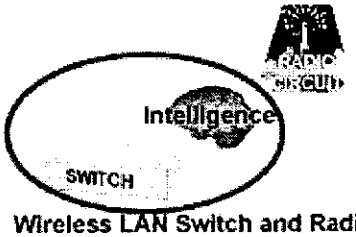
Ethernet Switch and Access Point

ภาพประกอบ 2.1 ความฉลาดอยู่ที่แอกเซสพอยต์

แอกเซสพอยต์มาตรฐาน IEEE802.11 จะมีวงจรสำหรับสร้างสัญญาณคลื่นวิทยุความถี่ต่าง ๆ และความสามารถในการบริหารและจัดการคลื่นตามที่เห็นในวงสีแดง ส่วนอีเทอร์เน็ตสวิตซ์เลเยอร์ 2 ทำหน้าที่เป็นจุดศูนย์กลางการเชื่อมต่อเพื่อส่งต่ออีเทอร์เน็ตแพ็กเก็ต

แอกเซสพอยต์ไม่สามารถส่งค่าการทำงานหรือข้อมูลการรักษาความปลอดภัยไปยังตัวอื่น ๆ ได้ เพราะว่าไม่มีโพรโทคอลมาตรฐานที่ใช้ทำหน้าที่นี้ แอกเซสพอยต์แต่ละตัวจึงทำงานแบบอิสระต่อกัน

Wireless LAN Switch



ภาพประกอบ 2.2 ความฉลาดอยู่ที่ Wireless LAN Switch

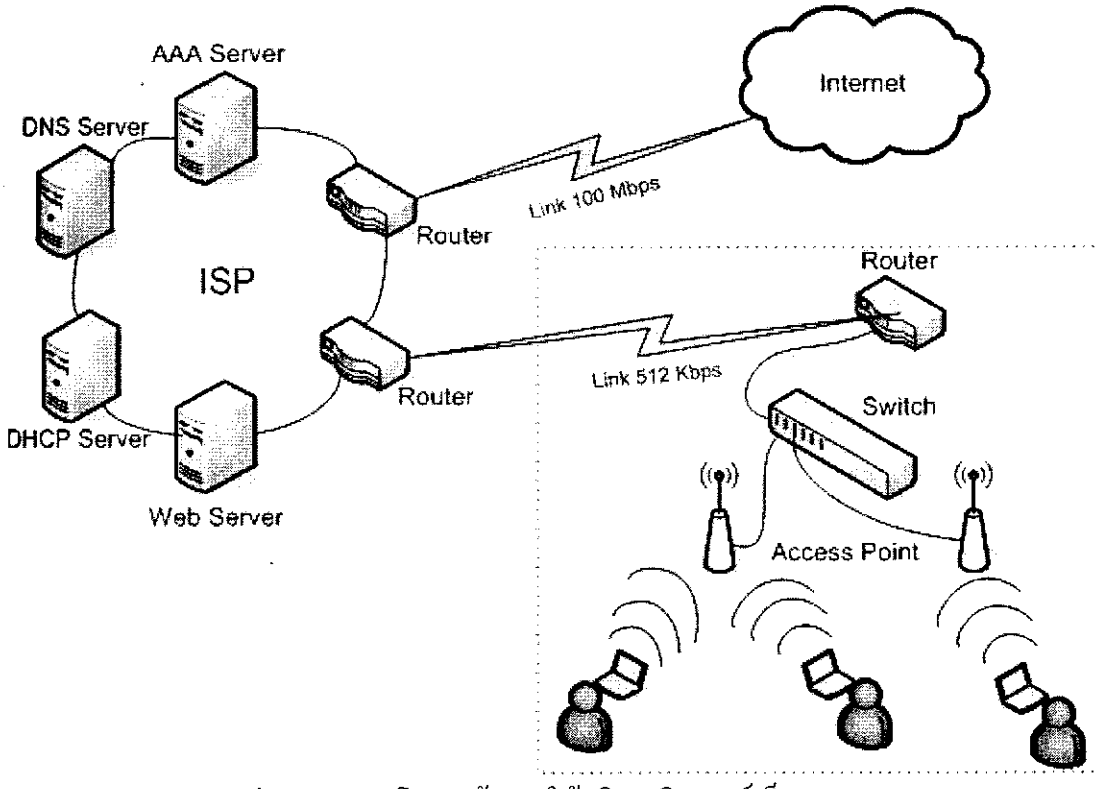
ในระบบเครือข่ายที่ใช้ Wireless LAN Switch ความสามารถในการจัดการเกือบทั้งหมดถูกย้ายจากตัวแอกเซสพอยต์ไปใส่รวมไว้ในสวิตซ์ ส่วนแอกเซสพอยต์นั้นทำหน้าที่เป็นตัวรับส่งสัญญาณคลื่นวิทยุอย่างมีประสิทธิภาพมาก Wireless LAN Switch ที่ส่วนกลางทำหน้าที่เป็นสวิตซ์เลเยอร์ 2 และควบคุมสัญญาณคลื่นวิทยุตามที่เห็นในวงสีแดง ความจริงก็คือความสามารถในการจัดการได้ย้ายมาอยู่ที่ Wireless LAN Switch ที่ส่วนกลางแล้ว

เพราะว่าความสามารถบางส่วนหรือทั้งหมดของหน้าที่การบริหารและจัดการสัญญาณคลื่นวิทยุได้ย้ายไปอยู่ที่ Wireless LAN Switch ที่ส่วนกลางแล้ว แอกเซสพอยต์แต่ละตัวจึงมีหน้าที่ทำงานให้ประสานกันและเปรียบเสมือนระบบที่มีเสาอากาศที่ใหญ่มากครอบคลุมเป็นวงกว้าง

2.4 Wireless Hotspot [5]

Wireless Hotspot หรือ Wi-Fi Hotspot คือ จุดหรือบริเวณพื้นที่ให้บริการอินเทอร์เน็ตไร้สายสาธารณะ ใช้เป็นช่องทางเชื่อมเครื่องคอมพิวเตอร์สู่อินเทอร์เน็ตเพื่อรับส่งอีเมล ดาวโหลดไฟล์ข้อมูล ค้นหาข้อมูลบนเว็บไซต์ เล่น Chat หรือกิจกรรมอื่น ๆ ที่สามารถทำได้บนอินเทอร์เน็ต โดยผู้ใช้งาน Wireless Hotspot ต้องมีเครื่องคอมพิวเตอร์โน้ตบุ๊ค พ็อกเก็ตพีซีที่ติดตั้งแลนการ์ดไร้สาย และชั่วโมงใช้งานอินเทอร์เน็ต (Hotspot User Account) จึงจะใช้จุดให้บริการอินเทอร์เน็ตไร้สายในบริเวณนั้นได้

โครงสร้างของ Wireless Hotspot เป็นการประยุกต์ใช้แลนไร้สายแบบ Infrastructure ที่มีองค์ประกอบพื้นฐานดังนี้



ภาพประกอบ 2.3 โครงสร้างจุดให้บริการอินเทอร์เน็ตสาธารณะ

1. Mobile Stations : ได้แก่ เครื่องคอมพิวเตอร์ไร้สาย พ็อกเก็ตพีซีไร้สาย หรืออุปกรณ์อื่น ๆ ที่สนับสนุนมาตรฐาน IEEE802.11b (Wi-Fi), มาตรฐาน IEEE802.11g
2. Access Point : ทำหน้าที่เป็นตัวกลางรองรับ Mobile Station เพื่อเชื่อมโยงเข้าสู่เครือข่ายของ Wireless Hotspot
3. Switch/Hub : ทำหน้าที่เป็นตัวกลางเชื่อมโยงระหว่างแอกเซสพอยต์หลาย ๆ เครื่องเข้ากับ Router ผ่านสายสัญญาณ UTP
4. Router : ทำหน้าที่ค้นหาเส้นทางส่งข้อมูลและเป็นอุปกรณ์เชื่อมไปยัง Router ของ ISP
5. High Speed Internet Connection : Link หรือเส้นทางเชื่อมระหว่าง Router ของ Wireless Hotspot ไปยัง Router ของ ISP เช่น DSL, ISDN, T, T3, E1 เป็นต้น
6. AAA Server : Authentication Authorization and Accounting (AAA) Server ทำหน้าที่พิสูจน์ตัวจริงและอนุญาตให้ผู้ใช้เข้าใช้งานเครือข่าย โดยผู้ใช้จะ

สามารถใช้งานเครือข่ายได้นั้นต้องมีบัญชีผู้ใช้อยู่ในฐานข้อมูลของ AAA Server

7. Internet Service Provider : ผู้ให้บริการอินเทอร์เน็ต (ISP)

2.5 NAT Router [7]

ในขณะที่ใช้งานอินเทอร์เน็ตที่บ้านโดยผ่านโมเด็ม เครื่องคอมพิวเตอร์จะได้รับเลขที่อยู่ไอพีมาหมายเลขหนึ่งโดยอัตโนมัติซึ่งถูกกำหนดจากเครื่องเซิร์ฟเวอร์ของผู้ให้บริการอินเทอร์เน็ต เลขที่อยู่ไอพีนี้คือเลขที่อยู่ไอพีจริง ๆ ที่ใช้กันในอินเทอร์เน็ตหรือที่เรียกกันว่า Public IP Address โดยจะถูกใช้เป็นเลขที่อยู่ไอพีประจำเครื่องพีซีนั้นชั่วคราวตลอดเวลาที่ยังคงใช้อินเทอร์เน็ตอยู่ และจะถูกดึงคืนหลังจากเลิกใช้งานเพื่อกำหนดให้ผู้ใช้รายอื่น ๆ ต่อไป

เลขที่อยู่ไอพีที่ได้รับมานี้ สามารถเอามาแชร์ให้กับเครื่องคอมพิวเตอร์เครื่องอื่นอีกที่อยู่ภายในแลนได้โดยใช้เทคโนโลยีที่เรียกว่า Network Address Translation หรือ NAT ซึ่งมีหลักการคือการแปลงเลขที่อยู่ไอพีของไคลเอนต์ที่อยู่ภายในแพ็กเก็ตทีซีพีให้กลายเป็นเลขที่อยู่ไอพีจริง (ที่ได้รับมานั้น) ก่อนจะส่งออกอินเทอร์เน็ต และในทำนองกลับกันจะแปลงเลขที่อยู่ไอพีที่อยู่ภายในแพ็กเก็ตทีซีพีที่ได้รับมาจากอินเทอร์เน็ตให้กลายเป็นเลขที่อยู่ไอพีของไคลเอนต์ที่ทำการสร้างการเชื่อมต่อออกไปนั้น ด้วยหลักการของ NAT นี้เองทำให้ไคลเอนต์แต่ละเครื่องสามารถติดต่อกับอินเทอร์เน็ตได้เสมือนว่ากำลังเชื่อมต่อกับอินเทอร์เน็ตโดยตรง เครื่องคอมพิวเตอร์ที่ให้บริการ NAT นี้เรียกว่า NAT Router นั่นเอง นอกจากนี้อุปกรณ์จำพวก Internet Sharing Device ก็ใช้หลักการของ NAT เช่นเดียวกัน

เทคโนโลยีของ NAT เรียกอีกอย่างว่า การซ่อนเลขที่อยู่ไอพี (IP Masquerade) เพราะว่าเครื่องคอมพิวเตอร์ในอินเทอร์เน็ตจะไม่สามารถรู้ว่าเลขที่อยู่ไอพีของไคลเอนต์เป็นหมายเลขใด

2.6 Captive Portal [8]

Captive Portal คือเทคนิคบังคับให้ไคลเอนต์ที่ใช้งานโพรโทคอล HTTP บนเครือข่ายต้องพบกับหน้าเว็บเพจสำหรับล็อกอินก่อนที่จะใช้อินเทอร์เน็ตตามปกติ หลักการทำงานของ Captive Portal คือดักจับแพ็กเก็ตทุกอย่างไม่สนใจว่าจะเป็นเลขที่อยู่ไอพีหรือพอร์ตจนกระทั่งผู้ใช้เปิดเบราว์เซอร์และพยายามเข้าใช้อินเทอร์เน็ต ในเวลานั้นเองเบราว์เซอร์จะถูกส่งต่อยังเว็บเพจ

หน้าหนึ่งที่ต้องการให้มีการพิสูจน์ตัวจริงและ/หรือชำระค่าใช้งาน หรืออย่างง่าย ๆ คือแสดงหน้าเงื่อนไขในการใช้งาน (Acceptable Use Policy) ที่ต้องการให้ผู้ใช้ยอมรับเงื่อนไข Captive Portal จะถูกใช้ในบริการประเภท Wi-Fi Hotspot และสามารถใช้ในการควบคุมการเข้าใช้เครือข่ายแบบมีสายได้เช่นกัน เว็บเพจที่ปรากฏขึ้นแก่ไคลเอนต์นั้นอาจจะเก็บอยู่ภายในเกตเวย์ หรือเว็บเซิร์ฟเวอร์ที่เก็บหน้านั้นไว้

เทคนิคที่เรียกว่า Walled Garden ถูกนำมาใช้เพื่อให้เครื่องที่อยู่ในรายการ Whitelisted สามารถผ่านขั้นตอนการพิสูจน์ตัวจริงไปได้ โดยตั้งค่าการทำงานที่เกตเวย์ รายชื่อเว็บเซิร์ฟเวอร์หลาย ๆ ชื่อจะอยู่ในรายการ Whitelisted (ตัวอย่างเช่นภายในหน้าเว็บล็อกอินจะมีเฟรมหรือข้อความที่เชื่อมโยงไปยังชื่อ URL ของเว็บเซิร์ฟเวอร์จำนวนหนึ่งที่ให้ข้อมูลเกี่ยวกับแนะนำบริการหรือโฆษณา) ยิ่งไปกว่านั้นรายการ Whitelisted นอกจากเป็นชื่อ URL แล้ว เกตเวย์บางตัวยังอาจให้เป็นหมายเลข TCP Port และ MAC Address ของไคลเอนต์เพื่อใช้ในการผ่านขั้นตอนล็อกอินได้ด้วย

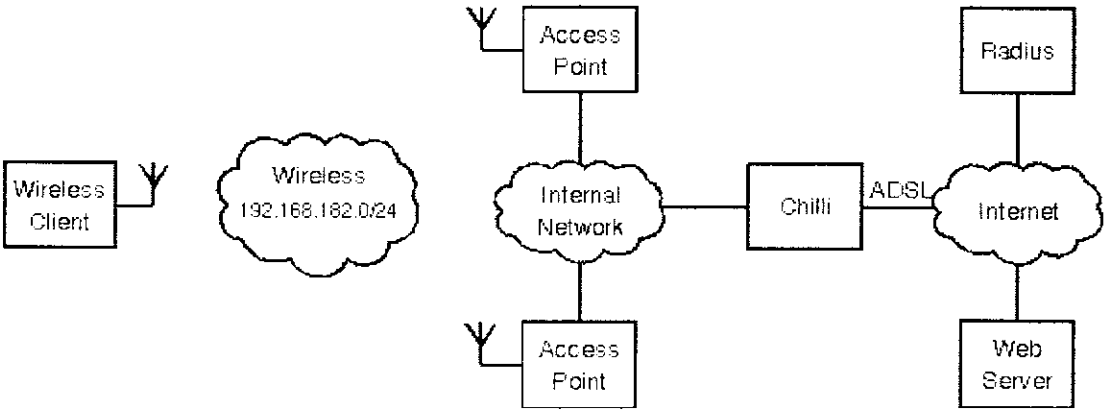
2.7 ChilliSpot [1]

ChilliSpot คือซอฟต์แวร์โอเพ่นซอร์สประเภท Captive Portal หรือ Wireless LAN Access Point Controller ใช้สำหรับการพิสูจน์ตัวจริงเพื่อเข้าใช้งานแลนไร้สาย สนับสนุนวิธีเว็บล็อกอินซึ่งเป็นคุณสมบัติมาตรฐานที่จะต้องมีใน Hotspot สาธารณะในปัจจุบัน สามารถเลือกใช้ RADIUS Server ใด ๆ ในการพิสูจน์ตัวจริง การกำหนดสิทธิ และการบันทึกการใช้งาน

ซอฟต์แวร์ชนิดไบนารีมีให้ดาวน์โหลดสำหรับระบบปฏิบัติต่อไปนี้ Redhat, Fedora, Debian, Mandrake และ OpenWRT ซอฟต์แวร์ที่ต้องนำไปคอมไพล์เป็นไบนารีเองมีให้ดาวน์โหลดสำหรับระบบปฏิบัติการ FreeBSD และซอร์สโค้ดภายใต้ข้อตกลงการใช้ซอฟต์แวร์โอเพ่นซอร์สมีให้ดาวน์โหลดสำหรับระบบปฏิบัติการ UNIX อื่น ๆ

สิ่งที่ต้องใช้ในการสร้าง Wireless Hotspot มีดังต่อไปนี้

- Internet Connection
- Wireless LAN Access Point
- ChilliSpot
- RADIUS Server
- Web Server



ภาพประกอบ 2.4 สิ่งที่ต้องใช้ในการสร้าง Wireless Hotspot

สามารถติดตั้ง RADIUS Server และ Web Server ลงในเครื่องเดียวกันที่ติดตั้ง ChilliSpot ได้ หรือแยกอยู่ต่างหากในอินเทอร์เน็ตก็ได้

Chilli คือชื่อโปรเซสของซอฟต์แวร์ที่ได้ติดตั้งลงในเครื่องไมโครคอมพิวเตอร์ สนับสนุนการพิสูจน์ตัวจริง 2 วิธี คือ

- Universal Access Method (UAM)
- Wireless Protected Access (WPA)

ด้วยวิธี UAM ไคลเอนต์จะร้องขอเลขที่อยู่ไอพีและได้รับการจัดสรรเลขที่อยู่ไอพีจาก Chilli เมื่อผู้ใช้เปิดเบราว์เซอร์ใช้อินเทอร์เน็ต Chilli จะจับแพ็กเก็ตของการเชื่อมต่อชนิดทีซีพีนั้นได้ และเบราว์เซอร์จะถูกส่งต่อยังหน้าเว็บเพจหน้าหนึ่งในเว็บเซิร์ฟเวอร์ที่ต้องการให้มีการพิสูจน์ตัวจริงด้วยชื่อผู้ใช้และรหัสผ่าน ซึ่งเบราว์เซอร์จะทำการเข้ารหัสข้อมูลที่ผู้ใช้ป้อนและส่งกลับไปยัง Chilli

ด้วยวิธี WPA การพิสูจน์ตัวจริงจะกระทำที่แอกเซสพอยต์ โดยจะมีการส่งข้อมูลไปมาระหว่างแอกเซสพอยต์กับ Chilli การใช้วิธี WPA จะทำให้การเชื่อมต่อเครือข่ายระหว่างแอกเซสพอยต์กับเครื่องไคลเอนต์มีการเข้ารหัสข้อมูล

ทั้งวิธี UAM และ WPA นั้น Chilli ส่งต่อการร้องขอการพิสูจน์ตัวจริงไปยัง RADIUS Server ซึ่งมันจะแจ้งกลับด้วยข้อความ Access-Accept ไปยัง Chilli หากการพิสูจน์ตัวจริงผู้ใช้งานสำเร็จ มิฉะนั้นจะส่งกลับด้วยข้อความ Access-Reject แทน

เว็บเซิร์ฟเวอร์สำหรับการพิสูจน์ตัวจริงจำเป็นต้องมีเพื่อที่จะใช้วิธี UAM แต่หากใช้วิธี WPA ก็ไม่ต้องมีเว็บเซิร์ฟเวอร์นี้ การติดต่อกับเว็บเซิร์ฟเวอร์จะใช้โพรโทคอล HTTP ในขณะที่ทำการพิสูจน์ตัวจริง จะไม่มีการติดต่อกลับจากเว็บเซิร์ฟเวอร์ไปยัง Chilli นั่นหมายความว่า Hotspot สามารถวางอยู่หลังเกตเวย์หรือ NAT Router ในขณะที่เว็บเซิร์ฟเวอร์ตั้งอยู่ในอินเทอร์เน็ต

ได้ ซอฟต์แวร์นี้ได้เตรียมไฟล์ชนิด cgi script ที่เป็นแบบฟอร์มคำถามชื่อผู้ใช้และรหัสผ่านสำหรับติดตั้งลงในเว็บเซิร์ฟเวอร์ให้ด้วย เมื่อผู้ใช้ใส่ข้อมูลแล้ว รหัสผ่านจะถูกเข้ารหัสเพื่อส่งกลับไปให้ Chilli ซึ่งข้อมูลนี้ถูกส่งต่อไปยัง RADIUS Server อีกที ควรจะใช้ SSL/TLS กับเว็บเซิร์ฟเวอร์เพื่อที่จะเข้ารหัสทั้งชื่อผู้ใช้และรหัสผ่าน

ซอฟต์แวร์ Chilli นี้ไม่ได้ให้ซอฟต์แวร์ RADIUS Server มาด้วย สำหรับงานเล็ก ๆ ให้ใช้ RADIUS Server ชนิดโอเพ่นซอร์ส เช่น FreeRADIUS, Cistron หรือ OpenRADIUS เป็นต้น

2.8 หลักการทำงานของ ChilliSpot [1],[2],[3],[4]

เป้าหมายของการนำ ChilliSpot มาใช้คือการติดตั้งเครื่องคอมพิวเตอร์เป็นเกตเวย์ที่จะบังคับผู้ใช้ให้ลงบันทึกเข้าที่หน้าเว็บเพจสำหรับล็อกอิน เกตเวย์จะมีอินเตอร์เฟสเชื่อมต่อเครือข่าย 2 อินเตอร์เฟส อินเตอร์เฟสแรก (eth0) จะเป็นแลนการ์ด (LAN Card) ที่ต่อกับอินเทอร์เน็ต ส่วนอีกอินเตอร์เฟส (eth1) ต่อกับเครือข่ายภายในซึ่งจะเป็นได้หลายอย่าง อาจเป็นแลนการ์ดที่ต่อกับแลนสวิตช์ (LAN Switch) ที่มีเครื่องคอมพิวเตอร์หรือแอกเซสพอยต์จำนวนหนึ่ง หรืออาจเป็นแลนการ์ดไร้สาย (Wireless LAN Card) ที่ทำให้เกตเวย์นี้เป็นแอกเซสพอยต์ไปในตัว

ChilliSpot จะทำงานกับอินเตอร์เฟสที่ต่อกับเครือข่ายภายใน (eth1) โดยใช้เคอร์เนลโมดูลชื่อ vtun ทำให้เกิดอินเตอร์เฟสเสมือน (tun0) จากนั้น ChilliSpot ติดตั้ง DHCP Server ขึ้นมาบนอินเตอร์เฟส tun0 นั้น

ทุกแพ็กเก็ตของไคลเอนต์ที่ส่งผ่านอินเตอร์เฟสนี้จะถูกปฏิเสธจนกว่ามันจะได้รับสิทธิเข้าใช้หลังจากลงบันทึกเข้าแล้วเท่านั้น เมื่อไคลเอนต์ที่ยังไม่มีสิทธิเข้าใช้พยายามติดต่อไปยังเว็บเพจใด ๆ ด้วยทีซีพีพอร์ต 80 หรือ 443 แพ็กเก็ตนั้นจะถูกสกัดกั้นโดยโปรเซส Chilli จากนั้นเว็บเซิร์ฟเวอร์จะได้รับการติดต่อจาก Chilli และส่งหน้าเว็บเพจสำหรับล็อกอินชื่อ hotspotlogin.cgi ที่เขียนด้วยภาษา Perl โดยใช้โพรโทคอล HTTPS

ไฟล์ hotspotlogin.cgi ที่ถูกส่งไปยังผู้ใช้นี้จะเป็นเว็บเพจที่มีช่องชื่อผู้ใช้และรหัสผ่าน ข้อมูลนี้จะกลับไปยังโปรเซส Chilli แล้วถูกส่งต่อไปยัง FreeRADIUS Server ซึ่งจะตรวจสอบว่าตรงกันกับในฐานข้อมูลหรือไม่ ฐานข้อมูลอาจเป็น MySQL หรืออื่น ๆ เช่น LDAP, Kerberos, Unix Password File หรือ Active Directory เป็นต้น

จากนั้นผู้ใช้จะได้รับเว็บเพจแจ้งว่าการพิสูจน์ตัวจริงถูกต้องพร้อมกับข้อความเชื่อมโยงไปยังชื่อ URL สำหรับลงบันทึกออก หรือได้รับเว็บเพจแจ้งปฏิเสธการเข้าใช้อย่างใดอย่างหนึ่ง

2.9 RADIUS [9]

RADIUS ย่อมาจาก Remote Authentication Dial In User Service เป็นโพรโทคอลด้านเครือข่ายที่ใช้จัดการในเรื่องการพิสูจน์ตัวจริง (Authentication) การกำหนดสิทธิ (Authorization) และการบันทึกการใช้งาน (Accounting) สำหรับการขอเข้าใช้บริการเครือข่ายใด ๆ คำศัพท์ที่มักใช้เรียกการที่ใครสักคนหรือเครื่องคอมพิวเตอร์สักเครื่องจะเชื่อมต่อเครือข่ายได้ต้องมีสิทธิเข้าใช้งานว่าการพิสูจน์ตัวจริง (Authentication) และเครือข่ายหรือบริการใดที่ไม่ต้องมีการพิสูจน์ตัวจริงจะเรียกว่าไม่จำกัดสิทธิหรือเปิด (Open)

RADIUS เป็นโพรโทคอลที่ใช้ในระบบงานทั้งที่เป็นโอเพ่นซอร์สและการค้า ระบบพื้นฐานเหล่านี้ถูกติดตั้งใช้งานโดยผู้ให้บริการด้านโทรคมนาคมเพื่อบริการลูกค้า และโดยบริษัทต่าง ๆ เพื่อบริการพนักงานที่อยู่นอกสำนักงาน

เมื่อมีการพิสูจน์ว่ามีสิทธิเข้าใช้งานแล้ว RADIUS จึงตรวจสอบว่าจะให้สิทธิหรืออนุญาตอะไรบ้าง และมีการบันทึกการใช้งาน กระบวนการเหล่านี้รวมเรียกว่า Authentication Authorization and Accounting ซึ่งเรียกย่อ ๆ ว่า AAA

เนื่องจากมีการสนับสนุนการใช้โพรโทคอล RADIUS นี้อย่างกว้างขวาง มันจึงเป็นที่นิยมใช้โดยผู้ให้บริการอินเทอร์เน็ต (ISP) ใช้ในแลนไร้สาย ในบริการอีเมล ในแอกเซสพอยต์ ในพอร์ตของอุปกรณ์เครือข่าย เว็บเซิร์ฟเวอร์ต่าง ๆ หรือบริการอื่น ๆ ที่ต้องการใช้ AAA Server

RADIUS นำมาใช้โดยผู้ให้บริการอินเทอร์เน็ตและบริษัทต่าง ๆ เกี่ยวกับการจัดการการเข้าใช้อินเทอร์เน็ตหรืออินทราเน็ตใช้ร่วมกับเทคโนโลยีด้านเครือข่ายที่หลากหลาย เช่น โมเด็ม DSL แลนไร้สาย และ VPN เป็นต้น

RADIUS Server ใช้หลักการ AAA เพื่อจัดการการเข้าใช้เครือข่ายโดยกระบวนการ 2 ขั้นตอน เรียกว่า AAA Transaction คือ

การพิสูจน์ตัวจริง และการกำหนดสิทธิ

รายละเอียดของการพิสูจน์ตัวจริงและการกำหนดสิทธิของ RADIUS เขียนไว้ใน RFC 2865

ผู้ใช้หรือในที่นี้คือ RADIUS Client ส่งการร้องขอไปยัง Network Access Server (NAS) เพื่อต้องการได้รับสิทธิเข้าใช้เครือข่ายด้วยข้อมูลผู้ใช้ซึ่งจะถูกส่งไปยังอุปกรณ์ NAS ทาง

โพรโทคอลระดับ Link-Layer เช่น Point-to-Point Protocol (PPP) ในกรณีของผู้ให้บริการ DSL หรือ Dial-Up

จากนั้น NAS ส่งข้อความ Access Request ไปยัง RADIUS Server เพื่อร้องขอการอนุญาตเข้าใช้ ในการร้องขอนี้ใช้ข้อมูลผู้ใช้ที่ประกอบด้วยชื่อผู้ใช้และรหัสผ่านหรืออาจเป็นข้อมูล Security Certificate ของผู้ใช้ รวมถึงข้อมูลที่ NAS รู้เกี่ยวกับผู้ใช้ เช่น หมายเลขเครือข่ายหรือหมายเลขโทรศัพท์ และข้อมูลเกี่ยวกับตำแหน่งที่ต่อกับ NAS เป็นต้น

RADIUS Server ตรวจสอบข้อมูลนั้นว่าถูกต้องหรือไม่โดยใช้วิธีการพิสูจน์ตัวจริงเหล่านี้คือ PAP, CHAP หรือ EAP การพิสูจน์ตัวจริงจะกระทำพร้อมกับตรวจสอบข้อมูลอื่น ๆ เช่น หมายเลขเครือข่ายหรือหมายเลขโทรศัพท์ สถานะบัญชีผู้ใช้ และสิทธิการเข้าถึงบริการเครือข่ายใดบ้าง ในอดีต RADIUS ตรวจสอบข้อมูลผู้ใช้ด้วยฐานข้อมูลชนิดไฟล์ข้อมูลธรรมดาของมันเอง แต่ในเวลาต่อมา RADIUS สามารถใช้ทั้งไฟล์ข้อมูลธรรมดาและฐานข้อมูลภายนอก เช่น SQL, Kerberos, LDAP หรือ Active Directory

RADIUS Server จะตอบกลับด้วยข้อความ 3 อย่างคือ Access Reject, Access Challenge หรือ Access Accept

Access Reject หมายถึง ผู้ใช้ถูกปฏิเสธการร้องขอใช้เครือข่ายอย่างไม่มีเงื่อนไข อาจมีสาเหตุจากใส่ข้อมูลชื่อผู้ใช้ผิด หรือไม่มีบัญชีผู้ใช้ หรือบัญชีผู้ใช้นั้นไม่มีการใช้งานนานแล้ว

Access Challenge หมายถึง ร้องขอข้อมูลเพิ่มเติมจากผู้ใช้เช่น รหัสผ่านอันที่สอง, PIN, Token หรือ Card เป็นต้น และใช้ในขั้นตอนการพิสูจน์ตัวจริงที่ซับซ้อนขึ้น

Access Accept หมายถึง ผู้ใช้ได้รับสิทธิเข้าใช้ เมื่อผู้ใช้พิสูจน์ตัวจริงแล้ว RADIUS Server จะตรวจสอบว่าผู้ใช้ได้รับอนุญาตให้ใช้บริการเครือข่ายใดบ้างตามที่ร้องขอ ตัวอย่างเช่น ผู้ใช้ที่ได้รับสิทธิใช้เครือข่ายไร้สายของบริษัท แต่อาจไม่ได้สิทธิในบริการ VPN เป็นต้น

แอตตริบิวต์ต่างๆ ของ Authorization ถูกนำมาให้ NAS ใช้ในการกำหนดเงื่อนไขการเข้าใช้ ตัวอย่างเช่นแอตตริบิวต์ต่าง ๆ ของ Authorization ข้างล่างนี้อาจรวมอยู่ในแพ็กเก็ต Access-Accept ที่ RADIUS Server ตอบกลับ ดังนี้

- เลขที่อยู่ไอพีที่จะกำหนดให้ผู้ใช้
- ระยะเวลานานที่สุดที่ผู้ใช้สามารถเชื่อมต่อได้
- รายการอนุญาตเข้าใช้ จัดลำดับคิว หรือข้อห้ามในการใช้งานของผู้ใช้
- พารามิเตอร์ต่าง ๆ ของโพรโทคอล L2TP
- พารามิเตอร์ต่าง ๆ ของ VLAN
- พารามิเตอร์ต่าง ๆ ของ Quality of Service (QoS)

การบันทึกการใช้งาน

รายละเอียดของการบันทึกการใช้งานเขียนไว้ใน RFC 2866

เมื่อ NAS อนุญาตการเข้าใช้เครือข่ายแก่ผู้ใช้แล้ว แพ็กเก็ต Accounting Start จะถูกส่งโดย NAS ไปยัง RADIUS Server เพื่อส่งสัญญาณเริ่มต้นใช้เครือข่าย ระเบียน "Start" บรรจุด้วยข้อมูลที่ใช้พิสูจน์ตัวจริงของผู้ใช้ หมายเลขเครือข่าย จุดที่เชื่อมต่อ และหมายเลข Session ที่ไม่ซ้ำ (A Unique Session Identifier)

ระเบียน Interim Accounting อาจจะถูกส่งโดย NAS ไปยัง RADIUS Server ตามช่วงเวลา เพื่อปรับสถานะของ Session ที่กำลังทำงานอยู่นั้นให้เป็นปัจจุบัน ระเบียน "Interrim" นำส่งระยะเวลาที่ใช้ไปของ Session และข้อมูลเกี่ยวกับการใช้งาน

สุดท้าย เมื่อการเข้าใช้เครือข่ายของผู้ใช้สิ้นสุดลง NAS ส่งระเบียน Accounting Stop ไปยัง RADIUS Server ให้ข้อมูลการใช้งานสุดท้ายเกี่ยวกับเวลา จำนวนแพ็กเก็ตที่รับส่ง จำนวนข้อมูลที่รับส่ง เหตุผลของการสิ้นสุดการเชื่อมต่อ และข้อมูลอื่น ๆ ที่เกี่ยวข้องกับการเข้าใช้เครือข่ายของผู้ใช้

วัตถุประสงค์หลักของข้อมูลพวกนี้คือเอาไว้ทำรายการบัญชีค่าใช้จ่ายตามการใช้งานของผู้ใช้คนนั้น ข้อมูลนี้ใช้เป็นสถิติและตรวจสอบเครือข่ายทั่วไปได้ด้วย

Roaming

RADIUS ถูกใช้เพื่อความสะดวกในการเข้าใช้งานในกลุ่มผู้ให้บริการอินเทอร์เน็ตด้วยกัน ตัวอย่างเช่นในหลาย ๆ บริษัทที่กำหนดให้บัญชีผู้ใช้เพียง 1 บัญชีสามารถใช้กับเครือข่ายสาธารณะได้เป็นจำนวนมาก RADIUS ช่วยทำเรื่องนี้ได้อย่างง่ายดายด้วยการใช้ชื่อ Realm โดยที่ RADIUS Server จะส่งต่อแพ็กเก็ต AAA Request นั้นไปดำเนินการตามชื่อ Realm แต่ละชื่อ

- Realms

Realm คือ ข้อความที่ต่อท้ายชื่อผู้ใช้และคั่นด้วยเครื่องหมาย "@" คล้ายกับโดเมนเนมของอีเมลแอดเดรส วิธีนี้เรียกว่า Postfix Notation ส่วนอีกวิธีเรียกว่า Prefix Notation เป็นการใส่ข้อความหน้าชื่อผู้ใช้และตามด้วยเครื่องหมาย "\" เป็นตัวคั่น RADIUS Server รุ่นใหม่ยอมให้ใช้ตัวอักษรอะไรก็ได้เป็นตัวคั่น แต่ที่นิยมใช้กันมากในทางปฏิบัติคือ "@" และ "\"

ถึงแม้ว่า Realm จะคล้ายกับโดเมนเนมของอีเมล แต่ในความเป็นจริงมันเป็นเพียงแค่ข้อความทั่วไปและไม่จำเป็นต้องเป็นชื่อโดเมนเนมจริง ๆ

- Proxy Operations

เมื่อ RADIUS Server ได้รับ AAA Request ที่เป็นชื่อผู้ใช้ที่มี Realm ใส่มาด้วย เซิร์ฟเวอร์จะค้นหาที่ตารางการตั้งค่าการทำงาน Realm หากพบว่ามีชื่อ Realm นั้นเซิร์ฟเวอร์จะทำหน้าที่เป็นตัวแทน (Proxy) ในการส่งต่อ Request ไปยังเซิร์ฟเวอร์ที่กำหนดไว้สำหรับ Realm นั้น เซิร์ฟเวอร์ที่เป็นตัวแทนนี้มีการถอด Realm ออกจาก Request ได้แต่เป็นการตั้งค่าการทำงานที่ขึ้นอยู่กับเซิร์ฟเวอร์ทั้งหมด นอกจากนั้นเราสามารถตั้งค่าการทำงานให้เซิร์ฟเวอร์ที่เป็นตัวแทนนั้นเพิ่ม ลบ หรือเขียน AAA Request ใหม่ได้

2.10 หลักการทำงานของ Transparent Proxying

เว็บไซต์ Transparent Cache Implementation Using Squid [10] ได้อธิบายหลักการทำงาน Transparent Caching ไว้ดังนี้ จะเรียกว่า Transparent Caching หรือ Transparent Proxying ได้ทั้งสองอย่าง เราสามารถกล่าวได้ว่าคือการกระทำอย่างหนึ่งที่เกี่ยวกับโพรโทคอล HTTP (ทีซีพีพอร์ตหมายเลข 80) ซึ่งเป็นทราฟฟิกที่ใช้กันโดยทั่วไปในอินเทอร์เน็ต ข้อแตกต่างก็คือถ้าใช้คำว่า Caching นั้นมีการเขียนข้อมูลเก็บลงดิสก์ที่เรียกว่าแคช (Cache) ขณะที่ใช้คำว่า Proxying นั้นก็จะไม่มีการเขียนแคช คำว่า Transparent นั้นหมายถึงการตั้งค่าอย่างหนึ่งให้มีการเปลี่ยนทิศทางแพ็กเก็ตที่มีพอร์ตหมายเลข 80 ซึ่งเป็นแพ็กเก็ตของไคลเอนต์ที่ส่งไปยังเว็บเซิร์ฟเวอร์ในอินเทอร์เน็ตให้ส่งต่อไปยังแคชเซิร์ฟเวอร์ (Cache Server) หรือพร็อกซี่เซิร์ฟเวอร์ (Proxy Server) เราสามารถตั้งค่า Squid ให้ทำงานแบบ Transparent Caching ได้ ในรูปแบบนี้ไคลเอนต์ไม่ต้องตั้งค่าใด ๆ ที่เบราว์เซอร์เพื่อใช้งานแคชเซิร์ฟเวอร์ แต่ Squid จะทำหน้าที่ไปเอาแพ็กเก็ตและเขียนแคชเอาไว้โดยที่ไคลเอนต์มองไม่เห็นการกระทำนี้ วิธีการนี้แก้ปัญหาในเรื่องความต้องการให้มีการใช้งานอินเทอร์เน็ตผ่านแคชเซิร์ฟเวอร์ เพราะว่าผู้ใช้ไม่รู้ว่ากำลังใช้งานอินเทอร์เน็ตผ่านแคชเซิร์ฟเวอร์

มีวิธีการตั้งค่า Transparent Caching ได้ 3 วิธี

1. Policy based routing

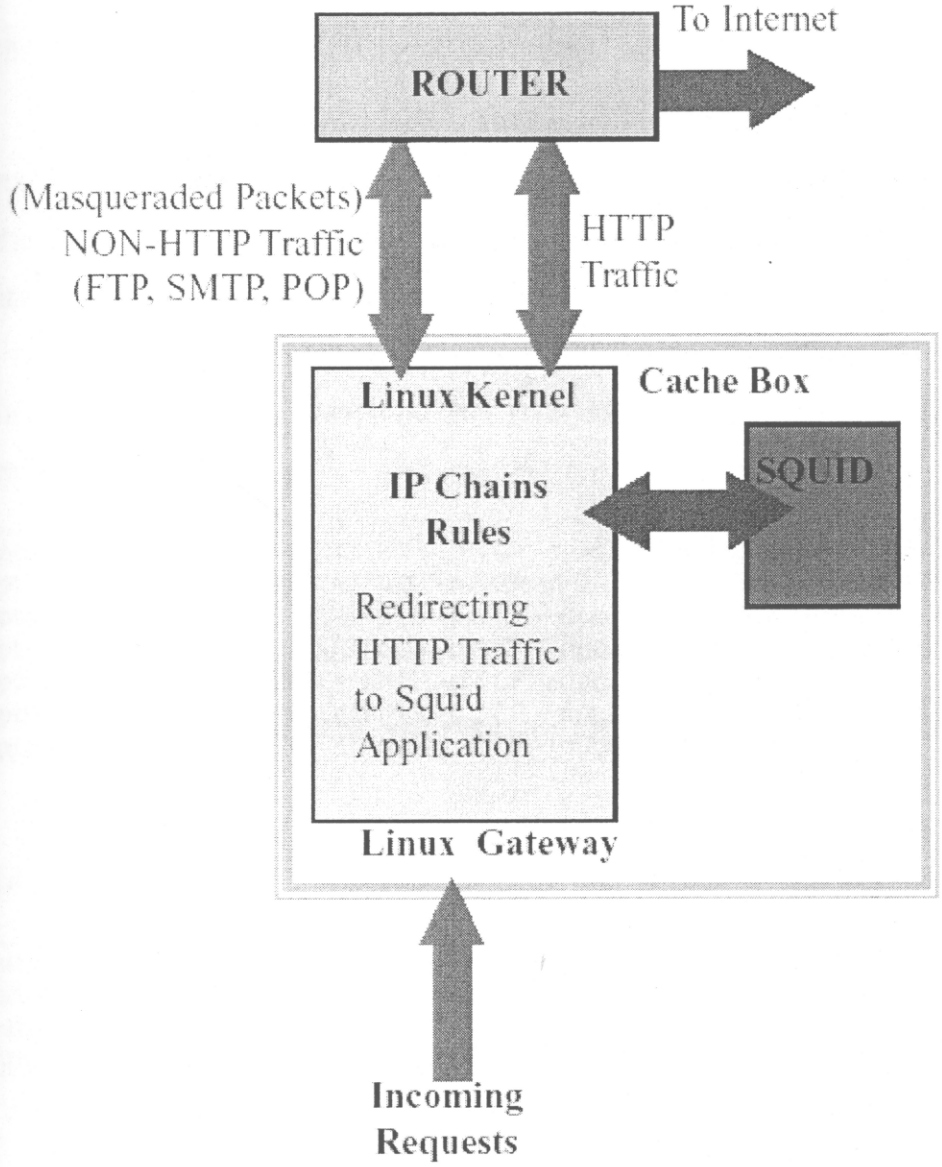
การตั้งค่าวิธีนี้ใช้อุปกรณ์จัดเส้นทางส่งทราฟฟิก HTTP ไปยังเครื่องที่ดำเนินงาน Squid ซึ่งเป็นไปตามการกำหนดค่า Policy based routing ในอุปกรณ์จัดเส้นทาง

2. Using smart switching

การตั้งค่าวิธีนี้ใช้สวิตช์เลเยอร์ 4 หรือ 7 ส่งทราฟฟิก HTTP ไปยังเครื่องที่ดำเนินงาน Squid

3. By Setting Squid Box as a Gateway

วิธีนี้ใช้กับเครือข่ายที่มีขนาดเล็กที่มีจำนวนไคลเอนต์น้อย โดยการตั้งค่าที่ไคลเอนต์ให้ชี้ดีฟอลต์เกตเวย์ไปที่เครื่องที่ดำเนินงาน Squid ซึ่งเป็นเกตเวย์ เมื่อเปรียบเทียบกับวิธีอื่น ๆ วิธีนี้จะมีขั้นตอนในการตั้งค่าการทำงานมากกว่า



ภาพประกอบ 2.5 Transparent Caching in Linux Gateway

แพ็กเก็ตทีซีพีที่จะไปยังพอร์ตหมายเลข 80 ในอินเทอร์เน็ตของไคลเอนต์ที่ถูกส่งต่อโดยสวิตช์หรืออุปกรณ์จัดเส้นทางไปยังเครื่องที่เป็นเกตเวย์ จะถูกส่งไปยังพอร์ตที่ Squid เปิดรอรับ การเปลี่ยนทิศทางส่งแพ็กเก็ตเหล่านี้ไม่สามารถทำโดย Squid ต้องทำโดยลินุกซ์เคอร์เนล (Linux

Kernel) โดยใช้โปรแกรม ipchains หรือ iptables เมื่อเคอร์เนลได้รับแพ็กเก็ตทีซีพีที่ไปพอร์ตหมายเลข 80 มันอ่านการตั้งค่าการทำงานไฟร์วอลล์ว่าให้เปลี่ยนแพ็กเก็ตไปที่ไหน เช่นเปลี่ยนไปที่พอร์ตหมายเลข 3128 ที่ Squid เปิดรออยู่ เป็นต้น

คำสั่งกำหนดค่า Port Redirection ในไฟร์วอลล์เพื่อเปลี่ยนทิศทางแพ็กเก็ตทีซีพีที่ไปพอร์ตหมายเลข 80 ให้ไปที่พอร์ตหมายเลข 3128 ด้วยโปรแกรม iptables ดังนี้

```
iptables -t nat -A PREROUTING -p TCP --dport 80 -j REDIRECT --to-port 3128
```

ส่วนแพ็กเก็ตที่จะไปยังพอร์ตหมายเลขอื่น ๆ ในอินเทอร์เน็ตเมื่อถูกส่งมายังเครื่องเกตเวย์ มันจะไม่ถูกส่งต่อไปหา Squid แต่จะสามารถออกสู่อินเทอร์เน็ตได้ก็ต่อเมื่อมีการตั้งค่าการทำงานของไฟร์วอลล์ให้อนุญาตพอร์ตเหล่านั้น พร้อมทั้งซ่อนเลขที่อยู่ไอพีของไคลเอนต์และออกไปด้วยเลขที่อยู่ไอพีของเกตเวย์ตามหลักการ NAT Router ในหัวข้อ 2.5

คำสั่งกำหนดค่า IP Masquerading ในไฟร์วอลล์เพื่อให้ไคลเอนต์สามารถใช้งานโพรโทคอล FTP (21, 20), SMTP (25), POP (110), SSH (22), TELNET (23) และ HTTPS (443) ในอินเทอร์เน็ตได้ ดังนี้

```
iptables -t nat -A POSTROUTING -p TCP -s 0/0 --dport 21 -j MASQUERADE
iptables -t nat -A POSTROUTING -p TCP -d 0/0 --dport 20 -j MASQUERADE
iptables -t nat -A POSTROUTING -p TCP --dport 25 -j MASQUERADE
iptables -t nat -A POSTROUTING -p TCP --dport 110 -j MASQUERADE
iptables -t nat -A POSTROUTING -p TCP --dport 22 -j MASQUERADE
iptables -t nat -A POSTROUTING -p TCP --dport 23 -j MASQUERADE
iptables -t nat -A POSTROUTING -p TCP --dport 443 -j MASQUERADE
```

การตั้งค่า Squid ให้ทำงานแบบ Transparent Caching โดยกำหนดค่าเหล่านี้ในไฟล์ squid.conf

```
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

2.11 สรุปท้ายบท

สำหรับบทนี้ได้กล่าวถึงรูปแบบการใช้งานแลนไร้สายประเภทต่าง ๆ ซึ่ง Wireless Hotspot เป็นรูปแบบหนึ่งและเป็นรูปแบบที่จะนำมาใช้ในงานวิจัยนี้ และให้ข้อมูลเรื่องการรักษาความปลอดภัยแลนไร้สายด้วยคุณสมบัติของแอกเซสพอยต์และด้วยอุปกรณ์ควบคุมแลนไร้สาย เทคโนโลยีที่นำมาใช้ในการให้บริการ Wireless Hotspot การใช้ RADIUS Server ในการพิสูจน์ตัวจริง และเทคนิค Captive Portal ซึ่งถูกกล่าวอ้างถึงในการติดตั้ง ChilliSpot นั้นเป็นอย่างไร อีกทั้งความรู้ที่จำเป็นต้องใช้ในการจัดทำลินุกซ์เกตเวย์ ความหมายของ NAT Router และ Transparent Proxying สำหรับแนวคิดและการออกแบบในงานวิจัยจะกล่าวถึงต่อไปในบทที่ 3

บทที่ 3

แนวคิดและการออกแบบในงานวิจัย

จากที่ได้กล่าวไปแล้วถึงที่มาของงานวิจัยในบทที่ 1 การศึกษาเทคโนโลยีที่เกี่ยวข้องในการจัดทำบริการ Wireless Hotspot ในบทที่ 2 สำหรับในบทนี้จะนำเสนอแนวคิดการเลือกเทคโนโลยีที่ใช้ในการพัฒนาต้นแบบการรักษาความปลอดภัยแลนไร้สายสำหรับแอกเซสพอยต์ราคาถูกด้วยวิธีการพิสูจน์ตัวจริงแบบเว็บล็อกอินโดยใช้ซอฟต์แวร์โอเพ่นซอร์ส เพื่อติดตั้งให้บริการ Wireless Hotspot

3.1 แนวคิดการเลือกเทคโนโลยี

จากการศึกษาเทคโนโลยีที่เกี่ยวข้องการจัดทำบริการ Wireless Hotspot นั้นจะมีองค์ประกอบที่สำคัญคือ ผู้ใช้งาน แอกเซสพอยต์ อุปกรณ์ที่ทำหน้าที่ควบคุมการเข้าใช้ มีประเด็นที่ใช้ในการพิจารณาดังนี้

ผู้ใช้งาน

ในมหาวิทยาลัย ผู้ใช้งานประกอบด้วยบุคคล 2 ประเภทคือ ผู้ที่ทำงานหรือเรียนอยู่ในมหาวิทยาลัย และผู้ที่มาร่วมทำงานเป็นครั้งคราวหรือแขกของมหาวิทยาลัย ดังนั้นเพื่อให้สะดวกแก่การให้บริการบุคคลทั้งสองประเภท เทคโนโลยีการพิสูจน์ตัวจริงแบบเว็บล็อกอินเป็นเทคโนโลยีที่เหมาะสม เพราะว่าสามารถให้บริการได้โดยไม่ต้องตั้งค่าใด ๆ ที่เครื่องคอมพิวเตอร์ของผู้ใช้งาน และให้ความปลอดภัยในการใช้แลนไร้สายได้ในระดับหนึ่งนั่นคือเว็บล็อกอินทำให้ผู้ใช้ต้องมีชื่อผู้ใช้และรหัสผ่านจึงเข้าใช้ได้ ร่วมกับการเข้ารหัสข้อมูลที่ส่งจากหน้าเว็บสำหรับล็อกอินที่ใช้โพรโทคอล HTTPS แทน HTTP

แอกเซสพอยต์

เนื่องจากในงานวิจัยนี้เน้นไปที่การนำแอกเซสพอยต์ราคาถูกมาใช้ ซึ่งแต่ละยี่ห้อก็จะมีคุณสมบัติและขีดความสามารถไม่เท่ากัน วิธีการเข้าไปกำหนดค่าการทำงานก็ไม่เหมือนกัน ดังนั้นการนำแอกเซสพอยต์ราคาถูกมาใช้หลายๆ ยี่ห้อก็ไม่น่าจะเป็นข้อจำกัด หรือไม่ควรจะต้องเลือกยี่ห้อใดยี่ห้อหนึ่ง เมื่อมีแอกเซสพอยต์หลายยี่ห้อ การเลือกใช้วิธีการรักษาความปลอดภัยโดยการตั้งค่าที่แอกเซสพอยต์จึงไม่เหมาะสม ในขณะที่การเลือกใช้อุปกรณ์ควบคุมแลนไร้สายที่วางอยู่ตรงกลางโดยมีแอกเซสพอยต์ทุกตัวไปเชื่อมต่อด้วยแล้วไม่ต้องแก้ไขการตั้งค่าเรื่องการรักษาความ

ปลอดภัยที่ตัวแอกเซสพอยต์ดูจะเหมาะสมกว่า อย่างไรก็ตามแอกเซสพอยต์ราคาถูกบางยี่ห้อก็จำเป็นต้องมีการตั้งค่าทางเครือข่ายเพื่อปิด (Disable) คุณสมบัติการเป็น DHCP Server เพื่อให้มันไม่ทำหน้าที่จัดสรรเลขที่อยู่ไอพีให้กับไคลเอนต์เอง แต่ทำหน้าที่ส่งผ่านแพ็กเก็ต DHCP จากอุปกรณ์ควบคุมแลนไร้สายไปยังไคลเอนต์เท่านั้น

อุปกรณ์ที่ทำหน้าที่ควบคุมการเข้าใช้

เนื่องจาก Wireless LAN Switch หรือ Controller ที่มีขายในท้องตลาดมีราคาสูงมาก ถึงแม้ว่าจะสามารถใช้ได้ทั้งกับแอกเซสพอยต์ที่ให้มาพร้อมระบบ และใช้ร่วมกับแอกเซสพอยต์ของยี่ห้ออื่น ๆ ผ่านทางช่องพอร์ตที่เรียกว่า 3rd Party Access Point ได้ก็ตาม แต่ปัจจัยเรื่องราคาและองค์ความรู้ที่จะได้จากการจัดทำอุปกรณ์ที่ทำหน้าที่ควบคุมการเข้าใช้ด้วยตนเองมีความสำคัญในการตัดสินใจเลือกศึกษาหาเทคโนโลยีในการให้บริการ Wireless Hotspot

จากการศึกษาค้นคว้าในอินเทอร์เน็ต จึงพบว่าเราสามารถสร้างอุปกรณ์ที่ทำหน้าที่ควบคุมการเข้าใช้งานโดยการติดตั้งซอฟต์แวร์สำหรับทำหน้าที่ดังกล่าวลงไปในเครื่องคอมพิวเตอร์เดสก์ท็อปทั่วไปที่มีแลนการ์ดจำนวน 2 การ์ด โดยที่เครื่องคอมพิวเตอร์นี้ทำหน้าที่เปรียบเสมือนเกตเวย์หรืออุปกรณ์จัดเส้นทางที่ส่งต่อแพ็กเก็ตเข้าออกอินเทอร์เน็ต และมีไฟร์วอลล์สำหรับอนุญาตการเข้าออกของพอร์ตที่ใช้งานเท่านั้น ซึ่งซอฟต์แวร์ดังกล่าวมีทั้งแบบการค้าและโอเพ่นซอร์ส การเลือกใช้ซอฟต์แวร์แบบโอเพ่นซอร์สจะเป็นทางเลือกที่เหมาะสมสำหรับสถานศึกษาและในงานวิจัยนี้ เพราะว่าการซื้อซอฟต์แวร์แบบการค้ามาติดตั้งจะทำให้ไม่สามารถต่อยอดของความรู้และปรับปรุงตามแนวทางที่ต้องการได้ อีกทั้งมีกลุ่มที่เป็นนักพัฒนาซอฟต์แวร์โอเพ่นซอร์สอยู่มากมายทั่วโลกที่มีการถามตอบเกี่ยวกับการทำงานของซอฟต์แวร์โอเพ่นซอร์ส จึงทำให้มีข้อมูลประกอบในการทำงานมากเพียงพอ จากเหตุผลดังกล่าวจึงเป็นที่มาในการเลือกใช้ซอฟต์แวร์สำหรับทำหน้าที่ควบคุมการเข้าใช้งาน และซอฟต์แวร์ชื่อ ChilliSpot เป็นซอฟต์แวร์โอเพ่นซอร์สที่ถูกเลือกมาใช้เพราะว่าสนับสนุนการพิสูจน์ตัวจริงแบบเว็บล็อกอิน และติดตั้งใช้กับระบบปฏิบัติการ Linux Fedora ได้

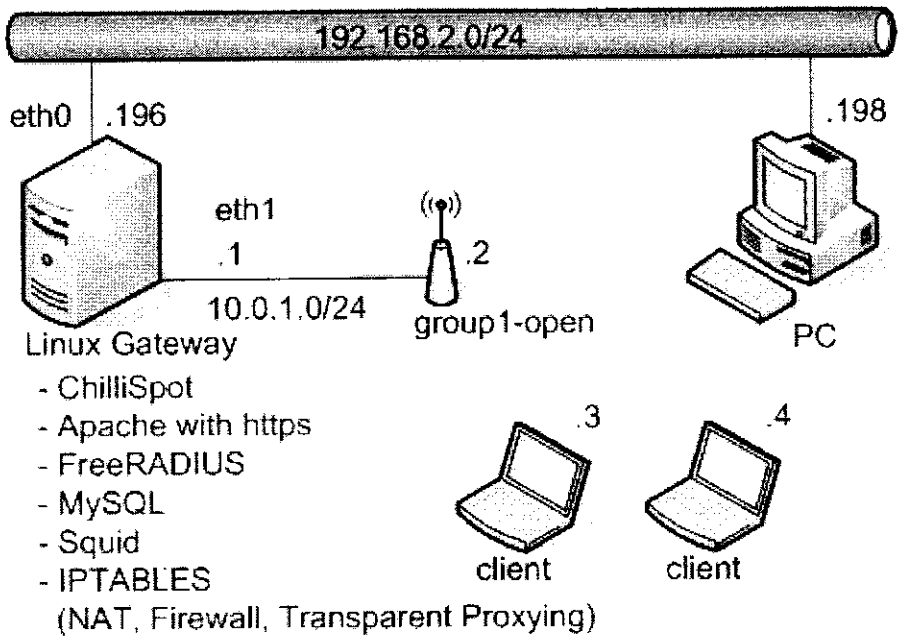
เมื่อพิจารณาถึงซอฟต์แวร์ที่จะเลือกมาใช้ในการพิสูจน์ตัวจริงเพื่อทำงานร่วมกับ ChilliSpot ส่วนมากจะเป็นซอฟต์แวร์ประเภท RADIUS Server ซอฟต์แวร์เหล่านี้มีทั้งที่เป็นแบบการค้าและโอเพ่นซอร์สเช่นกัน ซอฟต์แวร์ทางการค้าที่นิยมใช้กันมากคือ Funk Steel-Belted RADIUS ส่วนซอฟต์แวร์โอเพ่นซอร์สที่นิยมใช้กันมากคือ FreeRADIUS ซึ่งเป็นซอฟต์แวร์ที่มีนักพัฒนานำไปใช้งานกันอย่างกว้างขวางและมีคำแนะนำการติดตั้งหรือบล็อกถามตอบอยู่เป็นจำนวนมาก

FreeRADIUS ถูกออกแบบมาให้สามารถตั้งค่าการทำงานให้เลือกทำการพิสูจน์ตัวจริงด้วยชื่อผู้ใช้และรหัสผ่านที่อยู่ในไฟล์ชนิด Text File หรือฐานข้อมูลยอดนิยมหลายชนิด เช่น MySQL, LDAP หรือ Active Directory เป็นต้น นอกจากนี้มีเว็บเพจ "การติดตั้ง radius server ด้วยโปรแกรม freeradius" [11] ที่แนะนำว่าสามารถตั้งค่าการทำงานของ FreeRADIUS ให้ตรวจสอบชื่อผู้ใช้และรหัสผ่านของ UNIX หรือ IMAP Server ได้ การเลือกฐานข้อมูลชนิดใดขึ้นอยู่กับสภาพแวดล้อมของผู้ติดตั้ง เนื่องจากเป็นงานวิจัยที่มุ่งเน้นไปที่การสร้างต้นแบบที่เหมาะสมกับบริการ Wireless Hotspot ที่มีกลุ่มผู้ใช้คือผู้ที่ทำงานหรือเรียนอยู่ในมหาวิทยาลัย และผู้ที่มาร่วมทำงานเป็นครั้งคราวหรือแขกของมหาวิทยาลัย จึงเลือกที่จะใช้ MySQL เป็นฐานข้อมูลสำหรับเก็บชื่อผู้ใช้และรหัสผ่านสำหรับกลุ่มผู้ใช้ทุกกลุ่ม และเหตุผลสำคัญอีกประการหนึ่งคือ MySQL เป็นฐานข้อมูลที่มีการใช้งานอย่างแพร่หลาย มีหนังสือตำราและคำแนะนำในการเขียนโปรแกรมจัดการกับฐานข้อมูลชนิดนี้มากมายในอินเทอร์เน็ต นอกจากนี้ผู้วิจัยมีความสนใจที่จะพัฒนาโปรแกรมจัดการบัญชีผู้ใช้สำหรับใช้ในบริการ Wireless Hotspot ในโอกาสต่อไป

อย่างไรก็ตามในงานวิจัยนี้ไม่ได้มีการพัฒนาโปรแกรมจัดการบัญชีผู้ใช้เนื่องจากไม่อยู่ในขอบเขตของงาน แต่เพื่อให้ได้โปรแกรมมาอำนวยความสะดวกในการทำงาน จึงได้ค้นหาดูและพบว่ามีนักพัฒนากลุ่มหนึ่งพัฒนาโปรแกรมประเภทนี้ไว้แล้วอยู่ในขั้นที่สามารถใช้งานอย่างง่าย ๆ ได้ โปรแกรมนี้มีชื่อว่า phpMyPrepaid [12] สามารถจัดการบัญชีผู้ใช้ผ่านทางเว็บเบราว์เซอร์ที่สามารถสร้างบัญชีผู้ใช้ได้อย่างสะดวกและรวดเร็ว ดังนั้นการใช้ซอฟต์แวร์ดังกล่าวจึงเป็นทางเลือกที่เหมาะสม

3.2 การออกแบบ

เนื่องจากทำการทดลองในสภาพแวดล้อมของมหาวิทยาลัย จึงติดตั้งเครื่องทดสอบที่เป็นลินุกซ์เกตเวย์พร้อมซอฟต์แวร์โอเพ่นซอร์สที่จำเป็นทั้งหมดวางไว้ในแลนของศูนย์คอมพิวเตอร์ ซึ่งมีหมายเลขเครือข่ายเป็น 192.168.2.0/24



ภาพประกอบ 3.1 การเชื่อมต่อแลนไร้สายกับลินุกซ์เกตเวย์

ลินุกซ์เกตเวย์เป็นเครื่องไมโครคอมพิวเตอร์ชนิดเดสก์ท็อปที่ใช้หน่วยประมวลผลกลาง Pentium III 667 MHz หน่วยความจำ 512 MB และขนาดพื้นที่ว่างของฮาร์ดดิสก์ 20 GB ใส่แลนการ์ด 10/100 Mbps จำนวน 2 การ์ด โดยที่แลนการ์ดอันแรกจะเป็นอินเตอร์เฟสที่เชื่อมต่อไปยังแลนของศูนย์คอมพิวเตอร์ (eth0) และแลนการ์ดอันที่สองจะเป็นอินเตอร์เฟสที่เชื่อมต่อไปยังเครือข่ายภายในของแลนไร้สาย (eth1) ที่ประกอบด้วยแอกเซสพอยต์ที่ส่งสัญญาณคลื่นวิทยุภายใต้ SSID ชื่อ "group1-open" และไคลเอนต์จำนวนหนึ่งที่ต้องการใช้งานอินเทอร์เน็ต

ซอฟต์แวร์โอเพ่นซอร์สที่เลือกใช้ติดตั้งลงในลินุกซ์เกตเวย์ มีดังนี้

ติดตั้งระบบปฏิบัติการ Linux Fedora Core 6 ซึ่งเป็นที่คุ้นเคยเนื่องจากเป็นระบบปฏิบัติการที่ใช้สำหรับเซิร์ฟเวอร์ต่าง ๆ ในมหาวิทยาลัย

ติดตั้งซอฟต์แวร์ชื่อ ChilliSpot เพื่อทำหน้าที่ 2 อย่างคือจัดสรรเลขที่อยู่ไอพีให้กับไคลเอนต์ที่เชื่อมต่อ และตรวจสอบแพ็กเก็ตที่ผ่านอินเทอร์เฟส eth1 แพ็กเก็ตที่ผ่านได้ต้องเป็นแพ็กเก็ตของไคลเอนต์ที่ผ่านการพิสูจน์ตัวจริงแล้วเท่านั้น

ติดตั้งซอฟต์แวร์ชื่อ Apache Web Server เพื่อเก็บหน้าเว็บเพจสำหรับล็อกอินที่ประกอบด้วยช่องสำหรับใส่ชื่อผู้ใช้และช่องสำหรับใส่รหัสผ่าน เว็บเพจหน้านี้คือไฟล์ที่มีชื่อว่า hotspotlogin.cgi โดยมีการตั้งค่าให้ใช้โพรโทคอล HTTPS (ทีซีพีพอร์ตหมายเลข 443) เพื่อความปลอดภัยในการรับส่งข้อมูลชื่อผู้ใช้และรหัสผ่าน

ติดตั้งซอฟต์แวร์ชื่อ FreeRADIUS เพื่อรับข้อมูลการร้องขอพิสูจน์ตัวจริงของไคลเอนต์จาก ChilliSpot มาตรวจสอบกับข้อมูลชื่อผู้ใช้และรหัสผ่านในฐานข้อมูลที่เลือกใช้

ติดตั้งซอฟต์แวร์ชื่อ MySQL เพื่อใช้เป็นฐานข้อมูลสำหรับบัญชีผู้ใช้ที่จะใช้ในการทดลองนี้

ติดตั้งซอฟต์แวร์ชื่อ Squid เพื่อเป็นพร็อกซี่เซิร์ฟเวอร์ และทำรายงานการใช้งานเวิลด์ไวด์เว็บของไคลเอนต์ เนื่องจากทดลองในสภาพแวดล้อมของมหาวิทยาลัยที่มีการใช้งานพร็อกซี่เซิร์ฟเวอร์ จึงออกแบบให้มีการทำงานของ Squid ในรูปแบบ Parent – Child Proxy Server ระหว่าง Squid ในลินุกซ์เกตเวย์กับ Squid ในพร็อกซี่เซิร์ฟเวอร์ของมหาวิทยาลัย

แต่เพื่อให้สะดวกแก่ไคลเอนต์ที่จะไม่ต้องตั้งค่าพร็อกซี่ในเบราว์เซอร์ ใช้ iptables ทำ Transparent Proxy นอกจากนี้ยังใช้ iptables ทำ NAT เพื่อซ่อนเลขที่อยู่ไอพีของไคลเอนต์ และเป็นไฟร์วอลล์อนุญาตการเข้าออกของแพ็กเก็ตไปยังพอร์ตต่าง ๆ ในอินเทอร์เน็ตด้วย

และสุดท้ายเป็นซอฟต์แวร์ชื่อ phpMyPrepaid มีความสามารถในการจัดการบัญชีผู้ใช้ในฐานข้อมูลของซอฟต์แวร์ MySQL และใช้ร่วมกับ FreeRADIUS เพื่อกำหนดสิทธิการใช้ และมีความสามารถให้สั่งพิมพ์ชื่อผู้ใช้และรหัสผ่านในรูปแบบตั๋วเข้าใช้งาน (Prepaid Card) ได้ ซอฟต์แวร์นี้ยังต้องมีการปรับปรุงให้ดีขึ้นเนื่องจากยังอยู่ในขั้นเริ่มแรกของการพัฒนา ซอฟต์แวร์นี้จะไม่จำเป็นต้องใช้หากผู้ติดตั้งสามารถเขียนโปรแกรมจัดการบัญชีผู้ใช้ได้เอง หรือมีโปรแกรมอื่นที่ทำงานในลักษณะเดียวกันและมีขีดความสามารถที่ดีกว่า

3.3 สรุปท้ายบท

บทนี้ได้กล่าวถึงแนวคิดในการเลือกใช้เทคโนโลยีที่จะนำมาใช้ให้บริการ Wireless Hotspot และรายละเอียดการสร้างต้นแบบจากแนวคิดดังกล่าว เป็นการออกแบบที่ใช้ซอฟต์แวร์โอเพ่นซอร์สทั้งหมดทำงานร่วมกันบนระบบปฏิบัติการ Linux ภายในเครื่องเดียว สำหรับขั้นตอนการติดตั้งจะอยู่ในบทถัดไป

บทที่ 4

การติดตั้ง

สำหรับบทนี้จะอธิบายขั้นตอนการติดตั้งอุปกรณ์ควบคุมแลนไร้สายด้วย ChilliSpot สำหรับการพิสูจน์ตัวจริงแบบเว็บล็อกอิน ซึ่งแบ่งออกเป็น 3 ตอน ส่วนตอนที่ 4 เป็นการติดตั้งโปรแกรม phpMyPrepaid เพื่อเพิ่มความสะดวกในการจัดการบัญชีผู้ใช้ สำหรับผู้ที่สนใจวิธีติดตั้งแบบทำตามทีละขั้นอย่างละเอียดสามารถอ่านได้จากภาคผนวก

4.1 ขั้นตอนการติดตั้งในภาพรวม

ตอนที่ 1

- ติดตั้ง Linux Server
- ติดตั้งโปรแกรม Apache Web Server
- ติดตั้งโปรแกรม FreeRADIUS
- ทดสอบการพิสูจน์ตัวจริงด้วยชื่อผู้ใช้และรหัสผ่านของ UNIX
- ติดตั้งโปรแกรม ChilliSpot

เมื่อเสร็จสิ้นการติดตั้งในตอนที่ 1 นี้ จะทำให้ได้อุปกรณ์ควบคุมแลนไร้สายด้วย ChilliSpot โดยที่ไคลเอนต์ที่จะเข้าใช้งานได้ต้องมีชื่อผู้ใช้และรหัสผ่านของ UNIX ซึ่งเป็นการทดสอบการพิสูจน์ตัวจริงกับ FreeRADIUS และฐานข้อมูล UNIX

ตอนที่ 2

- ติดตั้งโปรแกรม MySQL
- สร้างฐานข้อมูล RADIUS ใน MySQL
- ตัวอย่าง RADIUS Attributes
- ทดสอบการพิสูจน์ตัวจริงด้วยชื่อผู้ใช้และรหัสผ่านของ MySQL
- sqlcounter

เมื่อเสร็จสิ้นการติดตั้งในตอนที่ 2 นี้ จะทำให้ได้อุปกรณ์ควบคุมแลนไร้สายด้วย ChilliSpot โดยที่ไคลเอนต์ที่จะเข้าใช้งานได้ต้องมีชื่อผู้ใช้และรหัสผ่านของ MySQL ซึ่งเป็นการทดสอบการพิสูจน์ตัวจริงกับ FreeRADIUS และฐานข้อมูล MySQL โดยใช้ตัวอย่างที่ได้มาจากอินเทอร์เน็ตนำมาดัดแปลงเพื่อทดสอบ RADIUS Attributes ที่จะใช้ในการกำหนดสิทธิการใช้งานในเรื่องระยะเวลานานที่สุดที่ผู้ใช้สามารถเชื่อมต่อได้ จำนวนข้อมูลที่ดาวน์โหลด/อัปโหลด และจำนวนครั้งที่อนุญาตการเข้าใช้ด้วยชื่อผู้ใช้เดียวกันในช่วงเวลาเดียวกัน การสร้างข้อมูลตัวอย่างนี้ใช้วิธีการพิมพ์ใหม่หรือคัดลอกคำสั่งลงไปในขณะที่ใช้งาน Command Line ของ MySQL

ตอนที่ 3

- ติดตั้งโปรแกรม Squid
- การทำ Transparent Proxy ด้วย iptables
- การบันทึกข้อมูลการใช้งานเวิลด์ไวด์เว็บ

ในตอนที่ 3 นี้เป็นความต้องการที่จะบันทึกข้อมูลการใช้งานเวิลด์ไวด์เว็บของไคลเอนต์ต่าง ๆ โดยการทำ Transparent Proxy ด้วย iptables ส่งแพ็กเก็ตที่จะไปยังทีซีพีพอร์ตหมายเลข 80 ในอินเทอร์เน็ตให้ไปหาโปรแกรม Squid เพื่อให้ Squid เป็นตัวแทนติดต่อกับเว็บเซิร์ฟเวอร์ และบันทึกข้อมูลการใช้งานซึ่งประกอบด้วย วันที่ เวลา เลขที่อยู่ไอพี โพรโทคอล และ URL

ตอนที่ 4

- ติดตั้งโปรแกรม phpMyPrepaid

ในตอนที่ 4 นี้ เป็นการติดตั้งโปรแกรมเพื่อเพิ่มความสะดวกในการจัดการบัญชีผู้ใช้ผ่านทางเว็บเบราว์เซอร์ ช่วยให้การสร้าง แก้ไข และลบบัญชีผู้ใช้ทำได้ง่ายขึ้น โดยไม่ต้องใช้วิธีพิมพ์ลงไปใน Command Line ของ MySQL

4.2 การติดตั้งตอนที่ 1

4.2.1 ติดตั้ง Linux Server

ติดตั้งระบบปฏิบัติการ Linux Fedora Core 6 จากแผ่นซีดีรอม เสร็จแล้วทำการปรับแต่งระบบปฏิบัติการ Linux หลังติดตั้งระบบ [13] ดังนี้

หลังจากระบบปฏิบัติการพร้อมใช้งานแล้ว ตั้งค่าเทียบเวลามาตรฐานด้วยคำสั่ง ntpdate ดังนี้

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

เพื่อให้การบันทึกวันที่และเวลาใกล้เคียงกับเครื่องคอมพิวเตอร์อื่น ๆ ในอินเทอร์เน็ต จะเป็นประโยชน์ในการตรวจสอบการเข้าใช้งานในภายหลัง จากนั้นเพิ่มเติมคำสั่งดังกล่าวไว้ในไฟล์ /etc/cron.daily/ntp.cron เพื่อให้ปรับให้เป็นปัจจุบันทุกวัน และไฟล์ /etc/rc.local เพื่อให้ปรับให้เป็นปัจจุบันทุกครั้งที่รีบูตเครื่อง

ปรับแพ็กเกจเพื่อให้ซอฟต์แวร์ที่ใช้เป็นเวอร์ชั่นล่าสุด ด้วยคำสั่ง

yum check-update

yum update

โดยจะมีการแก้ไขชื่อ Repository Server ที่จะขอใช้ในโฟลเดอร์ /etc/yum.repos.d ซึ่งในการติดตั้งนี้เลือกใช้เซิร์ฟเวอร์ที่ตั้งอยู่ในมหาวิทยาลัยเอง

แก้ไขไฟล์ /etc/selinux/config ที่เกี่ยวกับ Security-Enhanced Linux ให้เปลี่ยนจาก SELINUX=enforcing เป็น SELINUX=disabled เพื่อไม่ใช้งานในขณะนี้เพราะจะส่งผลต่อการแก้ไขการตั้งค่าการทำงาน และการติดตั้งโปรแกรม

4.2.2 ติดตั้งโปรแกรม Apache Web Server

ติดตั้งโปรแกรมด้วยคำสั่ง

yum install httpd

yum install httpd-manual

เพื่อให้สามารถส่งข้อมูลที่มีการเข้ารหัสข้อมูลในหน้าเว็บเพจสำหรับล็อกอินเมื่อใช้งาน ChilliSpot จึงติดตั้งโมดูล mod_ssl เพื่อใช้โพรโทคอล HTTPS ได้ ด้วยคำสั่ง

yum install mod_ssl

สั่งดำเนินงานโปรแกรมด้วยคำสั่ง

service httpd start

แล้วใช้คำสั่ง chkconfig httpd on เพื่อกำหนดให้ Apache Web Server ทำงานทุกครั้งที่รีบูตเครื่อง

หลังจากติดตั้ง Apache Web Server แล้วหากต้องการสั่งดำเนินงานหรือหยุดการทำงานให้ใช้คำสั่ง service httpd start และ service httpd stop ตามลำดับ

การแก้ไขการตั้งค่าการทำงานให้ทำที่ไฟล์ /etc/httpd/conf/httpd.conf และไฟล์อื่น ๆ ในไดเรกทอรี /etc/httpd/conf.d/ แล้วต้องสั่งรีสตาร์ทด้วยคำสั่ง service httpd restart และตรวจสอบว่า Apache ทำงานปกติหรือไม่ที่ไฟล์ /var/log/httpd/access.log

4.2.3 ติดตั้งโปรแกรม FreeRADIUS

ติดตั้งโปรแกรมด้วยคำสั่ง

yum install freeradius

สั่งดำเนินงานโปรแกรมด้วยคำสั่ง

service radiusd start

แล้วใช้คำสั่ง chkconfig radiusd on เพื่อกำหนดให้ FreeRADIUS ทำงานทุกครั้งที่รีบูตเครื่อง

หลังจากติดตั้ง FreeRADIUS แล้วหากต้องการสั่งดำเนินงานหรือหยุดการทำงานให้ใช้คำสั่ง service radiusd start และ service radiusd stop ตามลำดับ หรือในบางครั้งอาจต้องรันใน

โหมดดีบักเพื่อตรวจสอบการทำงานให้ใช้คำสั่ง radiusd -X แทนคำสั่ง service radiusd start และหยุดการทำงานด้วยการกดปุ่ม Ctrl - C

การแก้ไขการตั้งค่าการทำงานให้ทำที่ไฟล์ /etc/raddb/radiusd.conf และการกำหนดค่าเพื่ออนุญาตให้ RADIUS Client ใดบ้างสามารถร้องขอการพิสูจน์ตัวจริงกับ FreeRADIUS แก้ไขที่ไฟล์ /etc/raddb/clients.conf แล้วต้องสั่งรีสตาร์ทด้วยคำสั่ง service radiusd restart และตรวจสอบว่า FreeRADIUS ทำงานปกติหรือไม่ที่ไฟล์ /var/log/radius/radius.log และไฟล์อื่น ๆ ที่อยู่ในไดเรกทอรีเดียวกันนี้

4.2.4 ทดสอบการพิสูจน์ตัวจริงด้วยชื่อผู้ใช้และรหัสผ่านของ UNIX

ในขั้นตอนนี้จะใช้ชื่อผู้ใช้และรหัสผ่านของ UNIX ซึ่งผู้บริหารข่ายงานที่คุ้นเคยกับระบบปฏิบัติการ UNIX เข้าใจวิธีการทำอยู่แล้ว ทดสอบสร้างชื่อผู้ใช้ชื่อ chilli ด้วยคำสั่ง adduser chilli และตั้งรหัสผ่านด้วยคำสั่ง passwd chilli เป็น abcd1234 และจะต้องมีการตั้งค่าการทำงานของ FreeRADIUS ที่ไฟล์ /etc/raddb/radiusd.conf เพื่อทำการใส่เครื่องหมาย "#" หน้าบรรทัดข้อความ user = radiusd และ group = radiusd แก้ไขเป็นดังนี้

```
#user = radiusd
#group = radiusd
```

หลังจากแก้ไขไฟล์ต้องสั่งรีสตาร์ทโปรแกรมด้วยคำสั่ง

```
service radiusd restart
```

แล้วทดสอบด้วยคำสั่ง

```
radtest chilli abcd1234 localhost 0 testing123
```

ซึ่งจะมีการแจ้งข้อความ Access-Accept แสดงว่าการพิสูจน์ตัวจริงด้วยชื่อผู้ใช้และรหัสผ่านนี้ถูกต้อง โดยที่ localhost คือชื่อ RADIUS Server ที่ใช้ เลข 0 คือไม่ระบุหมายเลขพอร์ตที่ใช้ และคำว่า testing123 คือ Secret Key ที่ใช้ในการติดต่อกับ FreeRADIUS ซึ่งเป็นค่า default ที่ใคร ๆ ก็รู้ค่านี้ ในการใช้งานจริงควรเปลี่ยน Secret Key เป็นคำที่แตกต่างออกไปและเดาได้ยาก เช่น เปลี่ยนจาก testing123 เป็น mytestkey เป็นต้น

การเปลี่ยนแปลงค่า Secret Key ของ FreeRADIUS ต้องแก้ไขที่ไฟล์ /etc/raddb/clients.conf โดยที่ RADIUS Client ในที่นี้คือ 127.0.0.1 (เลขที่อยู่ไอพีของอินเตอร์เฟส loopback ซึ่งใช้ในการระบุถึงบริการที่ดำเนินงานอยู่ภายในเครื่อง) เพราะเป็นการใช้คำสั่ง radtest จากภายในเครื่องเดียวกับที่ติดตั้ง RADIUS Server

client 127.0.0.1 {

บรรทัดเดิม

secret = testing123

แก้ไขเป็น

secret = mytestkey

}

หลังจากแก้ไขไฟล์นี้แล้วต้องสั่งรีสตาร์ท FreeRADIUS ทุกครั้ง ในขณะนี้ได้เตรียมระบบที่เกี่ยวข้องในการพิสูจน์ตัวจริงพร้อมแล้ว ต่อไปจะเป็นการติดตั้งโปรแกรม ChilliSpot

4.2.5 ติดตั้งโปรแกรม ChilliSpot

ดาวน์โหลดโปรแกรม ChilliSpot สำหรับใช้งานกับระบบปฏิบัติการ Linux Fedora Core 6 จาก http://www.chillispot.info/download/chillispot-1.1.0.i386.rpm

ติดตั้งโปรแกรมด้วยคำสั่ง rpm -Uvh chillispot-1.1.0.i386.rpm แล้วตั้งค่าการทำงานโดยแก้ไขไฟล์ /etc/chilli.conf ให้เป็นดังนี้

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

อธิบายการตั้งค่าการทำงานได้ดังนี้ ใช้หมายเลขเครือข่าย 10.0.1.0/24 แทนค่า default 192.168.182.0/24 กำหนดให้ chilli ติดต่อกับ RADIUS Server ที่อยู่ภายในเครื่องเดียวกันนี้ กำหนดค่า radiussecret เป็น mytestkey ตรงกับค่า Secret Key ในไฟล์ /etc/raddb/clients.conf กำหนดค่า uamserver เป็น https://10.0.1.1/cgi-bin/hotspotlogin.cgi ซึ่งเป็นชื่อเว็บเพจที่ใช้ในขั้นตอนการล็อกอิน กำหนดค่า uamhomepage เป็นhttp://10.0.1.1/welcome.html เพื่อให้มีหน้าแนะนำบริการเพื่อเป็นข้อมูลแก่ผู้ที่เชื่อมต่อเข้ามา (ในหน้าเว็บเพจ welcome.html นี้จะมีเชื่อมโยงไปยัง uamserver อีกที) กำหนดค่า uamsecret เป็น ht2eb8ej6s4et3rg1ulp ค่านี้สำหรับการแลกเปลี่ยนคีย์ระหว่าง hotspotlogin.cgi กับ chilli ซึ่งจะต้องตรงกัน และสุดท้ายเป็นการกำหนดว่า chilli ใช้เลขที่อยู่ไอพี 10.0.1.1 ที่อินเตอร์เฟสเสมือน tun0 ที่สร้างขึ้น

ถัดไปคัดลอกไฟล์ hotspotlogin.cgi จากไดเรกทอรี /usr/share/doc/chillispot-1.1.0 ไปวางไว้ที่ /var/www/cgi-bin/ แล้วแก้ไขในไฟล์นี้โดยเอาเครื่องหมาย "#" ออกที่บรรทัดที่มีคำว่า $uamsecret และ $userpassword เป็นดังนี้

```
$uamsecret = "ht2eb8ej6s4et3rg1ulp"
$userpassword=1
```

เหตุผลที่ตั้งค่า $userpassword=1 เพื่อใช้ชื่อผู้ใช้และรหัสผ่านแบบข้อความธรรมดา (Clear Text) ซึ่งจะต้องตรงกับเขตข้อมูลรหัสผ่านของฐานข้อมูลที่เลือกใช้ ในการทดลองนี้ทุกฐานข้อมูลไม่ว่าจะเป็นชื่อผู้ใช้และรหัสผ่านของ UNIX หรือ MySQL จะใช้แบบนี้

ถัดไปสร้างไฟล์ welcome.html ซึ่งเป็นเว็บเพจแนะนำบริการดังภาพประกอบ 4.1 และนำไฟล์นี้ไปเก็บไว้ในไดเรกทอรี /var/www/html

Welcome to Our Hotspot, Wireless Network.

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

Click here to login

Enjoy.

ภาพประกอบ 4.1 เว็บเพจ welcome.html

จากภาพประกอบ 4.1 หน้าแนะนำบริการจะมีข้อความ Click here to login ซึ่งเป็นส่วนสำคัญที่จะเชื่อมโยงไปยังหน้าเว็บเพจสำหรับล็อกอิน ดังนี้

```
<a href="http://10.0.1.1:3990/prelogin">Click here to login</a>
```

โดยที่รายละเอียดภายในไฟล์ welcome.html สามารถดูได้จากภาคผนวก

ขั้นตอนต่อไปเป็นการตั้งค่าการทำงานไฟล์วอลล์ และ NAT โดยคัดลอกไฟล์ firewall.iptables ที่มีให้อยู่แล้วที่ /usr/share/doc/chillispot-1.1.0/firewall.iptables ไปเก็บไว้ที่ /etc โดยที่รายละเอียดภายในไฟล์ firewall.iptables สามารถดูได้จากภาคผนวก

เนื่องจากเครื่องนี้ทำหน้าที่เป็นลินุกซ์เกตเวย์ ต้องตั้งค่าการทำงานให้มีการรับส่งแพ็กเก็ตระหว่างอินเตอร์เฟส eth0 และ eth1 ด้วยคำสั่ง

```
echo "1" > /proc/sys/net/ipv4/ip_forward
```

แล้วแก้ไขในไฟล์ /etc/sysctl.conf ให้มีค่าเป็น net.ipv4.ip_forward = 1 เพื่อให้มีผลในทันทีสำหรับการรีบูตเครื่องในครั้งต่อไป

ตอนนี้การตั้งค่าการทำงานที่เกี่ยวข้องในการดำเนินงาน chilli เสร็จแล้ว

ลำดับในการสั่งดำเนินงานโปรแกรม ChilliSpot มีดังนี้

1. ตั้งค่าการทำงานแอกเซสพอยต์หรือไวร์เลสเร้าเตอร์ในส่วนที่เกี่ยวข้องกับ DHCP Server ให้เป็น Disable ตัวอย่างสำหรับแอกเซสพอยต์ยี่ห้อ Linksys รุ่น WAP54G, 3Com รุ่น 3CRWE454G72, Cisco รุ่น Aironet1100 (802.11b) และไวร์เลสเร้าเตอร์ยี่ห้อ NETGEAR รุ่น DG834G ดูรายละเอียดได้จากภาคผนวก
2. สั่งดำเนินงาน iptables เพื่อทำหน้าที่ไฟร์วอลล์ และ NAT ด้วยคำสั่ง

   sh /etc/firewall.iptables
3. สั่งดำเนินงาน chilli ด้วยคำสั่ง

   service chilli start
4. ตรวจสอบการทำงาน ด้วยคำสั่ง

   ifconfig

   ผลลัพธ์จะเห็นอินเตอร์เฟส tun0 มีไอพีแอดเดรส 10.0.1.1

ทดสอบการเข้าใช้ Wireless HotSpot ด้วยชื่อผู้ใช้ของ UNIX

ทดสอบนำเครื่องโน้ตบุ๊คเชื่อมต่อและเข้าใช้ด้วยชื่อผู้ใช้ chilli และรหัสผ่าน abcd1234 จะพบว่ามีหน้าต่างแสดงข้อความว่า Logged in to ChilliSpot พร้อมตัวเลขที่นับเวลาที่ใช้งานเพิ่มขึ้นเรื่อย ๆ

เพื่อให้การสั่งดำเนินงาน chilli ทำโดยอัตโนมัติเมื่อรีบูตเครื่อง ต้องเพิ่มคำสั่งเพื่อดำเนินงาน iptables และดำเนินงาน chilli ลงไฟล์ /etc/rc.local

4.3 การติดตั้งตอนที่ 2

4.3.1 ติดตั้งโปรแกรม MySQL

ติดตั้งโปรแกรมด้วยคำสั่ง

yum install mysql

yum install mysql-server

ติดตั้งโปรแกรมที่ทำให้ MySQL ทำงานร่วมกับ FreeRADIUS ได้

yum install freeradius-mysql

สั่งดำเนินงานโปรแกรมด้วยคำสั่ง

service mysqld start

แล้วใช้คำสั่ง chkconfig mysqld on เพื่อกำหนดให้ MySQL ทำงานทุกครั้งที่รีบูตเครื่อง

หลังจากติดตั้ง MySQL แล้วหากต้องการสั่งดำเนินงานหรือหยุดการทำงานให้ใช้คำสั่ง service mysqld start และ service mysqld stop ตามลำดับและหากต้องการรีสตาร์ทก็ใช้คำสั่ง service mysqld restart

ภายหลังติดตั้ง MySQL ใหม่ ๆ ยังไม่มีรหัสผ่านของ root ให้ตั้งค่าเป็น abcd1234 ด้วยคำสั่ง

/usr/bin/mysqladmin -u root password 'abcd1234'

4.3.2 สร้างฐานข้อมูล RADIUS ใน MySQL

จากการศึกษาเว็บเพจ "FreeRadius and MySQL HowTo Notes" [14] ที่ค้นหาในอินเทอร์เน็ต มีคำแนะนำการสร้างฐานข้อมูล RADIUS ใน MySQL จึงนำตัวอย่างนั้นมาดัดแปลงเพื่อใช้ทดสอบ RADIUS Attributes ที่ใช้กำหนดสิทธิการใช้งาน

ต่อไปจะเป็นการสร้างฐานข้อมูลชื่อ radius และชื่อผู้ใช้ชื่อ radius ที่มีสิทธิครบถ้วนในฐานข้อมูลนี้

เข้าทำงานในแบบวิธี Command Line ดังนี้

mysql -uroot -pabcd1234

สร้างฐานข้อมูลชื่อ radius ดังนี้

CREATE DATABASE radius;

GRANT ALL PRIVILEGES ON radius.* to 'radius'@'localhost' IDENTIFIED BY 'abcd1234';

FLUSH PRIVILEGES;

QUIT

นำเข้าเค้าร่างฐานข้อมูล (Database Schema) ลงในฐานข้อมูลชื่อ radius นั้น ซึ่ง FreeRADIUS เตรียมไฟล์เค้าร่างฐานข้อมูลดังกล่าวไว้ให้แล้ว (โปรดสังเกตว่าไดเรกทอรีชื่อ freeradius-1.1.3 ก็คือ FreeRADIUS เวอร์ชั่น 1.1.3) ใช้คำสั่งดังนี้

mysql -uroot -pabcd1234 radius < /usr/share/doc/freeradius-1.1.3/examples/mysql.sql

4.3.3 ตัวอย่าง RADIUS Attributes

ข้อมูลตัวอย่างที่ใช้ทดสอบดังนี้

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

เข้าทำงานในแบบวิธี Command Line ดังนี้

mysql -uroot -pabcd1234

ใส่ข้อมูลตัวอย่างดังนี้

use radius;

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 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 usergroup (UserName, GroupName) VALUES ('fredf', 'dynamic');

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 radgroupreply (GroupName, Attribute, Op, Value) VALUES ('dynamic', 'Service-Type', ':=', 'Login-User');

แก้ไขไฟล์ /etc/raddb/sql.conf เพื่อใช้ฐานข้อมูลชื่อ “radius” ที่สร้างขึ้นนี้

login = "radius"

password = "abcd1234"

radius_db = "radius"

แก้ไขไฟล์ /etc/raddb/radiusd.conf เพื่อให้ FreeRADIUS ทำการพิสูจน์ตัวจริงกับฐานข้อมูล MySQL โดยค้นหาบรรทัดที่ต้องการ ดังนี้

ในส่วน module { ... }

เอาเครื่องหมาย “#” ออกจากหน้าบรรทัดข้างล่างนี้

$INCLUDE ${confdir}/sql.conf

ในส่วน authorize { ... }

ใส่เครื่องหมาย “#” หน้าบรรทัดข้างล่างนี้

#files

เอาเครื่องหมาย “#” ออกจากหน้าบรรทัดข้างล่างนี้

sql

ในส่วน accounting { ... }
เอาเครื่องหมาย "#" ออกจากหน้าบรรทัดข้างล่างนี้
sql

สั่งรีสตาร์ท FreeRADIUS ด้วยคำสั่ง
service radiusd restart

4.3.4 ทดสอบการพิสูจน์ตัวจริงด้วยชื่อผู้ใช้และรหัสผ่านของ MySQL

ทดสอบโดยใช้ชื่อผู้ใช้ fredf ที่สร้างขึ้น ด้วยคำสั่งดังนี้
radtest fredf wilma localhost 0 mytestkey

ผลลัพธ์ที่แสดงว่าใช้ชื่อผู้ใช้และรหัสผ่านของ MySQL ได้แล้ว
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

4.3.5 sqlcounter

การดำเนินการให้สามารถใช้ RADIUS Attributes เพื่อเก็บข้อมูลระยะเวลาการใช้งานที่ใช้ไปจะต้องมีการใช้ sqlcounter จากการศึกษาในเรื่อง Rlm_sqlcounter [15] ให้ทำดังนี้

แก้ไขไฟล์ /etc/raddb/radiusd.conf โดยใส่ 3 บรรทัดนี้ไว้ท้ายสุดของส่วน authorize { ... }

noresetcounter
dailycounter

monthlycounter

ค้นหาและแทรก sqlcounter name ชื่อ noresetcounter ไว้ใกล้ ๆ กับ dailycounter ดังนี้

```
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}'"
}
```

ทดสอบการเข้าใช้ Wireless HotSpot ด้วยชื่อผู้ใช้ของ MySQL

ทดสอบนำเครื่องโน้ตบุ๊คเชื่อมต่อและเข้าใช้ด้วยชื่อผู้ใช้ fredf และพาสเวิร์ด wilma จะพบว่ามีหน้าต่างแสดงข้อความว่า Logged in to ChilliSpot พร้อมตัวเลขที่นับเวลาที่ใช้งาน (Session Time) ลดลงเรื่อย ๆ

4.4 การติดตั้งตอนที่ 3

4.4.1 ติดตั้งโปรแกรม Squid

ติดตั้งโปรแกรมด้วยคำสั่ง

```
yum install squid
```

สร้างไดเรกทอรีเพื่อเก็บข้อมูลเว็บแคช

```
squid –z
```

การตั้งค่าการทำงานในไฟล์ /etc/squid/squid.conf ดังนี้

http_port 3128 transparent

acl our_networks src 10.0.1.0/24

http_access allow our_networks

อธิบายการตั้งค่าได้ดังนี้ เพื่อให้ Squid ทำงานแบบวิธี Transparent Proxy และอนุญาตไคลเอนต์ที่อยู่ภายในเครือข่าย 10.0.1.0/24 เท่านั้น

กรณีที่มีพร็อกซี่/เว็บแคชเซิร์ฟเวอร์ของมหาวิทยาลัย ต้องกำหนดค่า 2 บรรทัดข้างล่างนี้

cache_peer cache.your.domain parent port 0 no-query

never_direct allow all

ตัวอย่างสำหรับมหาวิทยาลัยสงขลานครินทร์ เปลี่ยน cache.your.domain เป็นชื่อ cache.psu.ac.th และ port เป็น 8080 จะได้ดังนี้

cache_peer cache.psu.ac.th parent 8080 0 no-query

never_direct allow all

สั่งดำเนินงาน Squid ด้วยคำสั่ง

service squid start

แล้วใช้คำสั่ง chkconfig squid on เพื่อกำหนดให้ Squid ทำงานทุกครั้งที่รีบูตเครื่อง

หลังจากติดตั้ง Squid แล้วหากต้องการสั่งดำเนินงานหรือหยุดการทำงานให้ใช้คำสั่ง service squid start และ service squid stop ตามลำดับ

4.4.2 การทำ Transparent Proxy ด้วย iptables

แก้ไขแฟ้ม /etc/firewall.iptables โดยเพิ่มบรรทัดเหล่านี้

อนุญาตการเชื่อมต่อโพรโทคอลทีซีพี พอร์ตหมายเลข 3128 เข้ามาที่เครื่องนี้

$IPTABLES -A INPUT -p tcp -m tcp --dport 3128 --syn -j ACCEPT

แต่ไม่อนุญาตให้มีการเชื่อมต่อโพรโทคอลทีซีพี พอร์ตหมายเลข 3128 ผ่านอินเตอร์เฟส tun0

$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp --dport 3128 --syn -j DROP

อนุญาตให้มีการเชื่อมต่อโพรโทคอลทีซีพี พอร์ตหมายเลข 80 ผ่านอินเตอร์เฟส tun0 เมื่อปลายทางเป็นเลขที่อยู่ไอพีในชุดที่เป็น Private IP

$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

นอกจากนั้นให้ส่งต่อไปยังโปรแกรม Squid ที่เปิดโพรโทคอลทีซีพี พอร์ตหมายเลข 3128 รอรับ

$IPTABLES -t nat -A PREROUTING -i tun0 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 3128

และทุกครั้งที่มีการแก้ไขไฟล์นี้ ต้องสั่งดำเนินงานดังนี้

sh /etc/firewall.iptables

4.4.3 การเก็บข้อมูลการใช้เวิลด์ไวด์เว็บ

วิธีการเก็บข้อมูลที่ไคลเอนต์ติดต่อไปยังเว็บไซต์ต่าง ๆ สามารถทำได้หลายวิธี วิธีที่นำเสนอนี้เป็นการใช้ความสามารถของ Cron ที่มีอยู่แล้วในระบบปฏิบัติการ UNIX สั่งให้ Shell Script ที่เขียนขึ้นนั้นทำงานตามเวลาที่กำหนดเช่น ทุกคืน เป็นต้น

สร้างไฟล์ Shell Script ชื่อ rotate_and_keep_proxy_log เพื่อเก็บบรรทัดคำสั่งที่ใช้ในการ rotate log และเก็บข้อมูลการติดต่อไปยังเว็บไซต์ต่าง ๆ ในรูปแบบย่อจากไฟล์ access.log

ของ Squid เพื่อให้อ่านง่ายและประหยัดเนื้อที่ โดยจะต้องนำไฟล์ Shell Script นี้ไปไว้ที่ไดเรกทอรี /etc/cron.daily/ แล้วเปลี่ยนคุณลักษณะของไฟล์ด้วยคำสั่ง chmod +x rotate_and_keep_proxy_log

ข้อมูลภายในไฟล์มีดังนี้

```
#!/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}
```

ผลลัพธ์จะได้ไฟล์ access.log.cache.YYYYMMDD โดยที่ YYYY คือปีค.ศ. MM คือเดือน และ DD คือวันที่ เช่น access.log.cache.20071130 เป็นต้น

ตัวอย่างข้อมูล

```
Thu Nov 29 11:03:58 2007 10.0.1.4 GET http://www.google.co.th/
Thu Nov 29 11:07:00 2007 10.0.1.4 GET http://www.google.co.th/gen_204?
```

4.5 การติดตั้งตอนที่ 4

4.5.1 ติดตั้งโปรแกรม phpMyPrepaid

สร้างฐานข้อมูลชื่อ phpmyprepaid ใน MySQL โดยใช้คำสั่งดังนี้

CREATE DATABASE phpmyprepaid;

GRANT ALL PRIVILEGES ON phpmyprepaid.* to 'radius'@'localhost' IDENTIFIED BY 'abcd1234';

FLUSH PRIVILEGES;

แก้ไขไฟล์ /etc/raddb/sql.conf เพื่อให้ใช้ฐานข้อมูลชื่อ “phpmyprepaid” แทนฐานข้อมูลชื่อ “radius” ที่ตั้งค่าไว้ในตอนที่ 3

```
# Connect info
server = "localhost"
login = "radius"
```

password = "abcd1234"

Database table configuration

radius_db = "phpmyprepaid"

ดาวน์โหลดโปรแกรม phpMyPrepaid เวอร์ชั่น 0.4b3 จาก URL

http://downloads.sourceforge.net/phpmyprepaid/phpmyprepaid04b3.tgz

ทำการแตกไฟล์ออกมาในไดเรกทอรี /var/www/html/phpmyprepaid และเปลี่ยนสิทธิในไดเรกทอรีและไฟล์ให้เป็นของ Apache

เนื่องจากโปรแกรม phpMyPrepaid เขียนขึ้นด้วยภาษา PHP และใช้งานร่วมกับโปรแกรม RRDTOOL จึงต้องทำการติดตั้งเพิ่มด้วยคำสั่งดังนี้

yum install php

yum install php-mysql

yum install rrdtool

จากนั้นตั้งค่าการทำงานครั้งแรกของโปรแกรม phpMyPrepaid ผ่านทางเบราว์เซอร์ที่เครื่องเซิร์ฟเวอร์นี้โดยระบุ URL เป็น http://localhost/phpmyprepaid/www/install/setup.php ซึ่งจะมี 9 ขั้นตอน ส่วนใหญ่จะไม่ต้องแก้ไขค่าใด ๆ ให้ใช้ค่าที่เตรียมมาให้ เฉพาะในขั้นตอนที่ 6 เป็นการกำหนดชื่อผู้ใช้และรหัสผ่านของ Administrator สำหรับจัดการฐานข้อมูลชื่อ phpmyprepaid

ต่อไปเป็นการเรียกใช้โปรแกรมหลังจากตั้งค่าการทำงานครั้งแรกเสร็จแล้ว

โดยระบุ URL เป็น http://localhost/phpmyprepaid/www/ ที่เบราว์เซอร์ ขั้นตอนนี้จะต้องใช้ชื่อผู้ใช้และรหัสผ่านของ Administrator เพื่อเข้าทำงาน

ภาพประกอบ 4.2 หน้าสำหรับลงชื่อเข้าใช้โปรแกรม phpMyPrepaid

ภาพประกอบ 4.3 หน้าแรกโปรแกรม phpMyPrepaid

4.5.2 การสร้างบัญชีผู้ใช้

การสร้างบัญชีผู้ใช้อย่างรวดเร็ว (Quick Print) โปรแกรมจะเตรียม Billing Plan ไว้ 2 อย่างคือ 30 Minutes และ 10 Hours ซึ่งเป็นแบบ Timed Account

เมนูสร้างบัญชีผู้ใช้ (Create Accounts) จะมีแบบต่าง ๆ ให้เลือกดังนี้

- Timed Accounts คือ บัญชีผู้ใช้ที่ชื่อผู้ใช้ถูกสร้างขึ้นจากตัวอักษรภาษาอังกฤษโดยอัตโนมัติ เป็นบัญชีผู้ใช้ที่นับจำนวนเวลาที่ใช้งานตรวจสอบกับ Billing Plan ที่กำหนดค่าไว้
- Octets Accounts คือบัญชีผู้ใช้ที่ชื่อผู้ใช้ถูกสร้างขึ้นจากตัวอักษรภาษาอังกฤษโดยอัตโนมัติ เป็นบัญชีผู้ใช้ที่นับจำนวนไบต์ที่ใช้งานตรวจสอบกับ Billing Plan ที่กำหนดค่าไว้
- Subscriber Time คือ บัญชีผู้ใช้ที่ตั้งชื่อเองได้ตามใจชอบ พร้อมทั้งข้อมูล ชื่อ – นามสกุล เลขที่บัตรประจำตัว กำหนดจำนวนเวลาที่ให้ใช้ตามต้องการ
- Subscriber Octets คือ บัญชีผู้ใช้ที่ตั้งชื่อเองได้ตามใจชอบ พร้อมทั้งข้อมูล ชื่อ – นามสกุล เลขที่บัตรประจำตัว กำหนดจำนวนไบต์ที่ให้ใช้ตามต้องการ
- Expiration Accounts คือ บัญชีผู้ใช้ที่ชื่อผู้ใช้ถูกสร้างขึ้นจากตัวอักษรภาษาอังกฤษโดยอัตโนมัติ เป็นบัญชีผู้ใช้ที่เช็ควันที่หมดอายุตรวจสอบกับ Billing Plan ที่กำหนดค่าไว้

ตัวอย่างการสร้างบัญชีผู้ใช้อย่างรวดเร็ว เมื่อเลือก Billing Plan แบบ 30 Minutes จะได้ผลลัพธ์ดังนี้

Username	Password	Validity
qjaiaa	eyq	30 minutes

ภาพประกอบ 4.4 ตัวอย่างบัญชีผู้ใช้ที่สร้างด้วยโปรแกรม phpMyPrepaid

ทดสอบการเข้าใช้ Wireless Hotspot ด้วยชื่อผู้ใช้ที่สร้างด้วย phpMyPrepaid

ทดสอบนำเครื่องโน้ตบุ๊คเชื่อมต่อและเข้าใช้ด้วยชื่อผู้ใช้ qjaiaa และรหัสผ่าน cyq จะพบว่ามีหน้าต่างแสดงข้อความว่า Logged in to ChilliSpot พร้อมตัวเลขที่นับเวลาที่ใช้งาน (Session Time) ลดลงเรื่อย ๆ จาก 30 นาที ไปจนหมด และไม่สามารถใช้งานต่อได้

4.6 สรุปท้ายบท

สำหรับบทนี้ได้อธิบายขั้นตอนการติดตั้งอุปกรณ์ควบคุมแลนไร้สายด้วย ChilliSpot สำหรับการพิสูจน์ตัวจริงแบบเว็บล็อกอินด้วยการติดตั้งซอฟต์แวร์โอเพ่นซอร์สหลายโปรแกรมลงในเครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Linux Fedora Core 6 ในตอนแรกแสดงให้เห็นว่าสามารถใช้ชื่อผู้ใช้และรหัสผ่านของ UNIX จากนั้นเปลี่ยนไปใช้ชื่อผู้ใช้และรหัสผ่านจากฐานข้อมูล MySQL พร้อมตัวอย่าง RADIUS Attributes ที่ใช้นับจำนวนเวลาที่ใช้ไป แต่การสร้างบัญชีผู้ใช้เป็นการป้อนข้อมูลเข้าในแบบวิธี Command Line ของ MySQL ซึ่งเป็นแบบธรรมดาที่ใช้เวลามาก ในตอนต่อมาอธิบายถึงการติดตั้งโปรแกรม Squid และการทำ Transparent Proxy เพื่อเก็บข้อมูลการใช้งานเวิลด์ไวด์เว็บ และในตอนสุดท้ายอธิบายขั้นตอนการติดตั้งโปรแกรม phpMyPrepaid เพื่อใช้ในการสร้างบัญชีผู้ใช้ผ่านทางเบราว์เซอร์แทนการป้อนข้อมูลเข้าในแบบวิธี Command Line ของ MySQL ซึ่งสะดวกกว่ามาก

บทที่ 5

บทสรุป ปัญหาและข้อเสนอแนะ

สำหรับบทนี้จะกล่าวถึงบทสรุปของโครงงาน ปัญหาและอุปสรรคที่เกิดขึ้นระหว่างการทำโครงงานซึ่งนำเสนอวิธีการหรือข้อเสนอแนะเพื่อแก้ปัญหาดังกล่าว

6.1 บทสรุปของโครงงาน

ผลที่ได้จากงานวิจัยคือต้นแบบการรักษาความปลอดภัยแลนไร้สายสำหรับแอกเซสพอยต์ราคาถูกด้วยวิธีการพิสูจน์ตัวจริงแบบเว็บล็อกอินโดยใช้ซอฟต์แวร์โอเพ่นซอร์สชื่อ ChilliSpot ทำงานบนระบบปฏิบัติการ Linux Fedora Core 6 ใช้ FreeRADIUS ในการพิสูจน์ตัวจริงกับฐานข้อมูล MySQL ใช้ Squid เก็บข้อมูลการใช้งานเวิลด์ไวด์เว็บของไคลเอนต์ และใช้ phpMyPrepaid เป็นโปรแกรมจัดการบัญชีผู้ใช้และออกตั๋วเข้าใช้งานเพื่อให้บริการ Wireless Hotspot

นอกจากนี้มีการนำความรู้ที่ได้จัดทำเว็บเพจเผยแพร่ความรู้ชนิด How To เพื่อเป็นแหล่งความรู้สำหรับผู้สนใจ ซึ่งได้นำเว็บเพจดังกล่าวมาใส่ไว้ในภาคผนวกของเอกสารนี้ด้วยแล้ว และอ่านเพิ่มเติมได้ที่ http://mamboeasy.psu.ac.th/~wiboon.w/content/view/58/40/

6.2 ปัญหา/อุปสรรค และการแก้ปัญหา

ปัญหาและอุปสรรคที่เกิดขึ้นระหว่างการทำโครงงานคือ การเซตแอกเซสพอยต์หรือไวร์เลสเร้าเตอร์ที่จะนำมาใช้งานกับ ChilliSpot จะมีปัญหาในเรื่องความเข้าใจในการตั้งค่า Factory Default เพื่อยกเลิกรหัสผ่านและค่าอื่น ๆ ที่ตั้งไว้ก่อนหน้านี้ ต้องทำหลายครั้งจึงสำเร็จ สาเหตุอาจเกิดจากความไม่คุ้นเคยอุปกรณ์ในแต่ละยี่ห้อ ทำให้บางครั้งเข้าใจว่าทำสำเร็จแล้ว แต่ความจริงยังไม่สำเร็จ แต่ก็สามารถทำความเข้าใจและแก้ปัญหาไปได้ในเวลาต่อมา

ปัญหาต่อมาคือหลังจากตั้งค่าตามที่ต้องการได้แล้ว แอกเซสพอยต์หรือไวร์เลสเร้าเตอร์จะถูกนำไปเชื่อมต่อกับเซิร์ฟเวอร์ที่ติดตั้ง ChilliSpot และทดสอบใช้โน้ตบุ๊คเชื่อมต่อเครือข่ายเข้าใช้งาน เมื่อพบว่าไม่ทำงานตามที่ต้องการ จึงเข้าไปตรวจสอบที่แอกเซสพอยต์ แต่ไม่สามารถเข้าไปทางเบราว์เซอร์ได้อีก เพราะตอนนี้แอกเซสพอยต์ถูกตั้งค่าการทำงานให้ใช้เลขที่อยู่

ไอพีที่ได้รับจาก DHCP Server จึงต้องกลับไปตั้งค่า Factory Default ใหม่เพื่อใช้เลขที่อยู่ไอพีที่เป็นค่า default จากโรงงานที่แสดงอยู่ในคู่มือการใช้เพื่อให้เข้าไปตั้งค่าการทำงานได้อีก แต่เมื่อทำอยู่บ่อย ๆ ก็เกิดความเข้าใจมากขึ้น ก็ไม่เป็นอุปสรรคในการทำงานอีก

เนื่องจาก RADIUS Server เป็นเรื่องที่มีรายละเอียดมาก การทดสอบตั้งค่า RADIUS Attributes เพื่อการบันทึกการใช้งานต้องใช้เวลาลองผิดลองถูก จึงเสียเวลาไปค่อนข้างมาก เนื่องจากเป็นความรู้ที่ค่อนข้างจะหาตัวอย่างยากในอินเทอร์เน็ตและไม่มีใครให้สอบถามได้เพราะเป็นเรื่องเฉพาะทางจริง ๆ ยังไม่มีใครศึกษาในเรื่องดังกล่าว

6.3 ข้อเสนอแนะ

ต้นแบบที่ได้นี้เหมาะสมกับการให้บริการ Wireless Hotspot ซึ่งมีเพียงไคลเอนต์ใช้งานเท่านั้นหากต้องการนำไปใช้ในการควบคุมการใช้งานทั้งแลนและแลนไร้สาย หากมีเซิร์ฟเวอร์ที่ให้บริการอยู่ในแลน ควรเพิ่มเติมแลนการ์ดอีก 1 ใบสำหรับสร้างเครือข่ายสำหรับเซิร์ฟเวอร์ต่างหาก หรือตั้งค่าการทำงานของ ChilliSpot ให้มีการแบ่งเลขที่อยู่ไอพีจำนวนหนึ่งสำหรับเซิร์ฟเวอร์และตั้งค่าให้ไม่ต้องมีการพิสูจน์ตัวจริง อย่างไรก็ตามไม่ใช่เรื่องง่าย ๆ ในการประยุกต์ใช้ ChilliSpot สำหรับแนวทางอื่น ๆ เพราะว่าต้องมีการแก้ไขการตั้งค่าการทำงานของไฟร์วอลล์ที่ใช้คำสั่ง iptables ให้เหมาะสมอีกด้วย

การเก็บข้อมูลการใช้อินเทอร์เน็ตอื่นๆ นอกเหนือจากข้อมูลการใช้เวิลด์ไวด์เว็บที่เก็บจากไฟล์ access.log ของโปรแกรม Squid แล้วต้องใช้โปรแกรมอื่นมาช่วย เช่น syslog-ng หรือ tcpdump เป็นต้น ซึ่งเป็นเรื่องที่จะได้ศึกษาในรายละเอียดต่อไป

ผู้ที่จะนำต้นแบบนี้ไปใช้ควรมีการศึกษาการใช้โปรแกรม phpMyPrepaid และ RADIUS Attributes เพิ่มเติมเพื่อให้สามารถสร้างบัญชีผู้ใช้แบบต่าง ๆ ได้ตามต้องการ รวมทั้งต้องเพิ่มเติมความรู้การใช้งานระบบปฏิบัติการ Linux และคำสั่ง iptables เพื่อให้สามารถปรับแต่งการทำงานไฟร์วอลล์ได้ตามต้องการ

บรรณานุกรม

[1] เว็บไซต์ซอฟต์แวร์ ChilliSpot. **Open Source Wireless LAN Access Point Controller.** http://www.chillispot.org (สืบค้นเมื่อ 19 กรกฎาคม 2549).

[2] เว็บไซต์ Community Ubuntu Documentation. **WifiDocsChillispotHotspot.** https://help.ubuntu.com/community/WifiDocs/ChillispotHotspot (สืบค้นเมื่อ 19 กรกฎาคม 2549).

[3] **wireless: Chillispot Howto.** http://140.105.28.77:3455/1/62 (สืบค้นเมื่อ 19 กรกฎาคม 2549).

[4] **Authenticated Wireless Network w/ Open Source Tools.** http://www.jlc.org.il/lectures/42/ (สืบค้นเมื่อ 26 กรกฎาคม 2549).

[5] อำนาจ มีมงคล, อรรณพ ขันธิกุล. 2547. **ออกแบบและติดตั้งเครือข่าย Wireless LAN.** นนทบุรี. ไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็ตเตอร์.

[6] **Understanding Wireless LAN Switching.** http://www.connect802.com/wireless_switch.htm (สืบค้นเมื่อ 20 ธันวาคม 2550).

[7] สมเกียรติ รุ่งเรืองลดา. 2544. **คัมภีร์ Home Networking.** กรุงเทพ. โปรวิชั่น.

[8] เว็บไซต์ Wikipedia. **Captive portal.** http://en.wikipedia.org/wiki/Captive_portal (สืบค้นเมื่อ 20 ธันวาคม 2550).

[9] เว็บไซต์ Wikipedia. **RADIUS.** http://en.wikipedia.org/wiki/RADIUS (สืบค้นเมื่อ 20 ธันวาคม 2550).

[10] **Transparent Cache Implementation Using Squid.** http://www.visolve.com/squid/whitepapers/trans_caching.php (สืบค้นเมื่อ 12 กรกฎาคม 2550).

[11] วิภัทร ศรุติพรหม. **การติดตั้ง radius server ด้วยโปรแกรม freeradius.** http://rd.cc.psu.ac.th/content/view/35/46/ (สืบค้นเมื่อ 10 มกราคม 2550).

[12] เว็บไซต์ซอฟต์แวร์ phpMyPrepaid. **phpMyPrepaid.** http://sourceforge.net/projects/phpmyprepaid/ (สืบค้นเมื่อ 20 กรกฎาคม 2549).

[13] วิภัทร ศรุติพรหม. **การปรับแต่งระบบลินุกซ์หลังการติดตั้ง.** http://rd.cc.psu.ac.th/content/view/14/46/ (สืบค้นเมื่อ 10 มกราคม 2550).

[14] **FreeRadius and MySQL HowTo Notes.** http://www.frontios.com/freeradius.html (สืบค้นเมื่อ 29 กรกฎาคม 2549).

[15] เว็บไซต์ FreeRADIUS Wiki. **Rlm sqlcounter.**

http://wiki.freeradius.org/index.php?title=Rlm_sqlcounter (สืบค้นเมื่อ 10 มกราคม 2550).

ขั้นตอนการติดตั้ง

คัดลอกจากบล็อก Wiboon at PSU - chillispot wifi
http://mamboeasy.psu.ac.th/~wiboon.w/content/category/5/23/40/

การติดตั้งอุปกรณ์ควบคุมแลนไร้สายด้วย ChilliSpot สำหรับการพิสูจน์ตัวจริงแบบเว็บล็อกอิน

คัดลอกจากเว็บเพจเรื่อง "การทำ Wireless LAN Controller ด้วย ChilliSpot แบบ web login + freeradius + mysql + transparent proxy"
http://mamboeasy.psu.ac.th/~wiboon.w/content/view/58/40/

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 attributes
    - 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

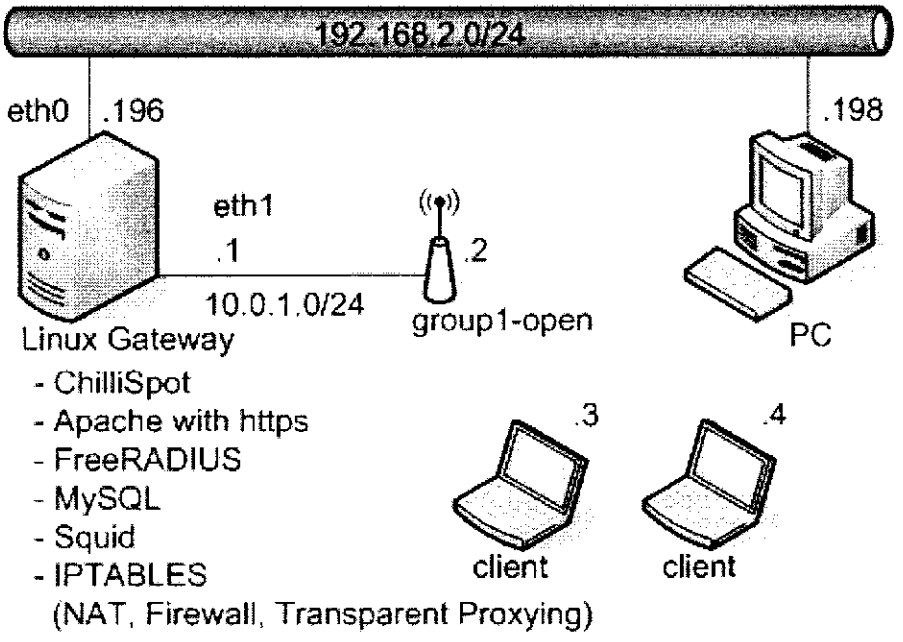
ตอนที่ 3

- 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 ต่อกับแอกเซสพอยต์ ได้รับแจก ip จาก chillispot server
- แอกเซสพอยต์ได้รับแจก ip จาก chillispot server
- ไคลเอนต์ที่มาต่อกับแอกเซสพอยต์ได้รับแจก ip จาก chillispot server ส่งต่อโดยแอกเซสพอยต์
- 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 ให้เปลี่ยนเป็นกราฟฟิคโหมดด้วยคำสั่ง startx
- เปิดวินโดวชื่อ terminal เพื่อใช้ในการปรับแต่งและรันคำสั่ง ดังนี้ คลิก Application, Accessories, Terminal
- โปรแกรม editor ที่ใช้ในการแก้ไขคำคือ 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. ตรวจสอบแลนการ์ดพร้อมใช้งานด้วยคำสั่ง

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
```

ต้องการให้ทุกครั้งที่รีบูตเครื่องมีการตั้งเวลาใหม่ 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 ศรุดพรหม 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
ให้เริ่มท่าเฉพาะ 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. แก้ไขให้ทำงานทุกครั้งที่รีบูตเครื่อง

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

แก้ไขให้ทำงานทุกครั้งที่รีบูตเครื่อง

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

การติดตั้งอุปกรณ์ควบคุมแลนไร้สายด้วย ChilliSpot สำหรับการพิสูจน์ตัวจริงแบบเว็บล็อกอิน

คัดลอกจากเว็บเพจเรื่อง "การทำ Wireless LAN Controller ด้วย ChilliSpot แบบ web login + freeradius + mysql + transparent proxy"
http://mamboeasy.psu.ac.th/~wiboon.w/content/view/58/40/

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 attributes
    - 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

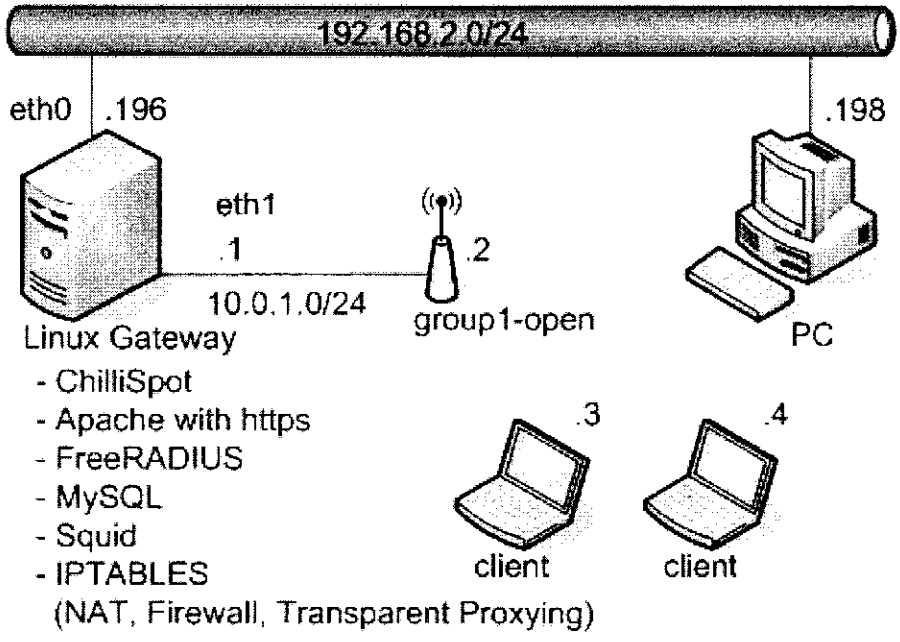
ตอนที่ 3

- 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 ต่อกับแอกเซสพอยต์ ได้รับแจก ip จาก chillispot server
- แอกเซสพอยต์ได้รับแจก ip จาก chillispot server
- ไคลเอนต์ที่มาต่อกับแอกเซสพอยต์ได้รับแจก ip จาก chillispot server ส่งต่อโดยแอกเซสพอยต์
- 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

ค่าแนะนำการติดตั้ง

- ในขั้นตอนที่ติดตั้งจากแผ่นซีดี ให้เลือก Package selection เป็น Software Development
- ในขั้นตอนที่ติดตั้งจากแผ่นซีดีครบแล้ว เมื่อรีบูตกลับมาให้ปิด SeLinux โดยเปลี่ยนจาก enforcing เป็น disabled

คำแนะนำการใช้งาน

- การคอนฟิกระบบจะง่ายขึ้น ให้ใช้วิธีการ copy และ paste คำสั่งหรือข้อความจากเอกสารที่กำลังอ่านอยู่นี้ หากภายหลังการติดตั้งได้รับหน้าจอเป็น text mode ให้เปลี่ยนเป็นกราฟฟิคโหมดด้วยคำสั่ง startx
- เปิดวินโดวชื่อ terminal เพื่อใช้ในการปรับแต่งและรันคำสั่ง ดังนี้ คลิก Application, Accessories, Terminal
- โปรแกรม editor ที่ใช้ในการแก้ไขคำคือ gedit เป็น full screen editor ใช้เมาส์คลิกวางตำแหน่ง cursor ได้ จบด้วยคลิกปุ่ม Save และคลิก X เพื่อปิดโปรแกรม

1.1.1 การปรับแต่งระบบลินุกซ์

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

1. ตรวจสอบแลนการ์ดพร้อมใช้งานด้วยคำสั่ง

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
```

ต้องการให้ทุกครั้งที่รีบูตเครื่องมีการตั้งเวลาใหม่ 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. แก้ไขให้ทำงานทุกครั้งที่รีบูตเครื่อง

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

แก้ไขให้ทำงานทุกครั้งที่รีบูตเครื่อง

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">
<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">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

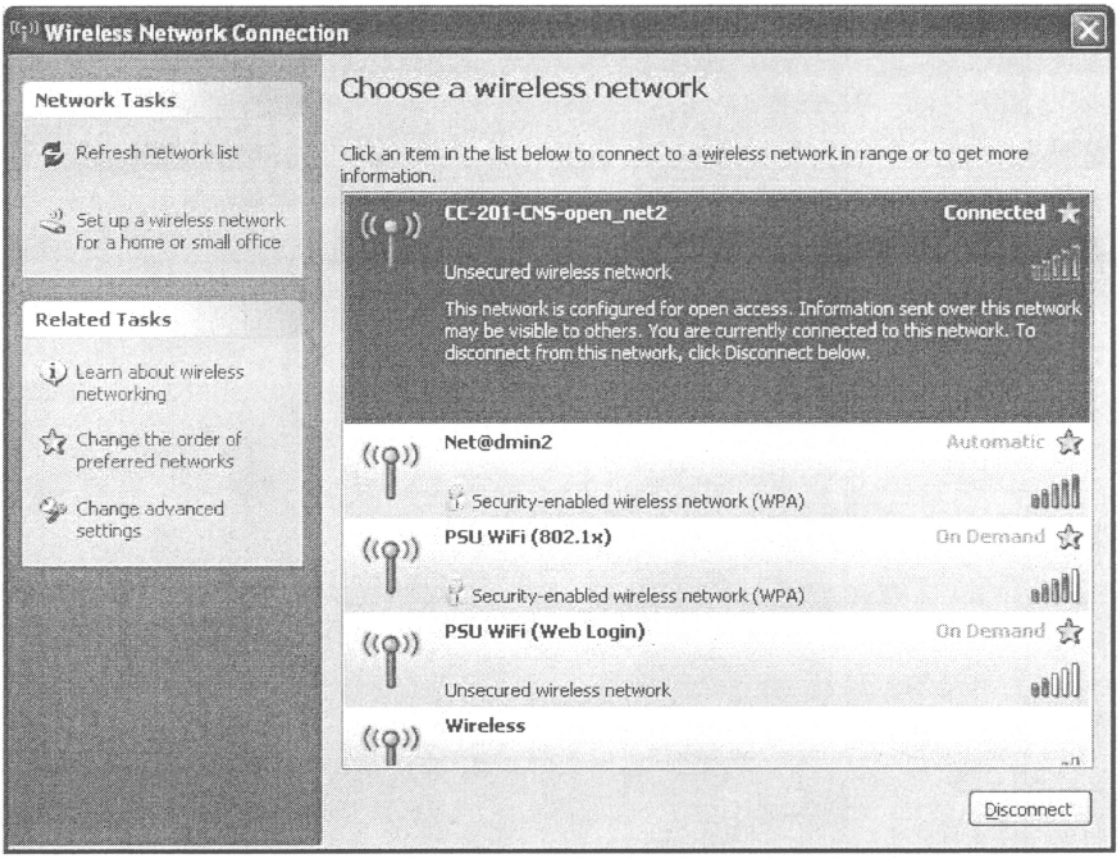
ผลลัพธ์

```
[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 ของแอกเซสพอยน์ และ 10.0.1.3 จะเป็น IP ของโน๊ตบุ๊คตัวแรกที่เชื่อมต่อ

16. เริ่มขั้นตอนทดสอบระบบที่เครื่องโน๊ตบุคดังนี้

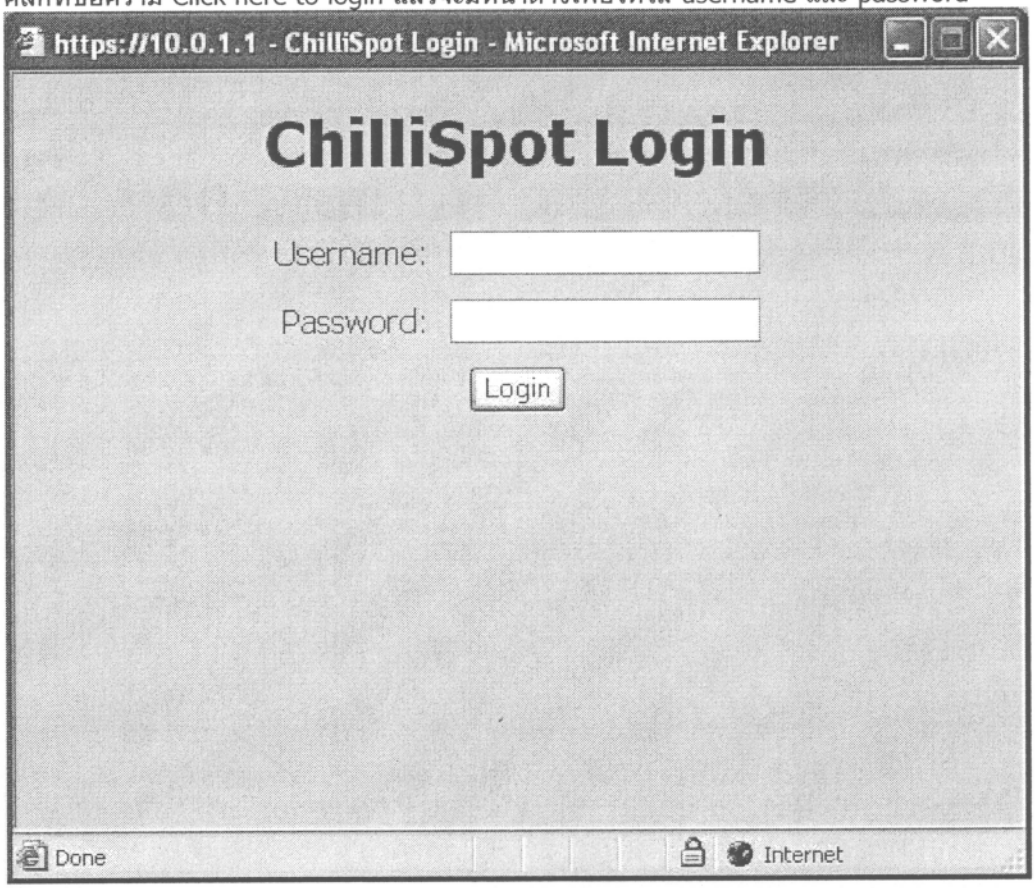
เริ่มทำการคอนเนค W-IFI



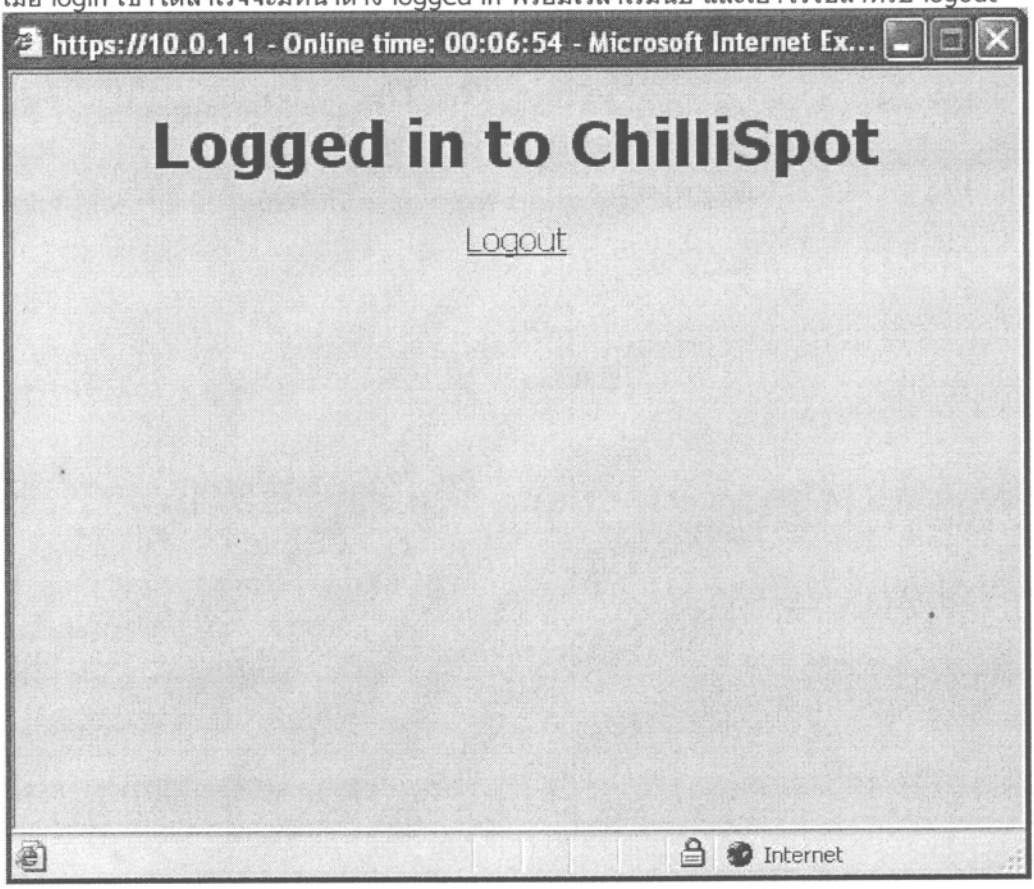
ที่บราวเซอร์ให้ยกเลิกการเซ็ตพร็อกซี่เซิร์ฟเวอร์

ที่บราวเซอร์ที่มีการเซ็ตหน้าโฮมเพจไว้ จะถูก redirect ไปยัง welcome.html ทันทีเมื่อเรียกโปรแกรม

คลิกที่ข้อความ Click here to login แล้วจะมีหน้าต่างเพื่อให้ใส่ username และ password



เมื่อ login เข้าได้สำเร็จจะมีหน้าต่าง logged in พร้อมเวลาเริ่มนับ และเอาไว้ใช้สำหรับ logout



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

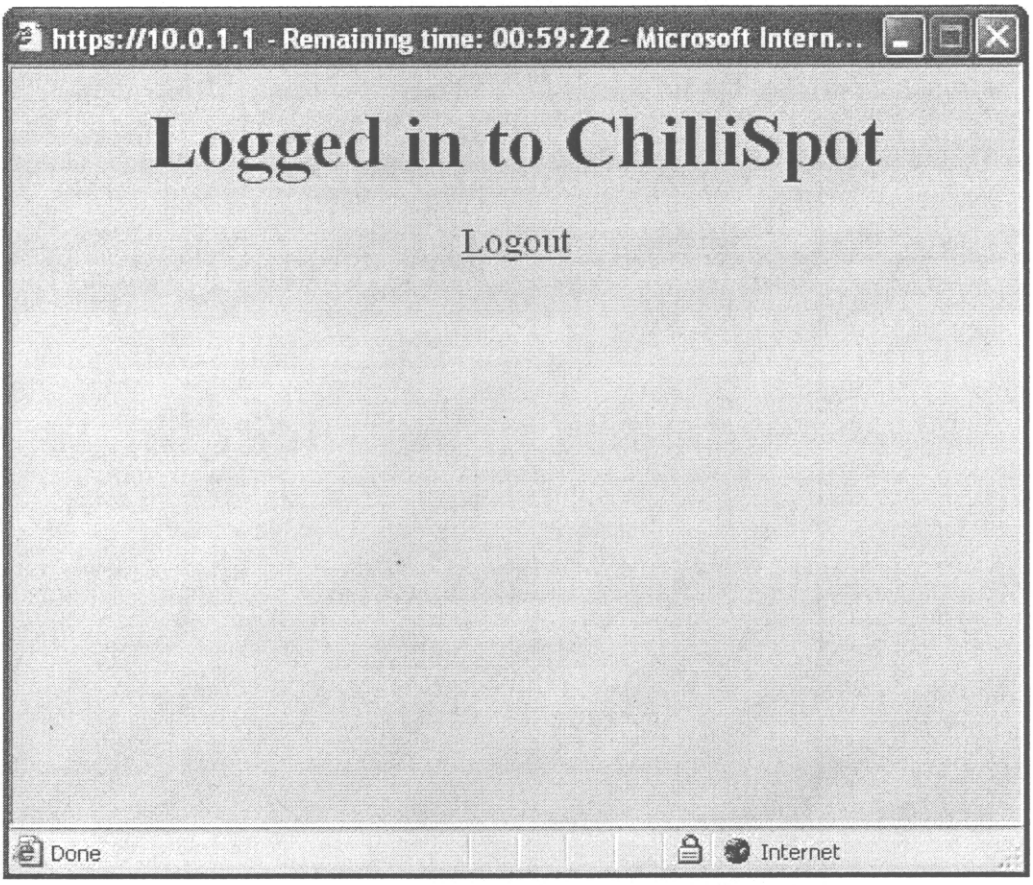
ผลลัพธ์

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

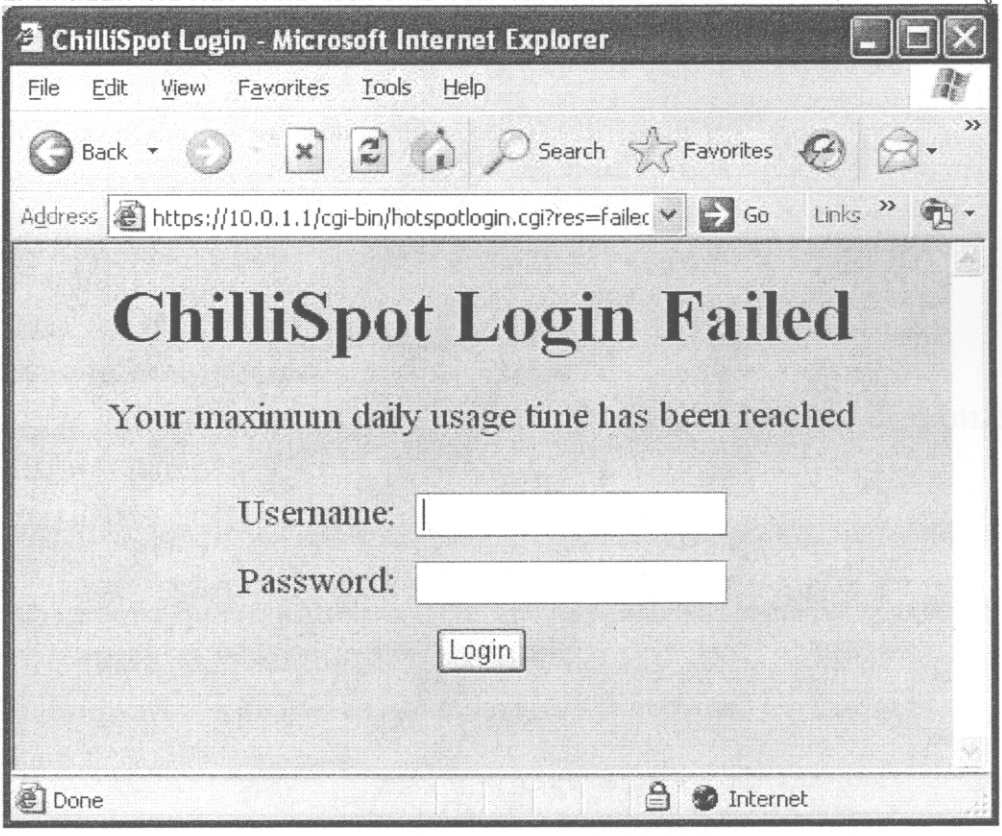
```
    sqlcounter noresetcounter {
        counter-name = Max-All-Session-Time
        check-name = Max-All-Session
        sqlmod-inst = sql
        key = User-Name
        reset = never
        query = "SELECT SUM(AcctSessionTime) FROM radacct WHERE
UserName='%{%k}'"
    }
```

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

ค่าแนะนำเพิ่มเติม

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

การติดตั้ง phpMyPrepaid 0.4b3 ใช้ร่วมกับ ChilliSpot

ขั้นตอน

1. หากยังไม่ติดตั้งโปรแกรม freeradius ทำตามดังนี้
   ติดตั้งโปรแกรม freeradius ด้วยคำสั่ง
   yum install freeradius

   แก้ไขให้ทำงานทุกครั้งที่รีบูตเครื่อง
   chkconfig radiusd on

   สั่งให้ทำงานด้วยคำสั่งว่า
   service radiusd start

   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

2. หากยังไม่ติดตั้งโปรแกรม mysql ให้ทำตามดังนี้
   ติดตั้งโปรแกรม mysql ด้วยคำสั่งดังนี้
   yum install mysql
   yum install mysql-server

   สั่งให้รันทุกครั้งที่รีบูตเครื่อง ด้วยคำสั่งดังนี้
   chkconfig mysqld on

   รัน mysqld ด้วยคำสั่ง
   service mysqld start

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

3. เข้าสู่โปรแกรม mysql ด้วย username คือ root และ password คือ abcd1234
   mysql -uroot -pabcd1234

4. สร้างฐานข้อมูลชื่อ phpmyprepaid
   CREATE DATABASE phpmyprepaid;

5. กำหนดสิทธิให้กับบัญชีผู้ใช้งานบน mysql คือ radius พร้อม password คือ abcd1234
   GRANT ALL PRIVILEGES ON phpmyprepaid.* to 'radius'@'localhost' IDENTIFIED BY 'abcd1234';
   FLUSH PRIVILEGES;

6. ออกจากคำสั่ง mysql
   quit

7. ติดตั้งโปรแกรมเพิ่ม
   yum install freeradius-mysql

8. แก้ไขไฟล์ /etc/raddb/radiusd.conf เพื่อเปิดใช้งาน mysql
   หาก freeradius เวอร์ชั่น 1.1.3
   ใน section module {}
   บรรทัดที่ 1248 เดิม # $INCLUDE ${confdir}/sql.conf
   แก้ไขโดยการเอาคอมเมนต์ออก เป็น $INCLUDE ${confdir}/sql.conf
   ใน section authorize {}
   บรรทัดที่ 1837 เดิม files
   แก้ไขโดยการใส่คอมเมนต์ เป็น #files
   บรรทัดที่ 1844 เดิม #sql
   แก้ไขโดยการเอาคอมเมนต์ออก เป็น sql
   ใน section accounting {}
   บรรทัดที่ 2001 เดิม #sql
   แก้ไขโดยการเอาคอมเมนต์ออก เป็น sql

   หาก freeradius เวอร์ชั่น 1.1.7
   จะอยู่ที่บรรทัด 1261, 1858, 1865, 2028 ตามลำดับ

   ผลลัพธ์ที่ต้องการ

```
module {
        $INCLUDE ${confdir}/sql.conf

authorize {
        #  Read the 'users' file
        #files

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

accounting {
        # Log traffic to an SQL database
        sql
```

9. แก้ไขแฟ้ม /etc/raddb/sql.conf เพื่อให้เรียกใช้ฐานข้อมูล phpmyprepaid ด้วยสิทธิเป็นผู้ใช้ radius ซึ่งมี password เป็น abcd1234

```
        # Connect info
        server = "localhost"
        login = "radius"
        password = "abcd1234"
        # Database table configuration
        radius_db = "phpmyprepaid"
```

10. เสร็จแล้วให้ restart ระบบ radiusd ใหม่ด้วยคำสั่ง
    service radiusd restart

11. ตอนนี้ ทั้ง freeradius และ mysql พร้อม database phpmyprepaid ว่าง ๆ พร้อมแล้ว ต่อไปจะทำการติดตั้งโปรแกรม phpmyprepaid แล้วรันโปรแกรมผ่านเว็บบราวเซอร์ จากนั้นจะเซ็ตค่าต่าง ๆ บนหน้าเว็บ ทำให้ได้ table ต่าง ๆ ที่จำเป็นใช้งานเกิดขึ้น

12. ดาวน์โหลดโปรแกรม phpmyprepaid เวอร์ชั่น 0.4b3 ด้วยคำสั่ง wget ดังนี้
wget http://downloads.sourceforge.net/phpmyprepaid/phpmyprepaid04b3.tgz

ย้ายเข้าไปในไดเรกทอรี /var/www/html
cd /var/www/html

คลายแฟ้มออกมาจะได้ไดเรกทอรี phpmyprepaid
tar -zxvf /root/phpmyprepaid04b3.gz

เข้าไปอ่านคำแนะนำการติดตั้งสักเล็กน้อยที่ไดเรกทอรี phpmyprepaid/doc
cd phpmyprepaid/doc
more INSTALL

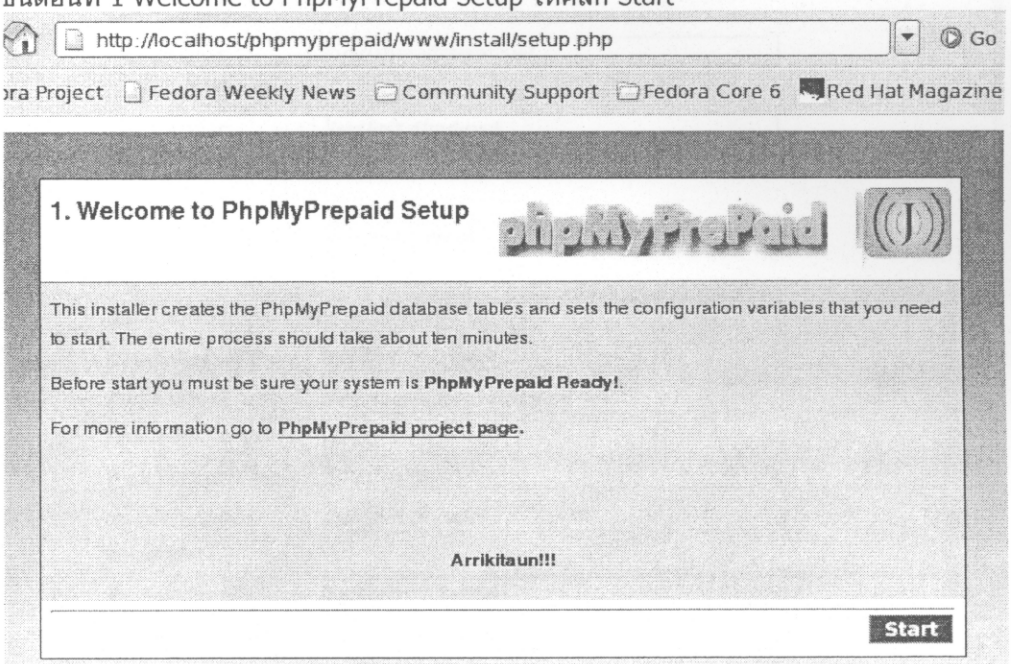
เปลี่ยนสิทธิความเป็นเจ้าของแฟ้มเป็น ผู้ใช้ชื่อ apache และกรุ๊ปชื่อ apache
chown -R apache:apache /var/www/html/phpmyprepaid

13. ติดตั้งโปรแกรม php และ rrdtool ด้วยคำสั่ง
yum install php
yum install php-mysql
yum install rrdtool

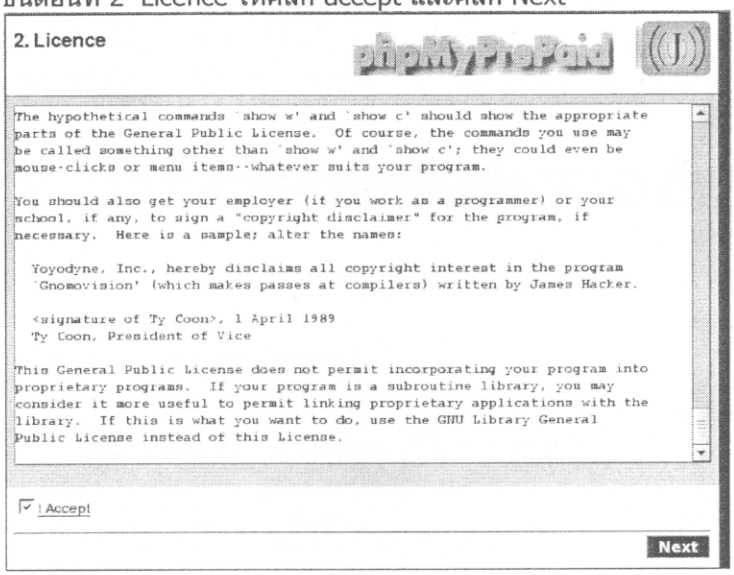
14. อยู่ที่เครื่องเซิร์ฟเวอร์ที่ติดตั้ง เข้า browser
แล้วไปยังเว็บไซต์ http://localhost/phpmyprepaid/www/install/setup.php

จะมีขั้นตอนให้ setup 9 ขั้นตอน

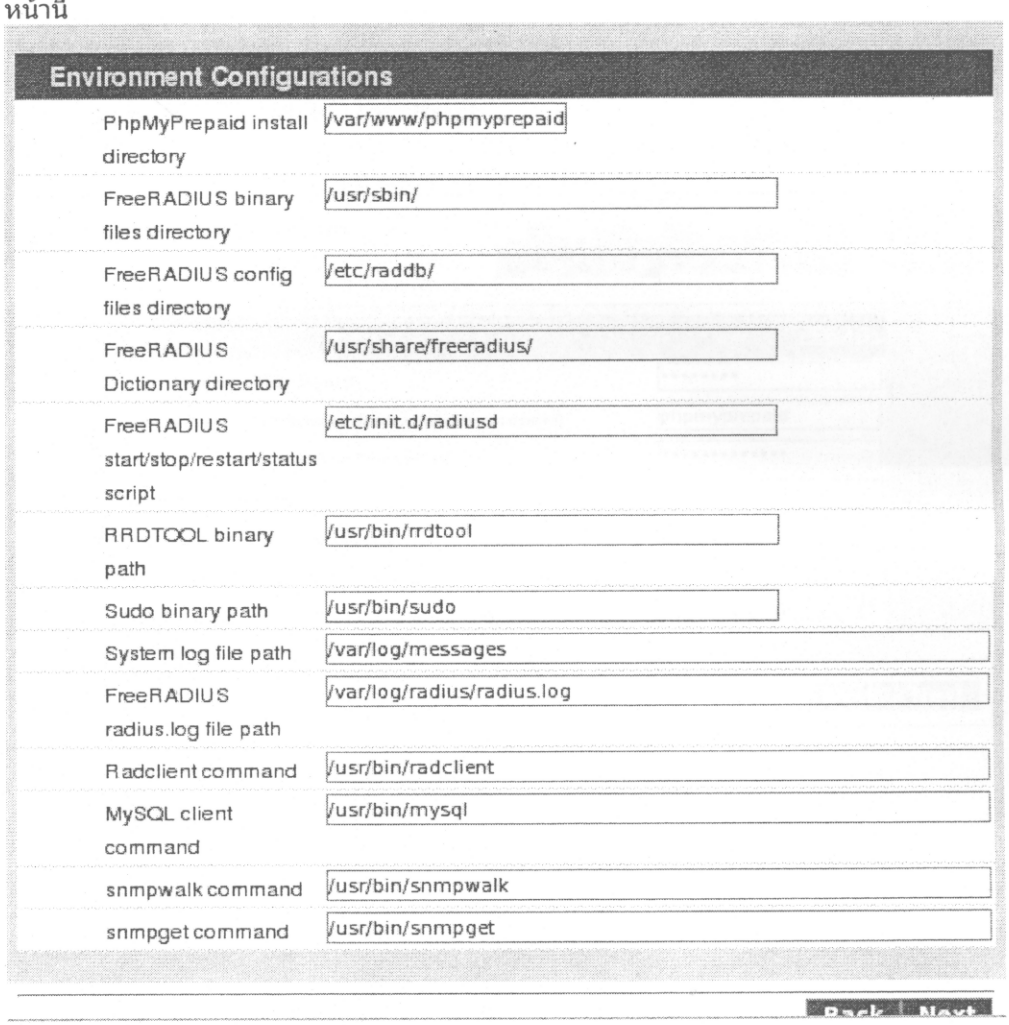
15. ขั้นตอนที่ 1 Welcome to PhpMyPrepaid Setup ให้คลิก Start



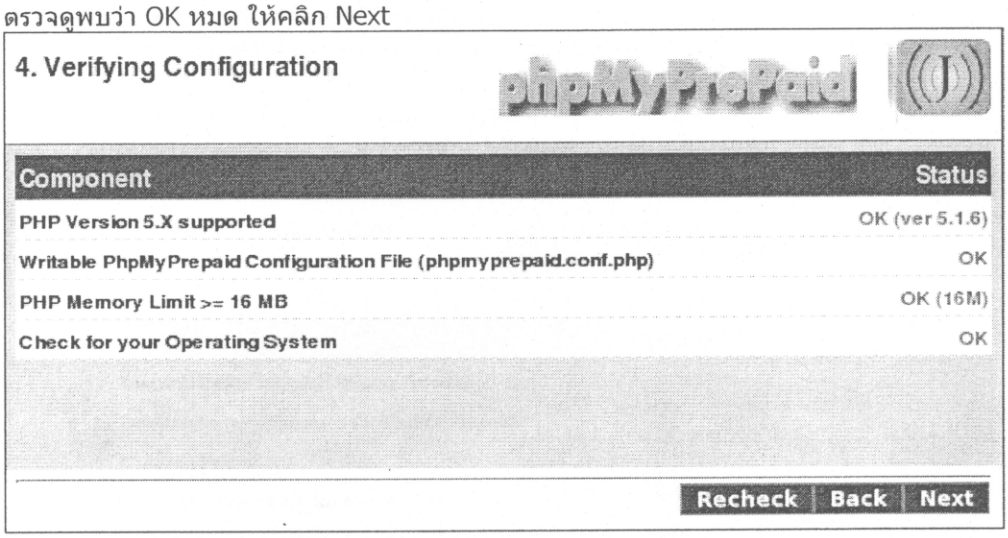
16. ขั้นตอนที่ 2 Licence ให้คลิก accept และคลิก Next



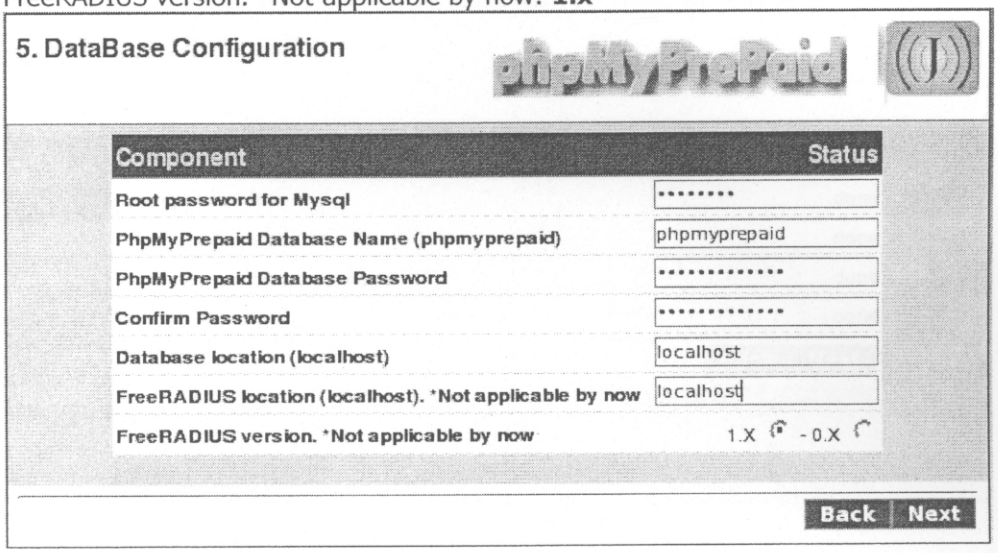
17. ขั้นตอนที่ 3 Environment Configurations ให้คลิก Next
ตรวจสอบดูว่าแต่ละช่องถูกต้องแล้ว ผมพบว่า ผมยังไม่ได้ติดตั้ง RRDTool จึงติดตั้งแล้วกลับมาหน้านี้



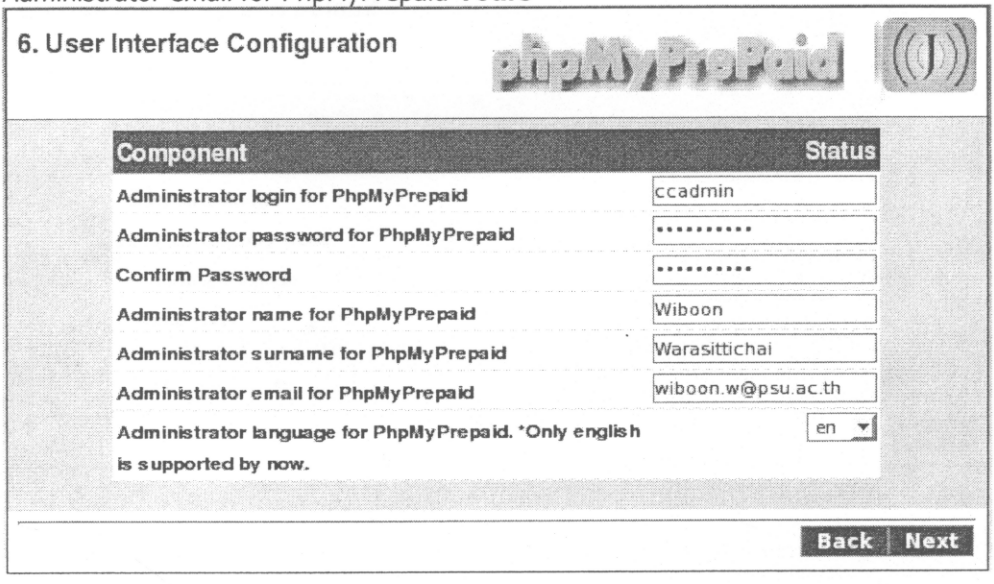
18. ขั้นตอนที่ 4 Verifying Configuration
ตรวจดูพบว่า OK หมด ให้คลิก Next



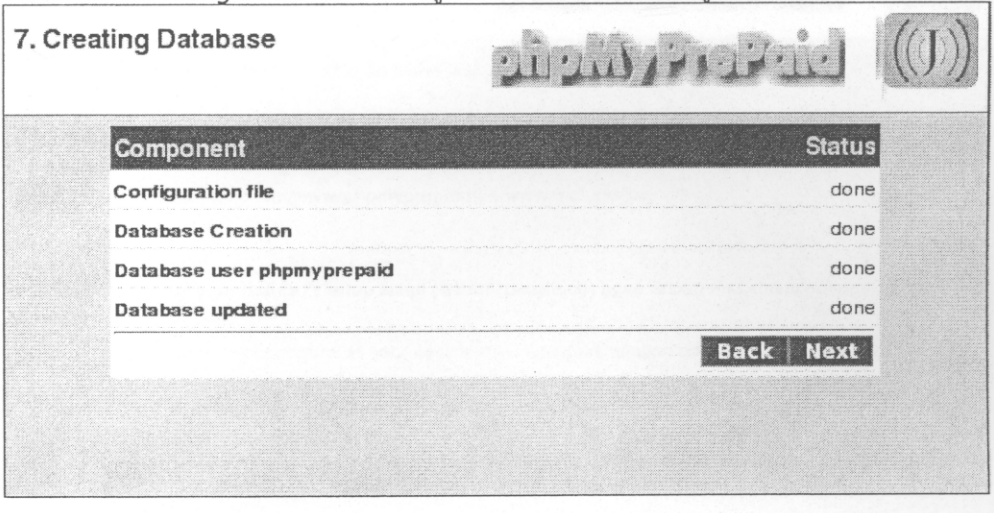
19. ขั้นตอนที่ 5 Database Configuration
Root password for Mysql: **abcd1234**
PhpMyPrepaid Database Name (phpmyprepaid): **phpmyprepaid**
PhpMyPrepaid Database Password: **abcd1234**
Confirm Password: **abcd1234**
Database location (localhost) **localhost**
FreeRADIUS location (localhost). *Not applicable by now **localhost**
FreeRADIUS version. *Not applicable by now: **1.x**



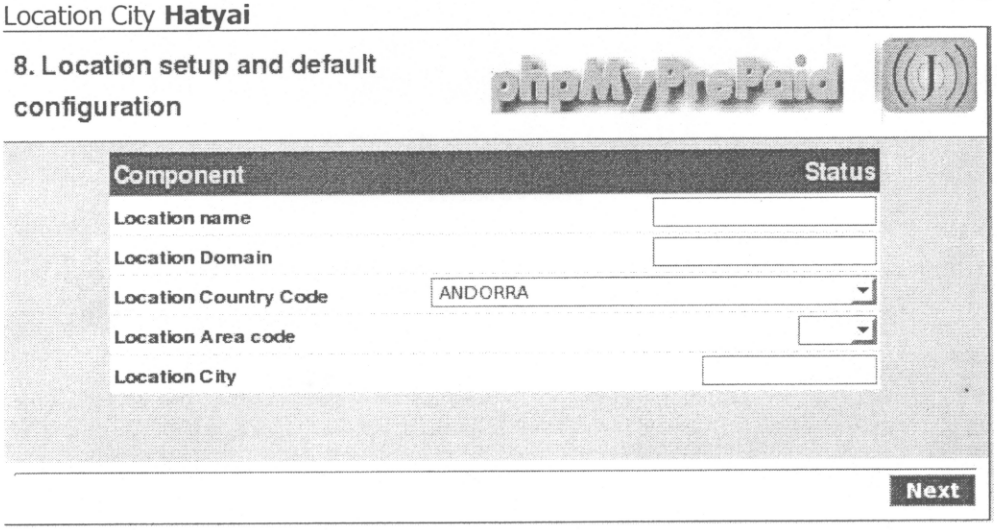
20. ขั้นตอนที่ 6 User Interface Configuration
Administrator login for PhpMyPrepaid **ccadmin**
Administrator password for PhpMyPrepaid **abcd1234**
Confirm Password **abcd1234**
Administrator name for PhpMyPrepaid **Yours**
Administrator surname for PhpMyPrepaid **Yours**
Administrator email for PhpMyPrepaid **Yours**



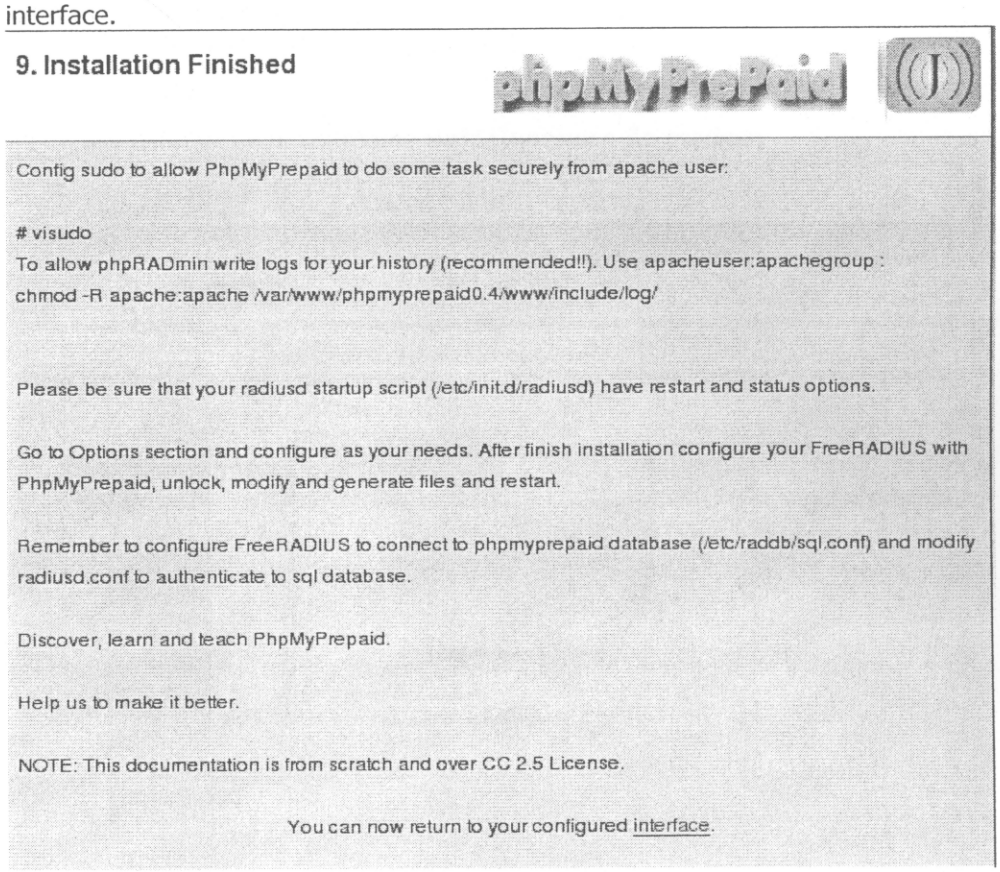
21. ขั้นตอนที่ 7 Creating Database สังเกตดูพบว่าจะมีคำว่า Done อยู่ 4 บรรทัด



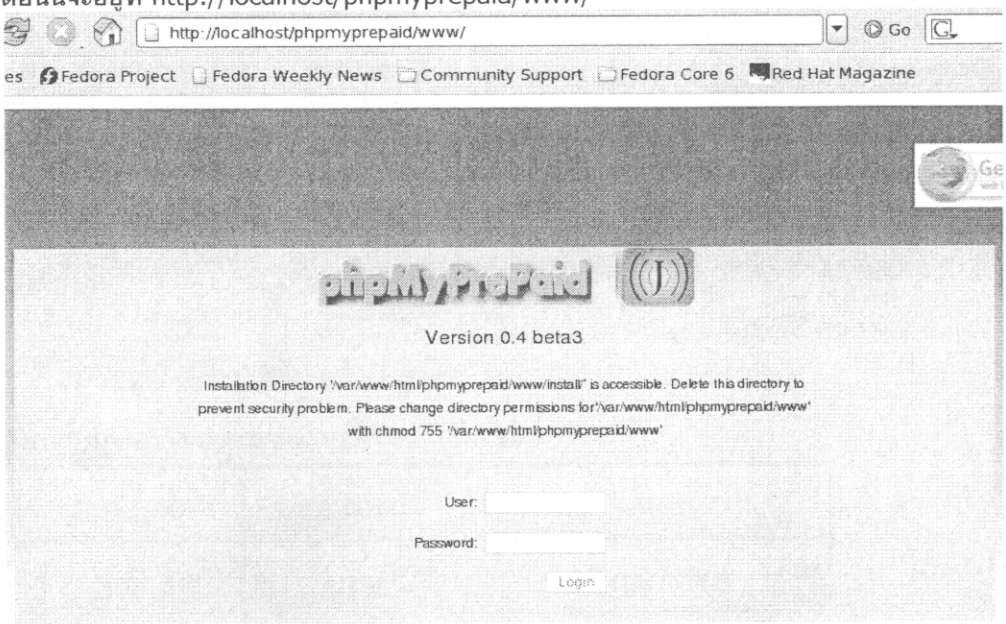
22. ขั้นตอนที่ 8 Location Setup and Default Configuration
Location name **FLR_2**
Location Domain **CC**
Location Country Code **THAILAND**
Location Area code **--**
Location City **Hatyai**



23. ขั้นตอนที่ 9 Installation Finished ให้คลิก You can now return to your configured interface.



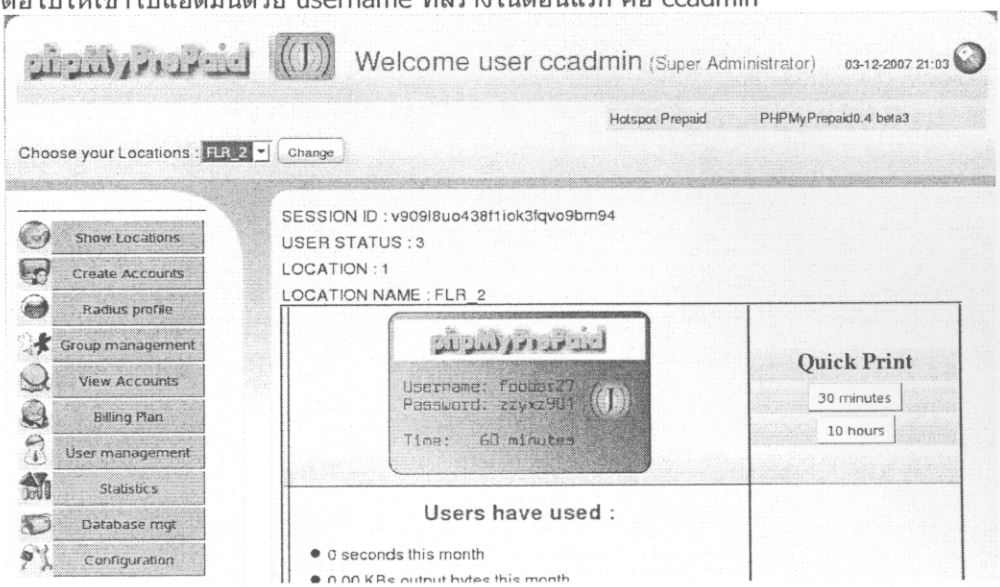
24. ตอนนี้จะอยู่ที่ http://localhost/phpmyprepaid/www/



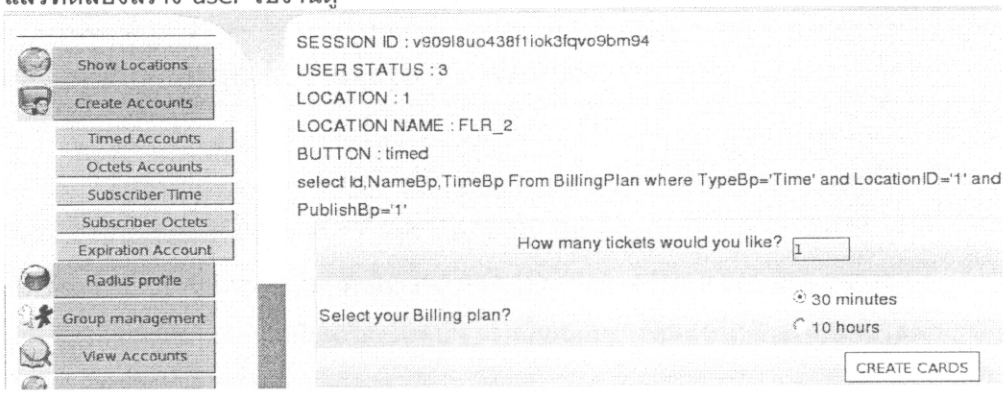
มีข้อความแจ้งให้เราลบไดเรกทอรี install ทิ้งไป ผมเลือกที่จะย้ายไปเก็บไว้ก่อนดังนี้
mv /var/www/html/phpmyprepaid/www/install/ /root/

และแจ้งว่าให้เราเปลี่ยนโหมดของแฟ้ม ให้ทำดังนี้
chmod 755 /var/www/html/phpmyprepaid/www

25. ต่อไปให้เข้าไปแอดมินด้วย username ที่สร้างในตอนแรก คือ ccadmin



แล้วทดลองสร้าง user ใช้งานดู



โปรแกรมจะสร้าง username และ password ให้

Username	Password	Validity
qjaiaa	eyq	30 minutes

26. ทดสอบด้วยคำสั่ง radtest
radtest *username password* localhost 0 mytestkey
จะได้ผลลัพธ์ว่า Access-Accept

27. ทดสอบกับโน้ตบุ๊ค

การเซตแอกเซสพอยต์ยี่ห้อ Linksys รุ่น WAP54G

1. set แอกเซสพอยต์ให้เป็น factory default โดยกดปุ่ม Reset ค้างไว้ประมาณ 10 วินาที
2. เครื่องจะมีหมายเลขไอพีเป็น 192.168.1.245 และ SSID เป็น linksys
3. ใส่เลข IP Address ให้กับเครื่องโน้ตบุ๊คเป็น 192.168.1.3 subnet mask 255.255.255.0
4. เชื่อมต่อเครื่องแอกเซสพอยต์เข้ากับเครื่องโน้ตบุ๊ค จากนั้นเปิดบราวเซอร์หน้าต่างใหม่แล้วใส่ 192.168.1.245 ในช่อง Address
5. เข้าสู่การคอนฟิกโดยช่อง Username ปล่อยว่างไว้และช่อง Password เป็น admin

การคอนฟิกแอกเซสพอยต์ให้ใช้แบบ Open ต่อผ่าน chillispot

คลิกแท็บ Wireless > Basic Wireless Settings

Mode: Mixed

Network Name(SSID): group1-open

Channel: เลือกตามหมายเลขกลุ่ม

SSID Broadcast: Enabled

คลิกปุ่ม Save Settings

คลิกแท็บ Setup > Network Setup

ในส่วน Configuration Type: เลือกตั้งหมายเลขไอพีแบบ Automatic Configuration-DHCP (สำคัญมาก chillispot จะทำงานไม่ได้ถ้าเลือกเป็น static)

คลิกปุ่ม Save Settings

หลังจากคลิกปุ่ม Apply ไปแล้วจะไม่สามารถเข้าคอนฟิกแอกเซสพอยต์ทางบราวเซอร์ได้อีกต่อไป เพราะมันลบเลขไอพี 192.168.1.245 ไปแล้ว และเปลี่ยนเป็นรับเลขไอพีจาก dhcp

ในขั้นนี้จะสามารถใช้งานแบบ Open และ Web Login ได้แล้ว

การเซตแอกเซสพอยต์ยี่ห้อ 3Com รุ่น 3CRWE454G72

1. set แอกเซสพอยต์ให้เป็น factory default โดยทำขั้นตอนดังนี้

ถอดสายไฟเลี้ยงออกจากตัวแอกเซสพอยต์

กดปุ่ม Reset ค้างไว้ในขณะที่เสียบสายไฟเลี้ยงกลับเข้าไป สักครู่ไฟ Alert จะกะพริบ ให้กดค้างไว้ประมาณ 30 วินาที แล้วปล่อยปุ่ม Reset รอให้แอกเซสพอยต์รีบูตขึ้นใหม่ ไฟ Alert จะดับไป

2. ใส่เลข IP Address ให้กับเครื่องโน้ตบุ๊คเป็น 169.254.3.5 subnet mask 255.255.0.0 และ default gateway 169.254.3.1

3. เชื่อมต่อแอกเซสพอยต์เข้ากับเครื่องโน้ตบุ๊ค จากนั้นให้รันโปรแกรม Setup ในแผ่นซีดีที่ให้มากับแอกเซสพอยต์ จะได้หน้าต่าง 3Com OfficeConnect Wireless 11g Access Point

4. คลิก Run Discovery Application จะปรากฏหน้าต่าง 3Com OfficeConnect Discovery V5.0 ให้คลิกเลือกอินเตอร์เฟสที่เป็นแลนการ์ดที่เชื่อมต่อกับแอกเซสพอยต์แล้วคลิกปุ่ม Next

5. โปรแกรมจะแสดงแอกเซสพอยต์ที่พบพร้อมหมายเลขไอพีในกลุ่ม 169.254.x.x ให้คลิกปุ่ม Next

6. ในหน้าต่างถัดมา คลิกปุ่ม Finish โปรแกรมจะเปิดบราวเซอร์เพื่อเข้าสู่การคอนฟิกแอกเซสพอยต์ให้โดยอัตโนมัติ

7. เข้าสู่การคอนฟิกโดยใช้ default Password เป็น admin

การคอนฟิกแอกเซสพอยต์ให้ใช้แบบ Open ต่อผ่าน chillispot

คลิก Wireless Settings ที่แถบด้านซ้าย

คลิกแท็บ Configuration

Enabel Wireless Networking: คลิกถูกที่เช็กบอกซ์

Channel: เลือกตามหมายเลขกลุ่ม

Service Area Name/SSID: group1-open

คลิกปุ่ม Apply

คลิก LAN Settings ที่แถบด้านซ้าย

IP Allocation Mode: เลือกตั้งหมายเลขไอพีแบบ Dynamic (DHCP) (สำคัญมาก chillispot จะทำงานไม่ได้ถ้าเลือกเป็น static)

คลิกปุ่ม Apply

หลังจากคลิกปุ่ม Apply ไปแล้วจะไม่สามารถเข้าคอนฟิกแอคเซสพอยน์ทางบราวเซอร์ได้อีกต่อไป เพราะมันเปลี่ยนเป็นรับเลขไอพีจาก dhcp

ในขั้นนี้จะสามารถนำไปใช้งานแบบ Open และ Web Login ได้เมื่อเชื่อมต่อกับ chillispot

การเซตแอกเซสพอยต์ยี่ห้อ Cisco รุ่น Aironet1100 (802.11b)

1. set แอกเซสพอยต์ให้เป็น factory default โดยทำขั้นตอนดังนี้

ถอดสายไฟเลี้ยงออกจากตัวแอกเซสพอยต์

กดปุ่ม MODE ค้างไว้ในขณะที่เสียบสายไฟเลี้ยงกลับเข้าไป และกดค้างไว้ประมาณ 10 วินาที LED บนตัวแอกเซสพอยต์เปลี่ยนเป็นสีแดง แล้วปล่อย แอคเซสพอยน์จะมีหมายเลขไอพีเป็น 10.0.0.1 และมี SSID เป็น tsunami

2. ใส่เลข IP Address ให้กับเครื่องโน้ตบุ๊คเป็น 10.0.0.3 subnet mask 255.255.255.0

3. เชื่อมต่อแอกเซสพอยต์เข้ากับเครื่องโน้ตบุ๊ค จากนั้นเปิดบราวเซอร์หน้าต่างใหม่ แล้วใส่ 10.0.0.1 ในช่อง Address

4. เข้าสู่การคอนฟิกโดยใช้ Username และ Password เป็น Cisco ทั้งสองค่า

การคอนฟิกแอกเซสพอยต์ให้ใช้แบบ Open ต่อผ่าน chillispot

คลิก NETWORK INTERFACES > Radio0-802.11B ที่แถบด้านซ้าย

คลิกแท็บ SETTINGS

Default Radio Channel: เลือกตามหมายเลขกลุ่ม

คลิกปุ่ม Apply

คลิก EXPRESS SET-UP ที่แถบด้านซ้าย

Configuration Server Protocol: คลิกเลือก DHCP (สำคัญมาก chillispot จะทำงานไม่ได้ถ้าเลือกเป็น static)

SSID: group1-open

คลิกปุ่ม Apply

หลังจากคลิกปุ่ม Apply ไปแล้วจะไม่สามารถเข้าคอนฟิกแอคเซสพอยน์ทางบราวเซอร์ได้อีกต่อไป เพราะมันลบเลขไอพี 10.0.0.1 ไปแล้ว และเปลี่ยนเป็นรับเลขไอพีจาก dhcp

ในขั้นนี้จะสามารถนำไปใช้งานแบบ Open และ Web Login ได้แล้ว

การเซตไวร์เลสเร้าเตอร์ยี่ห้อ NETGEAR รุ่น DG834G

1. set ไวร์เลสเร้าเตอร์ให้เป็น factory default โดยกดปุ่ม Restore Factory Setting ค้างไว้ประมาณ 10 วินาที LED test (เครื่องหมายถูก) จะติดขึ้นมา ให้ปล่อยปุ่มแล้วไวร์เลสเราเตอร์จะรีบูตขึ้นใหม่
2. เครื่องจะมีหมายเลขไอพีเป็น 192.168.0.1 และ SSID เป็น NETGEAR
3. ใส่เลข IP Address ให้กับเครื่องโน้ตบุ๊คเป็น 192.168.0.3 subnet mask 255.255.255.0
4. เชื่อมต่อเครื่องไวร์เลสเร้าเตอร์เข้ากับโน้ตบุ๊ค โดยต่อเข้าที่พอร์ต LAN พอร์ตใดพอร์ตหนึ่งบนไวร์เลสเร้าเตอร์ จากนั้นเปิดบราวเซอร์หน้าต่างใหม่แล้วใส่ 192.168.0.1 ในช่อง Address
5. เข้าสู่การคอนฟิกโดยใช้ Username เป็น admin และ Password เป็น password
6. คลิก Basic Settings ใต้หัวข้อ Setup ที่แถบด้านซ้าย
   Does Your Internet Connection Require A Login?: No
   Account Name: ไม่ใส่
   Domain Name: ไม่ใส่
   Internet IP Address: เลือก Get Dynamically From ISP
   Domain Name Server (DNS) Address: เลือก Get Dynamically From ISP
   NAT (Network Address Translation): เลือก Disable
   Router MAC Address: เลือก Use Default Address
   คลิกปุ่ม Apply

การคอนฟิกไวร์เลสเร้าเตอร์ให้ใช้แบบ Open ต่อกับ chillispot
คลิก Wireless Settings ใต้หัวข้อ Setup ที่แถบด้านซ้าย
   ในส่วน Wireless Network
      Name (SSID): ใส่ group1-open
      Region: เลือก Asia
      Channel: เลือกตามหมายเลขกลุ่ม
      Mode: เลือก g&b
   คลิกปุ่ม Apply
ในขั้นนี้จะสามารถใช้งานแบบ Open และ Web Login ได้แล้ว

ไฟล์ 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 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

# 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
```

ประวัติผู้เขียน

ชื่อ สกุล นายวิบูลย์ วราสิทธิชัย

คุณวุฒิ วิทยาศาสตร์บัณฑิต มหาวิทยาลัยสงขลานครินทร์ ปี พ.ศ. 2531

ตำแหน่ง นักวิชาการคอมพิวเตอร์ ระดับ 6
กลุ่มงานบริการระบบเครือข่ายและสื่อสาร
ศูนย์คอมพิวเตอร์ มหาวิทยาลัยสงขลานครินทร์

โทรศัพท์ 074-282128

ที่อยู่อีเมล wiboon.w@psu.ac.th

ประสบการณ์ในงานเขียน

- เอกสารประกอบการอบรมเรื่อง "การใช้ระบบปฏิบัติการ UNIX พื้นฐาน – CC0903REV-3" 2546
- เอกสารประกอบการอบรมเรื่อง "การใช้ Electronic Mail – CC0501REV-4" 2546