คู่มือการอบรมระบบการถ่ายทอดองค์ความรู้เกี่ยวกับการทดสอบอุปกรณ์เครือข่าย โครงการจ้างที่ปรึกษาเพื่อช่วยบริหารจัดการและดำเนินงานของศูนย์ประสานงานและปฏิบัติการ IPv6 ภายใต้โครงการจัดตั้งและดำเนินการศูนย์ประสานงานและปฏิบัติการ IPv6 ประจำปีงบประมาณ พ.ศ. 2557

โดย

ศูนย์ความรู้เฉพาะด้านอินเทอร์เน็ตยุคหน้า

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยสงขลานครินทร์

สารบัญ

หน้า

สารบัญ

หน้า

สารบัญ

หน้า

สารบัญ

หน้า

สารบัญรูปภาพ

หน้า

สารบัญรูปภาพ

หน้า

สารบัญรูปภาพ

หน้า

สารบัญตาราง

หน้า

หัวข้อที่ 1 ระบบปฏิบัติการและโปรแกรมประยุกต์

ระบบปฏิบัติการและโปรแกรมประยุกต์จะนำเสนอเกี่ยวกับการตั้งค่าการใช้งาน IPv6 บนระบบปฏิบัติการต่างๆ และข้อมูลการรองรับ IPv6 ของโปรแกรมประยุกต์ต่างๆ ที่ได้ดำเนินการทดสอบ หัวข้อนี้จึงแบ่งออกเป็นสองหัวข้อย่อยด้วยกันคือ การตั้งค่าการใช้งาน IPv6 ของระบบปฏิบัติการต่างๆ และผลการทดสอบการรองรับ IPv6 ของโปรแกรมประยุกต์ต่างๆ

1.1 การตั้งค่าการใช้งาน IPv6 ของระบบปฏิบัติการต่างๆ

การตั้งค่าการใช้งาน IPv6 ของของระบบปฏิบัติการต่างๆ ถูกแบ่งออกเป็น 3 กลุ่มด้วยกัน ได้แก่ Windows, Linux, mobile OS โดยการตั้งค่าการใช้งานในหัวข้อนี้ เราเตอร์ภายในระบบเครือข่ายจะต้องรองรับการให้บริการ IPv6

1.1.1 Windows

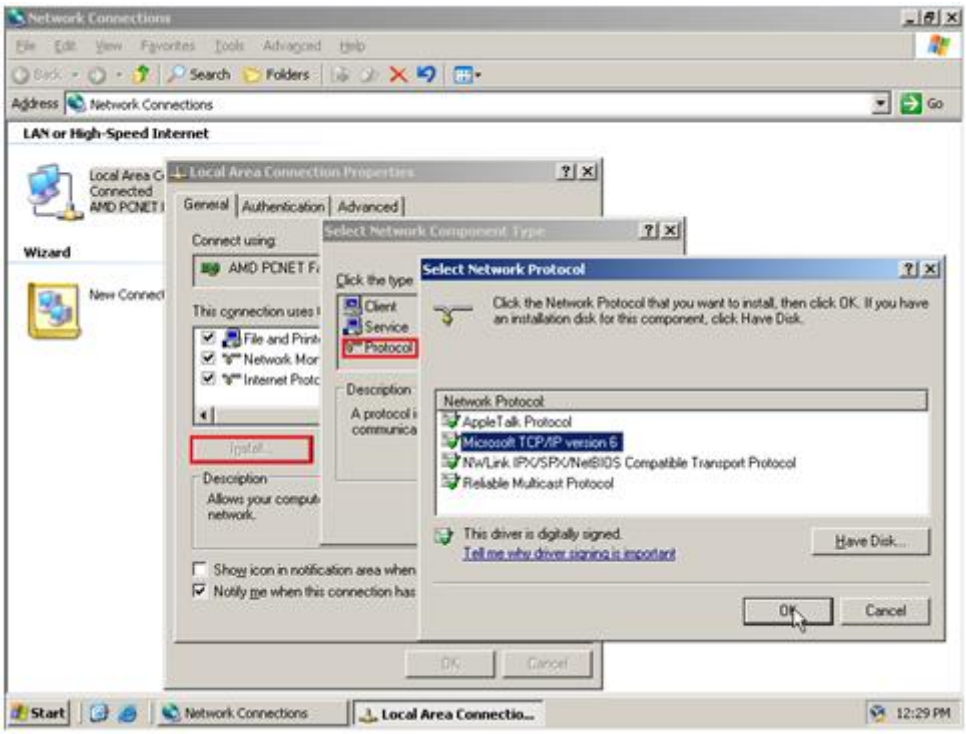
สำหรับ Windows แบ่งออกเป็น 2 กลุ่มด้วยกันตามลำดับการพัฒนาและความคล้ายคลึงกันในการใช้งาน กลุ่มแรกก็คือ Windows XP และ Windows 2003 Server ส่วนกลุ่มที่สองคือ Windows 7 และ Windows 2008 Server

- การตั้งค่า IPv6 บน Windows 2003 Server

Windows 2003 Server เป็นระบบปฏิบัติการสำหรับเซิร์ฟเวอร์จากไมโครซอฟท์ ซึ่งออกแบบมาเพื่อทดแทน Windows 2000 Server เนื่องจากเปิดตัวตั้งแต่ปี ค.ศ. 2003 Windows 2003 Server จึงยังไม่รองรับการใช้งาน IPv6 อย่างสมบูรณ์ และไม่ได้ติดตั้ง IPv6 ในระบบปฏิบัติการโดยอัตโนมัติ ดังนั้นหากผู้ใช้งานต้องการใช้งาน IPv6 ผู้ใช้งานต้องติดตั้ง IPv6 เพิ่มเติมด้วยตนเอง (สำหรับ Windows XP ก็มีลักษณะเช่นเดียวกัน)

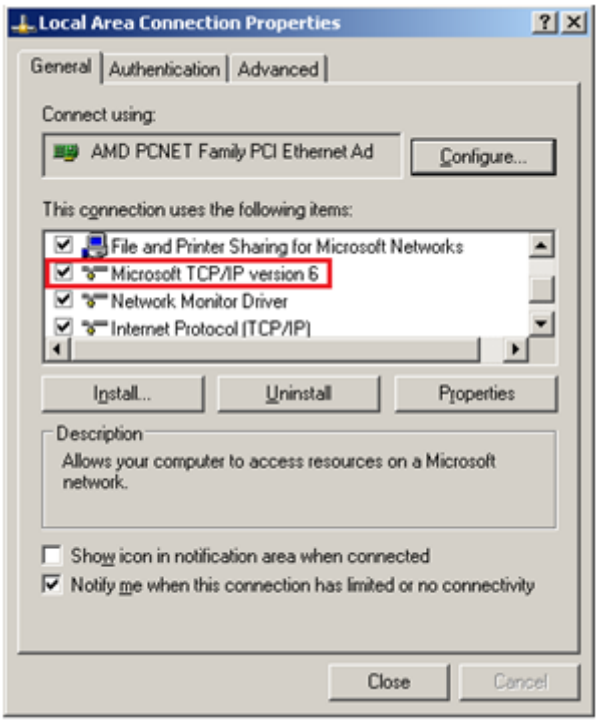
การติดตั้ง IPv6 บน LAN Interface ของ Windows 2003 Server

- คลิก Start, จากนั้นคลิกเลือก Control Panel, และดับเบิลคลิก Network Connections
- คลิกขวาที่ Local Area Connection ตัวที่ได้ทำการเสียบสายที่ต่อมาจาก Router จากนั้นคลิก Properties
- คลิก Install
- คลิกเลือก Protocol จากนั้นคลิก Add
- คลิกเลือก Microsoft TCP/IP version 6 แล้วคลิก OK
- คลิก Close เพื่อทำการบันทึกการเปลี่ยนแปลง



รูปที่ 1.1 ติดตั้ง Microsoft TCP/IP version 6 บน Windows 2003 Server

- เมื่อติดตั้งสำเร็จ Local Area Connection Properties จะมีลักษณะดังนี้



รูปที่ 1.2 ผลลัพธ์จากการติดตั้ง Microsoft TCP/IP version 6 บน Windows 2003 Server

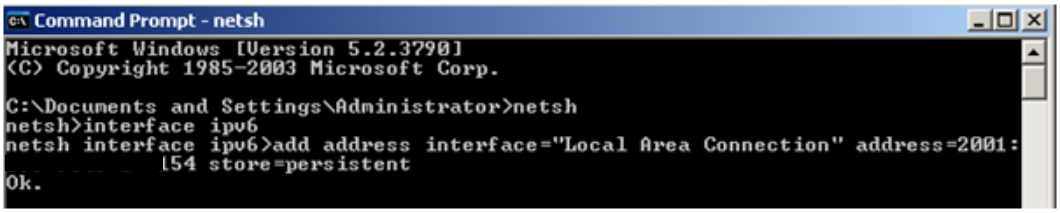
การเพิ่ม IPv6 Address แบบ Manual

การตั้งค่า IPv6 Address

- กดปุ่ม Windows + R จากนั้นจะปรากฏหน้าต่าง Run
- พิมพ์ cmd เพื่อเปิดโปรแกรม Command Prompt

- เมื่อปรากฏหน้าต่าง Command Prompt ให้พิมพ์ netsh จากนั้นกดปุ่ม ENTER
- พิมพ์ interface ipv6 จากนั้นกดปุ่ม ENTER
- จากนั้นพิมพ์คำสั่งดังข้างล่าง แล้วกดปุ่ม ENTER เพื่อเสร็จสิ้นการเพิ่ม IPv6 Address
- add address interface="Local Area Connection" address="2001:db8:x:x::154" store=persistent

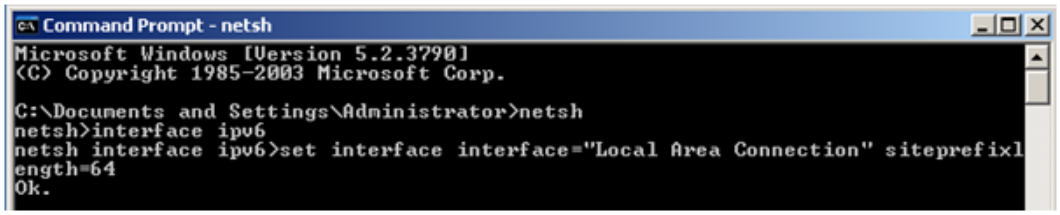
*TIP: ในกรณีที่ไม่ทราบชื่อ interface ให้รันคำสั่ง netsh interface show interface



รูปที่ 1.3 ตั้งค่า IPv6 Address ด้วย Command Prompt บน Windows 2003 Server

การตั้งค่า IPv6 Interface

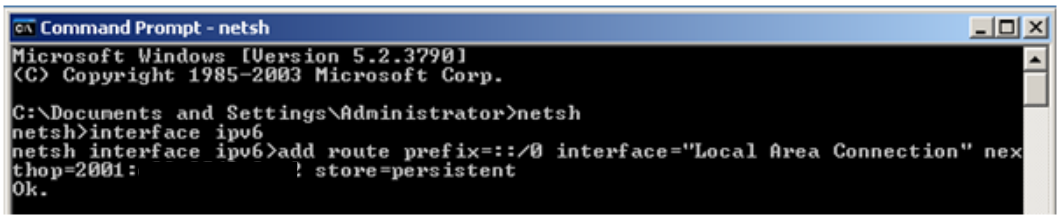
- เปิดโปรแกรม Command Prompt
- พิมพ์ netsh จากนั้นกดปุ่ม ENTER
- พิมพ์ interface ipv6 จากนั้นกดปุ่ม ENTER
- จากนั้นพิมพ์คำสั่งดังข้างล่าง แล้วกดปุ่ม ENTER เพื่อเสร็จสิ้นการตั้งค่า Interface
- set interface interface="Local Area Connection" siteprefixlength=64



รูปที่ 1.4 ตั้งค่า IPv6 Interface ด้วย Command Prompt บน Windows 2003 Server

การตั้งค่า Default Route ของ IPv6

- เปิดโปรแกรม Command Prompt
- พิมพ์ netsh จากนั้นกดปุ่ม ENTER
- พิมพ์ interface ipv6 จากนั้นกดปุ่ม ENTER
- จากนั้นพิมพ์คำสั่งดังข้างล่าง แล้วกดปุ่ม ENTER เพื่อเสร็จสิ้นการเพิ่ม Default Route
- add route prefix=::/0 interface="Local Area Connection" nexthop="2001:db8:x:x::2" store=persistent



รูปที่ 1.5 ตั้งค่า IPv6 Default Route ด้วย Command Prompt บน Windows 2003 Server

การตั้งค่า DNS server address

- เปิดโปรแกรม Command Prompt
- พิมพ์ netsh จากนั้นกดปุ่ม ENTER
- พิมพ์ interface ipv6 จากนั้นกดปุ่ม ENTER
- จากนั้นพิมพ์คำสั่งดังข้างล่าง แล้วกดปุ่ม ENTER เพื่อเสร็จสิ้นการเพิ่ม DNS server address
- add dnsservers "Local Area Connection" 2001:4860:4860::8888 index=1

*TIP: สามารถใช้คำสั่ง show dnsservers เพื่อแสดงผลลัพธ์ DNS server address

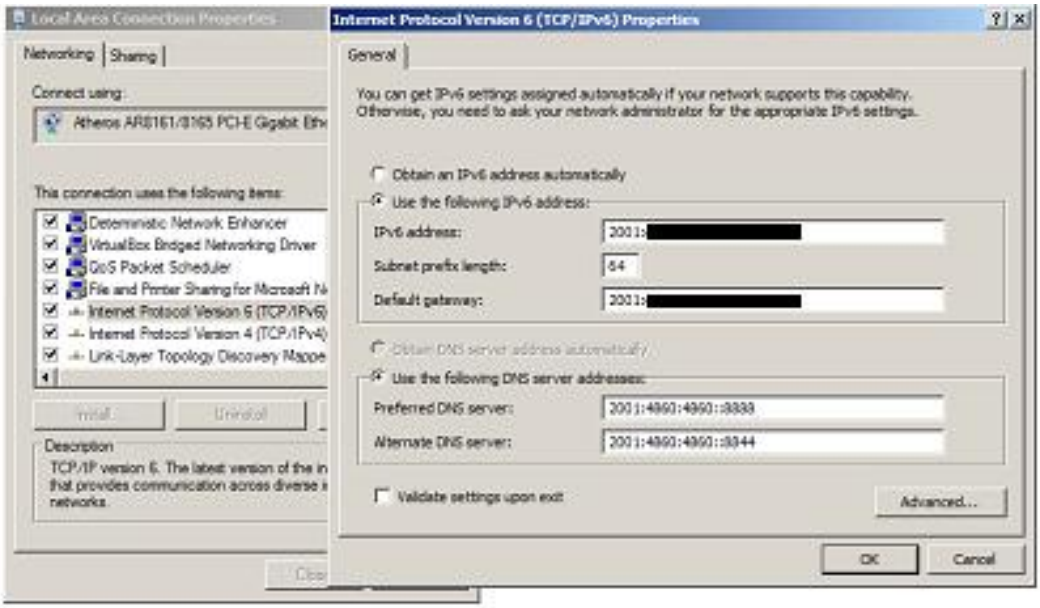
- แสดงผลลัพธ์หลังจากตั้งค่า IPv6 ด้วยคำสั่ง ipconfig

- การตั้งค่า IPv6 บน Windows 2008 Server

Windows 2008 Server เป็นระบบปฏิบัติการสำหรับเซิร์ฟเวอร์จากไมโครซอฟท์ ซึ่งออกแบบมาเพื่อทดแทน Windows 2003 Server โดย Windows 2008 Server ถูกปรับปรุงให้รองรับ IPv6 และติดตั้ง IPv6 มาโดยอัตโนมัติ (สำหรับ Windows 7 ก็มีลักษณะเช่นเดียวกัน)

การตั้งค่า IPv6 บน LAN Interface ของ Windows 2008 Server

- คลิก Start, จากนั้นคลิกเลือก Control Panel, และดับเบิลคลิก Network Connections
- คลิกขวาที่ Local Area Connection ตัวที่ได้ทำการเสียบสายที่ต่อมาจาก Router จากนั้นคลิก Properties
- คลิกเลือก Internet Protocol version 6 (TCP/IPv6) จากนั้นคลิก Properties
- คลิกเลือก Use the following IPv6 addresses
  - ช่อง IPv6 address: ระบุเป็น 2001:db8:x:x::154 (IPv6 address ที่ต้องการ)
  - ช่อง Subnet prefix length: ระบุเป็น 64
  - ช่อง Default Gateway: ระบุเป็น 2001:db8:x:x::2 (IPv6 address ของเกตเวย์เราเตอร์)
- คลิกเลือก Use the following DNS server addresses
  - ช่อง Preferred DNS server: ระบุเป็น 2001:4860:4860::8888 (Google Public DNS)



รูปที่ 1.6 ตั้งค่า IPv6 สำหรับ LAN Interface บน Windows 2008 Server

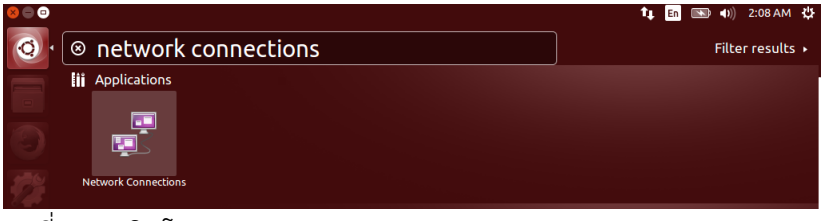
1.1.2 Linux

สำหรับ Linux นั้นเป็นระบบปฏิบัติการแบบ open source ทุกคนสามารถนำโค้ดของ linux ไปใช้งาน, แก้ไข, และแจกจ่ายได้อย่างเสรี ซึ่งนิยมรวมซอฟต์แวร์สำหรับใช้งานในด้านอื่นเป็นชุดเข้าด้วยกันในลักษณะเป็นแพ็กเกจ Linux ถูกปรับปรุงให้รองรับ IPv6 ได้อย่างรวดเร็ว แม้ว่า Linux จะมีด้วยกันหลากหลาย Distribution แต่คำสั่งที่ใช้คล้ายคลึงกัน ดังนั้นในหัวข้อนี้จะนำเสนอการตั้งค่าการใช้งาน IPv6 บน Ubuntu Desktop 14.04

การตั้งค่า IPv6 บน Ubuntu Desktop สามารถทำได้สองวิธีการด้วยกัน วิธีการแรกเป็นแบบ GUI ส่วนวิธีการที่สองเป็นแบบ Command Line ซึ่งทั้งสองวิธีมีรายละเอียดดังต่อไปนี้

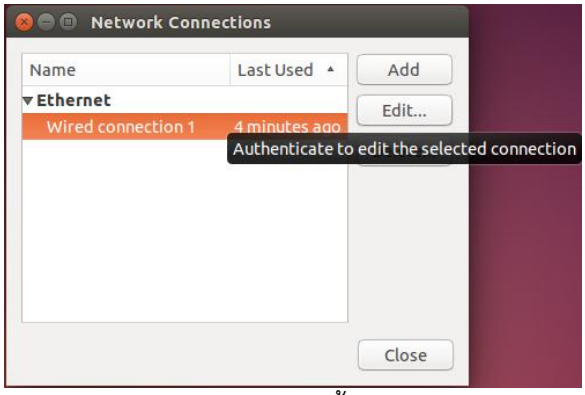
- การตั้งค่า IPv6 บน Ubuntu Desktop ผ่าน GUI

  - คลิกช่อง Search แล้วค้นหาคำว่า network connections จะปรากฏโปรแกรม Network Connections จากนั้นเปิดโปรแกรม



รูปที่ 1.7 เปิดโปรแกรม Network Connections บน Ubuntu Desktop

- คลิกเลือก Wired Connection 1 แล้วคลิก Edit



รูปที่ 1.8 เลือก Interface สำหรับตั้งค่าบน Ubuntu Desktop

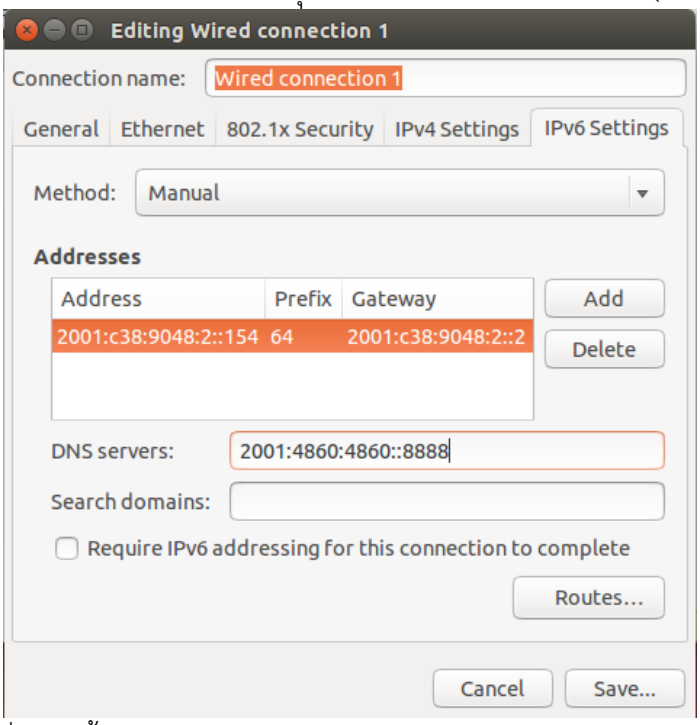
- คลิกแทบ IPv6 Setting จากนั้นเลือก Method: Manual แล้วกรอกข้อมูลต่อไปนี้ หลังจากนั้นกด Save เพื่อบันทึกข้อมูล

ช่อง Address: ระบุเป็น 2001:db8:x:x::154 (IPv6 address ที่ต้องการ)

ช่อง Prefix: ระบุเป็น 64

ช่อง Gateway: ระบุเป็น 2001:db8:x:x::2 (IPv6 address ของเกตเวย์เราเตอร์)

ช่อง DNS servers: ระบุเป็น 2001:4860:4860::8888 (Google Public DNS)



รูปที่ 1.9 ตั้งค่า IPv6 สำหรับ LAN Interface บน Ubuntu Desktop

- การตั้งค่า IPv6 บน Ubuntu Desktop ผ่าน Command Line

- คลิกช่อง Search แล้วค้นหาคำว่า terminal จะปรากฏโปรแกรม Terminal จากนั้นเปิดโปรแกรม Terminal แล้วพิมพ์คำสั่งต่อไปนี้

```
$service network-manager stop      (ปิดโปรแกรม Network Connection)
$ifdown eth0                       (ปิด interface eth0)
```

$vi /etc/network/interface (ตั้งค่า interface โดยเพิ่มบรรทัดต่อไปนี้)

```
iface eth0 inet6 static
address 2001:db8:x:x::154
netmask 64
gateway 2001:db8:x:x::2
```

$ifup eth0 (เปิด interface eth0)

$vi /etc/resolv.conf (ตั้งค่า DNS server address โดยเพิ่มบรรทัดต่อไปนี้)

```
nameserver 2001:4860:4860::8888
```

- แสดงผลลัพธ์หลังจากตั้งค่า IPv6 ด้วยคำสั่ง ifconfig

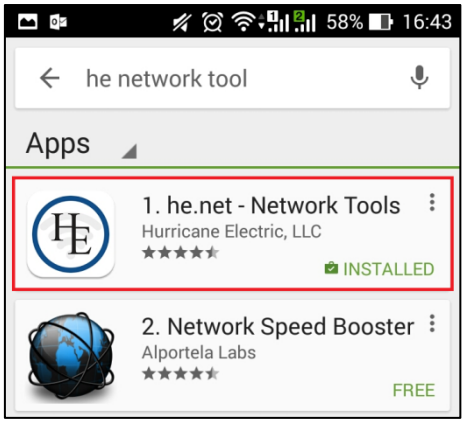
1.1.3 Mobile OS

Mobile OS นั้นเป็นกลุ่มระบบปฏิบัติการสำหรับสมาร์ทโฟน ซึ่งแบ่งออกเป็น 3 กลุ่มด้วยกัน ได้แก่ android, iOS และ Windows phone สำหรับ Mobile OS นั้นมีการอัพเดทอย่างสม่ำเสมอจึงรองรับการใช้งาน IPv6 และสามารถใช้งานได้อัตโนมัติโดยไม่จำเป็นต้องตั้งค่าเพิ่มเติม แม้ว่าระบบปฏิบัติการจะรองรับ IPv6 แต่ Mobile OS ก็ไม่มี GUI สำหรับใช้ตั้งค่า IPv6 แบบ Manual อีกทั้งยังแสดงผลแค่ IPv4 เท่านั้น ด้วยเหตุนี้ หากผู้ใช้งานต้องการทราบข้อมูล IPv6 ของเครือข่ายที่ใช้งาน ผู้ใช้จำเป็นต้องติดตั้งโปรแกรมด้านเน็ตเวิร์กเพิ่มเติม

- android

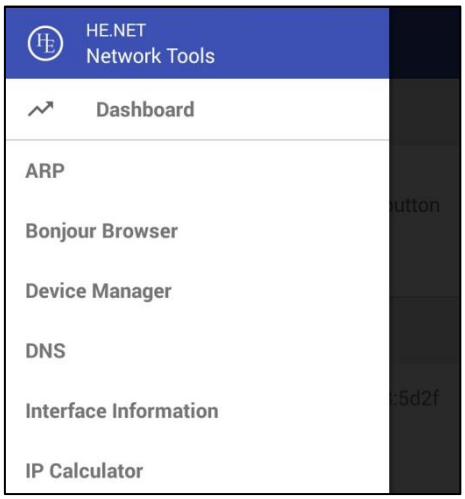
โปรแกรมด้านเครือข่ายสำหรับ android มีหลากหลายโปรแกรมด้วยกัน แต่ในที่นี้แนะนำให้ใช้โปรแกรมชื่อ Network Tools ของ Hurricane Electric เนื่องจากเป็นโปรแกรมที่มีคุณสมบัติหลากหลาย ยกตัวอย่างเช่น DNS, Ping, Traceroute, TCP port scan และ whois สำหรับการใช้งานโปรแกรมเพื่อตรวจสอบหมายเลข IPv6 ที่ได้รับมีดังต่อไปนี้

- เปิด play store เลือก Application จากนั้นค้นหาคำว่า he network tool แล้วติดตั้งโปรแกรม



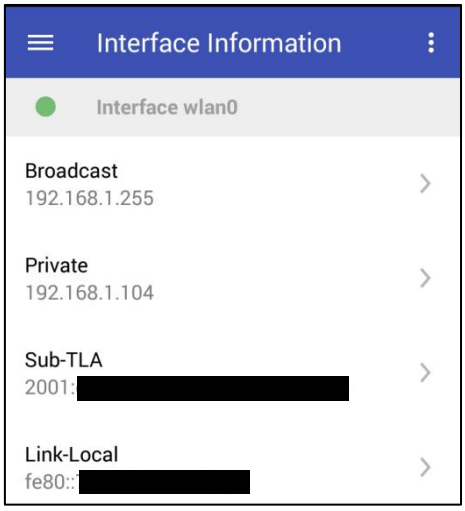
รูปที่ 1.10 ติดตั้ง Network Tools บน Android

- เปิดโปรแกรม Network Tools แล้วเลือก Dashboard จะได้ผลลัพธ์ดังต่อไปนี้



รูปที่ 1.11 เมนู Dashboard ของโปรแกรม Network Tools บน Android

- เลือก Interface Information โปรแกรมก็จะทำการแสดงรายละเอียดข้อมูลด้านเน็ตเวิร์กออกมา (สังเกตรายละเอียดของ Interface: wlan0 ซึ่งเป็นข้อมูล wireless)

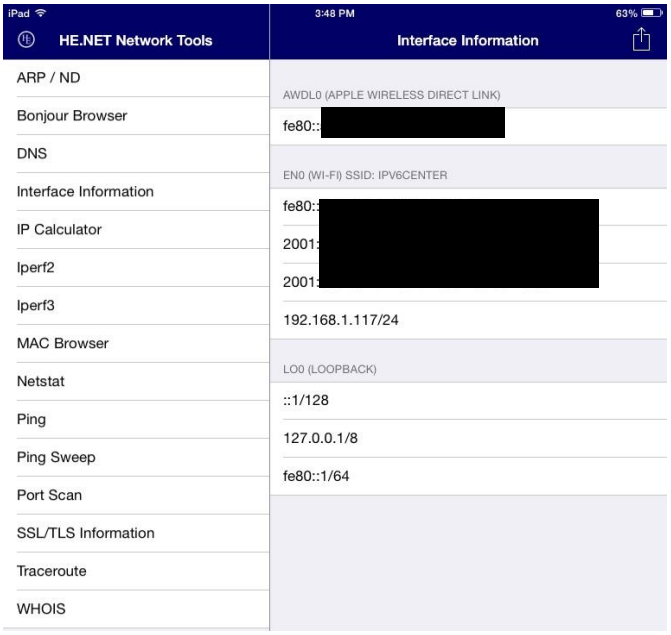


รูปที่ 1.12 รายละเอียดข้อมูลด้านเน็ตเวิร์กจากโปรแกรม Network Tools บน Android

- iOS

โปรแกรม Network Tools ของ Hurricane Electric ก็มีเวอร์ชันสำหรับ iOS เช่นเดียวกัน โดยการใช้งานโปรแกรม Network Tools เพื่อตรวจสอบหมายเลข IPv6 ที่ได้รับก็คล้ายกับใน android

- เปิดโปรแกรม Network Tools แล้วเลือก Interface Information โปรแกรมก็จะทำการแสดงรายละเอียดข้อมูลด้านเน็ตเวิร์กออกมา



รูปที่ 1.13 รายละเอียดข้อมูลด้านเน็ตเวิร์กจากโปรแกรม Network Tools บน iOS

- Windows Phone

โปรแกรม Network Tools ของ Hurricane Electric ไม่มีเวอร์ชันสำหรับ Windows Phone สำหรับ Windows Phone จึงใช้โปรแกรม IP address เพื่อแสดงข้อมูล IPv6 ที่ได้รับแทน โดยผลลัพธ์จากโปรแกรม IP address มีดังต่อไปนี้

รูปที่ 1.14 รายละเอียดข้อมูลด้านเน็ตเวิร์กจากโปรแกรม IP Address บน Windows Phone

1.2 การทดสอบการรองรับ IPv6 ของโปรแกรมประยุกต์

การรองรับ IPv6 ของโปรแกรมประยุกต์ได้ทดสอบโปรแกรมประยุกต์ทั้งส่วนของ Desktop และ Mobile โดยโปรแกรมประยุกต์ที่ถูกทดสอบเป็นโปรแกรมที่นิยมใช้งานทั่วไป เช่น Browser, Online Storage, Mail Client และ Anti-virus รายละเอียดของผลการทดสอบการรองรับ IPv6 ของโปรแกรมประยุกต์สำหรับ Desktop แสดงดังตารางที่ 1.1 และรายละเอียดของผลการทดสอบการรองรับ IPv6 ของโปรแกรมประยุกต์สำหรับ Mobile แสดงดังตารางที่ 1.2

ตารางที่ 1.1 ผลการทดสอบการรองรับ IPv6 ของโปรแกรมประยุกต์สำหรับ Desktop

Application	Windows 7		Window 8		MacBook OSx	
	Dual-stack	Native IPv6	Dual-Stack	Native IPv6	Dual-Stack	Native IPv6
Browser						
Chrome	✓	✓	✓	✓	✓	✓
Version	32.0.1700	32.0.1700	41.0.2272	41.0.2272	41.0.2272	41.0.2272
Firefox	✓	✓	✓	✓	✓	✓
Version	30.0	30.0	37.0	37.0	34.0.5	34.0.5
Safari	-	-	-	-	✓	✓
Version	-	-	-	-	8.0.4	8.0.4
IE	✓	✓	✓	✓	-	-
Version	8.0.7601	8.0.7601	11.0.7	11.0.7	-	-
Online Storage						
Dropbox	✓	✗	✓	✗	✓	✗
Version	3.2.9	3.2.9	3.2.9	3.2.9	3.4.6	3.4.6
Drive	✓	✓	✓	✓	✓	✗
Version	1.17	1.17	1.2	1.2	1.21	1.21
Mail Client						
Mail(Default)	-	-	-	-	✓	✓
Version	-	-	-	-	8.2	8.2
Thunderbird	✓	✓	✓	✓	-	-
Version	31.5.10	31.5.10	31.5.10	31.5.10	-	-
Outlook	✓	✓	✓	✓	-	-
Version	2010	2010	2007	2007	-	-

ตารางที่ 1.1 ผลการทดสอบการรองรับ IPv6 ของโปรแกรมประยุกต์สำหรับ Desktop (ต่อ)

Application	Windows 7		Window 8		MacBook OSx	
	Dual-stack	Native IPv6	Dual-Stack	Native IPv6	Dual-Stack	Native IPv6
Anti-virus						
Avira	✓	✗	✓	✗	-	-
Version	1.1.34	1.1.34	15.0.8	15.0.8	-	-
Avast	✓	✓	✓	✓	-	-
Version	2015.10.2	2015.10.2	2015.10.2	2015.10.2	-	-
Avg	✓	✓	✓	✓	-	-
Version	2015.0.5863	2015.0.5863	2015.0.5863	2015.0.5863	-	-
McAfee	-	-	✓	✗	-	-
Version	-	-	12.8.397	12.8.397	-	-
Messaging						
Line	✓	✗	✓	✗	✓	✗
Version	4.0.0.278	4.0.0.278	4.0.0.278	4.0.0.278	3.9.1	3.9.1

ตารางที่ 1.2 ผลการทดสอบการรองรับ IPv6 ของโปรแกรมประยุกต์สำหรับ Mobile

Application	Android		Apple iOS		Windows Phone	
	Dual-stack	Native IPv6	Dual-Stack	Native IPv6	Dual-Stack	Native IPv6
Browser						
Chrome	✓	✓	✓	✓	-	-
Version	39.0.2171.93	39.0.2171.93	41.0.2272.56	41.0.2272.56	-	-
Firefox	✓	✓	-	-	-	-
Version	36.0.2	36.0.2	-	-	-	-
Safari	-	-	✓	✓	-	-
Version	-	-	600.14	600.14	-	-
IE	-	-	-	-	✓	✓
Version	-	-	-	-	unknown	unknown
Online Storage						
Dropbox	✓	✓	✓	✓	✓	✓
Version	2.4.9.00	2.4.9.00	3.8	3.8	unknown	unknown
Drive	✓	✓	✓	✓	-	-
Version	2.1.495.05.74	2.1.495.05.74	3.4.34149	3.4.34149	-	-

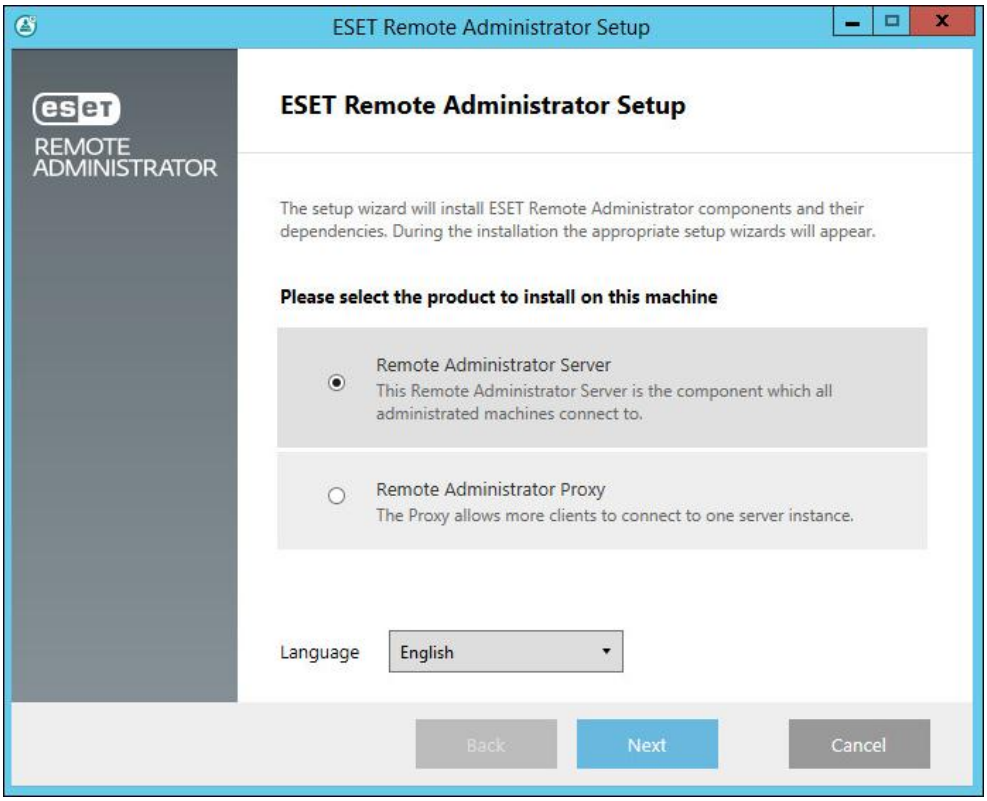
ตารางที่ 1.2 ผลการทดสอบการรองรับ IPv6 ของโปรแกรมประยุกต์สำหรับ Mobile (ต่อ)

Application	Android		Apple iOS		Windows Phone	
	Dual-stack	Native IPv6	Dual-Stack	Native IPv6	Dual-Stack	Native IPv6
Mail Client						
Mail(Default)	✓	✓	✓	✓	✓	✓
Version	1.7.0	1.7.0	unknown	unknown	*outlook	*outlook
Gmail	✓	✓	✓	✓	-	-
Version	5.0.1	5.0.1	4	4	-	-
Outlook	✓	✓	-	-	✓	✓
Version	7.8.2.12	7.8.2.12	-	-	unknown	unknown
Anti-virus						
Avast	✓	✓	-	-	-	-
Version	4.0.7880	4.0.7880	-	-		
Avg	✓	✓	-	-	-	-
Version	4.3	4.3	-	-	-	-
McAfee	✓	✗	-	-	-	-
Version	4.3.1.616	4.3.1.616	-	-	-	-
Messaging						
Line	✓	✓	✓	✓	✓	✗
Version	5.0.2	5.0.2	1.0.0	1.0.0	unknown	unknown

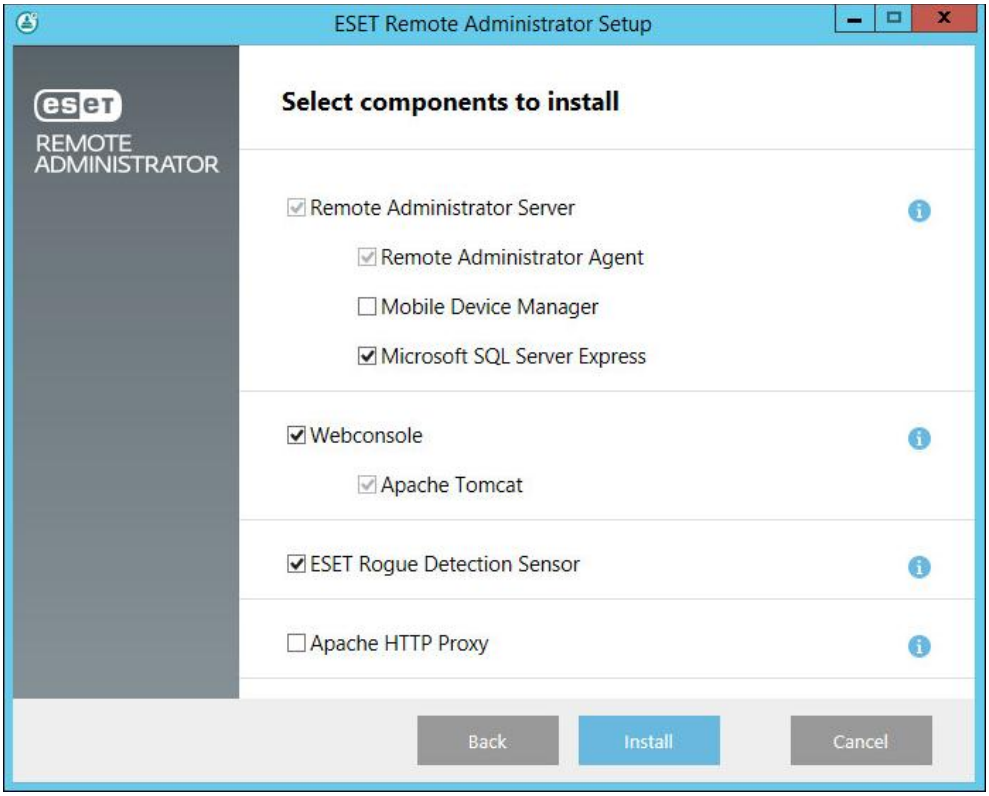
1.2.1 การทดสอบการรองรับ IPv6 ของโปรแกรมแสกนไวรัสแบบ corporate

โปรแกรมแสกนไวรัสแบบ corporate นิยมใช้ในสำหรับหน่วยงานระดับองค์กร ซึ่งจะแบ่งการอุปกรณ์ออกเป็น 2 ส่วนด้วยกัน ได้แก่ Anti-virus Server และ Anti-virus Client (Endpoint) โดย Anti-virus Server จะคอยอัพเดทฐานข้อมูลไวรัสจากผู้ให้บริการ นอกจากนั้นยังคอยตรวจสอบและบันทึกข้อมูลไวรัสจาก Anti-virus Client ซึ่งจะช่วยให้ผู้ดูแลเครือข่ายทราบถึงภัยคุกคามจากไวรัสได้อย่างทันท่วงที Anti-virus Server ยังสามารถกำหนดการทำงานของ Anti-virus Client เช่น ตั้งเวลาการแสกนไวรัส และอัพเดทฐานข้อมูลไวรัส เป็นต้น เนื่องจากการทดสอบโปรแกรมแสกนไวรัสแบบ corporate ค่อนข้างใช้เวลาและมีปัญหาเกี่ยวกับ licensing ดังนั้นในการทดสอบครั้งนี้จึงทำการทดสอบเพียงโปรแกรมแสกนไวรัสของ Eset (Eset Remote Administrator)

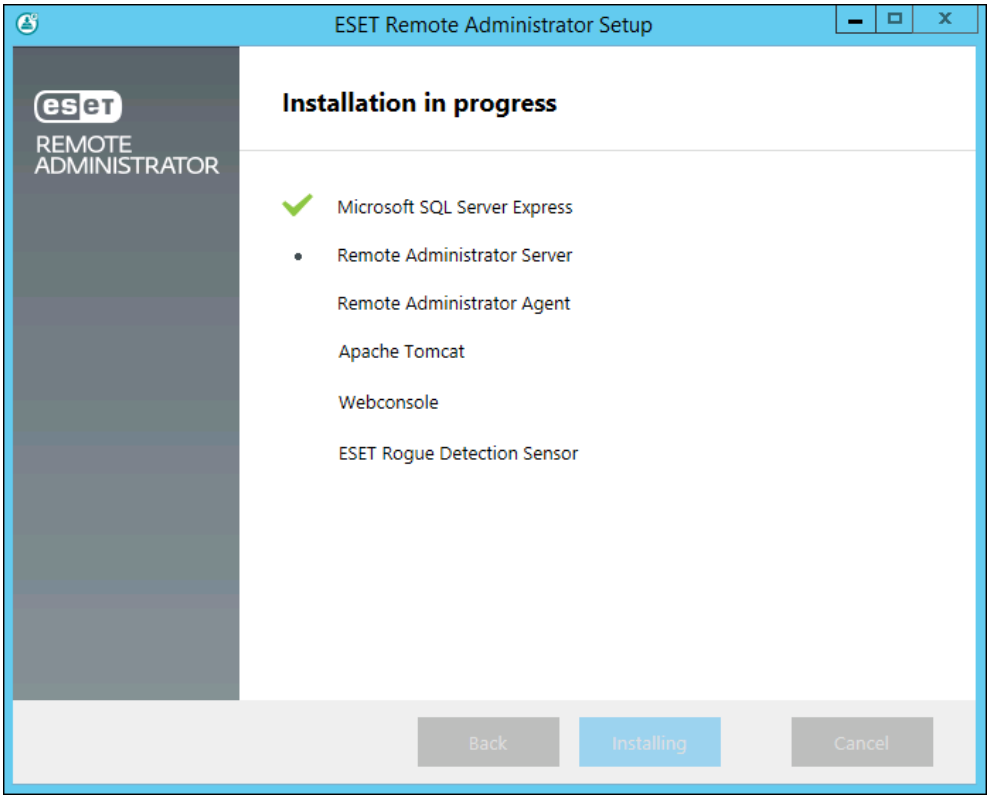
การติดตั้งโปรแกรม Eset Remote Administrator



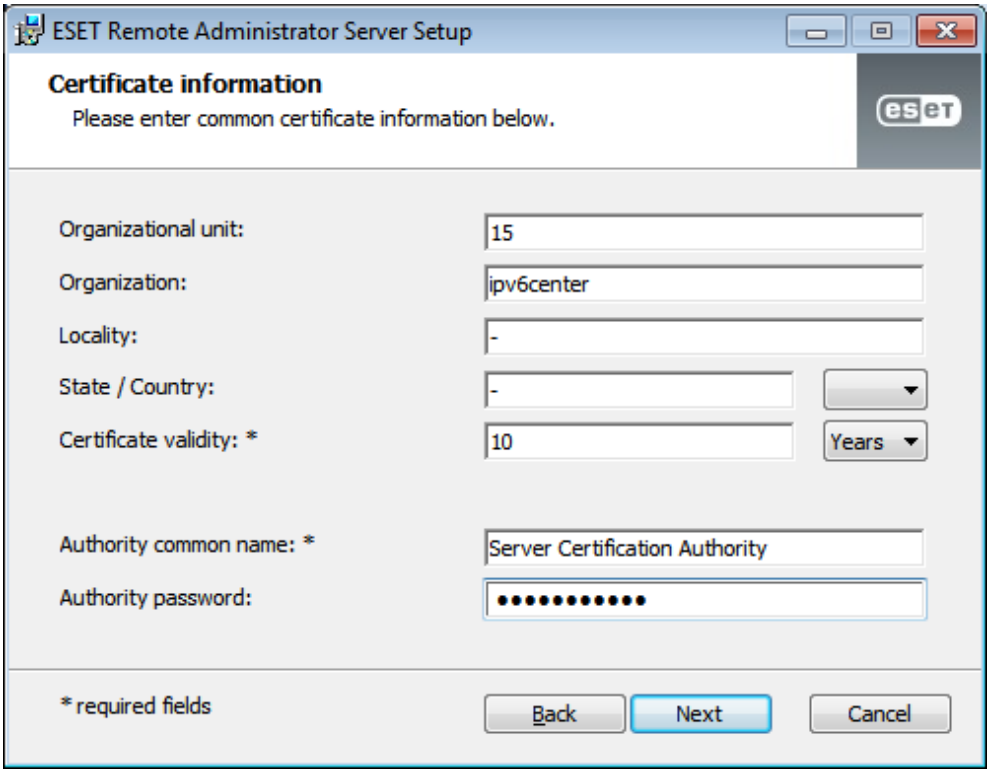
รูปที่ 1.15 ขั้นตอนการติดตั้ง ESET Remote Administrator (1)



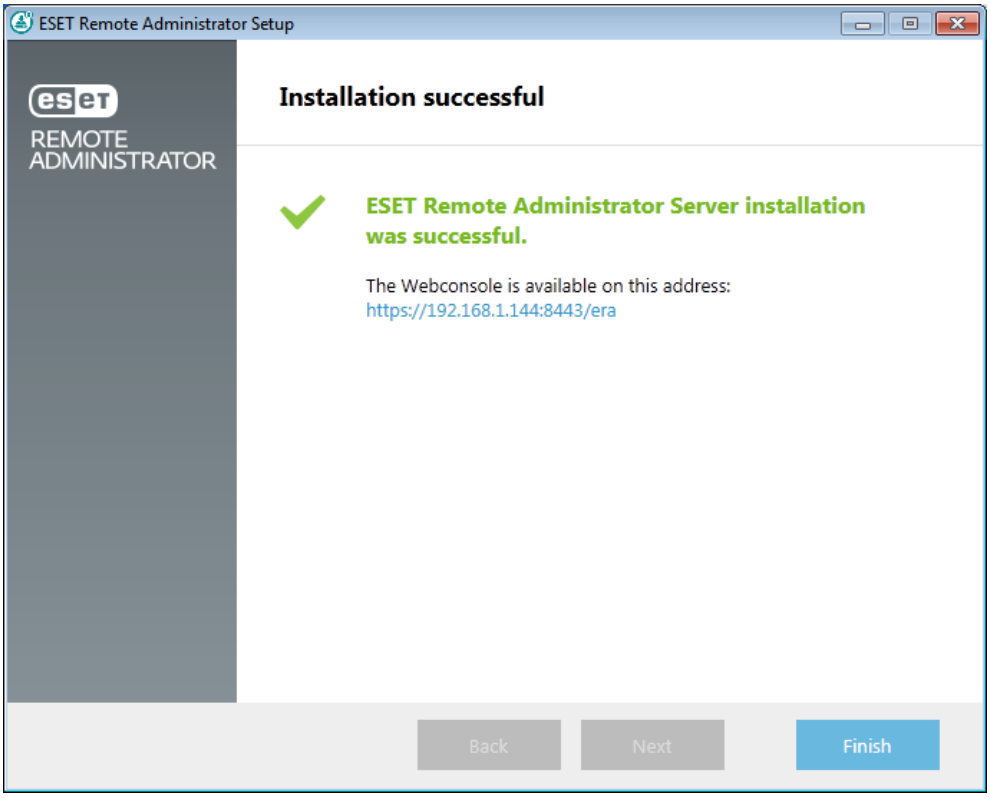
รูปที่ 1.16 ขั้นตอนการติดตั้ง ESET Remote Administrator (2)



รูปที่ 1.17 ขั้นตอนการติดตั้ง ESET Remote Administrator (3)



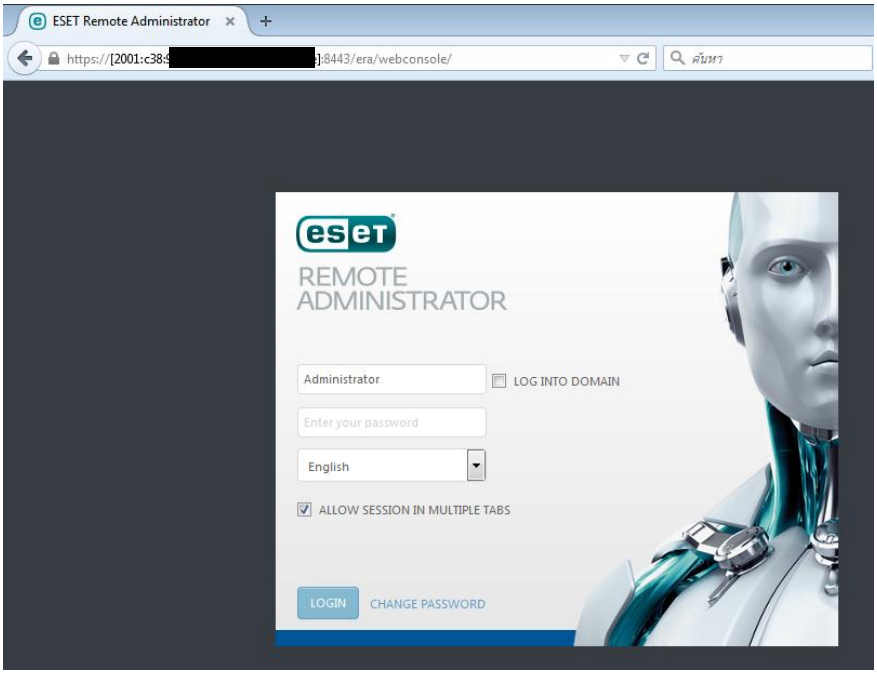
รูปที่ 1.18 ขั้นตอนการติดตั้ง ESET Remote Administrator (4)



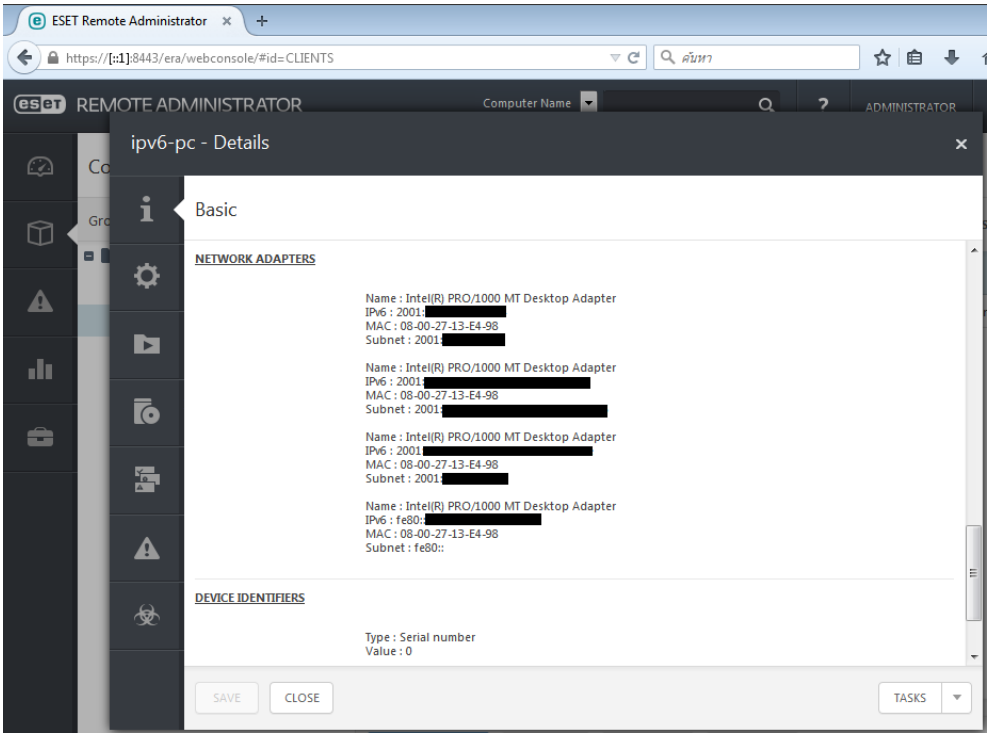
รูปที่ 1.19 ขั้นตอนการติดตั้ง ESET Remote Administrator (5)

ผลลัพธ์การทดสอบการใช้งาน IPv6

ESET Remote Administrator เป็นโปรแกรมแบบ web-base ซึ่งทั้งบริการของเว็บและบริการของโปรแกรมแสกนไวรัสต่างก็รองรับ IPv6 โดยจากภาพข้างล่างเป็นการทดสอบบริการของเว็บและแสดงผลการทำงานของ ESET Remote Administrator บน IPv6 native



รูปที่ 1.20 การใช้งาน ESET Remote Administrator ด้วย IPv6



รูปที่ 1.21 แสดงผลการทำงานของ ESET Remote Administrator บน IPv6 native

หัวข้อที่ 2 NAT64 & DNS64

2.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

ระบบเชื่อมต่อผ่านตัวกลางสู่ IPv6 (IPv6 Gateway) ที่นำเสนอในคู่มือนี้ได้พยายามปรับปรุงข้อจำกัดต่าง ๆ ในการปรับเปลี่ยนเครือข่ายจาก IPv4 สู่ IPv6 ที่มีอยู่ โดยอาศัยระบบเชื่อมต่อผ่านตัวกลางสู่ IPv6 (IPv6 Gateway) ทำการแปลงข้ามไอพีระหว่าง IPv4 กับ IPv6 และที่สำคัญที่สุดคือได้ทดสอบการใช้งานจากเครือข่าย ที่มีแต่หมายเลข IPv6 address (IPv6 Native) ทำการแปลงข้ามไปยังอินเตอร์เน็ตที่เป็น IPv4 ในปัจจุบันเพื่อใช้งาน Application ต่าง ๆ โดยที่ผู้ใช้งาน ไม่จำเป็นต้องทราบว่าปัจจุบันได้ใช้เครือข่ายที่เป็น IPv6 Native อยู่ ซึ่งระบบนี้สามารถรองกับทุกระบบปฏิบัติการที่สามารถรองรับ IPv6

การติดต่อสื่อสารจากเครือข่าย IPv6 ไปยังเครือข่าย IPv4 ผ่านระบบเชื่อมต่อผ่านตัวกลางสู่ IPv6 (IPv6 Gateway) เป็นการนำ DNS64 เข้ามาใช้ เพื่อช่วยในการแปลง Domain name จาก IPv4 records ไปเป็น IPv6 records และจะทำการ Address Mapping โดยการแปลง IPv4 ให้เป็นรูปแบบของเลขฐาน 16 แล้วนำไป map เข้ากับ prefix กับชุด IPv6 address จึงทำให้ระบบเชื่อมต่อผ่านตัวกลางสู่ IPv6 สามารถทำการแปลงแพ็กเก็ตเพื่อส่งต่อไปยังเครื่องปลายทางได้อย่างถูกต้อง ที่ช่วยทำให้เครื่องลูกข่ายจากเครือข่าย IPv6 สามารถติดต่อไปยังเครื่องแม่ข่ายที่อยู่ในเครือข่าย IPv4 โดยผู้ใช้งานไม่จำเป็นต้องทราบการตั้งค่าใด ๆ เพิ่มเติม

Preserve IPv4

ปัจจุบัน IPv4 address ซึ่งมีจำนวนบิตสำหรับกำหนด IP address จำนวน 32 บิต สามารถที่จะให้บริการได้ประมาณ 4.29 พันล้านหมายเลข ซึ่งไม่เพียงพอต่อความต้องการในปัจจุบันอีกต่อไป เนื่องจากความต้องการใช้งานอินเตอร์เน็ตมีเพิ่มมากขึ้นอย่างต่อเนื่อง จึงได้มีการพัฒนาเทคนิคต่างๆ เพื่อที่จะทำให้ IPv4 address สามารถขยายการใช้งานต่อไปอีกได้เรียกว่า “Preserve IPv4” ซึ่งมีตัวอย่างเทคนิคดังต่อไปนี้

- NAT44 เป็นเทคนิคที่ใช้กันในปัจจุบัน คือ ผู้ให้บริการจะจัดสรร Public IP ไปยังหน่วยงานต่าง ๆ แล้วภายในก็ใช้ Private IP address ไม่จำเป็นต้องเพิ่มอุปกรณ์อื่นเพิ่มเติมแต่วิธีการนี้ยังมีข้อจำกัดในเรื่องของจำนวน sessions จำกัดเมื่อมีการทำ NAT

- NAT444 วิธีการนี้ ผู้ให้บริการจะจัดสรร Private IP ไปให้โหนดต่างๆแทนการจัดสรร Public IP ไปให้อย่างในปัจจุบัน โดยถ้าองค์กรใดต้องการ Public IP ก็ค่อยจัดสรรไปให้เป็นรายองค์กรไป

- Address plus port (A+P) เป็นวิธีที่หลีกเลี่ยงการใช้ NAT คือ ผู้ให้บริการจะจัดสรรหมายเลข IP address เบอร์เดียวกันไปยังโหนดต่างๆ โดยที่จะกำหนด ช่วงหมายเลขของ port ที่แต่ละโหนดจะได้รับข้อมูลแตกต่างกันไป ต้องใช้ Port Range Router NAT ทั้งฝั่ง End host กับ Service provider ดังนั้น ICMP message ต้องมีการใส่ข้อมูลช่วงหมายเลข port พิเศษเพิ่มเติมเข้าไป เพราะภายใน ICMP message ไม่มีช่องใส่หมายเลข port ทำให้ Application บางตัวต้องการใช้งาน port พิเศษที่อยู่นอกช่วงหมายเลข port จะใช้งานไม่ได้

IPv4/IPv6 migration and transition techniques

การปรับเปลี่ยนการเชื่อมต่อในเครือข่ายอินเทอร์เน็ตจาก IPv4 ไปเป็น IPv6 ไม่สามารถทำได้อย่างทันทีทันใด เนื่องจากเครือข่ายที่ใช้งานอยู่ ณ.ปัจจุบันยังเชื่อมต่อกันด้วย IPv4 ซึ่งหากผู้ให้บริการเครือข่าย

ต้องการที่จะปรับปรุงระบบให้รองรับการใช้งาน IPv6 ก็จำเป็นมีเทคนิคต่างๆที่จะช่วยให้เครือข่ายสามารถที่จะให้บริการ IPv6 แก่ผู้ใช้บริการได้เรียกว่า “IPv6 transition” โดย IPv6 Transition จะแบ่งออกเป็น 3 เทคนิคหลักๆ ได้แก่ Dual stack, Translation และ Tunneling

Translation

- NAT-PT เป็นการแปลงตำแหน่งที่อยู่บนเครือข่าย (Network Address Translation) คล้ายกับที่มีใน IPv4 แต่ได้เพิ่มประสิทธิภาพในการทำงาน โดยเพิ่มการทำ Protocol Translation ขึ้นมาด้วย ซึ่งในปัจจุบัน การใช้งาน NAT-PT ถือว่าเป็นหนทางสุดท้ายที่จะใช้ในการดำเนินการแล้ว เนื่องจากมีเทคนิคหรือวิธีการอื่นๆ ที่มีประสิทธิภาพมากกว่า

- Address Family Translation (AFT) คือการเปลี่ยน header และชนิดของ address (IPv4, IPv6) ใน IP packet ซึ่งเทคนิคของ AFT นี้มีอยู่ 2 วิธีหลักๆ ซึ่งก็คือการทำ NAT64 หรือ NAT46

- Dual-Stack Lite (DS-Lite) ใช้หลักการการทำ tunneling มาใช้เพื่อที่จะทำการ encapsulation IPv4 packet ด้วย IPv6 packet ซึ่งจะเรียกการดำเนินการเช่นนี้ว่า “IPv4-in-IPv6” Tunnel จะถูกสร้างระหว่างอุปกรณ์ฝั่งเกตเวย์ของผู้ใช้งาน กับอุปกรณ์ของผู้ให้บริการซึ่งการสร้าง tunnel จะสร้างผ่าน ISP core network ทำให้ภายใน ISP core network ไม่มีความจำเป็นที่จะต้องใช้งาน IPv4 address ในการใช้งาน เมื่อมีการ encapsulation ipv4 packet แล้วส่งมาถึงปลายทางของ tunnel อุปกรณ์ของผู้ให้บริการก็จะต้องทำการ decapsulation เพื่อให้ได้ IPv4 packet กลับมา แต่เนื่องจาก DS-lite กำหนดให้ IPv4 address สำหรับผู้ใช้งานเป็น private IPv4 address เท่านั้น จึงออกแบบให้มีการทำ NAT เพื่อที่จะทำให้สามารถส่ง IPv4 packet ดังกล่าวเข้าสู่ IPv4 internet ได้ แต่การทำ NAT ของกระบวนการ DS-lite นั้นไม่สามารถดำเนินการโดยใช้เพียงแค่ข้อมูลของ inside IPv4 source address + port กับ outside IPv4 source address + port ได้ เนื่องจาก IPv4 ของผู้ใช้งานแต่ละคนอาจมีการซ้ำซ้อนกันทำให้ไม่สามารถระบุกลับไปยังปลายทางที่ถูกต้องได้ และยังขาดข้อมูลของ IPv6 address ของฝั่งผู้ใช้งาน ดังนั้นการทำ NAT ของกระบวนการ DS-lite จึงต้องมีการบันทึกข้อมูลของ IPv6 address ของผู้ใช้งานเข้าไปด้วย

Tunneling

- 6to4 เป็นกลไกการเปลี่ยนแปลงทางอินเทอร์เน็ตสำหรับการปรับเปลี่ยนจาก IPv4 สู่ IPv6 ซึ่ง 6to4 จะอนุญาต IPv6 packets ถูกส่งผ่าน IPv4 network โดยไม่จำเป็นต้องกำหนดค่าอุโมงค์ (tunnel) อย่างชัดเจน โดยที่เซิร์ฟเวอร์รีเลย์พิเศษจะจัดการการเชื่อมต่อสื่อสารระหว่างเครือข่าย 6to4 กับเครือข่าย native IPv6 การกำหนด IPv6 ใช้การตั้งค่าอัตโนมัติซึ่งต้องการ 64 บิตสำหรับโฮส และอีก 64 บิตสำหรับเน็ตเวิร์ก รวมเป็น 128 บิต โดยที่มีรายละเอียดดังนี้ 16 บิตแรกคือ IPv6 prefix ซึ่งถูกกำหนดค่าเป็น 2002: จากนั้น 32 บิตถัดมาคือ IPv4 address และอีก 16 บิตสุดท้ายจะถูกเลือกแบบสุ่มโดยเราเตอร์ เพื่อให้รวมกันเป็น 64 บิต ส่วนที่เหลืออีก 64 บิตซึ่งก็คือ IPv6 host นั้นจะถูกกำหนดให้ไม่ซ้ำกันเพื่อนำมารวมกันเป็น IPv6 ที่สมบูรณ์

- IPv6 rapid deployment (6rd) เป็นเทคนิคการทำ tunneling ล่าสุด พัฒนาต่อจาก 6to4 โดยจะเป็นการ tunneling แบบ auto โดย ISP สามารถใช้ IPv6 prefix address ของตัวเองได้ แทนการใช้ Prefix พิเศษ (2002::/16) ที่ใช้ใน 6to4 ทำให้ผู้ดูแลระบบสามารถกำหนด domain ของ IPv4 address ที่สามารถใช้งานได้ และสามารถถูกควบคุมการจัดการการกำหนดเส้นทาง (routing) ทั้งหมดของ 6rd ได้โดยตรง ส่งผลให้สามารถที่จะแก้ไขปัญหาด้านการกำหนดเส้นทาง (routing) และสามารถใช้งานร่วมกับ PrivateIPv4 address ได้

6RD domain จะประกอบด้วย 2 ส่วน ซึ่งก็คือ 6RD Customer Edge และ 6RD Border Relay โดยที่ IPv6 packet ที่ถูกห่อหุ้มด้วย IPv4 packet จะถูกส่งไปมาระหว่าง 6RD CEs และ 6RD BRs ที่อยู่ภายในเครือข่ายของผู้ให้บริการ โดยที่ IPv6 packet ที่จะสามารถเดินทางผ่าน 6RD BR ได้ก็จะมีเฉพาะแพ็กเก็ตที่จะเดินทางออกไปยังภายนอกเครือข่าย หรือแพ็กเก็ตที่เดินทางเข้ามาจากเครือข่ายภายนอกเท่านั้น

กระบวนการ 6RD จะทำการแบ่ง IPv6 address ออกเป็น 3 ส่วนหลักๆ ได้แก่ 6RD delegated prefix, subnet ID และ interface ID ซึ่งจำนวนบิตที่ถูกกำหนดในแต่ละส่วนสามารถปรับเพิ่มขึ้นหรือลดจำนวนลงก็ได้ขึ้นอยู่กับการนำไปประยุกต์กับการใช้งาน แต่โดยทั่วไปมักจะกำหนดให้จำนวนบิตสำหรับ interface ID มีค่าคงที่เท่ากับ 64 บิต ในส่วนของ 6RD delegated prefix จะแบ่งย่อยออกเป็น 2 ส่วน ก็คือ 6RD prefix และ IPv4 address ซึ่งในส่วนของ 6rd prefix จะใช้ IPv6 network ของผู้ให้บริการ และในส่วน IPv4 address ใน 6RD delegated prefix ก็ไม่จำเป็นต้องใช้จำนวนบิตเพื่อแสดงค่า IPv4 address เท่ากับ 32 บิตเสมอเหมือนกับ 6to4 เพราะ 6RD สามารถทำการ encode IPv4 address เพื่อลดจำนวนบิตที่จะใช้แสดงค่า IPv4 address ลงได้ โดยการทำการ encode จะกำหนดจำนวนบิตที่ถูกตัดทิ้งก่อน แล้วทำการกำหนดค่าให้กับแต่ละบิตที่ถูกตัดออกไป ส่วนจำนวนบิตที่เหลือก็จะใช้เป็น IPv4 address ของ 6rd delegated prefix ทำให้สามารถจับคู่กันระหว่างค่าของจำนวนบิตที่ถูกตัดออกไป และค่าใน IPv4 address ของ 6rd delegated prefix เพื่อรวมกลับมาเป็น IPv4 address ที่ถูกต้อง ด้วยเหตุนี้จึงทำให้ 6rd สามารถที่จะปรับแต่งการจัดสรร IPv6 ได้อย่างหลากหลาย และเหมาะสมกับการใช้งานของแต่ละเครือข่าย

- IPv4 Residual Deployment (4rd) เป็นการทำ tunneling เพื่อที่จะให้ IPv4 packet สามารถที่จะส่งผ่าน IPv6 network โดยการนำ IPv4 packet มาห่อหุ้มด้วย IPv6 packet ซึ่งเป็นกระบวนการที่กลับกันกับ 6RD เนื่องจาก 4RD ต้องการลดการใช้งาน IPv4 ภายในเครือข่ายให้น้อยที่สุด โดยที่อุปกรณ์เครือข่ายที่อยู่ภายใน core network ก็ไม่จำเป็นที่จะต้องมี IPv4 address เพราะ IPv4 packet จะถูกห่อหุ้มอยู่ภายใน IPv6 packet เมื่อผ่าน core network ทำให้ core network ใช้งานเฉพาะ IPv6 protocol ก็เพียงพอแล้ว ทำให้อุปกรณ์ในส่วน core network จึงมีการประมวลผลลดลง เนื่องจากทำการประมวลผลเพียงแค่ IPv6 protocol

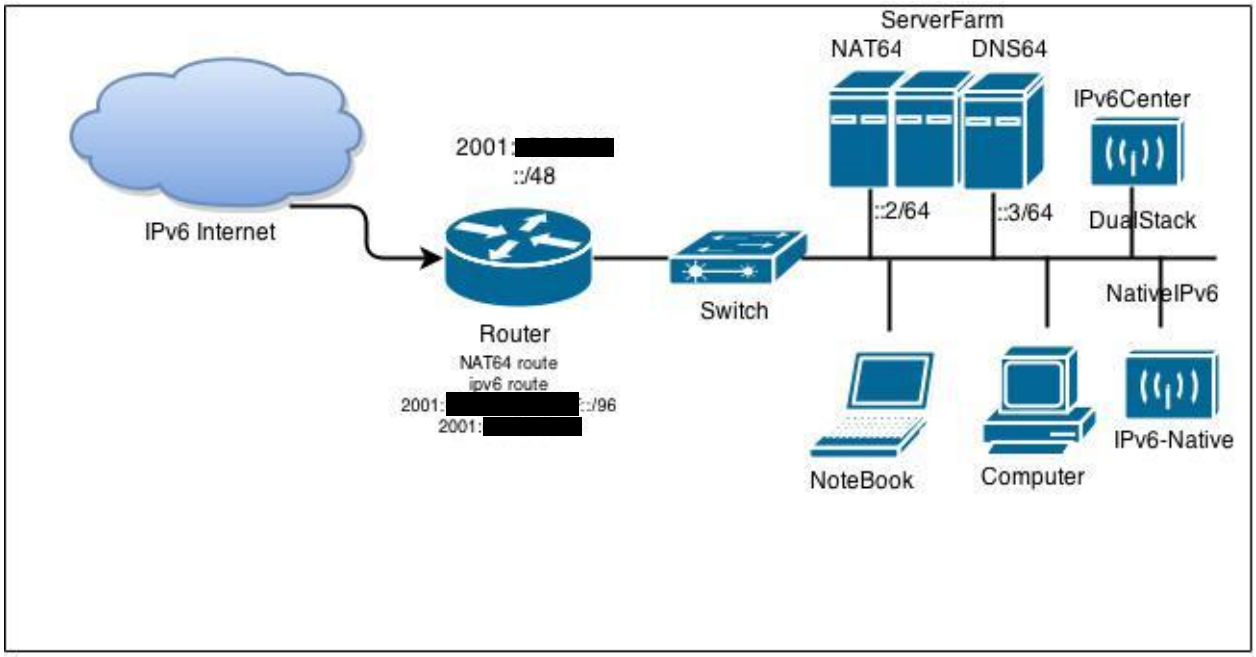
4RD ยังเป็นเทคนิคที่ยังเป็น Draft อยู่ แต่ใช้วิธี automatic Mapping แบบ stateless ระหว่าง IPv6 กับ IPv4 เทคนิคจะคล้ายกับ DS-Lite แต่ไม่มีการใช้ LSN (large-scale NAT)

- Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) เป็น IPv6 transition ที่ใช้สำหรับช่วยให้เครื่องที่ต้องการใช้งาน IPv6 address สามารถใช้งาน IP แบบ Dual-Stack ได้ โดยใช้หลักการการ encapsulation IPv6 packet ลงใน IPv4 packet เพื่อส่งผ่านเครือข่าย IPv4 ซึ่ง ISATAP ใช้การสร้าง tunnel แบบ automatic tunneling ที่รองรับทั้งการเชื่อมต่อแบบ host-to-host, host-to-router และ router-to-host อีกทั้ง ISATAP ยังสามารถใช้งานได้ทั้ง Public IPv4 และ Private IPv4 สำหรับส่วนประกอบที่ต้องใช้ในสร้างการเชื่อมต่อแบบ ISATAP มี 3 ส่วนได้แก่ ISATAP host, ISATAP router และ DNS server โดยที่ ISATAP host คือเครื่องที่ต้องการใช้งาน IPv6 ด้วย ISATAP ในส่วน ISATAP router เป็นเหมือนกับ default gateway สำหรับ logical subnet ของ IPv6 prefix นี้ และ DNS server จะเป็นผู้ระบุ ISATAP router ให้กับ ISATAP host

การกำหนด IPv6 สำหรับ ISATAP จะกำหนดเป็น ISATAP_interface_identifier::0:5EFE:w.x.y.z ซึ่ง w.x.y.z ก็คือ private IPv4 address หรือ interface_identifier::200:5EFE:w.x.y.z ซึ่ง w.x.y.z ก็คือ public IPv4 address ซึ่งมีการกำหนดค่าของ U bit เป็นไปตามรูปแบบของ EUI-64 โดยที่ค่า ISATAP_interface_identifier จะเป็นค่าที่กำหนดขึ้นมาสำหรับใช้งาน Logical Subnet ซึ่งมีค่าเท่ากับ 64

บิต ดังนั้น IPv6 prefix ที่จะกำหนดให้สำหรับ logical subnet ก็จะสามารถกำหนดขอบเขตการเชื่อมต่อของ ISATAP ได้ โดยหากกำหนดให้ใช้ IPv6 prefix เป็น link-local (FE80::/64) หรือ unique local ก็จะเชื่อมต่อผ่าน IPv6 ได้เฉพาะใน Intranet เท่านั้น แต่หากกำหนดให้ใช้ IPv6 prefix เป็น global prefixes ก็จะสามารถใช้เชื่อมต่อกับเครือข่าย IPv6 อื่นๆได้

2.2 การติดตั้ง NAT64 และ DNS64



รูปที่ 2.1 ติดตั้ง tayga สำหรับแปลงไอพีไปกลับระหว่าง IPv6 <-> IPv4

การหา package ที่จะติดตั้ง

$sudo apt-cache search tayga

การติดตั้ง package

$sudo apt-get install tayga

แก้ไขไฟล์คอนฟิก tayga

$sudo vi /etc/default/tayga

แก้ไขไฟล์คอนฟิกสำหรับใช้งาน

$sudo vi /etc/tayga.conf

```
tun-device nat64
ipv4-addr 192.168.255.1
prefix 2001:db8:x:x:ffff::/96
dynamic-pool 192.168.255.0/24
data-dir /var/spool/tayga
```

การรันโปรแกรม tayga

$sudo /etc/init.d/tayga restart

การตรวจสอบไฟล์ log ว่าสามารถรันหรือไม่

$sudo tail -n 50 /var/log/messages

$sudo tail -n 50 /var/log/syslog

$sudo ps aux | grep tayga

$sudo ip addr add 192.168.255.1 dev nat64

$sudo ip addr add 2001:db8:x:x::1 dev nat64

$sudo ip route add 192.168.255.0/24 dev nat64

$sudo ip route add 2001:db8:x:x:ffff::/96 dev nat64

การติดตั้ง DNS64

ใช้ bind9 ในการทำ DNS64

$sudo apt-get install bind9

เพิ่ม config เข้าไป

sudo vi /etc/bind/conf/named.conf.options

```
dns64 2001:db8:x:x:ffff::/96 {
        clients { any; };
};
```

$sudo service bind9 restart

การแก้ไข dns ของ host client

$sudo vi /etc/resolv.conf

```
nameserver 2001:db8:x::3
```

การ config router

ให้ใช้ route ของ nat64

ipv6 route 2001:db8:x:x:FFFF::/96 2001:db8:x::2

ipv6 route 2001:db8:x:x::/64 2001:db8:x::2

2.3 การทดสอบ NAT64 และ DNS64

$ping6 2001:db8:x:x:ffff::192.168.255.1

```
 ping6 2001:db8:x:x:ffff::192.168.255.1
PING 2001:db8:x:x:ffff::192.168.255.1(2001:db8:x:x:ffff:0:c0a8:ff01) 56 data bytes
64 bytes from 2001:db8:x:x:ffff:0:c0a8:ff01: icmp_seq=1 ttl=64 time=0.068 ms
64 bytes from 2001:db8:x:x:ffff:0:c0a8:ff01: icmp_seq=2 ttl=64 time=0.099 ms
64 bytes from 2001:db8:x:x:ffff:0:c0a8:ff01: icmp_seq=3 ttl=64 time=0.095 ms
```

$telnet www.sanook.com 80

```
Trying 2001:db8:x:x:ffff:0:cb97:81a2...
Connected to www.gslb.sanook.com.
Escape character is '^]'.
```

$dig www.sanook.com aaaa

```
www.sanook.com.          169  IN   CNAME  www.gslb.sanook.com.
www.gslb.sanook.com.  76  IN   AAAA   2001:db8:x:x:ffff:0:cb97:82e2
```

อ้างอิง

1. http://www.slideshare.net/max_posedon/ipv6-at-home?qid=f3b8c3f5-90e6-4687-be38-17f4d2437a8d&v=default&b=&from_search=6
2. http://www.queret.net/blog/2011/11/internet-sans-ipv4-...-le-nat64/

Configuration File

Config NAT64

vi /etc/tayga.conf

```
tun-device nat64
ipv4-addr 192.168.255.1
prefix 2001:db8:x:x:ffff::/96
dynamic-pool 192.168.255.0/24
data-dir /var/spool/tayga
```

Config DNS64

vi /etc/bind/conf/name.conf.option

```
options {
//tong    directory "/var/cache/bind";
        directory "/data/named";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        forwarders {
                2001:4860:4860::8888;
                2001:4860:4860::8844;
        };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;
# query range you allow
        allow-query { any; };
      allow-query-cache { any;  };

# the range to transfer zone files
      allow-transfer { any; };

# recursion range you allow
      recursion yes;
#       allow-recursion { any; };
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
        dns64 2001:db8:x:x:ffff::/96 {
                clients { any; };
        };
};
```

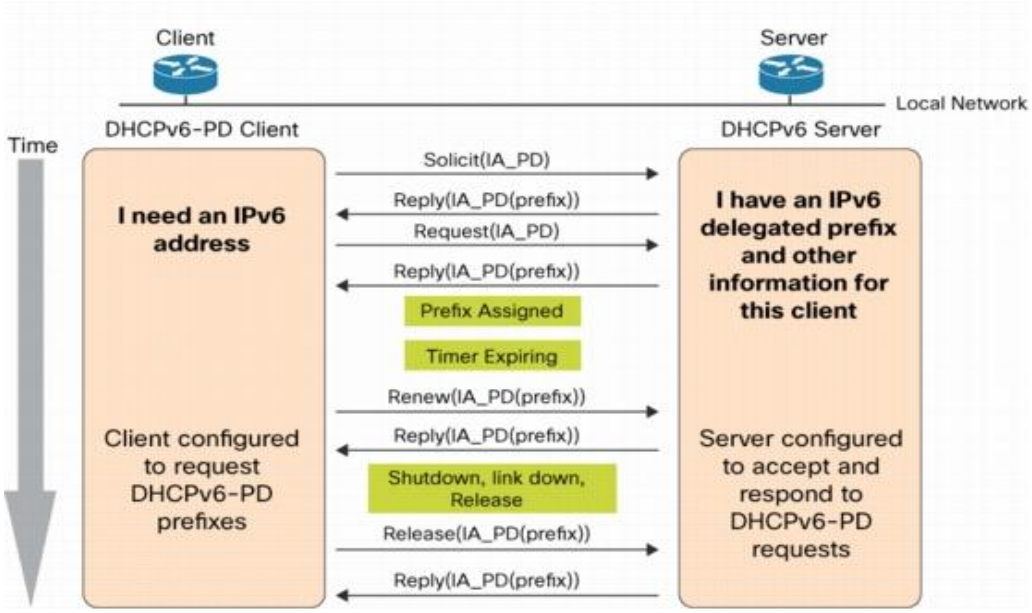
หัวข้อที่ 3 DHCPv6 & Stateless Autoconfiguration

3.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

3.1.1 DHCPv6

DHCPv6 เป็น Network Protocol ที่ใช้ตั้งค่าหมายเลข IPv6, IPv6 prefixes และข้อมูลอื่นๆ เช่น DNS สำหรับเครื่องลูกข่าย การตั้งค่าด้วย DHCPv6 มีหลักการทำงานคล้ายๆกับ DHCPv4 เครื่องลูกข่ายอาจกำหนดหมายเลข IPv6 แบบอัตโนมัติด้วย Stateless Address Autoconfiguration (SLAAC) แต่รับข้อมูลอื่นๆ ผ่าน DHCPv6

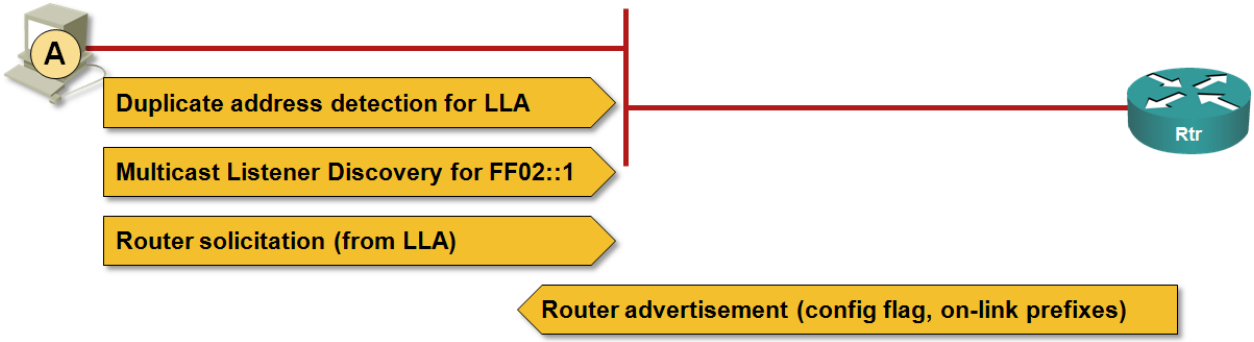
เนื่องจากข้อมูลหลายๆอย่างไม่สามารถดำเนินการแบบ stateless ได้จึงจำเป็นที่จะต้องจัดสรรโดยใช้ DHCPv6 โดยข้อมูลที่ SLAAC ไม่สามารถกำหนดให้ได้ SLAAC สามารถกำหนดให้เครื่องลูกข่ายร้องขอจาก DHCPv6 แทน ด้วยเหตุนี้ทำให้ DHCPv6 มีความยืดหยุ่นในการจัดสรร IPv6 และข้อมูลที่จำเป็นอื่นๆ สูงกว่า SLAAC อีกทั้งยังร้องรับการเพิ่มเติม OPTION ใหม่ๆในอนาคตได้เป็นอย่างดี DHCPv6 จึงเป็นอีกหนึ่งโพรโตคอลที่มีความสำคัญสำหรับใช้งาน IPv6



รูปที่ 3.1 หลักการทำงานของ DHCPv6

3.1.2 Stateless Address Autoconfiguration (SLAAC)

SLAAC เป็นโพรโตคอลที่ใช้สำหรับตั้งค่า IPv6 แบบอัตโนมัติโดยใช้ Neighbor Discovery Protocol เมื่อเครื่องลูกข่ายเชื่อมต่อเครือข่าย เครื่องลูกข่ายสามารถค้นหาเกตเวย์เราเตอร์, เครื่องลูกข่ายอื่นๆ, IPv6 prefix (RFC 2461) และ DNS server (RFC 6106) ในกรณีที่เราเตอร์ต้องประกาศข้อมูลดังกล่าว เราเตอร์ต้องติดตั้ง RADVD ซึ่งเป็นซอฟแวร์ open-source ที่ใช้สำหรับตั้งค่าเพื่อกำหนดข้อมูลที่จะใช้สำหรับประกาศในเครือข่าย



รูปที่ 3.2 หลักการทำงานของ SLAAC

3.2 การติดตั้ง DHCPv6 และ RADVD

3.2.1 ความต้องการของระบบ

OS: เป็น Unix และ Unix-like operating system

โดยใน Testbed ใช้เป็น Ubuntu

3.2.2 ขั้นตอนการติดตั้ง

2.2.1 DHCPv6

sudo apt-get -y install isc-dhcp-server

2.2.2 RADVD

sudo apt-get -y install radvd

3.3 การ Config เพื่อรองรับ IPv6

การตั้งค่าเพื่อจัดสรรข้อมูล IPv6 ให้กับเครื่องลูกข่ายแบ่งออกเป็น 3 รูปแบบด้วยกัน ได้แก่ SLAAC, Stateless DHCPv6 และ Stateful DHCPv6 สำหรับ SLAAC จะเป็นการจัดสรรข้อมูล IPv6 โดยใช้ RADVD เพียงอย่างเดียว ส่วน Stateless DHCPv6 และ Stateful DHCPv6 จะเป็นการจัดสรรข้อมูล IPv6 โดยใช้ DHCPv6 และ RADVD ควบคู่ไปด้วยกัน โดยรายละเอียดการตั้งค่าของทั้ง 3 รูปแบบมีดังต่อไปนี้

3.3.1 SLAAC

รูปแบบนี้กำหนดให้ Radvd จัดสรรข้อมูล Default Gateway, DNS Server Address และ IPv6 prefix ให้กับเครื่องลูกข่าย แต่วิธีการนี้เครื่องลูกข่ายที่ใช้ Windows จะไม่สามารถรับ DNS Server Address ได้ เนื่องจากการประกาศ DNS Server Address เพิ่งได้รับการนิยามเพิ่มเติมภายหลัง แต่สำหรับเครื่องลูกข่ายใช้ Linux ก็สามารถใช้งานได้ปกติ ข้อจำกัดสำหรับวิธีการนี้คือ เครื่องลูกข่ายจะใช้งาน Temporary Address ซึ่งยากต่อการควบคุมการใช้งานของผู้ดูแลระบบ

sudo sysctl -w net.ipv6.conf.all.forwarding=1

sudo vi /etc/radvd.conf

```
interface eth0
{
        AdvManagedFlag off;
        AdvSendAdvert on;
        AdvOtherConfigFlag off;
        MinRtrAdvInterval 3;
        MaxRtrAdvInterval 60;
        prefix 2001:db8:x:x::/64  {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr on;
        };
        RDNSS 2001:db8:x:x::2 {
        };
};
```

sudo /etc/init.d/radvd restart

3.3.2 Stateless DHCPv6

การตั้งค่าในรูปแบบนี้กำหนดให้ใช้ DHCPv6 ประกาศ DNS Server Address เท่านั้น ส่วน SLAAC ประกาศ Default Gateway และ IPv6 prefix การจัดสรร IPv6 address รูปแบบนี้ เครื่องลูกข่ายยังคงใช้งาน Temporary Address ได้ เนื่องจากใช้การประกาศ IPv6 prefix ด้วย SLAAC อย่างไรก็ตาม ข้อดีของการจัดสรร IPv6 address รูปแบบนี้คือสามารถประกาศข้อมูลอื่นๆ ให้กับเครื่องลูกข่ายผ่าน DHCPv6 option โดยการใช้งาน stateless DHCPv6 ของ Windows Server 2008 ใช้หลักการดำเนินการเช่นเดียวกัน (ในการทดสอบใช้ Windows Server 2008 เป็นเครื่อง server และใช้ Ubuntu เป็น default gateway ซึ่งติดตั้ง RADVD)

- Config SLAAC (RADVD)

sudo sysctl -w net.ipv6.conf.all.forwarding=1

sudo vi /etc/radvd.conf

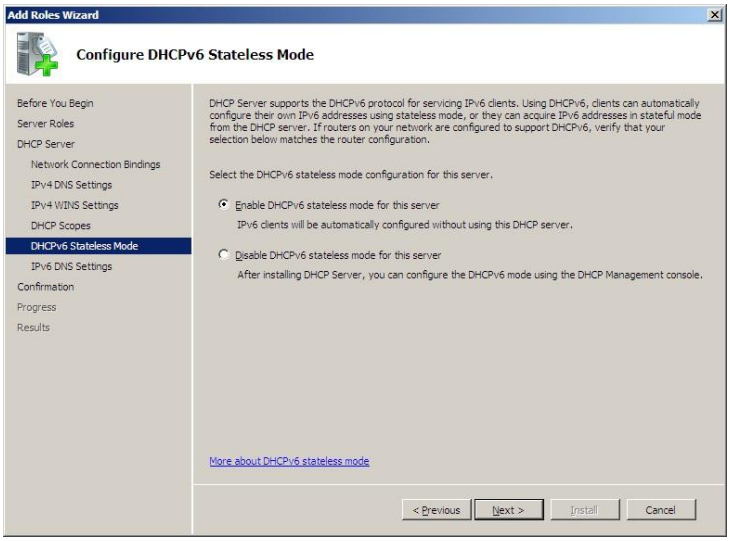
```
interface eth0
{
        AdvSendAdvert on;
        AdvManagedFlag on;
        AdvOtherConfigFlag off;
        AdvReachableTime 0;
        AdvRetransTimer 0;
        AdvCurHopLimit 64;
```

```
        AdvDefaultLifetime 1800;
        AdvHomeAgentFlag off;
        AdvDefaultPreference medium;
        AdvSourceLLAddress on;
        AdvLinkMTU 1500;
        prefix 2001:db8:x:x::/64  {
                AdvOnLink on;
                AdvAutonomous on;
                AdvRouterAddr on;
        };
}; # End of interface definition
```

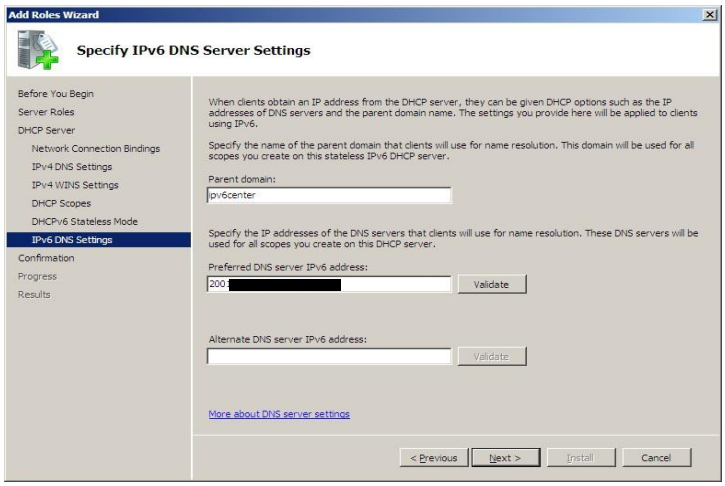
sudo /etc/init.d/radvd restart

- Config DHCPv6 (stateless DHCPv6 ของ Windows Server 2008)

ติดตั้ง DHCP roles



รูปที่ 3.3 เปิดการใช้งาน DHCPv6: Stateless Mode



รูปที่ 3.4 ตั้งค่า IPv6 DNS สำหรับประกาศใน DHCPv6

3.3.3 Stateful DHCPv6

รูปแบบนี้สามารถจัดสรรข้อมูล IPv6 ทั้ง Default Gateway, DNS Server Address และ IPv6 address ให้กับเครื่องลูกข่ายได้อย่างครบถ้วน โดยไม่มีข้อจำกัดเกี่ยวกับระบบปฏิบัติการของเครื่องลูกข่าย การตั้งค่าในรูปแบบนี้กำหนดให้ใช้ DHCPv6 ประกาศ DNS Server Address และ IPv6 address แบบ stateful ส่วน SLAAC ประกาศ Default Gateway เท่านั้น โดยการจัดสรร IPv6 address รูปแบบนี้สามารถกำหนดไม่ให้เครื่องลูกข่ายใช้งาน Temporary Address ได้ ซึ่งก็จะช่วยให้ผู้ดูแลระบบสามารถควบคุมการใช้งาน IPv6 address ของเครื่องลูกข่ายได้ง่ายยิ่งขึ้น

- Config SLAAC (RADVD)

sudo sysctl -w net.ipv6.conf.all.forwarding=1

sudo vi /etc/radvd.conf

```
interface eth0
{
        AdvSendAdvert on;
        AdvManagedFlag on;
        AdvOtherConfigFlag off;
        AdvReachableTime 0;
        AdvRetransTimer 0;
        AdvCurHopLimit 64;
        AdvDefaultLifetime 1800;
        AdvHomeAgentFlag off;
        AdvDefaultPreference medium;
        AdvSourceLLAddress on;
        AdvLinkMTU 1500;
}; # End of interface definition
```

sudo /etc/init.d/radvd restart

- Config DHCPv6

sudo touch /var/lib/dhcp/dhcpd6.leases (สร้างไฟล์สำหรับเก็บข้อมูล IPv6)

sudo vi /etc/default/isc-dhcp-server (แก้ไขตัวแปรในไฟล์ให้มีค่าต่อไปนี้)

```
DHCPD_CONF=/etc/dhcp/dhcpd6.conf
OPTIONS="-6"
INTERFACES="eth0"
```

sudo vi /etc/dhcp/dhcpd6.conf

```
default-lease-time 600;
max-lease-time 7200;
authoritative;
log-facility local7;
```

```
option dhcp6.name-servers 2001:db8:x::3;
#host client {
#    host-identifier option dhcp6.client-id 00:03:00:01:00:50:56:82:7a:fd;
#    fixed-address6 2001:db8:2:1::2;
#}

subnet6 2001:db8:x:x::/64 {
      range6 2001:db8:x:x::1000 2001:db8:x:x::2000;
}
```

```
sudo /etc/init.d/isc-dhcp-server restart
```

note: ในกรณีที่ restart DHCP server ไม่สำเร็จให้ตรวจสอบว่า IPv6 ที่กำหนดบน interface eth0 ตรงกับที่ config ใน /etc/dhcp/dhcpd6.conf หรือไม่ และสร้างไฟล์ /var/lib/dhcp/dhcpd6.leases สำหรับเก็บข้อมูล IPv6 address ที่ได้รับการจัดสรรแล้วหรือไม่ สำหรับข้อผิดพลาดอื่นๆสามารถตรวจสอบได้จาก /var/log/syslog

Config Stateful DHCPv6 สำหรับ CISCO iOS 15.2

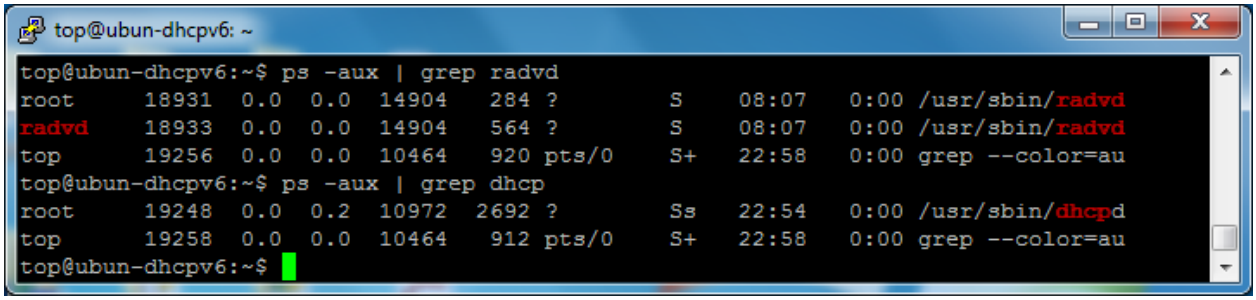
```
R1#sh run
Building configuration...

Current configuration : 1981 bytes
!
! Last configuration change at 13:53:39 UTC Fri Jun 5 2015
upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
```

```
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
ipv6 dhcp pool dhcpv6
 address prefix 2001:DB8::/64 lifetime infinite infinite
 dns-server 2001:4860:4860::8888
 domain-name testv6
!
multilink bundle-name authenticated
!
redundancy
!
ip tcp synwait-time 5
!
interface GigabitEthernet0/0
 no ip address
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 ipv6 address 2001:DB8::1/64
 ipv6 enable
 ipv6 nd prefix default no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd ra suppress
 ipv6 dhcp server dhcpv6
!
ip forward-protocol nd
no ip http server
no ip http secure-server
no cdp log mismatch duplex
!
control-plane
!
mgcp profile default
!
gatekeeper
```

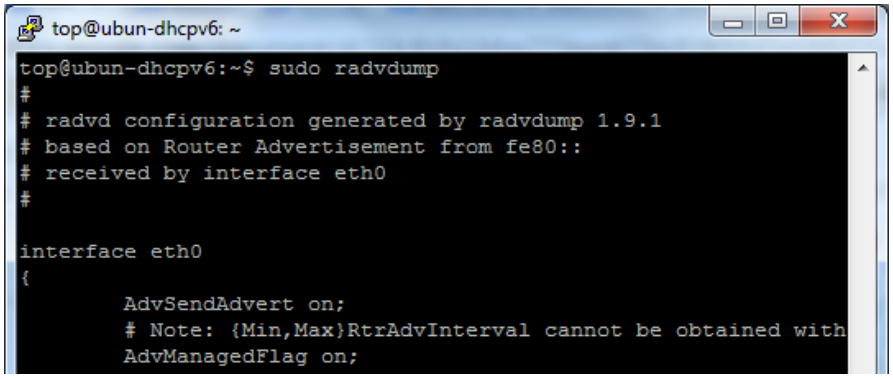
```
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
 transport input all
!
end
```

3.4 การทดสอบการทำงาน

การทดสอบบนเครื่องเราเตอร์ว่ามีการรัน DHCPv6 และ RADVD ด้วยคำสั่งต่อไปนี้



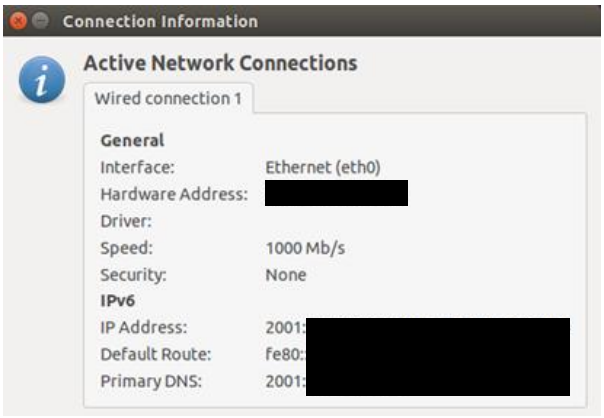
รูปที่ 3.5 แสดงผลการทดสอบการรัน DHCPv6 และ RADVD



รูปที่ 3.6 แสดงผลการทดสอบการประกาศข้อมูลด้วย RADVD

3.4.1 SLAAC

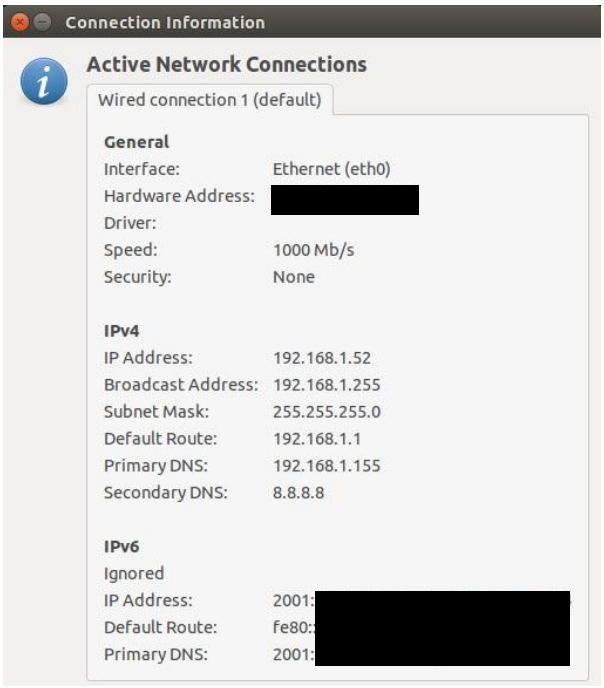
ผลการทดสอบบนเครื่องลูกข่ายได้ผลลัพธ์ดังต่อไปนี้



รูปที่ 3.7 แสดงข้อมูล IPv6 ที่เครื่องลูกข่ายได้รับจาก SLAAC

3.4.2 Stateless DHCPv6

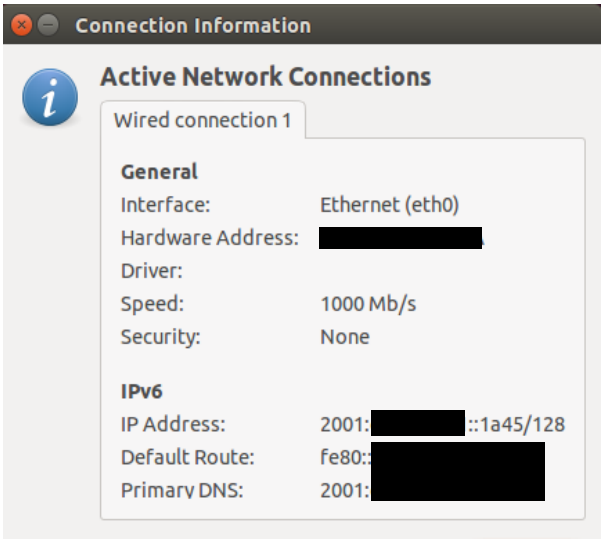
ผลการทดสอบบนเครื่องลูกข่ายได้ผลลัพธ์ดังต่อไปนี้



รูปที่ 3.8 แสดงข้อมูล IPv6 ที่เครื่องลูกข่ายได้รับจาก Stateless DHCPv6

3.4.3 Stateful DHCPv6

ผลการทดสอบบนเครื่องลูกข่ายได้ผลลัพธ์ดังต่อไปนี้

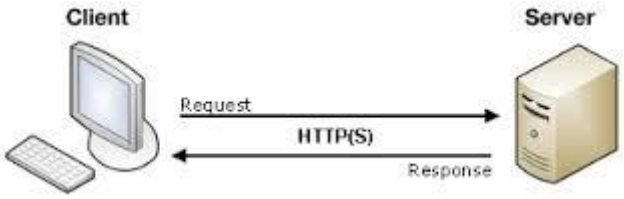


รูปที่ 3.9 แสดงข้อมูล IPv6 ที่เครื่องลูกข่ายได้รับจาก Stateful DHCPv6

หัวข้อที่ 4 Web Server

4.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

Web Server อาศัยการทำงานแบบ HTTP (Hypertext Transfer Protocol) เป็น Protocol เบื้องต้นที่ทำงานบน Transmission Control Protocol (TCP) ที่ใช้ในการจัดรูปแบบ การรับส่ง การเชื่อมโยงเอกสาร และสื่อผสมต่างๆ เช่นรูปภาพ ข้อความ รวมไปถึงภาพเคลื่อนไหว และข้อมูลเสียง ซึ่งเป็นการบริการพื้นฐานของ World Wide Web (WWW)



รูปที่ 4.1 หลักการทำงานของ HTTP

มีการทำงานที่มีทั้งฝั่งเซิร์ฟเวอร์ จัดเตรียม และส่งข้อมูลต่างๆ ที่มีการร้องขอจากทางด้านฝั่ง Client โดยใช้ Web Browser ในการร้องขอข้อมูล จากฝั่ง Server และนำมาแสดงผลให้กับผู้ใช้งาน ปกติแล้ว Apache Web Server ทำงานที่ Port 80 สำหรับ HTTP และ Port 443 สำหรับ HTTPS

4.2 การติดตั้ง Web Server

4.2.1 ความต้องการของระบบ

Apache Web Server

OS: ต้องเป็น Unix และ **Unix-like operating system (Linux, BSD ฯลฯ)** เท่านั้น แต่สามารถใช้งานบน **Windows และ OS อื่นๆ** สามารถดูวิธีการได้ที่ Other platform หรือใช้งานผ่าน AppServNetwork บน Windows และ MAMP & MAMP PRO บน OSX

Disk Space: ใช้พื้นที่ประมาณ 10 MB และมีพื้นที่เหลือสำหรับ Apache อย่างน้อย 50 MB (ทั้งนี้ พื้นที่ใช้งานขึ้นอยู่กับหลายองค์ประกอบ เช่น Configuration, Module อื่นๆ และพื้นที่เว็บไซต์ของผู้ติดตั้ง)

NGINX Web Server

OS ที่ใช้งานร่วมกับ NGINX ได้ (อ้างอิงจาก http://nginx.org/en/)

- FreeBSD 3 -10 / i386; FreeBSD 5 -10 / amd64;
- Linux 2.2 - 3 / i386; Linux 2.6 -3 / amd64; Linux 3 / armv6l, armv7l, aarch64;
- Solaris 9 / i386, sun4u; Solaris 10 / i386, amd64, sun4v;
- AIX 7.1 / powerpc;
- HP-UX 11.31 / ia64;
- Mac OS X / ppc, i386;
- Windows XP, Windows Server 2003

IIS Web Server

OS : Windows Server โดยที่ IIS ต้องการ **Administrative Credentials** โดยคุณต้องมีสิทธิ์ของ administrator เสียก่อน ในการติดตั้งและ config IIS server (อ้างอิงจาก Install IIS 7.5 on windows server 2008)

4.3 Installation and Configuration สำหรับ IPv6 Web Server

4.3.1 Apache

Apache web server เป็น web server ที่ยอดนิยมที่สุดในตอนนี้ ใน Linux distribution ส่วนใหญ่ได้รวม apache เข้าไว้ใน repository ของตัวเอง โดยในคู่มือนี้ใช้ Linux Ubuntu 14.04 โดยเราสามารถใช้ “apt” ซึ่งเป็น Package management ของ Ubuntu ให้การติดตั้งจาก repository ของ Ubuntu ได้โดยใช้คำสั่ง

```
sudo apt-get update
sudo apt-get install apache2
```

apt-get จะทำการติดตั้ง apache web server ลงบนเครื่องและ start service ให้อัตโนมัติ และเมื่อ Ubuntu Linux ของเราไม่ได้ Disable IPv6 เอาไว้ ตัว apache จะเปิด service ให้สามารถใช้งานได้ทั้งบน IPv4 และ IPv6 สามารถตรวจสอบได้ด้วยคำสั่ง “netstat -tanp” ซึ่งจะเห็นได้ว่า apache ทำการ listen บน port 80 ที่ “any” (::) ip address บนเครื่องนี้เรียบร้อยแล้ว

```
tcp6       0      0 :::80                   :::*                    LISTEN      6754/apache2
```

รูปที่ 4.2 ผลลัพธ์หลังจากการ start service apache web server บน ubuntu

การทดสอบด้วย web browser

โดยปกติแล้ว ในการทดสอบว่า web server ทำงานได้นั้น เราจะทดสอบโดยเปิด web browser และใส่ URL ลักษณะนี้

```
http://your_server_IPv4_address
```

ในทำนองเดียวกันกับ IPv6 เราสามารถทดสอบ โดยใช้ IPv6 Address อยู่ภายใต้เครื่องหมาย **[ ]** เช่น

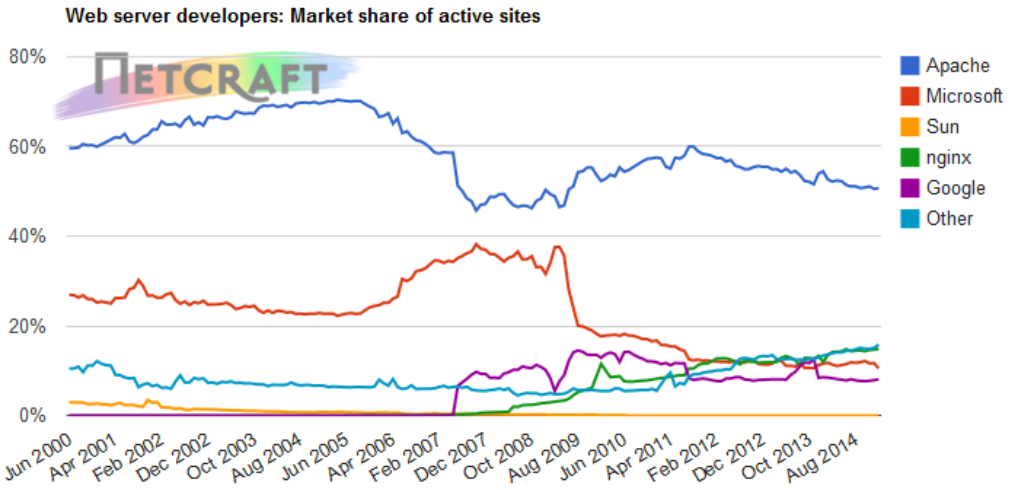
```
http://[your_server_IPv6_address]
```

ดังตัวอย่างเช่น Apache web server ที่ติดตั้งสำหรับ Testbed นี้ **http://[2001:db8:x::6]/**

รูปที่ 4.3 ผลการทดสอบการใช้งาน IPv6 Web Server ของ apache

4.3.2 Nginx

Nginx เป็น Web server อีกค่ายหนึ่งที่มีความสามารถไม่แพ้ Apache ด้วยความที่ตัวเล็ก ไม่กินทรัพยากรเครื่องมาก รองรับการให้บริการได้มาก ทำให้ Nginx เป็นที่นิยมมากขึ้นเรื่อยๆในระยะหลังมานี้



รูปที่ 4.4 สัดส่วนการใช้งาน Web Server

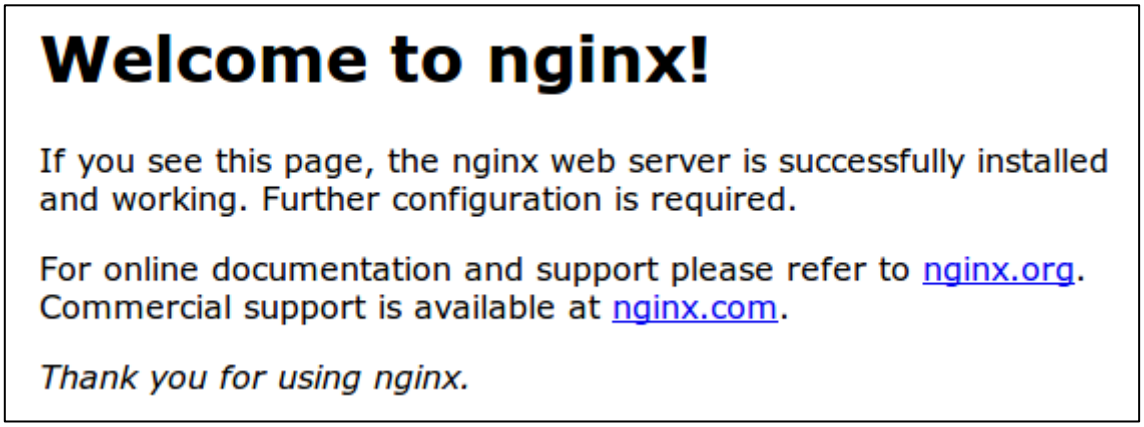
สามารถติดตั้ง Nginx ได้ด้วยคำสั่ง

```
sudo apt-get update
sudo apt-get install nginx
```

จากคำสั่งการติดตั้งด้วย apt-get นี้ เมื่อติดตั้งเรียบร้อยแล้ว ระบบจะทำการ Start service ของ Nginx ขึ้นมาอัตโนมัติ สามารถทดสอบด้วย Web browser ได้ตามปกติด้วย IP address หรือ domain ที่ตั้งไว้

```
http://your_server_IPv4_address
```

ก็จะพบกับหน้า Landing page ที่เป็น default ของ Nginx ลักษณะนี้



รูปที่ 4.5 หน้าเว็บ default ของ nginx

สำหรับ IPv6

โดยปกติแล้ว Nginx ที่ติดตั้งมาจะมี configuration สำหรับ binding ทั้ง IPv4 และ IPv6 เอาไว้ให้อยู่แล้วที่ไฟล์ /etc/nginx/sites-enabled/default ในลักษณะนี้

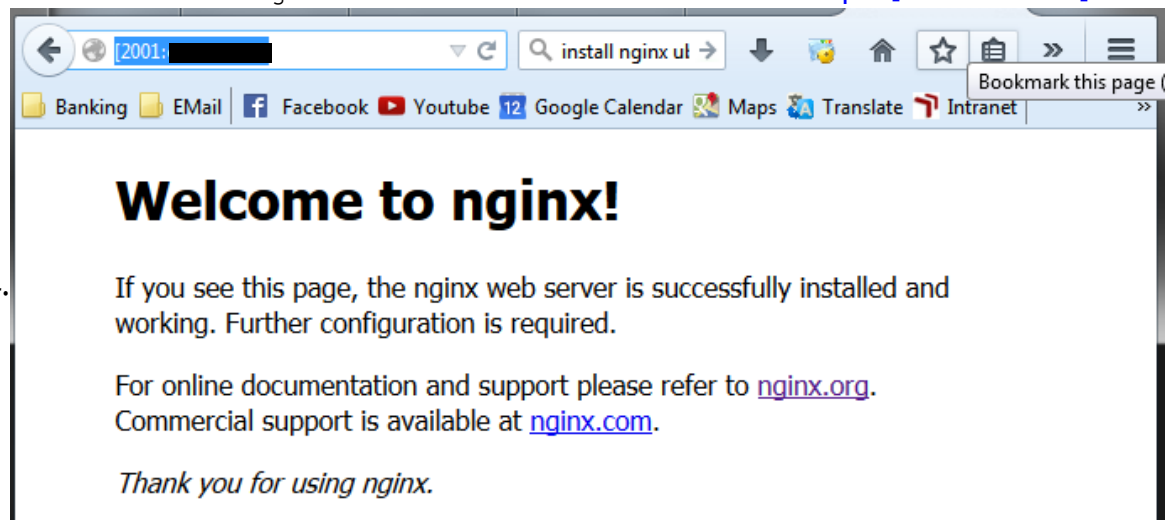
```
listen 80 default_server;
listen [::]:80 default_server ipv6only=on;
```

ในทำนองเดียวกันกับ IPv4 เราสามารถทดสอบ โดยใช้ IPv6 Address อยู่ภายใต้เครื่องหมาย **[ ]** เช่น

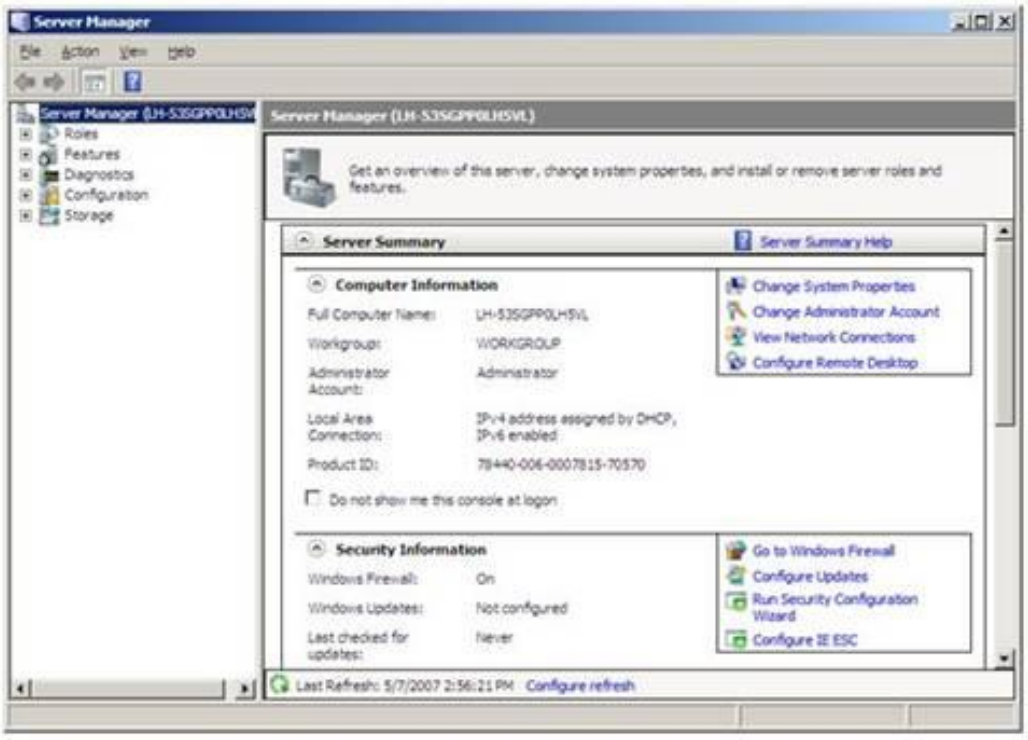
```
http://[your_server_IPv6_address]
```

ดังตัวอย่างเช่น Nginx web server ที่ติดตั้งสำหรับ Testbed นี้ http://[2001:db8:x::6]/

4.

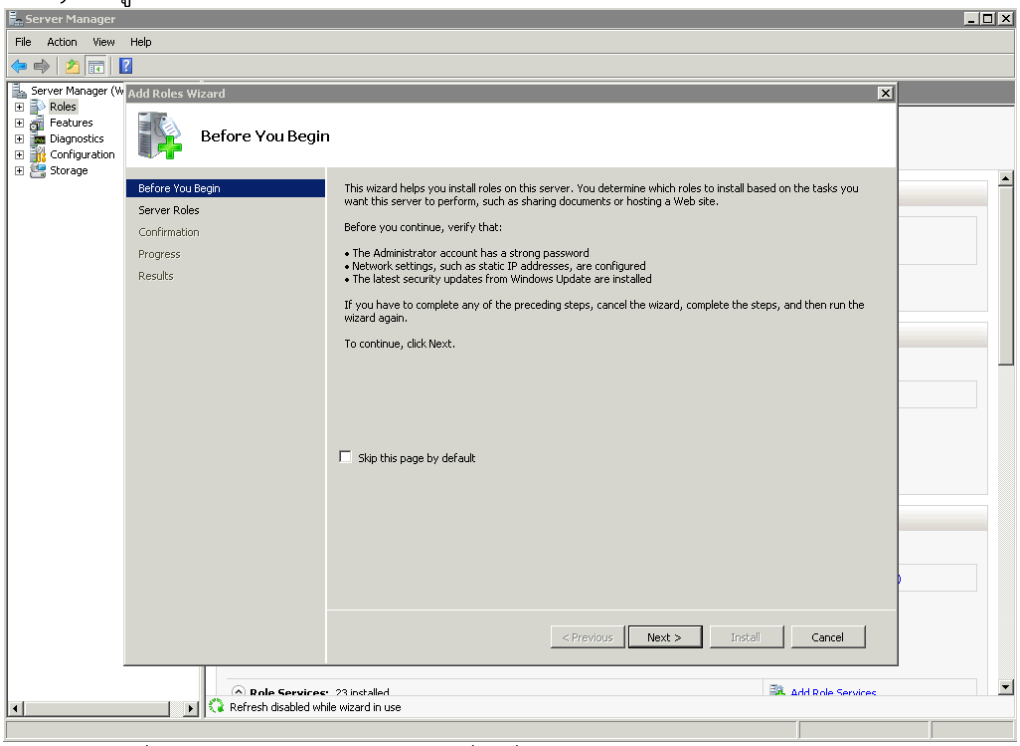


- Click Start –> All Programs –> Administrative Tools –> Server Manager.



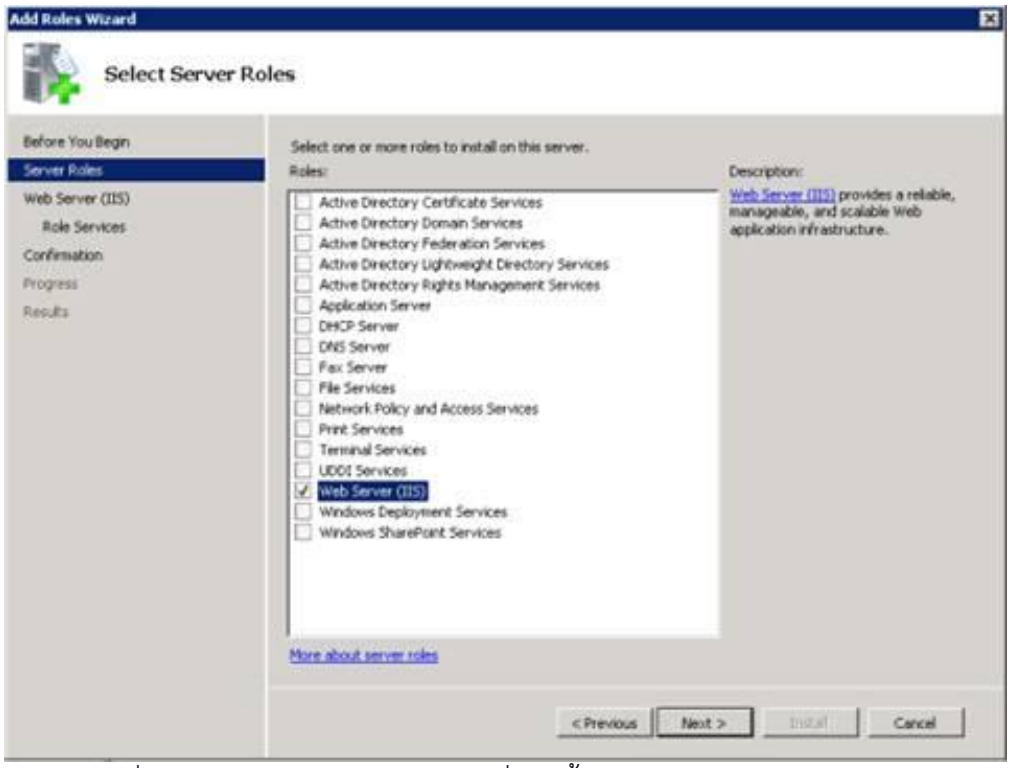
รูปที่ 4.7 แสดง Server Manager ของ Windows 2008

- ในหน้าต่าง Server Manager เลื่อนลงมาที่ Roles Summary คลิกคำว่า Add Roles จะเจอหน้าให้ Verify ข้อมูลให้คลิก



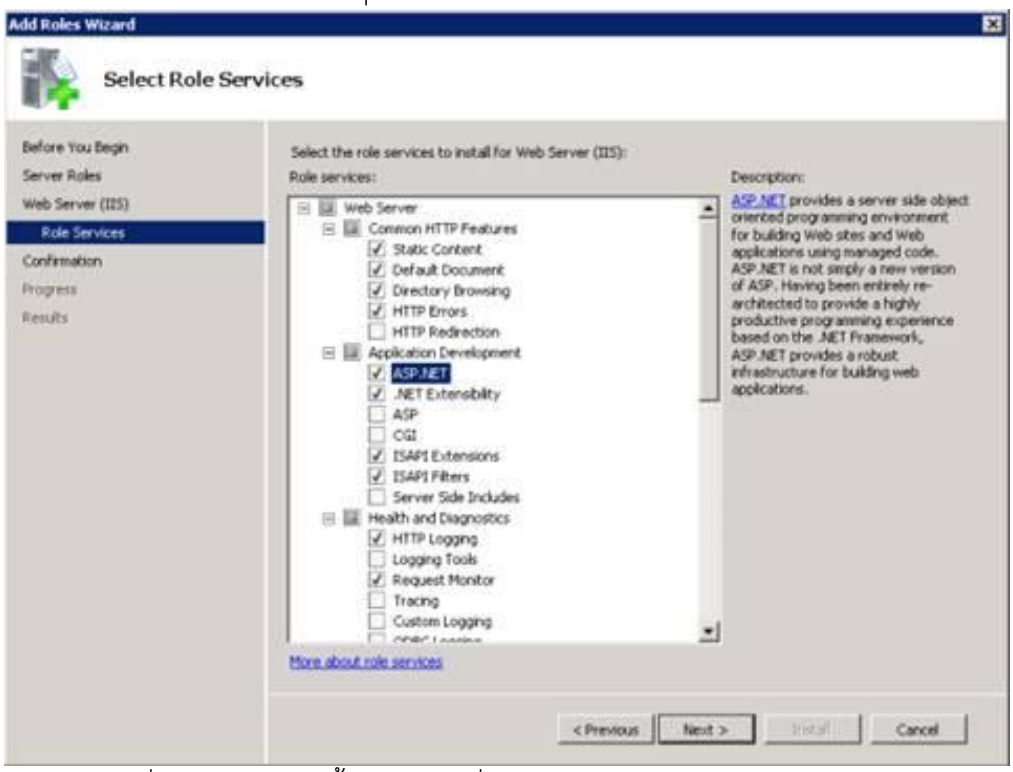
รูปที่ 4.8 แสดงการ add role เพื่อเพิ่มเติม service บน Windows 2008

- หลังจากนั้นให้เลือก Web Server (IIS) และคลิก Next เพื่อดำเนินขั้นตอนต่อไป



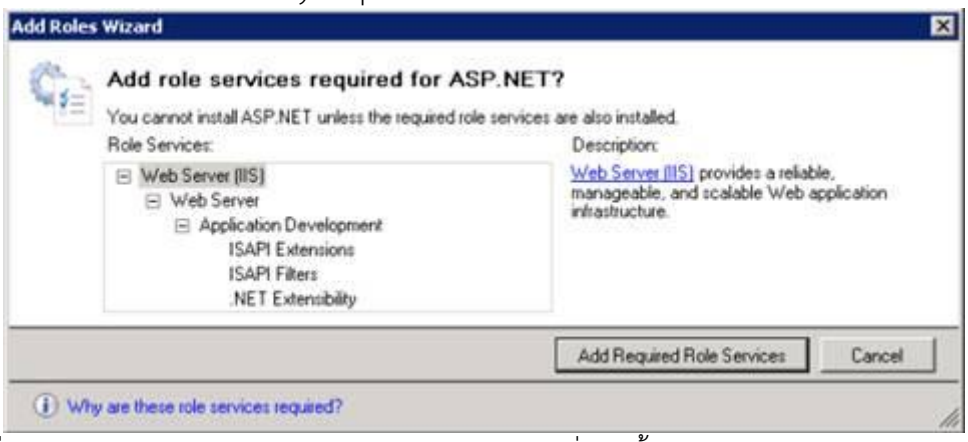
รูปที่ 4.9 เลือก Web Server (IIS) เพื่อติดตั้ง service บน Windows 2008

- เลือก Select Service ที่จำเป็นๆ เช่น ASP.NET



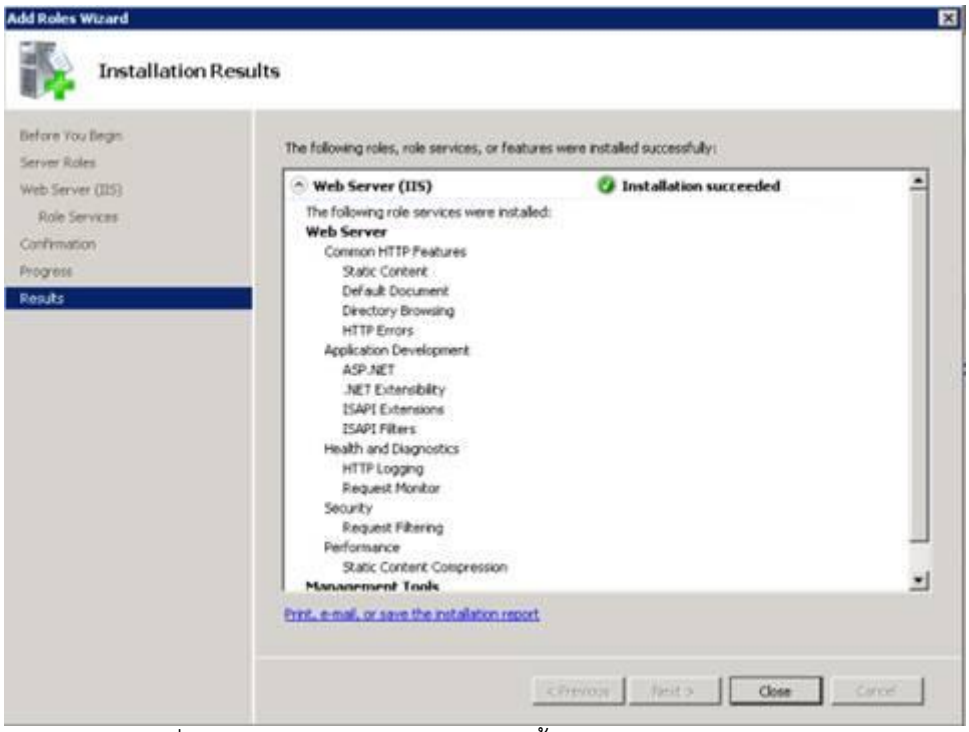
รูปที่ 4.10 เลือกติดตั้ง Service ที่จำเป็นสำหรับ IIS บน Windows 2008

- หลังจากนั้นกดเลือก Add any required role services



รูปที่ 4.11 เลือก Add any required role services เพื่อติดตั้ง ASP.NET บน Windows 2008

- ถึงขั้นตอนนี้เราได้ทำการติดตั้ง IIS เป็นที่เรียบร้อยแล้ว และมี Default คือ ASP.NET เราสามารถพัฒนาเว็บไซต์ด้วยภาษา ASP.NET เพื่อมาติดตั้งใน Server นี้ได้เลย



รูปที่ 4.12 แสดงผลลัพธ์จากการติดตั้ง IIS บน Windows 2008

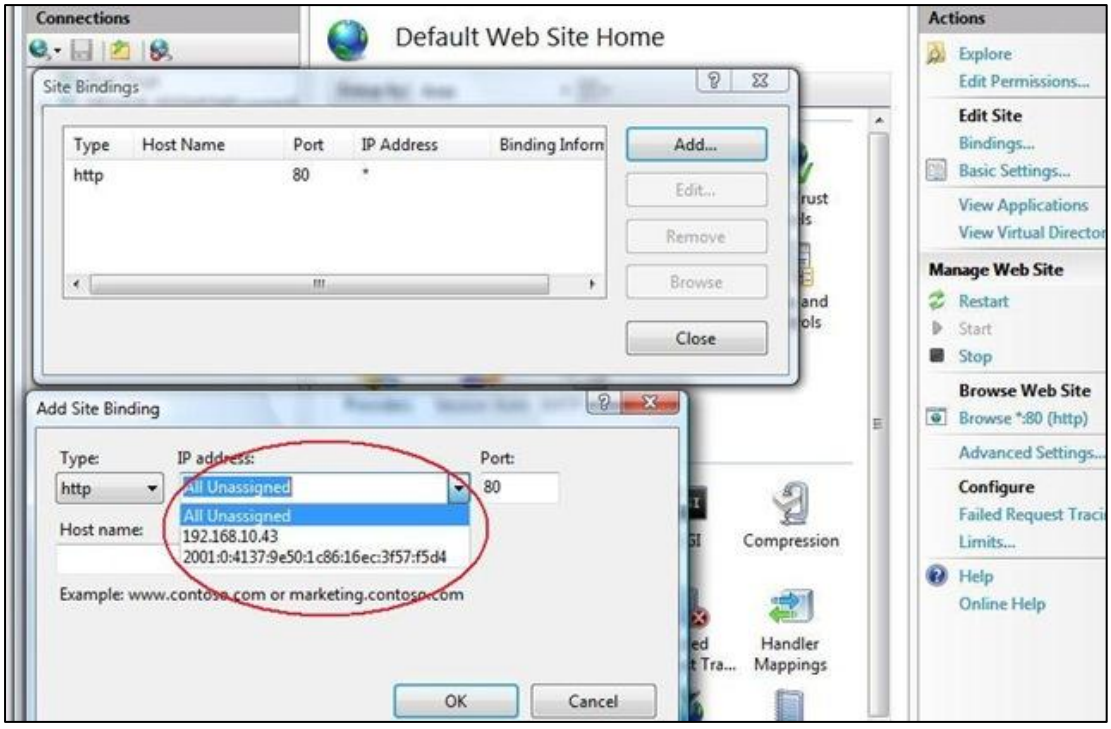
- ทดลอง test ระบบ โดยพิมพ์ที่ Address bar : http://localhost จะแสดงผลลัพธ์ดังรูป

รูปที่ 4.13 ผลการทดสอบการใช้งาน Web Server ของ IIS

การ Setup สำหรับรองรับ IPv6

โดยปกติแล้ว เมื่อ Windows Server 2008 R2 รองรับการใช้งาน IPv6 แล้ว IIS Web Server ก็จะไม่ต้องทำอะไร และสามารถใช้งาน IPv6 ได้เลย

แต่ในกรณีที่ IIS ไม่ได้ bind port กับ any (::) หรือ IPv6 Address ใดๆ เอาไว้ เราสามารถ Biding ได้เองผ่าน “inetmgr” (IIS7 configuration tool) ในส่วนของ IP Address ที่เป็น drop down list จะมี IP address ที่เครื่องเรามีอยู่ รวมทั้ง IPv6 ด้วย โดยเราสามารถเลือกได้จาก dropdown list นี้ได้เลย หรือสามารถพิมพ์ในตารางนี้ได้เลย



รูปที่ 4.14 การ Biding IPv6 address ด้วย “inetmgr” บน IIS7 configuration tool

อีกวิธีหนึ่งคือ

ใช้ command line “netsh” เพื่อกำหนดการ binding IPv6 address ให้กับ HTTP service ตามรูปแบบดังนี้

```
netsh http show iplisten
netsh http add iplisten ipaddress=ipv6address
```

เช่น

```
netsh http add iplisten ipaddress=fe80::1
หรือ
netsh http add iplisten ipaddress=::
```

ทดสอบด้วย Web Browser เช่นเดิม ในทำนองเดียวกันกับ IPv4 เราสามารถทดสอบ โดยใช้ IPv6 Address อยู่ภายใต้เครื่องหมาย **[ ]** เช่น

```
http://[your_server_IPv6_address]
```

หัวข้อที่ 5 DNS Server

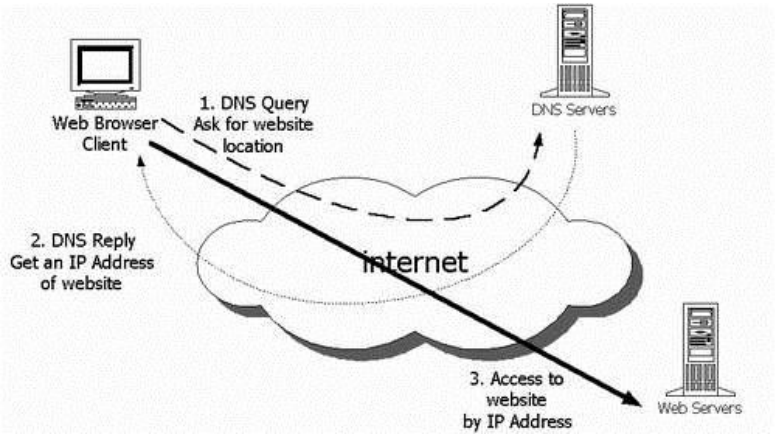
5.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

DNS Server (Domain Name System Server) คือ บริการสำหรับการตั้งชื่อให้กับ IP Address เพื่อสะดวกในการจดจำและใช้งาน เปรียบเสมือนการเปิดสมุดโทรศัพท์หรือสมุดหน้าเหลือง เพื่อใช้ในการค้นหาที่อยู่หรือเบอร์โทรที่ต้องการติดต่อในระบบการเรียกใช้งาน DNS Server ก็เป็นหลักการเดียวกัน เมื่อมีการค้นหาชื่อของ IP Address จากเครื่องคอมพิวเตอร์จะมีการส่งชื่อไปยัง DNS Server เพื่อถามถึง IP ของเครื่องที่ต้องการติดต่อด้วยใน File หรือ Database เมื่อค้นพบ DNS Server จะทำการตอบกลับ ซึ่ง DNS จะแบ่งออกส่วนต่างๆ คือ

- Name Resolvers คือเครื่อง client ที่ต้องการสอบถามหมายเลข IP จะเรียกว่า resolver ซึ่ง software ที่ทำหน้าที่เป็น resolver นั้นจะถูกสร้างมาโดย Application หรือ library ที่มีอยู่ใน client
- Domain Name Space คือฐานข้อมูลระบบ DNS ที่มีโครงสร้างเป็นต้นไม้ โดยแต่ละ Note สามารถมีโดเมนย่อย (Subdomain) ซึ่งจะใช้จุดทศนิยม (.) เป็นตัวแบ่งระหว่างโดเมนหลักและโดเมนย่อย
- Name Servers คือเครื่องคอมพิวเตอร์ที่โปรแกรมทำงานและมีฐานข้อมูลบางส่วนของระบบ DNS ซึ่ง Server จะทำการตอบกลับการร้องขอจากเครื่อง client ทันทีโดยจะค้นหาข้อมูลในฐานข้อมูลของตัวเองก่อน ถ้าไม่เจอจะส่งต่อการร้องขอไปยัง DNS Server อื่น ถ้า Name Server มีข้อมูลของโดเมนแสดงว่า Server นั้นเป็นเจ้าของโดเมนเรียกว่า Authoritative แต่ถ้าไม่มีเรียกว่า Non-Authoritative

หลักการทำงาน

การทำงานของระบบ DNS Server นั้น เริ่มจากเครื่องคอมพิวเตอร์ Client ต้องการทราบหมายเลข IP Address ของเครื่องปลายทางที่ต้องการติดต่อด้วยจึงส่งคำขอไปยังเครื่อง DNS Server เมื่อ DNS Server ได้รับคำขอแล้วก็จะไปค้นหาข้อมูลในฐานข้อมูลแล้วส่งคำตอบกลับไปยังเครื่อง Client เมื่อเครื่อง Client รู้ IP Address แล้วจึงสามารถติดต่อกับเครื่องปลายทางได้ ดังรูป



รูปที่ 5.1 หลักการทำงานของ DNS

ข้อจำกัดในการตั้งชื่อของระบบ DNS

DNS จะรับรู้เฉพาะตัวอักษรละติน (ASCII character set) ใน RFC 1035 ระบุว่าสัญลักษณ์ที่ใช้ได้ในโดเมนเนม คือ

- ตัวอักษร a ถึง z (case insensitive)
- เลข 0 ถึง 9
- เครื่องหมายยัติภังค์ (-)

5.2 การติดตั้ง ปรับแต่ง และการทดสอบ DNS Server

- การติดตั้งและ config DNS Server บน Ubuntu 14.04

5.2.1 ติดตั้ง DNS Server โดยใช้คำสั่ง

```
# apt-get –y install bind9
```

เมื่อติดตั้ง DNS Server เสร็จ file config ต่างๆ จะถูกเก็บไว้ใน Directory /etc/bind/ โดยจะมี file ที่สำคัญดังนี้

```
named.conf
named.conf.options
```

5.2.2 จัดระเบียบ file config และแก้ไข file named.conf

เพื่อความสะดวกและเป็นระเบียบในการ config DNS Server ให้ดำเนินการดังนี้

```
# mkdir /etc/bind/conf
```

ย้าย file named.conf ต่าง ๆ ไปไว้ใน Directory /etc/bind/conf

```
# mv /etc/bind/named.conf.* /etc/bind/conf
```

แก้ไข file named.conf

```
# vi /etc/bind/named.conf
แก้ไขในส่วนของ include จาก
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

```
เป็น
include "/etc/bind/conf/named.conf.options";
include "/etc/bind/conf/named.conf.local";
include "/etc/bind/conf/named.conf.default-zones";
```

5.2.3 เปิด function ต่าง ๆ โดยแก้ไข file named.conf.options

```
# vi /etc/bind/conf/named.conf.options
```

แก้ไข path ที่ใช้เก็บ file config zone ให้เป็น path ที่เราต้องการ

```
directory “/var/cache/bind”;
```

เอาเครื่องหมาย // ในส่วนของ forwarders ออกและเพิ่ม ipv6 dns ของ google เพื่อให้ dns server ไปถามข้อมูล dns จาก dns server ของ google

```
forwarders {
        2001:4860:4860::8888;
        2001:4860:4860::8844;
};
```

เพิ่มในส่วนของการอนุญาตให้เครื่องอื่นๆ สามารถที่จะติดต่อ dns server ของเครื่องได้

```
# query range you allow
          allow-query { any; };
          allow-query-cache { any;  };
# the range to transfer zone files
          allow-transfer { any; };
# recursion range you allow
        recursion yes;
        allow-recursion { any; };
```

เพิ่มในส่วนที่ให้เครื่องสามารถรับข้อมูล dns ที่เป็น ipv6

```
listen-on-v6 { any; };
```

สามารถเช็คความถูกต้องของการ config dns server ได้ด้วยคำสั่ง (ถ้าไม่มี error อะไรแสดงว่า config ได้ถูกต้องแล้ว)

```
named-checkconf /etc/bind/named.conf
```

สามารถ Restart service ได้ด้วยคำสั่งต่อไปนี้

```
# service bind9 restart
หรือ
# /etc/init.d/bind9 restart
```

5.3 การทดสอบ DNS Server

คำสั่งที่ใช้ในการทดสอบการทำงานของ DNS Server

- host
- nslookup
- dig

การทดสอบด้วยคำสั่ง host

```
root@ubun-dns:~# host -t aaaa www.ipv6.testbed.local
www.ipv6.testbed.local has IPv6 address 2001:db8:x::6

root@ubun-dns:~# host -t mx ipv6.testbed.local
ipv6.testbed.local mail is handled by 10 mail.ipv6.testbed.local.
```

การทดสอบด้วยคำสั่ง nslookup

```
root@ubun-dns:~# nslookup
> server 2001:db8:x::3
Default server: 2001:db8:x::3
Address: 2001:db8:x::3#53
> set type=aaaa
> www.ipv6.testbed.local
www.ipv6.testbed.local    has AAAA address 2001:db8:x::6
> set type=mx
> ipv6.testbed.local
ipv6.testbed.local          mail exchanger = 10 mail.ipv6.testbed.local.
> exit
```

การทดสอบด้วยคำสั่ง dig

```
dig -6 @2001:4860:4860::8888 www.google.co.th
อธิบายความหมายของคำสั่งดังนี้
(dig [ใช้ ipv6 ในการถาม] @[ipv6 ของเครื่องที่ต้องการถาม] [web ที่ต้องการรู้ ip])
```

จะได้ข้อมูลที่เป็นส่วนของคำตอบที่ server dns ของตัวเองตอบมาตามนี้

```
;; ANSWER SECTION:
www.google.co.th.    299    IN    A    61.19.2.50
www.google.co.th.    299    IN    A    61.19.2.25
www.google.co.th.    299    IN    A    61.19.2.30
www.google.co.th.    299    IN    A    61.19.2.49
www.google.co.th.    299    IN    A    61.19.2.40
www.google.co.th.    299    IN    A    61.19.2.54
www.google.co.th.    299    IN    A    61.19.2.39
www.google.co.th.    299    IN    A    61.19.2.35
www.google.co.th.    299    IN    A    61.19.2.45
www.google.co.th.    299    IN    A    61.19.2.59
www.google.co.th.    299    IN    A    61.19.2.34
www.google.co.th.    299    IN    A    61.19.2.55
www.google.co.th.    299    IN    A    61.19.2.44
www.google.co.th.    299    IN    A    61.19.2.29
www.google.co.th.    299    IN    A    61.19.2.20
www.google.co.th.    299    IN    A    61.19.2.24
```

5.4 ความสัมพันธ์ของ DNS กับ Service ต่างๆ และการนำไปใช้งานจริง

Web Server: Web Server สามารถใช้งานด้วยชื่อ domain name ผ่าน web browser ได้ ดังตัวอย่าง ได้ทำการ map DNS record เอาไว้แล้วด้วยชื่อโดเมน www.ipv6.testbed.local เป็น IPv6 address (AAAA) “2001:db8:x::6” ทำให้เราสามารถเข้าเว็บด้วย URL ที่เป็นชื่อที่มีความหมาย ง่ายในการจำ http://www.ipv6.testbed.local แทนที่จะเป็นหมายเลข IPv6 http://[2001:db8:x::6]

รูปที่ 5.2 ผลลัพธ์จากการสร้าง DNS record สำหรับ Web Server

Mail Server: DNS Server มีบทบาทสำคัญกับการทำงานของ Mail Server ตลอดเวลา เราใช้ DNS server เพื่อกำหนด **MX** (Mail Exchange) ให้กับ “โดเมน” ของเรา ดังตัวอย่างการทดสอบ

```
root@ubun-dns:~# host -t mx ipv6.testbed.local
ipv6.testbed.local mail is handled by 10 mail.ipv6.testbed.local.
```

จะเห็นว่า โดเมน “ipv6.testbed.local” มี email server ชื่อ “mail.ipv6.testbed.local” ดูแลโดเมนของเราอยู่ เป็นการประกาศบอกโลกภายนอกหรือ Internet ว่า mail server ของเราอยู่ที่ไหนซึ่งจะสัมพันธ์กับ AAAA record ซึ่งจะบอกอีกทีว่า mail server ที่ดูแลโดเมนเรามี IP address อะไร (ในที่นี้ mail server มีแต่ IPv6 อย่างเดียว)

```
root@ubun-dns:~# host  mail.ipv6.testbed.local
mail.ipv6.testbed.local has IPv6 address 2001:db8:x::9
```

ทำให้สามารถรับ-ส่ง Email จากภายนอก Internet มายัง domain ของเราได้

หัวข้อที่ 6 Centralized Log Server

6.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

การใช้งานและเข้าถึงอินเทอร์เน็ตในยุคนี้สามารถใช้งานได้จากทั้ง IPv4 และ IPv6 อาจเกิดการกระทำผิดทางอินเทอร์เน็ตได้ทุกเมื่อไม่ว่าจะด้วยความตั้งใจหรือไม่ก็ตาม จากการออกกฎหมาย พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีข้อความในมาตราที่ 26 กำหนดไว้ว่า

"ผู้ให้บริการ ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ไว้ไม่น้อยกว่า 90 วัน นับแต่ วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่ จะสั่งให้ผู้ให้บริการผู้ใด เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ไว้เกิน 90 วันแต่ไม่เกิน 1 ปีเป็นกรณีพิเศษ เฉพาะราย และเฉพาะคราวก็ได้ ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็น เพื่อให้สามารถ ระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง"

Syslogd

Syslogd เป็นกลไกที่ใช้ในการเก็บข้อมูล log ของ kernel และ application บนระบบ Unix และ Linux โดยเป็น daemon ที่ถูกติดตั้งมาให้พร้อมกับระบบปฏิบัติการในเกือบทุกระบบ โดยผู้ดูแลระบบสามารถปรับแต่งไฟล์ configuration เพื่อควบคุมการทำงานของ syslogd ได้ เช่น ให้ syslogd [1-3] เก็บข้อมูลไปไว้ที่ไฟล์ใด หรือให้ส่งข้อมูล log นี้ไปเก็บไว้ยังเครื่องอื่นในเครือข่าย

syslogd มีสิ่งสำคัญสำหรับแบ่งประเภทและควบคุมข้อมูล log คือ Facility และ Priority โดยที่ Facility เป็นข้อมูลที่อธิบายถึงแหล่งกำเนิดของข้อมูล log นั้นๆ ส่วน Priority จะแสดงถึงระดับความสำคัญของเหตุการณ์ที่ทำให้เกิดข้อมูล log ขึ้น ดังนั้นข้อมูล log ทุกอันจำเป็นต้องมี facility และ priority เสมอ

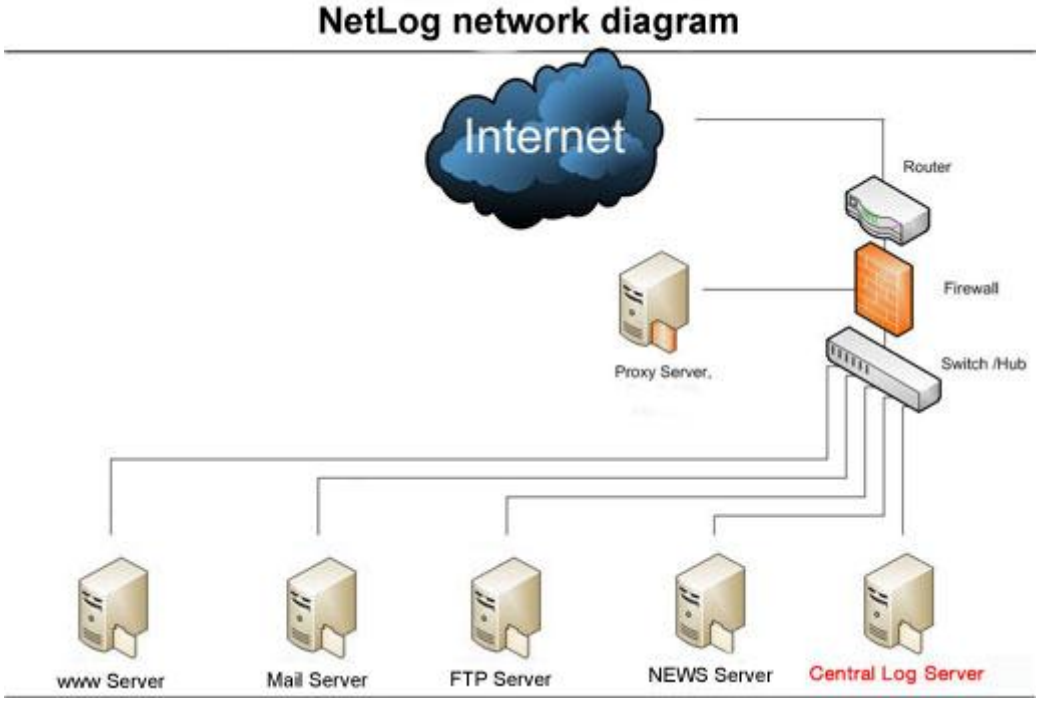
Syslog-ng (Syslog new generation)

syslog-ng สามารถแก้ไขข้อบกพร่องส่วนใหญ่ของ syslog

- syslog-ng สามารถทำงานได้ทั้งบน TCP และ UDP
- syslog-ng สามารถทำการกรอง (filter) ข้อมูลได้ด้วย regular expression
- syslog-ng สามารถทำงานในรูปแบบที่อ้างอิง priority/facility ได้ ดังนั้น มันจึงสามารถทำงานแทนที่ syslog ได้
- syslog-ng สนับสนุน log forwarding ซึ่งทำให้สามารถทราบได้ว่า ต้นทางของ log ถูกส่งมาจากเครื่องใด และผ่านเครื่องใดมาบ้าง
- ที่สำคัญ syslog-ng ยังมีรูปแบบของไฟล์ configuration ที่ง่าย แต่มีความยืดหยุ่นสูง สามารถนำไปประยุกต์ใช้ให้ตรงความต้องการได้โดยง่าย

6.2 รูปแบบการใช้งาน

Centralized Log Server โดยปกติแล้วจะนำไปวางไว้ในเครือข่ายเดียวกันกับ เครื่องที่ให้บริการอื่นๆ ที่ต้องการส่ง Log มาเก็บยัง Centralized Log Server นี้ เพื่อไม่เป็นการส่งข้อมูลที่เป็นความลับออกนอกเครือข่าย และไม่เพิ่มภาระให้กับ Gateway ของเครือข่าย



รูปที่ 6.1 การนำ Centralized Log Server ไปใช้งาน

ประเภทของข้อมูล Log ที่ Centralized Log Server จัดเก็บได้

- System Log หรือจาก Syslog Protocol ต่างๆ
  เช่น Authentication, Mail, Kernel, Daemon, Cron, News และอื่นๆ
- จาก Server Software ต่างๆ ที่รองรับ Syslog Protocol
  เช่น Apache, Asterisk, VsFTPd เป็นต้น
- Log จากอุปกรณ์เครือข่าย ที่รองรับการส่ง Log ผ่าน Syslog Protocol
  เช่น Router

6.3 การติดตั้ง

6.3.1 ความต้องการของระบบ

CPU: 1 GHz ขึ้นไป

RAM: 2GB ขึ้นไป

HDD: 40 GB ขึ้นไป

Required Softwares: web server, mysql, php, syslog-ng

หมายเหตุ: ทั้งนี้ขนาดของ HDD ขึ้นอยู่กับปริมาณของข้อมูล log ที่เก็บด้วย โดย 40 GB สามารถเก็บข้อมูล log ทั้งที่เป็น file รวมทั้ง database ได้ไม่เกิน 1 ล้าน Records ต่อวัน เป็นเวลา 90 วัน

6.3.2 ขั้นตอนการติดตั้ง Syslog-ng

ใน Operating system version ใหม่ๆ จะติดตั้ง rsyslog แทน syslog daemon เดิม ที่ทำหน้าที่เก็บ event log อยู่แล้ว แต่เราสามารถเลือกติดตั้ง syslog-ng แทน rsyslog ได้

การติดตั้งบน Redhat, Fedora, CentOS (yum)

คำสั่งที่ใช้ในการติดตั้งผ่าน yum

```
# yum install syslog-ng
```

การติดตั้งบน Debian, Ubuntu (apt-get)

คำสั่งที่ใช้ในการติดตั้งผ่าน apt-get

```
# apt-get install syslog-ng-core
```

Operating system ที่ใช้ SELinux (SE = Security Enhanced) เช่นใน Redhat, Fedora, CentOS เราต้อง config SELinux เพื่ออนุญาตให้รับ log ที่ port 514 ได้

```
# semanage -a -t syslogd_port_t -p udp 514
```

ถ้าเราใช้ iptables ในการจัดการ firewall ของ OS เราต้องเพิ่ม iptables rule เพื่อให้ firewall อนุญาต traffic ของ log ที่จะส่งเข้ามายัง port 514

```
# iptables -A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT
# iptables -A INPUT -m state --state NEW -m tcp -p tcp --dport 514 -j ACCEPT
```

Start Service

เมื่อติดตั้งเรียบร้อยแล้ว ระบบจะ Start service ให้อัตโนมัติ แต่ถ้าไม่ เราสามารถสั่งได้โดย

```
# /etc/init.d/syslog-ng start
หรือ
# service syslog-ng start
```

6.4 การ Config syslog-ng และการรองรับ IPv6

การแก้ไขไฟล์ **syslog-ng.conf**

การปรับแต่ง Option ใน Syslog-ng

```
options {
        chain_hostnames(off);
        use_dns(no);
        use_fqdn(no);
        owner("root");
        group("adm");
        perm(0640);
        chain_hostnames (off);
        create_dirs (yes);
        keep_hostname (no);
        log_fifo_size (536870912);
        stats_freq(60);
        flush_lines(100);
        flush_timeout(1000);
};
```

ส่วนที่กำหนดให้รอรับ Log บน IPv6 คือ

```
source log_network {
        tcp6(port(514));
};
```

การกำหนดให้ Log Server จัดการ log ที่ส่งเข้ามาและแยกจัดเก็บลงไฟล์ด้วย Macro

```
destination log_file {
        file("/data/log/$HOST/$YEAR/$MONTH/$DAY/$HOST-$FACILITY-$YEAR-$MONTH-$DAY.log" );
};
```

Log ที่ถูกส่งมาจะถูกแยกด้วย Macro ตามชื่อ host -> ปี -> เดือน -> วัน และแยกไฟล์ตาม Facility หรือ ประเภทของ Log ตัวอย่างเช่น

```
/data/log/2001:db8:x::2/2015/05/01/2001:db8:x::2-auth-2015-05-01.log
```

จากตัวอย่าง ไฟล์ดังกล่าวถูกสร้างด้วย log ที่ส่งมาจากเครื่องหมายเลข IP “**2001:db8:x::2**” ของวันที่ 1 พฤษภาคม 2015 โดยเป็น log ประเภท **Authentication Log** เป็นต้น

6.5 การกำหนดให้ Server ต่างๆ ส่ง Log มายัง Centralized Log Server

การส่ง Authentication Log และข้อมูลทั่วไปของระบบ

ณ เครื่องแม่ข่ายที่ต้องการส่ง Log มา ให้เพิ่มบรรทัดดังต่อไปนี้ในไฟล์ /etc/rsyslog.conf

```
auth,authpriv,daemon,cron.info                    @@[2001:db8:x::5]:514
```

จะเป็นการส่ง log เป็น auth,authpriv (เกี่ยวกับ authentication เช่น SSH) daemon (software ที่รันเป็น daemon บางตัว) , cron (การทำงานตาม schedule ที่ตั้งไว้) ไปยัง Log Server ผ่าน TCP

6.5.1 Apache Web Server

สำหรับ apache web server แล้ว โดยทั่วไปจะเป็นการจัดเก็บ log ลงไฟล์ แต่เราสามารถกำหนดให้เรียกใช้โปรแกรม logger เพื่อจัดส่ง log ลง syslog ภายในเครื่องตัวเองก่อน โดยเพิ่มในส่วน Configuration file เพื่อให้ Apache ส่ง log (ชนิด combined) สู่ syslog ด้วย facility local2 เช่น แก้ไขไฟล์ /etc/apache/apache.conf

```
CustomLog "|/usr/bin/logger -p local2.info" combined
```

เมื่อเราส่ง log ของ Apache ลง syslog ภายในเครื่องตัวเอง แล้ว ในส่วนของ /etc/rsyslog.conf เพิ่มในส่วนของ local2 เพื่อส่ง log ไปยัง syslog server ด้วย

```
auth,authpriv,daemon,cron,local2.info                    @@[2001:db8:x::5]:514
```

6.5.2 Vsftpd (FTP Server)

สำหรับ vsftpd ต้องทำสองส่วนเช่นกัน ดังนี้

1. ใน Configuration file ของ vsftpd (/etc/vsftpd/vsftpd.conf) ให้เพิ่มบรรทัดนี้

```
syslog_enable=YES
```

Vsftpd จะทำการเก็บ log ลง syslog เพิ่ม และ log นี้จะไปอยู่ใน /var/log/messages ด้วย facility “ftp” ส่วน log เดิมที่เป็น xferlog ก็จะยังเก็บอยู่เหมือนเดิม ตาม Config ที่เรากำหนดไว้ เพียงแต่เพิ่มส่วนของ syslog เข้ามา

2. ใน /etc/syslog.conf ต้องกรองส่วนของ facility ftp ส่งไปยัง log server

```
auth,authpriv,daemon,cron,ftp.info                    @@[2001:db8:x::5]:514
```

แต่ถ้าไม่ต้องการให้เก็บ log นี้ลงไปรวมกันในไฟล์ /var/log/messages ซ้ำซ้อนกัน ให้แก้ไขดังนี้

```
*.info;mail.none;authpriv.none;cron.none;ftp.none          /var/log/messages
```

6.5.3 Software Daemon อื่นๆ

Software Daemon อื่นๆ ส่วนใหญ่สามารถส่ง log ลง syslog อยู่แล้ว เพียงแต่ Config เพิ่มเติมให้ syslogd โยน log ไปยัง log server ดังนี้

Named (Bind) - ใช้ facility daemon ของ syslog ส่งไปยัง syslog server

```
auth,authpriv,daemon,cron.info                    @@[2001:db8:x::5]:514
```

Sendmail,postfix – ใช้ facility mail ของ syslog ส่งไปยัง syslog server

```
auth,authpriv,daemon,mail,cron.info               @@[2001:db8:x::5]:514
```

ntpd (Network Time daemon) ใช้ facility ของ daemon ส่งไปยัง syslog server

```
auth,authpriv,daemon,cron.info                    @@[2001:db8:x::5]:514
```

6.6 การทดสอบ

การทดสอบเบื้องต้นด้วยคำสั่ง loggen ที่มากับ software syslog-ng อยู่แล้ว

รูปแบบคำสั่ง

```
loggen -6 -S -i -s [size(byte)] -r [rate] -I [interval] ::1 514
```

ตัวอย่างเช่น

```
loggen -6 -S -i -s 200 -r 10 -I 10 ::1 514
```

ความหมาย คือ เป็นการส่ง Log ด้วย IPv6 protocol แบบ Streaming, Inet family ด้วยขนาด 200 Byte ความเร็ว 10 logs ต่อวินาที ด้วยระยะเวลา 10 วินาที ไปยัง IPv6 เครื่องตัวเอง ที่ port 514

ผลการรันที่แสดงหน้าจอ

```
root@ubuntu-log:~# loggen -6 -S -i -s 200 -r 10 -I 10 ::1 514
average rate = 10.78 msg/sec, count=108, time=10.019, (average) msg size=200,
bandwidth=2.10 kB/sec
```

ผลการจัดเก็บ Log จะต้องเข้าไปดูที่ File ใน Directory ตามที่เราตั้ง Macro ที่ Config file ของเรา จะทำให้เกิดไฟล์นี้ขึ้นมา

```
/data/log/::1/2015/05/01/::1-auth-2015-05-01.log
```

ซึ่งมีเนื้อหาในไฟล์ดังนี้

```
May 01 23:57:41 ::1 prg00000[1234]: seq: 0000000075, thread: 0000, runid: 143231
3855, stamp: 2015-05-22T23:57:41
PADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPAD
DPADDPADDPADDPADDPADDPADD
May 01 23:57:42 ::1 prg00000[1234]: seq: 0000000076, thread: 0000, runid: 143231
3855, stamp: 2015-05-22T23:57:42
PADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPADDPAD
DPADDPADDPADDPADDPADDPADD
```

6.6.1 ตัวอย่างการทดสอบรับ Authentication Log เช่น SSH Service

ที่เครื่อง ต้นทางที่เป็นผู้ส่ง Log กำหนดการส่งดังนี้

```
auth,authpriv.*          @@[2001:db8:x::5]:514
```

เมื่อมีเหตุการณ์ การ Login เข้ามายัง Server เครื่องนี้ จะมีการส่ง log ไปยัง Log server IP 2001:db8:x::5 ทำให้มีไฟล์เกิดขึ้นใน Directory นี้ “/data/log/**2001:db8:x::3**/2015/05/01” คือ

- 2001:db8:x::3-**auth**-2015-05-01.log
- 2001:db8:x::3-**authpriv**-2015-05-01.log

โดยมีเนื้อหาเกี่ยวกับ Service ที่ใช้ในการ Authentication ในตัวอย่างนี้มาจากโปรแกรม SSH

```
May 01 03:21:10 2001:db8:x::3 sshd[8305]: Accepted password for mon from 2001
:db8:x::2 port 59744 ssh2
```

6.6.2 ตัวอย่างการทดสอบรับ Daemon Log เช่น DNS Server

ที่เครื่อง ต้นทางที่เป็นผู้ส่ง Log กำหนดการส่งดังนี้

```
daemon.*        @@[2001:db8:x::5]:514
```

เนื้อหาที่ไฟล์บน Log Server จะมี message ที่ถูกส่งมาเช่นในไฟล์นี้ ดังตัวอย่าง

File: /data/log/**2001:db8:x::3**/2015/05/01/2001:db8:x::3-**daemon**-2015-05-01.log

```
May 01 03:21:23 2001:db8:x::3 named[8462]: BIND 9 is maintained by Internet S
ystems Consortium,
May 01 03:21:23 2001:db8:x::3 named[8462]: Inc. (ISC), a non-profit 501(c)(3)
 public-benefit
May 01 03:21:23 2001:db8:x::3 named[8462]: corporation.  Support and training
 for BIND 9 are
May 01 03:21:23 2001:db8:x::3 named[8462]: available at https://www.isc.org/s
upport
```

หัวข้อที่ 7 Mail Server

7.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

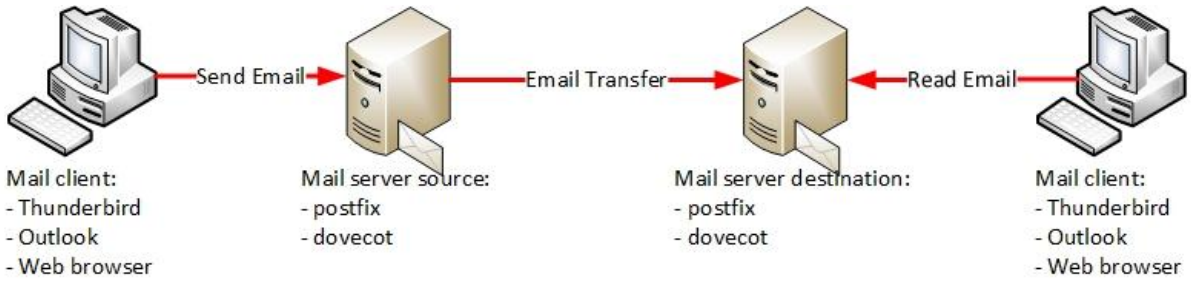
Mail Server คือเครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการรับ ส่ง และ จัดเก็บ email ของบุคคลหรือองค์กร โดย mail server สามารถตั้งไว้ที่ผู้ให้บริการ ISP (เช่น hotmail.com, gmail.com ฯลฯ) หรือในองค์กรของตัวเอง

การรับส่ง e-mail จะประกอบด้วย 2 ส่วนด้วยกันคือ

1) Mail Server
2) Mail Client

- **ลักษณะการทำงาน**

ผู้ใช้งานเมื่อต้องการจะส่ง email จะใช้เครื่องมือต่างๆ ไม่ว่าจะเป็น application (ได้แก่ outlook, thunderbird ฯลฯ) หรือ web browser ซึ่งเรียกว่า mail client ในการส่งข้อมูล email และคำสั่งไปยัง mail server เพื่อให้ mail server ทำการส่ง mail ต่อไปยัง mail server ปลายทาง เช่น mail server hotmail ส่ง email ไปยัง mail server gmail เป็นต้น และสำหรับการอ่าน email ก็เช่นกัน mail client จะเป็นเครื่องมือที่ช่วยให้ผู้ใช่อ่าน email ใน mail server ได้ ซึ่งกระบวนการทั้งหมดนี้จะมี DNS Server เป็นตัวดูแลเพื่อให้ email ไปยัง mail server ที่ถูกต้อง

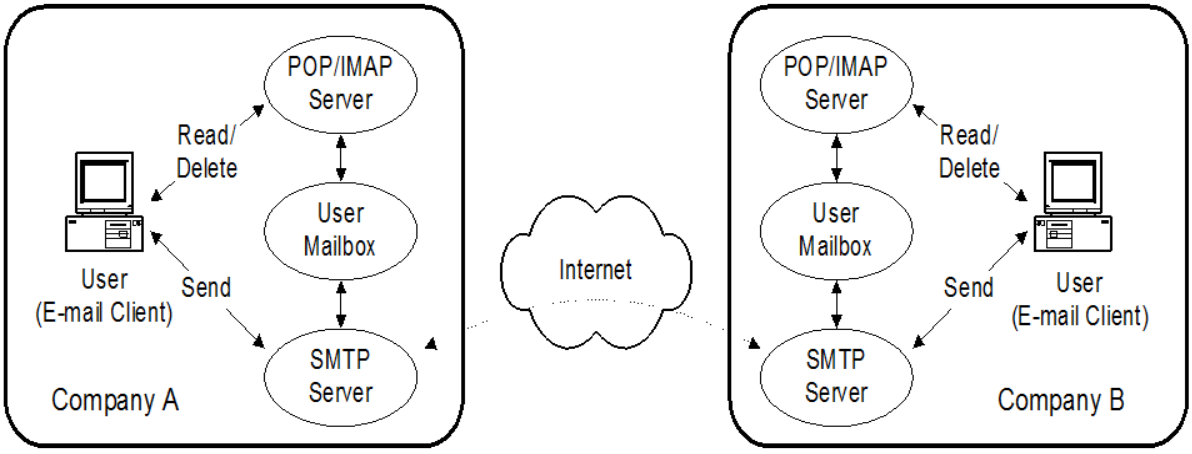


รูปที่ 7.1 หลักการทำงานของ Mail Server

Protocol คือข้อกำหนด ที่ใช้เพื่อเป็นมาตรฐาน สำหรับการสื่อสารระหว่าง เครือข่ายคอมพิวเตอร์ สำหรับ mail server ก็มี protocol ที่ใช้กำกับและดูแลเช่นกัน ได้แก่ SMTP, pop3, imap

- **SMTP** (Simple Mail Transfer Protocol) คือ protocol ที่เป็นมาตรฐานหลักในการรับ / ส่ง email ในระบบเครือข่าย
- **pop3** (Post Office Protocol) คือ protocol ที่ใช้ในการดึง email จาก mail server เมื่อ mail client เข้ามาอ่าน email protocol pop3 จะทำการส่ง email ไปยัง mail client และลบ email ที่อยู่ใน mail server ออก
- **imap** (Internet Message Access Protocol) คือ protocol ที่ให้ mail client เข้าไปอ่าน email ใน mailbox ใน mail server โดยไม่ได้ดึง email ออกมายังเครื่องผู้ใช้งาน

การส่ง / การรับ / การอ่าน Email



รูปที่ 7.2 การส่ง / การรับ / การอ่าน Email

Mail Exchange (MX)

Mail Exchange คือ กระบวนการของ DNS Server ในส่วนของ MX Record จะเป็นตัวบอกว่า email จะถูกส่งไปยัง mail server ปลายทางตัวไหน โดย SMTP ของ mail server ต้นทางจะตรวจสอบ MX ของโดเมนที่ต้องการจะส่งไปจาก DNS เพื่อส่ง email ไปยัง mail server ตามที่ MX Record ระบุไว้

ตัวอย่างเช่น ต้องการส่ง email ไปยังผู้รับปลายทางชื่อ thong@ipv6.testbed.local จะมีขั้นตอนการทำงานดังนี้

- จาก user ส่ง mail ไปถึง mail server
- mail server ต้นทางจะตรวจสอบ MX ของ DNS zone “ipv6.testbed.local”
- DNS จะตอบกลับมาว่า MX ของ mail server ปลายทางชื่อ “**mail.ipv6.testbed.local**”
- และหาหมายเลข IP address ของ mail.ipv6.testbed.local ได้ว่าเป็น IPv6 คือ “**2001:db8:x::9**”
- mail server ต้นทาง จะติดต่อเพื่อส่ง email ไปยังเครื่องปลายทางหมายเลข IPv6 ข้างต้น
- เครื่อง mail.ipv6.testbed.local จะนำ email บันทึกลงใน mailbox ของ user thong ในที่สุด

สามารถตรวจสอบ MX จาก DNS server ด้วยคำสั่ง host -t mx <domain>

```
# host –t mx ipv6.testbed.local
ipv6.testbed.local mail is handled (pri=1) by mail.ipv6.testbed.local

ตัวอย่างอื่นๆเช่น
#host –t mx cnn.com
cnn.com mail is handled (pri=10) by mail.tuner.com
cnn.com mail is handled (pri=30) by alfw2.tuner.com
```

7.2 การติดตั้ง ปรับแต่ง และทดสอบระบบ mail server บน Ubuntu 14.04

Application เบื้องต้น

- postfix (SMTP Mail Server)
- dovecot (POP/IMAP Server)
- thunderbird (Mail Client)
- Outlook (Mail Client)

7.2.1 ขั้นตอนการติดตั้ง และปรับแต่ง

การติดตั้ง postfix และ dovecot

1. **ติดตั้ง Mail Server โดยใช้คำสั่ง**

```
# apt-get –y install postfix dovecot-core dovecot-imapd dovecot-pop3d
```

เมื่อติดตั้งแล้วจะมี configuration file ที่เกี่ยวข้องดังนี้

```
/etc/postfix/main.cf
/etc/dovecot/dovecot.conf
```

2. **File main.cf**

main.cf เป็น file ที่ใช้ config parameter ต่างๆ ของโปรแกรม postfix โดยจะมี parameter ที่สำคัญๆ ดังนี้

myhostname	ใช้กำหนดชื่อ host ของ mail server
alias_maps	อ้างถึง file aliases ที่ใช้กำหนดชื่อ user หรือ file user group mail
alias_database	อ้างถึง file aliases.db ที่ได้จากการใช้คำสั่ง newaliases
myorigin	ใช้กำหนดชื่อของโดเมนที่ใช้ในการส่ง mail
mydestination	กำหนดว่าเครื่องนี้ต้องทำหน้าที่เป็นปลายทางของ domain อะไรบ้าง
relayhost	เป็นการ relay mail ไปให้ server อื่นส่งแทน
mynetworks	กลุ่มของหมายเลขไอพีที่ยินยอมให้ออกสู่ภายนอก หรือ Relaying นั้นเอง
mailbox_size_limit	กำหนดขนาดของ mailbox ของทุก user ขนาดเป็น byte
inet_interfaces	Interface ที่เราจะกำหนดให้ postfix นั้นทำงานด้วย
inet_protocols	กำหนดได้ 3 ค่า “ipv4, ipv6, all”

ค่าที่จำเป็นต้องใช้หลักๆเป็นอันดับแรกคือ inet_protocols, myhostname, myorigin, mydestination

ตัวอย่างการตั้งค่าของ IPv6 mail testbed

inet_protocols ipv6

กำหนดว่า mail server เครื่องนี้รอรับการเชื่อมต่อจาก mail server ด้วย IPv6 เท่านั้น
(*ถ้าต้องการให้เป็น dual stack ให้กำหนดเป็น “all” จะรอรับทั้ง IPv4 และ IPv6)

myhostname mail.ipv6.testbed.local

เพื่อกำหนดชื่อ host ของ mail server เครื่องนี้

myorigin ipv6.testbed.local

กำหนดว่าส่ง mail ออกข้างนอกด้วยโดเมนของเครื่องนี้ คือ @ipv6.testbed.local

mydestination ipv6.testbed.local

กำหนดให้รับ email ที่ส่งมาหาโดเมนนี้ @ipv6.testbed.local เท่านั้น

3. **File dovecot.conf**

สำหรับกำหนดค่าต่างๆให้กับ imap, pop server สำหรับการจัดการ mail box ของ user ผ่าน email client (MS Outlook, Mozilla thunderbird, Mac Mail, ฯลฯ) ส่วนที่สำคัญสำหรับการเชื่อมต่อระหว่าง Client กับ Server ผ่าน IPv6 คือ parameter “listen”

listen = *, ::

* คือรับ connection ผ่าน IPv4 interface ทุก interface

:: คือรับ connection ผ่าน IPv6 interface ทุก interface

ถ้า listen = * จะรับ connection จาก client ที่เป็น IPv4 อย่างเดียว
เช่นกัน
ถ้า listen = :: จะรับ connection จาก client ที่เป็น IPv6 อย่างเดียว
ในกรณีที่ต้องการทำเป็น **Dual stack** กำหนดตามค่า default คือ listen = *,::

7.3 การทดสอบระบบ Mail Server

7.3.1 ทดสอบการทำงานของ postfix

เริ่มการทำงานของ postfix โดยใช้คำสั่ง

```
# /etc/init.d/postfix start
หรือ
# service postfix start
```

postfix ทำงานจะทำงานอยู่ภายใต้เบื้องหลัง (daemon) สามารถตรวจสอบได้โดยใช้คำสั่ง

```
# ps -ef | grep postfix
root     10338     1  0 May20 ?        00:00:00 /usr/lib/postfix/master
postfix  10340 10338  0 May20 ?        00:00:00 qmgr -l -t unix -u
postfix  10343 10338  0 May20 ?        00:00:00 tlsmgr -l -t unix -u -c
postfix  15470 10338  0 09:19 ?        00:00:00 pickup -l -t unix -u -c
```

เมื่อ daemon ทำงานตัวมันจะเปิด port 25 เพื่อรอรับการเชื่อมต่อในการขอส่ง email ดังนั้นเราสามารถดูได้ว่า port 25 เปิดทำงานเพื่อรอรับการเชื่อมต่อ (LISTEN) หรือไม่โดยใช้คำสั่ง

```
# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN
tcp6       0      0 :::25                   :::*                    LISTEN
```

การทดสอบด้วยคำสั่ง Telnet เข้าที่ port 25 เพื่อส่ง email

```
# telnet 2001:db8:x::9 25
Trying 2001:db8:x::9...
Connected to 2001:db8:x::9.
Escape character is '^]'.
220 mail.ipv6.testbed.local ESMTP Postfix (Ubuntu)
mail from:thong@ipv6.testbed.local
250 2.1.0 Ok
rcpt to:user@gmail.com
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Test send mail to gmail
.
250 2.0.0 Ok: queued as BEBD94013E
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

7.3.2 ทดสอบการทำงานของ dovecot

เริ่มการทำงานของ dovecot โดยใช้คำสั่ง

```
# service dovecot start
```

เมื่อ dovecot ทำงานในแต่ละ protocol จะเปิด port ที่แต่ละ protocol ต้องใช้งาน IMAP ใช้งาน port 110 ส่วน POP3 ใช้งาน port 143 สามารถตรวจสอบได้โดยใช้คำสั่ง

```
# netstat -tan
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN
tcp6       0      0 :::110                  :::*                    LISTEN
tcp6       0      0 :::143                  :::*                    LISTEN
```

ทดสอบการเชื่อมต่อ telnet เข้าไปที่ port ของแต่ละ protocol

IMAP

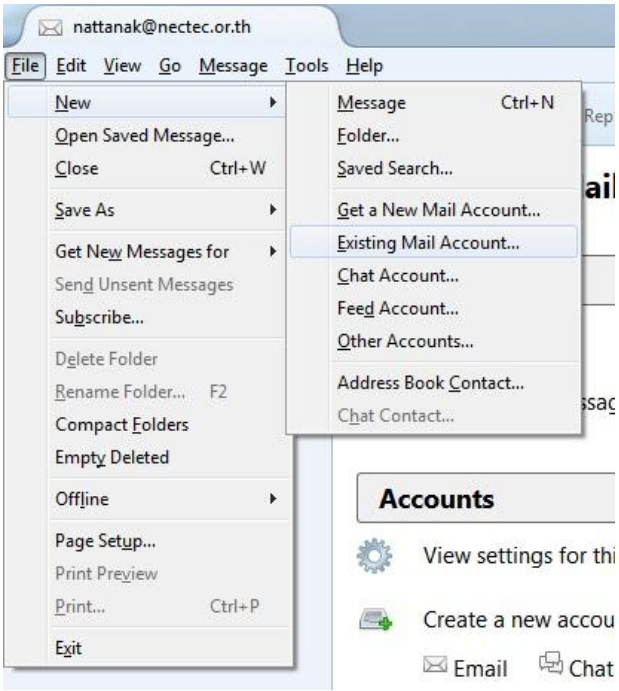
```
# telnet 2001:db8:x::9 110
Trying 2001:db8:x::9...
Connected to 2001:db8:x::9.
Escape character is '^]'.
+OK Dovecot (Ubuntu) ready.
user thong
+OK
pass ************
+OK Logged in.
quit
+OK Logging out.
Connection closed by foreign host.
```

POP3

```
# telnet 2001:db8:x::9 143
Trying 2001:db8:x::9...
Connected to 2001:db8:x::9.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR
LOGIN-REFERRALS ID ENABLE IDLE STARTTLS
AUTH=PLAIN] Dovecot (Ubuntu) ready.
1 logout
* BYE Logging out
1 OK Logout completed.
Connection closed by foreign host.
```

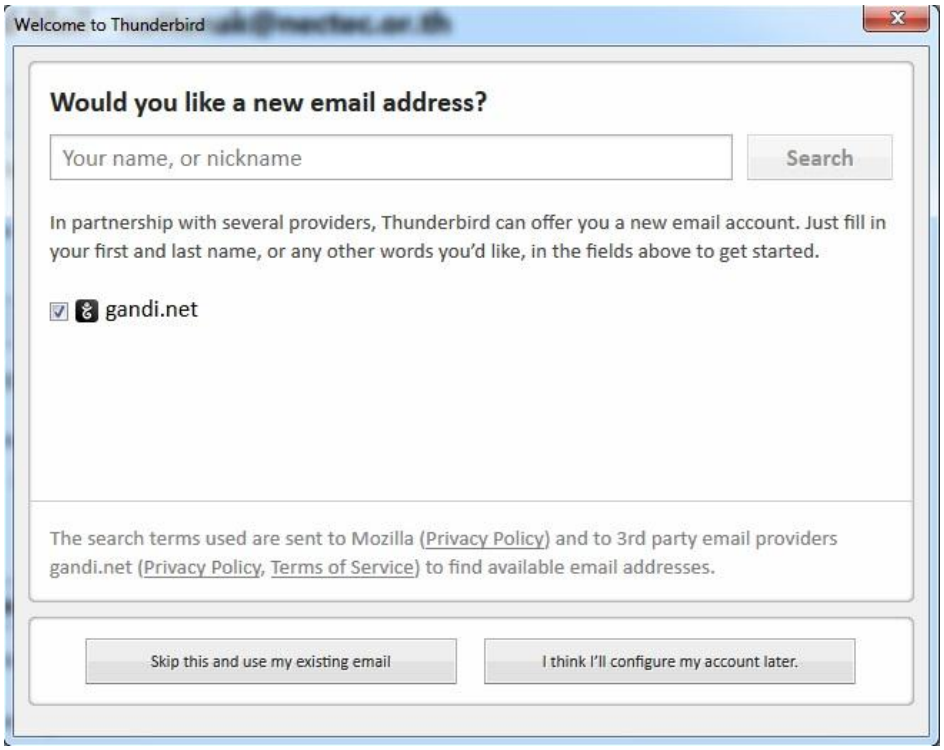
7.4 ขั้นตอนการปรับแต่ง Mail Client โดยใช้โปรแกรม thunderbird V.31.5.0

1. คลิกที่ File -> New -> Mail Account...



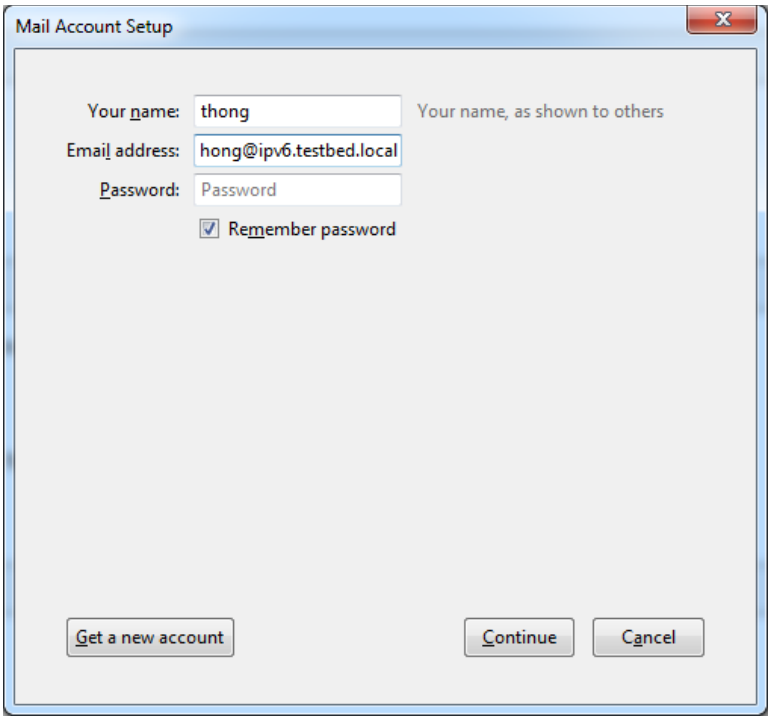
รูปที่ 7.3 การตั้งค่า Mail Account ด้วย thunderbird

2. คลิกที่ “Skip this and use my existing email”



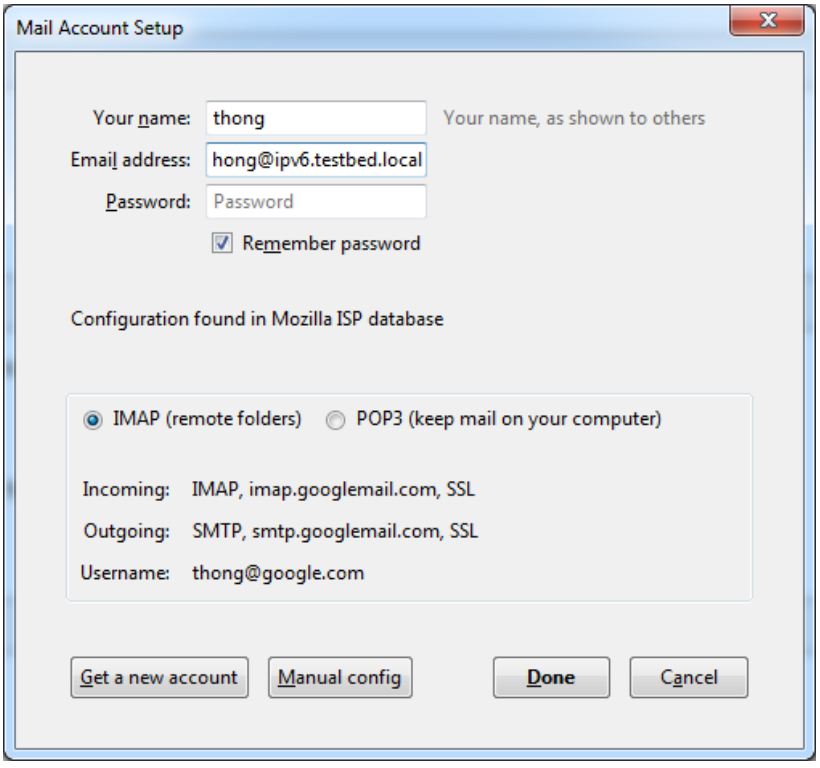
รูปที่ 7.4 การตั้งค่า Mail Account ด้วย thunderbird (1)

3. ปรากฏหน้าต่าง Mail Account Setup โดยให้ใส่ข้อมูลในช่อง “Your name”, “Email address” จากนั้นคลิกที่ปุ่ม “Continue”



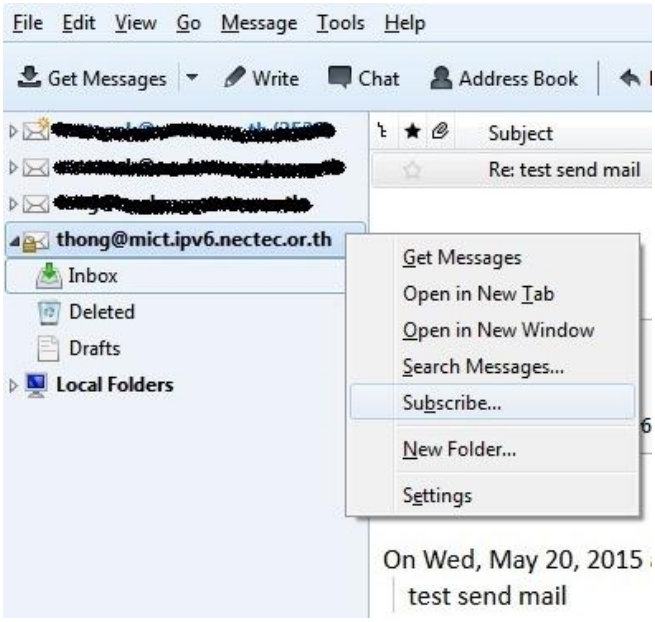
รูปที่ 7.5 การตั้งค่า Mail Account ด้วย thunderbird (2)

4. เราสามารถเลือก protocol ที่ใช้อ่าน email ว่าจะเป็นแบบ IMAP / POP3 จากนั้นให้คลิกที่ปุ่ม “Done”



รูปที่ 7.6 การตั้งค่า Mail Account ด้วย thunderbird (3)

5. จะปรากฏชื่อ Email ที่ได้เชื่อมต่อเรียบร้อย จากนั้นให้ทำการ add subscribe เพื่อให้เห็น personal folder ที่แต่ละ user ได้สร้างไว้ โดยคลิกขวาที่ user@ipv6.testbed.local -> Subscribe...



รูปที่ 7.7 การตั้งค่า Mail Account ด้วย thunderbird (4)

6. จะปรากฏหน้าต่าง Subscribe และให้เลือก folder ที่ต้องการในช่อง “Select the folders to subscribe to” จากนั้นคลิกปุ่ม “OK”

รูปที่ 7.8 การตั้งค่า Mail Account ด้วย thunderbird (5)

หัวข้อที่ 8 Firewall

8.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

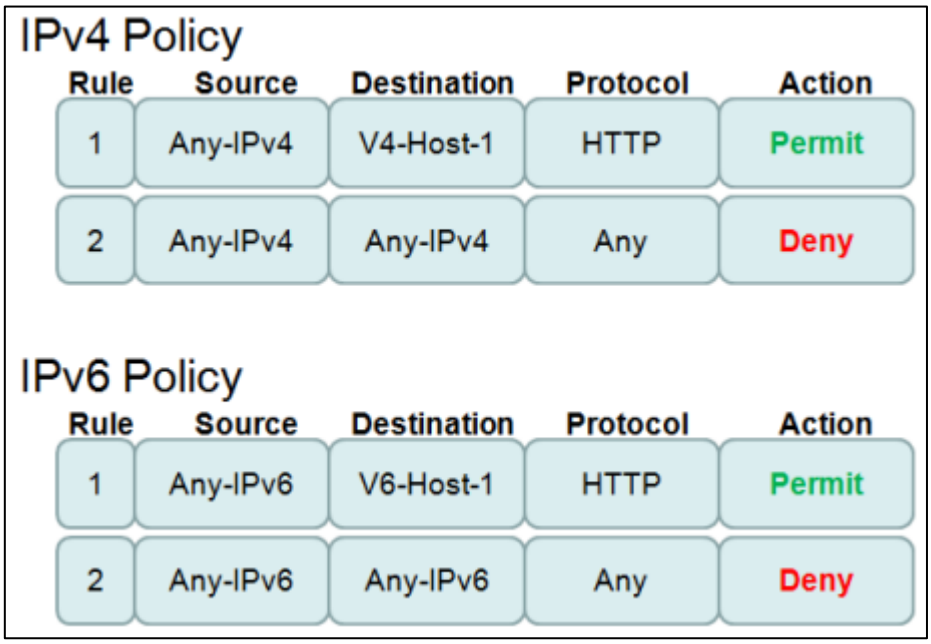
ไฟร์วอลล์ (อังกฤษ: firewall; ศัพท์บัญญัติ ด่านกันบุกรุก) คือซอฟต์แวร์หรือฮาร์ดแวร์ในระบบเครือข่าย ซอฟต์แวร์หรือฮาร์ดแวร์ในระบบเครือข่ายหน้าที่ของไฟร์วอลล์คือเป็นตัวกรองข้อมูลสื่อสารโดยการกำหนดกฎและระเบียบมาบังคับใช้โดยเฉพาะเรื่องของการดูแลระบบเครือข่ายโดยความผิดพลาดของการปรับแต่งอาจส่งผลทำให้ไฟร์วอลล์มีช่องโหว่และนำไปสู่สาเหตุของการโจรกรรมข้อมูลคอมพิวเตอร์ได้

ในปัจจุบันมีการโจมตีเครือข่ายของหน่วยงานจากผู้ไม่ประสงค์ดีเพิ่มขึ้นอย่างมากทำให้เครือข่ายเกิดการใช้งานไม่ได้หรือใช้งานได้ช้าไม่สามารถให้บริการแก่ผู้ใช้ที่อยู่ภายในหน่วยงานหรือนอกหน่วยงานได้ หน่วยงานจึงมีความจำเป็นต้องติดตั้ง Firewall เพื่อรักษาเครือข่ายให้มีความปลอดภัยและสามารถใช้งานได้อย่างต่อเนื่อง

V•T•E	Firewall software	[hide]
Application firewall · Context-based access control · Personal firewall · Stateful firewall · Unified threat management · Virtual firewall		
Linux	**Apps**	ipchains · Netfilter (L7-filter · NuFW · ipset · iptables) · nftables · FireHOL · Firestarter · Shorewall · Uncomplicated Firewall · MoBlock · Privoxy · Squid
	Distros	SmoothWall · IPCop · IPFire · OpenWrt · Zeroshell · Untangle
BSD	**Apps**	PF · NPF · ipfirewall · IPFilter
	Distros	M0n0wall · pfSense
OS X	NetBarrier X4 · VirusBarrier X6 · PeerGuardian · Little Snitch	
Windows	**Commercial**	Avira · Check Point Integrity · **Comodo Internet Security** · Glasswire · Jetico Personal Firewall · Kaspersky Internet Security · McAfee Personal Firewall Plus · Microsoft Forefront Threat Management Gateway · Norton 360 · Norton Personal Firewall · Norton Internet Security · Online Armor Personal Firewall · Outpost Firewall Pro · PC Tools Internet Security · Symantec Endpoint Protection · Windows Firewall · Windows Live OneCare · WinGate · WinRoute · ZoneAlarm
	Freeware	**Comodo Internet Security** · Glasswire · Online Armor Personal Firewall · PC Tools Internet Security · ZoneAlarm
	Open-source	PeerBlock · PeerGuardian
Appliances	Novell BorderManager · Vyatta · ZoneAlarm Z100G · Zorp firewall	
Comparison of firewalls · List of router or firewall distributions		

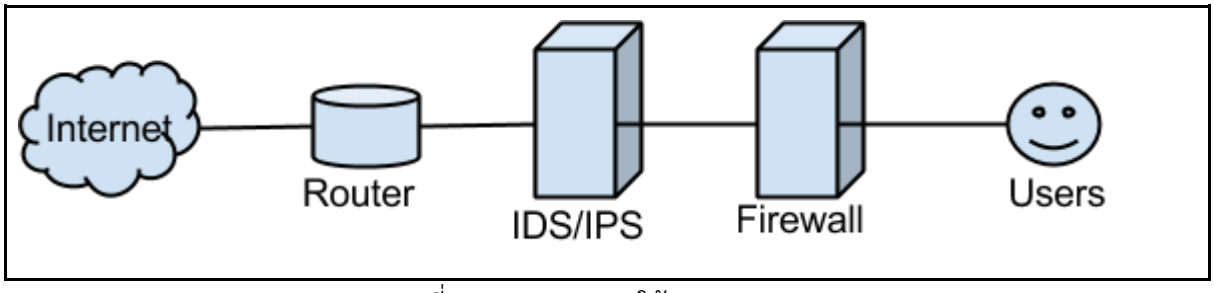
รูปที่ 8.1 ข้อมูลเปรียบเทียบ Firewall ของแต่ละระบบปฏิบัติการ

การกำหนดกฎของ IPv4/IPv6



รูปที่ 8.2 การกำหนดกฎของ IPv4/IPv6

รูปแบบการใช้งาน



รูปที่ 8.3 รูปแบบการใช้งาน Firewall

8.2 การติดตั้ง

8.2.1 ip6tables

โปรแกรม ip6tables เป็นโปรแกรมที่ไว้สำหรับปิดกั้น port บน Linux สำหรับ IPv6

การเช็ค rules

$sudo ip6tables -nvL

การเพิ่ม rules

$sudo ip6tables -I INPUT -p tcp --dport 80 -j REJECT

$sudo ip6tables -I INPUT -p icmp -j DROP

$sudo ip6tables -I INPUT -p tcp --dport 25 -j ACCEPT

$sudo ip6tables -A INPUT -j REJECT

การลบ rules

$sudo ip6tables -D INPUT 1 ; ลบ rules ที่ 1

$sudo ip6tables -D INPUT -p icmp -j DROP ; ลบ rules block icmp

8.2.2 fwsnort

เพื่อเพิ่มกฎการทำงานของ Firewall โปรแกรม Fwsnort เป็น Firewall Opensource ที่มีการติดตั้งและใช้งานไม่ยาก และมีความปลอดภัยในการใช้งานโดยใช้คู่กับ ip6tables ในการปิดการเข้าถึงและโจมตีบริการต่างในเครือข่ายของหน่วยงาน

การอัพเดท package

$sudo apt-get update

การติดตั้งโปรแกรม fwsnort

$sudo apt-get install fwsnort

การติดตั้งอัพเดท rules

$sudo fwsnort -6 --update-rules

การปรับแต่ง fwsnort

$sudo vi /etc/fwsnort/fwsnort.conf

HOME_NET	2001:db8:x::/48;
UPDATE_RULES_URL	http://rules.emergingthreats.net/open/snort-2.9.0/emerging-all.rules;

การติดตั้ง rules แบบระบุ rules

$sudo fwsnort --include-type backdoor,ddos,web-attacks

การติดตั้ง rules เข้าไปใน fwsnort

$cd /etc/fwsnort/snort-rules

$ls

$sudo fwsnort -6 --update

$sudo fwsnort -6

```
[+] Testing /sbin/ip6tables for supported capabilities...
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
    Snort Rules File          Success   Fail      Total

[+] emerging-all.rules        10026     5726      15752
[+] scan.rules                13        5         18
[+] web-attacks.rules         46        0         46
                              =============================
                              10085     5731      15816
[+] Generated ip6tables rules for 10085 out of 15816 signatures: 63.76%

[+] Logfile: /var/log/fwsnort/fwsnort.log
[+] ip6tables script (individual commands): /var/lib/fwsnort/fwsnort_iptcmds.sh

    Main fwsnort ip6tables-save file: /var/lib/fwsnort/fwsnort.save

    You can instantiate the fwsnort policy with the following command:

    /sbin/ip6tables-restore < /var/lib/fwsnort/fwsnort.save

    Or just execute: /var/lib/fwsnort/fwsnort.sh
```

8.3 การทดสอบ

```
64 bytes from 2001:db8:x::7: icmp_seq=19 ttl=64 time=0.339 ms
64 bytes from 2001:db8:x::7: icmp_seq=20 ttl=64 time=0.432 ms        ←---------drop icmpv6
64 bytes from 2001:db8:x::7: icmp_seq=30 ttl=64 time=0.309 ms
64 bytes from 2001:db8:x::7: icmp_seq=31 ttl=64 time=0.358 ms
64 bytes from 2001:db8:x::7: icmp_seq=32 ttl=64 time=0.331 ms        ←-------- Reject icmpv6
From 2001:db8:x::7 icmp_seq=34 Destination unreachable: Port unreachable
From 2001:db8:x::7 icmp_seq=35 Destination unreachable: Port unreachable
From 2001:db8:x::7 icmp_seq=36 Destination unreachable: Port unreachable
^C
--- 2001:db8:x::7 ping statistics ---
36 packets transmitted, 13 received, +4 errors, 63% packet loss, time 35093ms
rtt min/avg/max/mdev = 0.295/0.348/0.432/0.036 ms
```

ผลลัพธ์แสดงการ DROP และ REJECT port icmpv6

```
Chain INPUT (policy ACCEPT 55 packets, 5256 bytes)
```

```
 pkts bytes target     prot opt in     out     source               destination
   14  1376 REJECT     icmpv6     *      *       ::/0                 ::/0                 reject-with icmp6-port-unrea
chable
    0     0 DROP       icmp     *      *       ::/0                 ::/0
 1430  134K FWSNORT_INPUT  all      !lo    *       ::/0                 ::/0

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    5   520 FWSNORT_FORWARD  all      !lo    *       ::/0                 ::/0

Chain OUTPUT (policy ACCEPT 32 packets, 4000 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1190  286K FWSNORT_OUTPUT  all      *      !lo     ::/0                 ::/0

Chain FWSNORT_FORWARD (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 FWSNORT_FORWARD_ESTAB  tcp      *      *       ::/0                 ::/0                 ctstate
ESTABLISH
ED
    0     0 LOG        udp      *      *       ::/0                 ::/0                 udp STRING match  "|535353535
343534353ffd06668|" ALGO name bm TO 65535 STRING match  "|665389e19568a41a|" ALGO name bm
FROM 55 TO 65535 /* sid:2009
285; msg:ET SHELLCODE Bindshell2 Decoder Shellcode (UDP); classtype:shellcode-detect;
reference:url,doc.emergingthreat
s.net/2009285; rev:2; FWS:1.6.3; */ LOG flags 4 level 4 prefix "[1] SID2009285 "
    0     0 LOG        udp      *      *       ::/0                 ::/0                 udp STRING match  "|000002030
06c6f63|" ALGO name bm FROM 78 TO 65535 STRING match  "|006263703a2f2f|" ALGO name bm FROM
87 TO 65535 /* sid:2000335;
 msg:ET P2P Overnet (Edonkey) Server Announce; classtype:policy-violation;
reference:url,www.overnet.com; rev:9; FWS:1
```

ผลลัพธ์แสดง rules ของ ip6tables และ snort

อ้างอิง

1. http://th.wikipedia.org/wiki/ไฟร์วอลล์
2. http://itfanatic.com/?q=node/61
3. https://www.snort.org
4. http://cipherdyne.org/fwsnort
5. http://pubpages.unh.edu/~stk/IPv6/ip6tables.html
6. http://ifzenelse.net/en/secure-your-centos-linux-server-prevent-attacks-iptables-and-fwsnort

หัวข้อที่ 9 ระบบตรวจจับและป้องกันผู้บุรุกในเครือข่าย IDS/IPS

9.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

9.1.1 Intrusion Detection System (IDS)

IDS หรือระบบตรวจจับการบุกรุกเป็นเครื่องมือสำหรับการรักษาความปลอดภัยอีกประเภทหนึ่งที่ใช้สำหรับตรวจตรวจจับความพยายามที่จะบุกรุกเครือข่ายโดยระบบจะแจ้งเตือนผู้ดูแลระบบเมื่อมีการบุกรุกหรือมีการพยายามที่จะบุกรุกเครือข่าย โดย IDS นั้นไม่ใช่ระบบที่ใช้ป้องกันการบุกรุกแต่เป็นระบบที่คอยแจ้งเตือนภัยเท่านั้นหน้าที่หลักของ IDS คือแจ้งเตือนการเข้าใช้เครือข่ายที่ผิดปกติ โดยประเด็นสำคัญคือ เหตุการณ์ใดคือสิ่งที่ถือว่าผิดปกติ ดังนั้นการใช้ IDS นั้นก็ขึ้นอยู่กับว่าอะไรที่จะแจ้งเตือนให้ทราบซึ่งจะขึ้นอยู่กับสภาวะของระบบในขณะนั้นปัญหาอย่างหนึ่งของ IDS คือบางที IDS ไม่สามารถตรวจจับการบุกรุกได้ และปัญหาที่สำคัญที่สุดของ IDS คือ โดยส่วนใหญ่แล้ว IDS ไม่สามารถป้องกันการบุกรุกได้โดยทันทีหรือแบบเรียลไทม์ เช่น การโจมตีแบบ DoS (Denial of Services) หรือ DDos (Distributed Denial of Services) จากปัญหาเหล่านี้จึงมีการคิดค้นเทคโนโลยีใหม่ขึ้นมาเรียกว่า IPS (Intrusion Prevention System) ซึ่งสามารถตรวจจับการบุกรุกและหยุดการบุกรุกได้อย่างทันทีเครื่องมืออีกอย่างหนึ่งที่มักใช้ร่วมกับ IDS/IPS ในการดักจับการบุกรุกคือฮันนีพ็อต (Honey pot) หรือเป้าหมายลวง

9.1.2 Intrusion Prevention System (IPS)

IPS ในยุคแรกนั้นการหยุดการบุกรุกทำได้โดยการส่งสัญญาณ TCP Reset เพื่อจัดการกับเซสชันที่คาดว่าจะเป็นการบุกรุก หรืออาจจะเข้าไปเปลี่ยนแปลงกฎในไฟร์วอลล์แบบอัตโนมัติ ซึ่งบางครั้งก็อาจเกิดความผิดพลาดได้ แต่ก็มีการปรับปรุงให้ IPS ฉลาดขึ้น ซึ่งสามารถเรียนรู้เทคนิคการเจาะระบบในรูปแบบต่างๆ ได้อย่างละเอียด IPS รุ่นใหม่ที่มีความฉลาดมากขึ้นนั้น มีการนำเทคโนโลยีขั้นสูงในการวิเคราะห์ข้อมูล เช่น Neural Network และ Fuzzy Logic ซึ่งจะทำให้ลดปัญหาการแจ้งเตือนที่ผิดพลาดลงไปได้อย่างมาก

หลักการทำงานของ IPS

หลักการทำงานของ IPS จะใช้หลักการที่เรียกว่า “Inline” หรือที่เรียกว่า “Gateway IDS” ซึ่งก็คือการนำ IPS ไปกั้นกลางบนเส้นทางการส่งข้อมูล โดยไม่ต้องมีการกำหนดหมายเลขไอพีให้กับ IPS แต่ปัญหาก็คือ หากตัว IPS เกิดเสีย ถ้า IPS ไม่สามารถบายพาสตัวเองได้ ก็จะทำให้เกิดปัญหาในการรับ-ส่งข้อมูลระหว่างต้นทางกับปลายทาง ตลอดจนถ้า IPS ตัดสินใจผิด การบล็อกแพ็กเก็ตที่ IPS คิดว่าเป็นการบุกรุก แต่จริงๆ เป็นการใช้งานธรรมดาก็จะเกิดปัญหาอีกเช่นกัน

9.1.3 เป้าหมายลวง (Honey Pot)

Honey Pot หรือเป้าหมายลวง ก็คือ ช่องโหว่ (Vulnerability) ที่เราปล่อยให้มีบนเครื่องเซิร์ฟเวอร์ เพื่อลวงให้แฮคเกอร์เข้ามาเจาะระบบ โดยเราจะใช้ระบบฮันนีพ็อต เพื่อดักจับการเจาะระบบของแฮคเกอร์ ทำให้เราสามารถเรียนรู้วิธีการเจาะระบบของแฮคเกอร์อย่างละเอียด อีกทั้งเราสามารถสืบหาตัวแฮคเกอร์ได้ก่อนที่จะเจาะระบบจริงของเรา โดยฮันนีพ็อตจะใช้ความสามารถ “Stealth Logging” ของระบบในการบันทึกหลักฐานเพื่อใช้ในการสืบจับแฮคเกอร์

แม้ว่าฮันนีพ็อต จะทำให้เราได้ศึกษาการเจาะระบบของแฮคเกอร์ รวมถึงสามารถตรวจจับไวรัสหรือเวิร์มได้ แต่หากว่าเราออกแบบระบบเป้าหมายลวงไม่ดี จะทำให้แฮคเกอร์สามารถใช้ระบบเป้าหมายลวงที่เราทำไว้นำไปใช้เจาะระบบของคนอื่นอีกที

9.1.4 ทำไมต้องมี IDS/IPS

เนื่องจากภัยคุกคามจากอินเทอร์เน็ตและเครือข่ายคอมพิวเตอร์ในปัจจุบันอยู่ในระดับที่สูงมาก การติดตั้งไฟร์วอลล์ อย่างเดียวคงไม่เพียงพอ IDS/IPS จึงเป็นสิ่งจำเป็นที่จะต้องมีในระบบการรักษาความปลอดภัยในเครือข่ายของทุกองค์กร ต่อไปนี้คือเหตุผลที่ว่าทำไมต้องมีระบบ IDS/IPS

- เพื่อเป็นเครื่องมือสำหรับการสืบสวนหาบุคคลที่โจมตี บุกรุก หรือใช้ระบบในทางที่ผิด
- เพื่อตรวจจับความพยายามที่จะบุกรุกเครือข่ายและป้องกันก่อนที่จะเกิดการโจมตีจริงๆ
- เพื่อเก็บสถิติเกี่ยวกับความพยายามที่บุกรุกหรือโจมตีและนำข้อมูลไปวิเคราะห์ภัยคุกคามที่อาจจะเกิดขึ้นกับองค์กรได้
- เพื่อเป็นเครื่องมือในการวัดประสิทธิภาพในการป้องกันภัยของระบบการรักษาความปลอดภัยอื่น เช่น ไฟร์วอลล์ เป็นต้น

ตารางที่ 9.1 ข้อดีและข้อเสียของ Suricata และ Snort

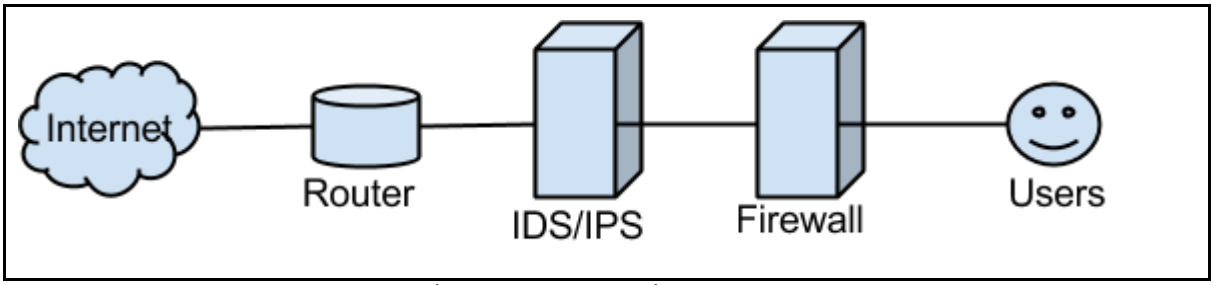
Parameter	Suricata	Snort
IPS feature	optional while compiling (--enable-nfqueue)	Snort_inline or snort used with -Q option
Rules	• VRT::Snort rules • EmergingThreats rules	• VRT::Snort rules • SO rules • EmergingThreats rules
Threads	Multi-thread	Single-thread
Ease of install	Not available from packages. Manual installation.	Relatively straightforward. Installation also available from packages.
Documentation	Few resources on the Internet	Well documented on the official website and over the Internet
Event logging	Flat file, database, unified2 logs for barnyard	
IPv6 support	Fully supported	Supported when compiled with --enable-ipv6 option.
Capture accelerators	PF_RING, packet capture accelerator	None, use of libpcap

ตารางที่ 9.1 ข้อดีและข้อเสียของ Suricata และ Snort (ต่อ)

Parameter	Suricata	Snort
Configuration file	suricata.yaml, classification.config, reference.config, threshold.config	snort.conf, threshold.conf
Offline analysis (pcap file)	yes	
Frontends	Sguil, Aanval, BASE, FPCGUI (Full Packet Capture GUI), Snortsnarf	

9.2 การติดตั้ง IDS/IPS

การติดตั้งโปรแกรม Suricata และ Snort มาใช้ใน IDS/IPS



รูปที่ 9.1 รูปแบบการเชื่อมต่อ IDS/IPS

9.2.1 การติดตั้ง Package Suricata

- $sudo apt-get update ; สำหรับปรับปรุง Package
- $sudo apt-cache search suricata ; สำหรับหา Package
- $sudo apt-get install suricata ; สำหรับติดตั้ง Package

9.2.2 การคอนฟิก Suricata

- $sudo cp /etc/suricata/suricata-debian.yaml /etc/suricata/suricata.yaml
  ; copy ไฟล์ตัวอย่างใส่ในไฟล์ config suricata
- $sudo nano /etc/suricata/suricata.yaml ; แก้ไขไฟล์คอนฟิก

default-log-dir: /var/log/suricata/

- $sudo /etc/init.d/suricata restart
- $sudo tail -f /var/log/suricata/stats.log ; ตรวจสอบไฟล์ log stat ของ suricata

9.2.3 การเพิ่มกฎของ suricata

- $sudo apt-get install oinkmaster ; ติดตั้งโปรแกรม oninkmaster
- $sudo nano /etc/oinkmaster.conf ; แก้ไขไฟล์ oninkmaster.conf

เพิ่ม # หน้า rule ที่ไม่ต้องการ
url = http://www.snort.org/pub-bin/oinkmaster.cgi/<oinkcode>/snortrules-snapshot-2.7.tar.gz
ลบ # หน้า rule ที่ต้องการ
http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz

- $sudo mkdir /etc/suricata/rules ; สร้างโฟลเดอร์ rules ขึ้นมา
- $sudo oinkmaster -C /etc/oinkmaster.conf -o /etc/suricata/rules ; รันโปรแกรม oninkmaster เพื่อนำกฎต่างๆไปใส่ในโฟลเดอร์ rules
- $sudo nano /etc/suricata/suricata.yaml ; แก้ไขไฟล์ suricata.yaml

```
default-rule-path: /etc/suricata/rules
rule-files:
 - botcc.rules
 - ciarmy.rules
 - compromised.rules
 - drop.rules
 - dshield.rules
 - emerging-activex.rules
 - emerging-attack_response.rules
 - emerging-chat.rules
 - emerging-current_events.rules
 - emerging-dns.rules
 - emerging-dos.rules
 - emerging-exploit.rules
 - emerging-ftp.rules
 - emerging-games.rules
 - emerging-icmp_info.rules
# - emerging-icmp.rules
 - emerging-imap.rules
 - emerging-inappropriate.rules
 - emerging-malware.rules
 - emerging-misc.rules
 - emerging-mobile_malware.rules
 - emerging-netbios.rules
 - emerging-p2p.rules
```

```
 - emerging-policy.rules
 - emerging-pop3.rules
 - emerging-rpc.rules
 - emerging-scada.rules
 - emerging-scan.rules
 - emerging-shellcode.rules
 - emerging-smtp.rules
 - emerging-snmp.rules
 - emerging-sql.rules
 - emerging-telnet.rules
 - emerging-tftp.rules
 - emerging-trojan.rules
 - emerging-user_agents.rules
# - emerging-virus.rules
 - emerging-voip.rules
 - emerging-web_client.rules
 - emerging-web_server.rules
 - emerging-web_specific_apps.rules
 - emerging-worm.rules
# - rbn-malvertisers.rules
# - rbn.rules
 - tor.rules
 - decoder-events.rules # available in suricata sources under rules dir
 - stream-events.rules  # available in suricata sources under rules dir
 - http-events.rules    # available in suricata sources under rules dir
 - smtp-events.rules    # available in suricata sources under rules dir

classification-file: /etc/suricata/rules/classification.config
reference-config-file: /etc/suricata/rules/reference.config

address-groups:
 HOME_NET: "[2001:db8:x::/48]"
```

9.2.4 การรันโดยอัตโนมัติเมื่อปิดเปิดเครื่องใหม่

- $sudo nano /etc/default/suricata/

```
RUN=yes
IFACE=eth0
SURCONF=/etc/suricata/suricata.yaml
LISTENMODE=nfqueue
NFQUEUE=1
```

- $sudo service suricata restart ; เริ่มการทำงาน service suricata ใหม่
- หรือ $sudo suricata -c /etc/suricata/suricata.yaml -q 0 ; สำหรับดู console หน้าจอ

```
20/5/2015 -- 09:17:22 - <Info> - This is Suricata version 1.4.7 RELEASE
20/5/2015 -- 09:17:22 - <Info> - CPUs/cores online: 1
20/5/2015 -- 09:17:22 - <Info> - Enabling fail-open on queue
20/5/2015 -- 09:17:22 - <Info> - NFQ running in standard ACCEPT/DROP mode
20/5/2015 -- 09:17:22 - <Info> - allocated 3670016 bytes of memory for the defrag hash... 65536
buckets of size 56
20/5/2015 -- 09:17:22 - <Info> - preallocated 65535 defrag trackers of size 144
20/5/2015 -- 09:17:22 - <Info> - defrag memory usage: 13107056 bytes, maximum: 33554432
20/5/2015 -- 09:17:22 - <Info> - AutoFP mode using default "Active Packets" flow load balancer
20/5/2015 -- 09:17:22 - <Info> - preallocated 1024 packets. Total memory 4360192
20/5/2015 -- 09:17:22 - <Info> - allocated 229376 bytes of memory for the host hash... 4096 buckets of
size 56
20/5/2015 -- 09:17:22 - <Info> - preallocated 1000 hosts of size 120
20/5/2015 -- 09:17:22 - <Info> - host memory usage: 349376 bytes, maximum: 16777216
20/5/2015 -- 09:17:22 - <Info> - allocated 3670016 bytes of memory for the flow hash... 65536 buckets
of size 56
20/5/2015 -- 09:17:22 - <Info> - preallocated 10000 flows of size 272
20/5/2015 -- 09:17:22 - <Info> - flow memory usage: 6390016 bytes, maximum: 33554432
20/5/2015 -- 09:17:22 - <Info> - IP reputation disabled
20/5/2015 -- 09:17:22 - <Info> - using magic-file /usr/share/file/magic
20/5/2015 -- 09:17:22 - <Info> - Delayed detect disabled
20/5/2015 -- 09:17:24 - <Info> - 46 rule files processed. 16481 rules successfully loaded, 0 rules failed
20/5/2015 -- 09:17:38 - <Info> - 16489 signatures processed. 953 are IP-only rules, 5960 are inspecting
packet payload, 12326 inspect application layer, 72 are decoder event only
20/5/2015 -- 09:17:38 - <Info> - building signature grouping structure, stage 1: adding signatures to
signature source addresses... complete
20/5/2015 -- 09:17:38 - <Info> - building signature grouping structure, stage 2: building source address
list... complete
20/5/2015 -- 09:17:38 - <Info> - building signature grouping structure, stage 3: building destination
address lists... complete
20/5/2015 -- 09:17:39 - <Warning> - [ERRCODE: SC_ERR_FOPEN(44)] - Error opening file:
```

```
"/etc/suricata//threshold.config": No such file or directory
20/5/2015 -- 09:17:39 - <Info> - Core dump size set to unlimited.
20/5/2015 -- 09:17:39 - <Info> - fast output device (regular) initialized: fast.log
20/5/2015 -- 09:17:39 - <Info> - Unified2-alert initialized: filename unified2.alert, limit 32 MB
20/5/2015 -- 09:17:39 - <Info> - http-log output device (regular) initialized: http.log
20/5/2015 -- 09:17:39 - <Info> - Fast log output initialized, filename: alert-pcapinfo.log
20/5/2015 -- 09:17:39 - <Info> - Using log dir /var/log/suricata/
20/5/2015 -- 09:17:39 - <Info> - using normal logging
20/5/2015 -- 09:17:39 - <Info> - alert-debug output device (regular) initialized: alert-debug.log
20/5/2015 -- 09:17:39 - <Info> - Syslog output initialized
20/5/2015 -- 09:17:39 - <Info> - drop output device (regular) initialized: drop.log
20/5/2015 -- 09:17:39 - <Info> - binding this thread 0 to queue '0'
20/5/2015 -- 09:17:39 - <Info> - setting queue length to 4096
20/5/2015 -- 09:17:39 - <Info> - setting nfnl bufsize to 6144000
20/5/2015 -- 09:17:39 - <Info> - fail-open mode should be set on queue
20/5/2015 -- 09:17:39 - <Info> - stream "max-sessions": 262144
20/5/2015 -- 09:17:39 - <Info> - stream "prealloc-sessions": 32768
20/5/2015 -- 09:17:39 - <Info> - stream "memcap": 33554432
20/5/2015 -- 09:17:39 - <Info> - stream "midstream" session pickups: disabled
20/5/2015 -- 09:17:39 - <Info> - stream "async-oneside": disabled
20/5/2015 -- 09:17:39 - <Info> - stream "checksum-validation": enabled
20/5/2015 -- 09:17:39 - <Info> - stream."inline": enabled
20/5/2015 -- 09:17:39 - <Info> - stream.reassembly "memcap": 67108864
20/5/2015 -- 09:17:39 - <Info> - stream.reassembly "depth": 1048576
20/5/2015 -- 09:17:39 - <Info> - stream.reassembly "toserver-chunk-size": 2560
20/5/2015 -- 09:17:39 - <Info> - stream.reassembly "toclient-chunk-size": 2560
20/5/2015 -- 09:17:39 - <Info> - all 3 packet processing threads, 3 management threads initialized,
engine started.
```

set interface ให้อยู่ใน mode promisc

$sudo ifconfig eth0 promisc

set ip6tables ให้อยู่ใน mode nfqueue

$sudo ip6tables -I FORWARD -j NFQUEUE

9.3 การทดสอบ IPS/IDS

สร้าง rules เพื่อทดสอบ alert

$sudo vi /etc/suricata/rules/user.rules

```
alert ip any any -> any any (msg:"ICMP detected"; sid:2; rev:1;)
```

$sudo nmap -6 -p1-65535 -sV -sS -O localhost ; การ scan port เพื่อทดสอบ suricata

$sudo tail -f /var/log/suricata/fast.log ; เช็คจาก log ของ suricata

```
05/20/2015-09:17:40.275311  [**] [1:2:1] ICMP detected [**] [Classification: (null)] [Priority: 3]
{IPv6-ICMP} 2001:0db8:x:0000:0000:0000:0000:0007:128 ->
2404:6800:4001:0800:0000:0000:0000:1011:0
05/20/2015-09:20:54.847477  [**] [1:2:1] ICMP detected [**] [Classification: (null)] [Priority: 3]
{IPv6-ICMP} 2001:0db8:x:0000:0000:0000:0000:0007:128 ->
2001:0f00:1fff:0002:0000:0000:0000:0005:0
```

การ dump packet ipv6

```
$sudo tcpdump -i eth0 -vv ip6
```

การสร้าง rules เพื่อ drop packet

$sudo vi /etc/suricata/rules/user.rules

```
drop ip any any -> any any (msg:"ICMP detected"; sid:2; rev:1;)
```

เริ่มโปรแกรม suricata ใหม่เพื่อให้ทำการ drop packet

```
sudo suricata -c /etc/suricata/suricata.yaml -q 0
```

ตรวจสอบจาก fast.log ของ suricata

$sudo tail -f /var/log/suricata/fast.log ; เช็คจาก log ของ suricata

```
05/20/2015-09:45:16.441312  [Drop] [**] [1:2:1] ICMP detected [**] [Classification: (null)]
[Priority: 3] {IPv6-ICMP} 2001:0db8:x:0000:0000:0000:0000:0007:128 ->
2404:6800:4001:0802:0000:0000:0000:1013:0
```

อ้างอิง

1 .https://sites.google.com/site/thanawateiei996/ids-ips

2. http://www.aldeid.com/wiki/Suricata-vs-snort

3. https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_Installation

4. https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Basic_Setup

5. https://www.howtoforge.com/how-to-set-up-an-ips-intrusion-prevention-system-on-fedora-17

6. http://samiux.blogspot.com/2013/01/howto-suricata-on-ubuntu-1204-lts-server.html

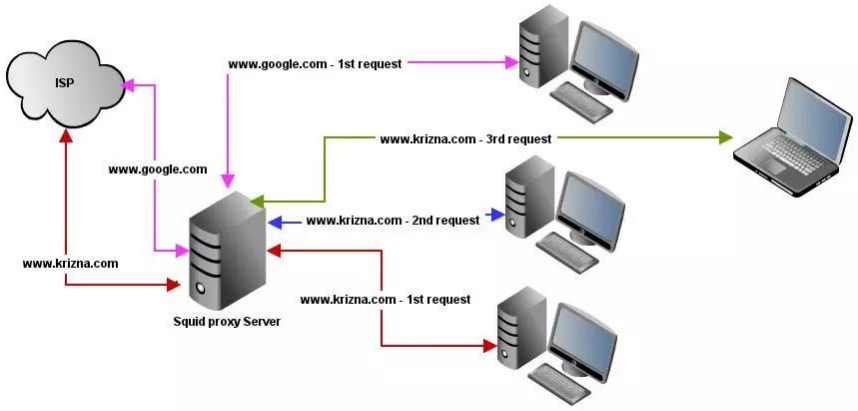
7. http://taosecurity.blogspot.com/2014/01/suricata-20beta2-as-ips-on-ubuntu-1204.html

หัวข้อที่ 10 Proxy Server

10.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

Proxy Server คือเครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการต่างๆ แทนเครื่องเซิร์ฟเวอร์จริงๆ ที่ตั้งอยู่ในอินเตอร์เน็ต ซึ่งมีหน้าที่สำหรับเก็บข้อมูลที่ผู้ใช้บริการได้เรียกข้อมูลมาจากอินเตอร์เน็ต โดยผ่านทาง web browser ทำให้ผู้ใช้บริการรายต่อไปที่ต้องการค้นหาข้อมูลเดิมซ้ำกับที่มีผู้อื่นเรียกใช้บริการไว้ สามารถที่จะเรียกดูข้อมูลจากเครื่องแม่ข่าย Proxy Server ได้โดยตรง โดยไม่ต้องร้องขอข้อมูลจากอินเตอร์เน็ตซึ่งจะช่วยลดปริมาณของการร้องขอข้อมูลลงได้

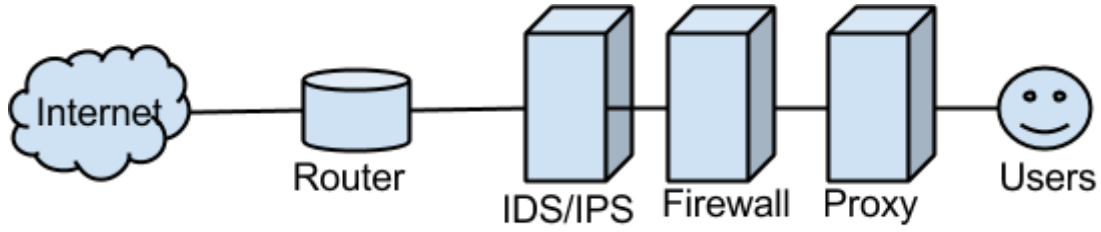
ขั้นตอนการทำงานของ Proxy Server นั้นเริ่มขึ้นเมื่อผู้ใช้ติดต่อ web sever ผ่าน Proxy Server เครื่องจะทำการตรวจสอบก่อนว่ามีข้อมูลที่ผู้ใช้ต้องการอยู่ในเครื่องอยู่แล้วหรือไม่ ถ้ายังไม่มีก็จะไปเรียกข้อมูลมาให้ใหม่ และจัดเก็บไว้ในเครื่องเพื่อคอยให้บริการแก่ผู้ใช้ครั้งต่อไป แต่หากพบว่ามี Proxy Server จะทำการตรวจสอบว่าข้อมูลที่มีอยู่กับแหล่งข้อมูลที่ต้องการ ว่ามีความทันสมัยตรงกันหรือไม่ ถ้าข้อมูลตรงกันจะทำการส่งข้อมูลที่มีอยู่ในเครื่องไปให้ผู้ใช้ทันที แต่ถ้าไม่ตรงกัน Proxy จะไปดึงข้อมูลจากแหล่งข้อมูลมาให้ใหม่ ซึ่งการทำงานในลักษณะนี้คล้ายกับการทำงานของ Cache ในคอมพิวเตอร์ นั่นคือเป็นทางผ่านก่อนเชื่อมต่อออกสู่อินเตอร์เน็ต โดยเมื่อเข้าเว็บเพจจากเครื่องลูกข่ายที่เชื่อมผ่าน proxy จะช่วยให้ดาวน์โหลดได้รวดเร็วกว่าปกติ ในกรณีที่เว็บดังกล่าวนั้นเคยเข้ามาก่อนแล้ว เพราะข้อมูลที่เคยเข้าถูกเก็บไว้ใน proxy server



รูปที่ 10.1 หลักการทำงานของ Proxy Server

10.2 รูปแบบการใช้งาน

การนำ Testbed หรือ Server นี้ไปใช้งานในเครือข่ายอย่างไร แสดงถึงการเชื่อมต่อ



รูปที่ 10.2 รูปแบบการเชื่อมต่อ Proxy

10.3 การติดตั้ง

10.3.1 ความต้องการของระบบ

CPU: Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz

RAM: 1024MB

HDD: 50GB

Required Software: squid

10.3.2 การเตรียมความพร้อมก่อนการติดตั้ง

Linux Ubuntu 14.04LTS

$sudo apt-get update

$sudo apt-get install build-essential bison autoconf

10.3.3 ขั้นตอนการติดตั้ง

- การติดตั้ง squid proxy

  $sudo apt-get install squid

  $cd /etc/squid3/

  $sudo vi /etc/squid3/squid.conf

```
acl localnet src 2001:db8:x::/48
http_access allow localnet
```

$sudo service squid3 restart

- การทดสอบหลังการติดตั้ง

  $sudo ps aux | grep squid

```
proxy     7801  0.0  1.9 113212 19912 ?        Ss   14:22   0:00 /usr/sbin/squid3 -N -YC -f
/etc/squid3/squid.conf
proxy     7803  0.0  0.1  12672  1064 ?        Ss   14:22   0:00 (logfile-daemon) /var/log/squid3/access.log
```

$sudo tail -f /var/log/squid3/cache.log

```
2015/05/20 14:22:36| Loaded Icons.
2015/05/20 14:22:36| HTCP Disabled.
2015/05/20 14:22:36| Pinger socket opened on FD 11
2015/05/20 14:22:36| Squid plugin modules loaded: 0
2015/05/20 14:22:36| Adaptation support is off.
2015/05/20 14:22:36| Accepting HTTP Socket connections at local=[::]:3128 remote=[::] FD 9 flags=9
2015/05/20 14:22:36| pinger: Initialising ICMP pinger ...
2015/05/20 14:22:36| pinger: ICMP socket opened.
2015/05/20 14:22:36| pinger: ICMPv6 socket opened
2015/05/20 14:22:37| storeLateRelease: released 0 objects
```

10.4 การ Config เพื่อรองรับ IPv6

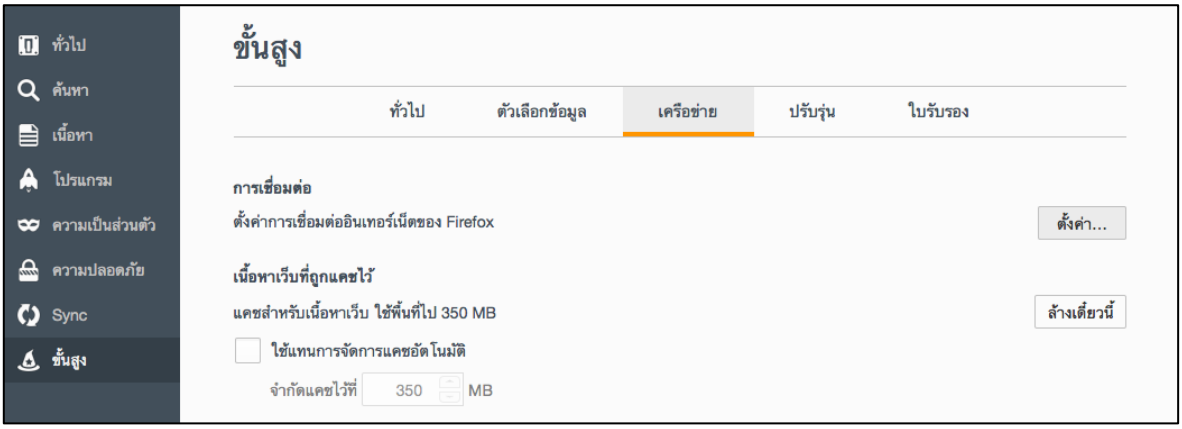
10.4.1 squid รองรับ ipv6 แล้วไม่ต้องปรับแก้อะไร

$sudo netstat -nlptu

```
tcp6       0      0 :::3128                 :::*                    LISTEN      7801/squid3
```

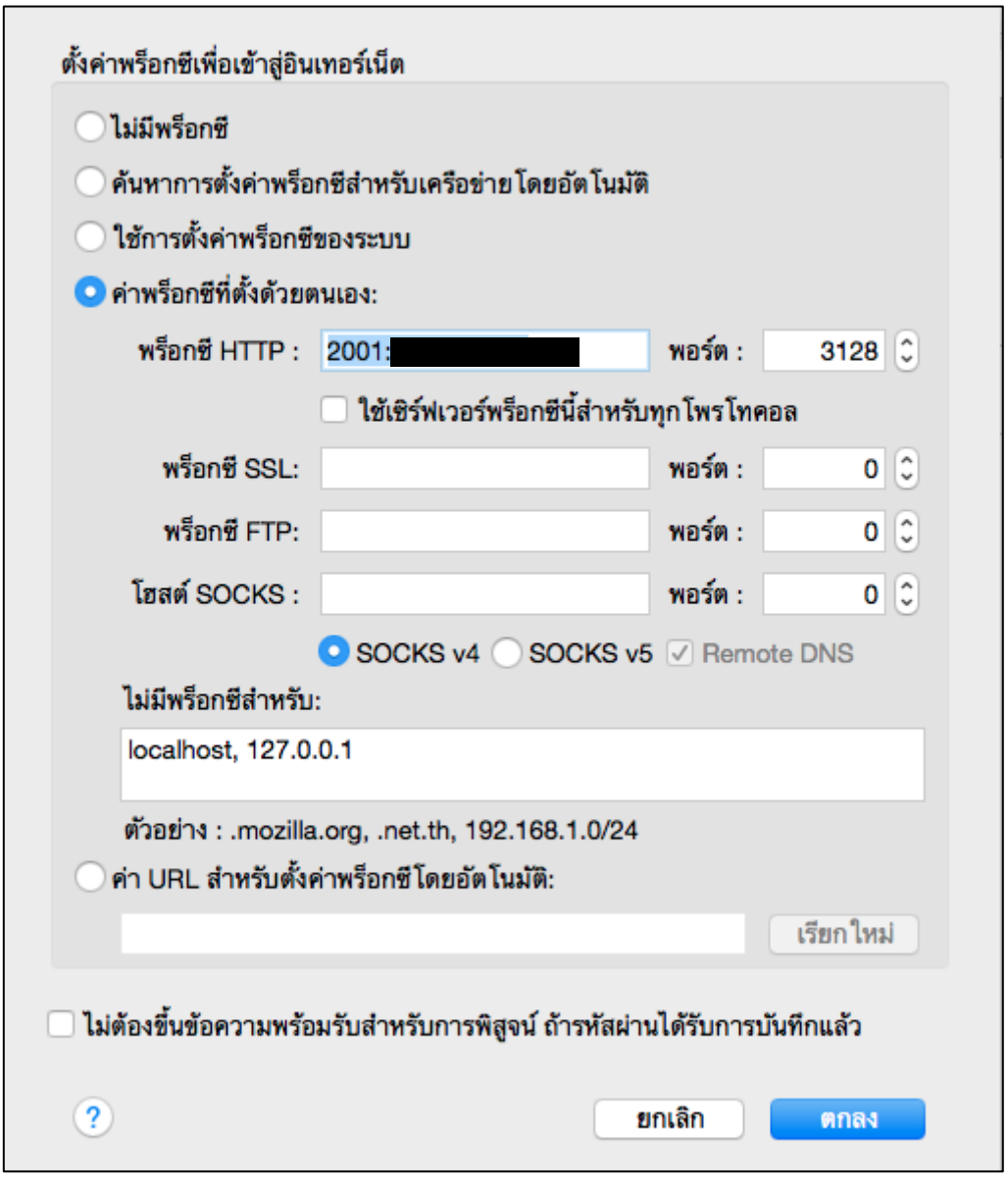
10.5 วิธีการใช้งาน

เครื่องผู้ใช้งานเปิด browser ในตัวอย่าง firefox แล้วเข้าไปยังตั้งค่า



รูปที่ 10.3 เครื่องผู้ใช้งานเปิด brower ในตัวอย่าง firefox แล้วเข้าไปยังตั้งค่า

ตั้งค่าการเชื่อมต่อกดตั้งค่า



รูปที่ 10.4 ตั้งค่าการเชื่อมต่อกดตั้งค่า

10.6 การทดสอบ

$sudo tail -f /var/log/squid3/access.log

```
1432108238.013    620 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 3698 POST
http://ocsp.apple.com/ocsp04-appleistca2g101 - HIER_DIRECT/2001:db8:x:x:ffff:0:1197:1c05
application/ocsp-response

1432108238.026    692 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 3698 POST
http://ocsp.apple.com/ocsp04-appleistca2g101 - HIER_DIRECT/2001:db8:x:x:ffff:0:1197:1c05
application/ocsp-response

1432108239.893    1142 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 3698 POST
```

http://ocsp.apple.com/ocsp04-appleistca2g101 - HIER_DIRECT/2001:db8:x:x:ffff:0:1197:1c05 application/ocsp-response

1432108242.119 286 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 2226 POST http://evsecure-ocsp.verisign.com/ - HIER_DIRECT/2001:db8:x:x:ffff:0:172c:9b1b application/ocsp-response

1432108242.343 228 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 2226 POST http://evsecure-ocsp.verisign.com/ - HIER_DIRECT/2001:db8:x:x:ffff:0:172c:9b1b application/ocsp-response

1432108242.380 248 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 2270 POST http://sb.symcd.com/ - HIER_DIRECT/2001:db8:x:x:ffff:0:172c:9b1b application/ocsp-response

1432108242.402 62 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 921 POST http://ocsp.digicert.com/ - HIER_DIRECT/2001:db8:x:x:ffff:0:7512:ed1d application/ocsp-response

1432108242.571 215 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 2270 POST http://sb.symcd.com/ - HIER_DIRECT/2001:db8:x:x:ffff:0:172c:9b1b application/ocsp-response

1432108252.640 216 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 2193 POST http://sd.symcd.com/ - HIER_DIRECT/2001:db8:x:x:ffff:0:172c:9b1b application/ocsp-response

1432108252.931 728 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 912 POST http://clients1.google.com/ocsp - HIER_DIRECT/2404:6800:4001:806::200e application/ocsp-response

1432108253.446 88 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 912 POST http://clients1.google.com/ocsp - HIER_DIRECT/2404:6800:4001:806::200e application/ocsp-response

10.7 การเพิ่มการกำหนดสิทธิ์ในการใช้งาน

10.7.1 แก้ไขไฟล์คอนฟิก

$sudo vi /etc/squid3/squid.conf

```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid3/passwd
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 4 hours
auth_param basic casesensitive off
acl foo proxy_auth REQUIRED
http_access allow foo
#acl localnet src 2001:db8:x::/48
#http_access allow localnet
```

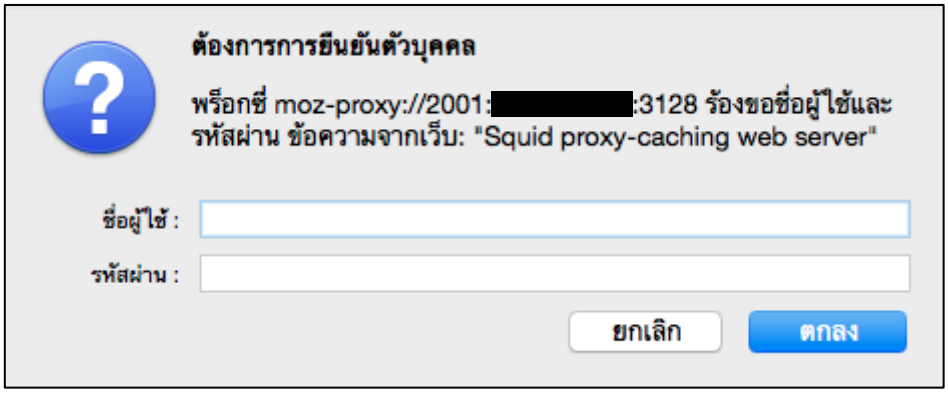
$sudo service squid3 restart

10.7.2 สร้าง user สำหรับเข้าใช้ proxy

$sudo htpasswd -c /etc/squid3/passwd user1

$sudo chmod o+r /etc/squid3/passwd

10.8 ทำการทดสอบการเข้าใช้ proxy ของผู้ใช้



รูปที่ 10.5 แสดงการยืนยันตัวบุคคล

10.8.1 ให้กรอกชื่อผู้ใช้และรหัสผ่านเพื่อเข้าใช้งาน

10.8.2 เช็คการเข้าใช้งานจาก log squid

$sudo tail -f /var/log/squid3/access.log

```
eusiphonetab/1/H.27/s28661686080489? user1 HIER_DIRECT/2001:db8:x:x:ffff:0:42eb:8ac3
image/gif
1432109115.422    602 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 61189 GET
http://images.apple.com/iphone/home/images/promos/promo_iphone_business_large.png
user1 HIER_DIRECT/2600:140b:13::b833:c6c0 image/png
1432109115.522    704 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 153167 GET
http://images.apple.com/iphone/home/images/promos/promo_tile_researchkit_large.jpg
user1 HIER_DIRECT/2600:140b:13::b833:c6c0 image/jpeg
1432109115.673    935 2001:db8:x:x:d53f:666:8649:45ae TCP_MISS/200 265770 GET
http://images.apple.com/v/iphone/home/n/images/hero_large.jpg user1
HIER_DIRECT/2600:140b:13::b833:c6c0 image/jpeg
```

อ้างอิง

1. http://www.mindphp.com/คู่มือ/73-คืออะไร/2097-proxy-server-คืออะไร.html
2. www.squid-cache.org
3. http://wiki.squid-cache.org/Features/Authentication

หัวข้อที่ 11 464xlat

11.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

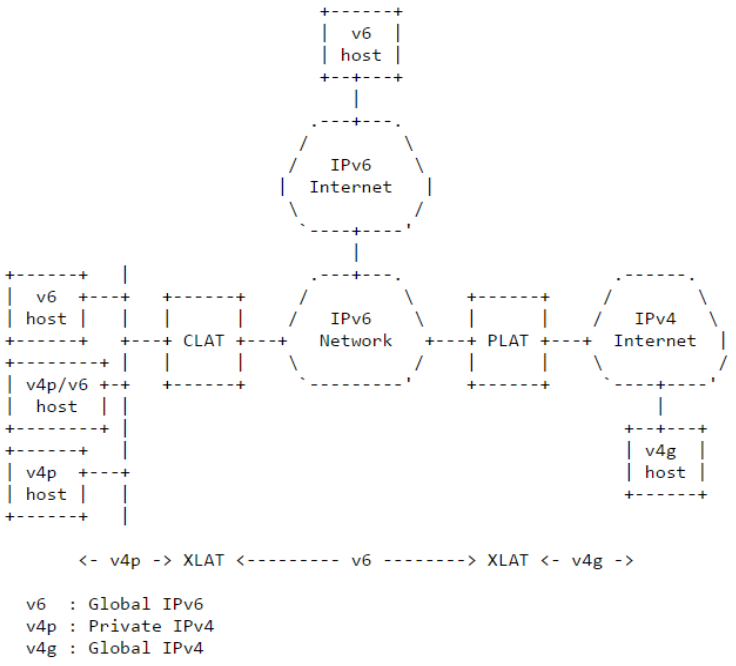
464xlat เป็นกระบวนการเปลี่ยนถ่ายที่ใช้สำหรับสร้างการเชื่อมต่อ IPv4 ผ่านเครือข่าย IPv6 464xlat รองรับการใช้งาน IPv4 รูปแบบ client-server เท่านั้น ซึ่ง server ต้องใช้งาน Public IPv4 address 464xlat เป็นกระบวนการเปลี่ยนถ่ายแบบ double-translation กล่าวคือมีการ translation ด้วย NAT46 และ NAT64 ควบคู่ไปด้วยกันเพื่อส่งข้อมูลผ่านเครือข่าย IPv6 เนื่องจากเป็นการดำเนินการแบบ double-translation, 464xlat จึงไม่จำเป็นต้องใช้งาน DNS64 เพิ่มเติม อุปกรณ์ที่ดำเนินการ translation ฝั่งผู้ใช้งานเรียกว่า Customer-side translator (CLAT) และอุปกรณ์ที่ดำเนินการ translation ฝั่งผู้ให้บริการเรียกว่า Provider-side translator (PLAT) CLAT ทำหน้าที่จับคู่ private IPv4 address กับ IPv6 address แบบ 1:1 ส่วน PLAT ทำหน้าที่จับคู่ IPv6 address กับ public IPv4 address แบบ N:1

11.2 รูปแบบการใช้งาน

รูปแบบการใช้งาน 464xlat แบ่งออกเป็นสองรูปแบบด้วยกัน ได้แก่ wireline network และ wireless 3GPP network

11.2.1 wireline network

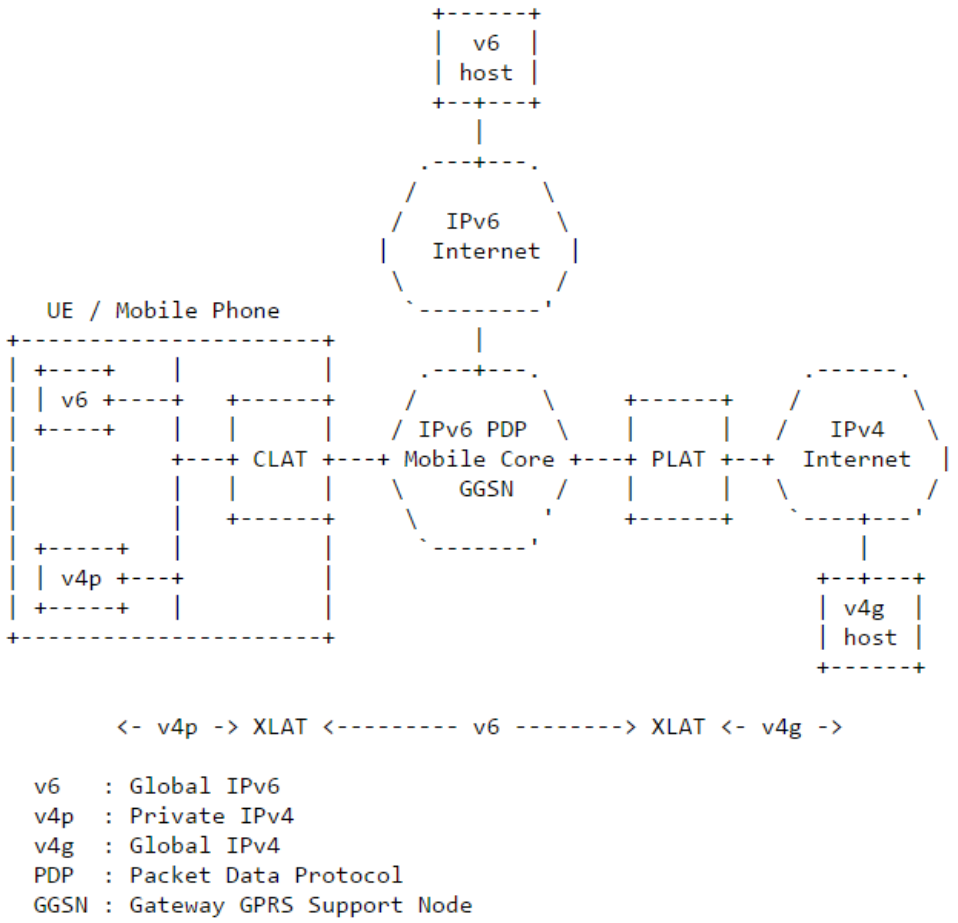
ในรูปแบบนี้, private IPv4 host สามารถติดต่อไปยัง IPv4 internet ได้โดยอาศัยการ translate บน CLAT และ PLAT สำหรับ IPv6 host สามารถติดต่อไปยัง IPv6 internet ได้โดยตรง ในรูปแบบนี้เกตเวย์ของผู้ใช้งาน (CPE) ไม่เพียงแต่ต้องรองรับหลักการทำงานของ CLAT แต่ยังต้องสามารถเป็น IPv6 router เพื่อจัดการ IPv6 traffic ทั้งหมด



รูปที่ 11.1 464xlat แบบ wireline network

11.2.2 wireless 3GPP network

ในรูปแบบนี้, อุปกรณ์ของผู้ใช้งานต้องรองรับหลักการทำงานของ CLAT โดยอุปกรณ์ของผู้ใช้งานจะใช้ private IPv4 address และกำหนด default route ไปยัง local network stack ของตนเอง (สร้าง IPv4 default route ไปยังอีก interface ของตนเอง)



รูปที่ 11.2 464xlat แบบ wireless 3GPP network

สำหรับซอฟแวร์ที่จำเป็นต่อการให้บริการ 464xlat แบ่งออกเป็น 3 กลุ่ม คือ

- **PLAT**

  ecdysis (http://ecdysis.viagenie.ca/)

  TAYGA (http://www.litech.org/tayga/)

  linuxnat64

  OpenBSD PF

  Cisco Systems ---- Cisco ASR1000 Series (IOS-XE 3.4.0S～)

  Juniper Networks ---- SRX Series (JUNOS 10.4～)

  A10 Networks ---- AX Series (ACOS 2.6.4～)

  F5 Networks ---- BIG-IP Series (11.1～)

- **CLAT ใน 3GPP network (mobile)**

  Android (https://android-review.googlesource.com/#/c/34490)

  Nokia (https://code.google.com/p/n900ipv6/wiki/README)

- **CLAT ใน wireline network**

  มีเพียง vendor ที่พัฒนาอุปกรณ์ออกมา แต่มีการนำ TAYGA มาประยุกต์ใช้เป็น CLAT

  TAYGA (http://www.litech.org/tayga/)

11.3 การติดตั้ง 464xlat

464xlat ในการทดลองได้ทดลองเพียงรูปแบบเดียวคือ wireline network เนื่องจากไม่สามารถทดลองบน 3GPP network ได้ ข้อมูลในการติดตั้งและ config ทั้งหมดจึงเป็นรูปแบบ wireline network เพียงอย่างเดียว

11.3.1 การติดตั้ง PLAT (ecdysis NAT64)

M1: ecdysis Linux live CD (http://ecdysis.viagenie.ca/download/ecdysis-fedora- 20-x86_64-20140422.iso)

M2: download sourcecode: (http://ecdysis.viagenie.ca/download/ecdysis-openbsd -4.6-amd64-20100226.tar.gz

```
$./configure
$make
$sudo make install
```

11.3.2 การติดตั้ง CLAT (TAYGA NAT46)

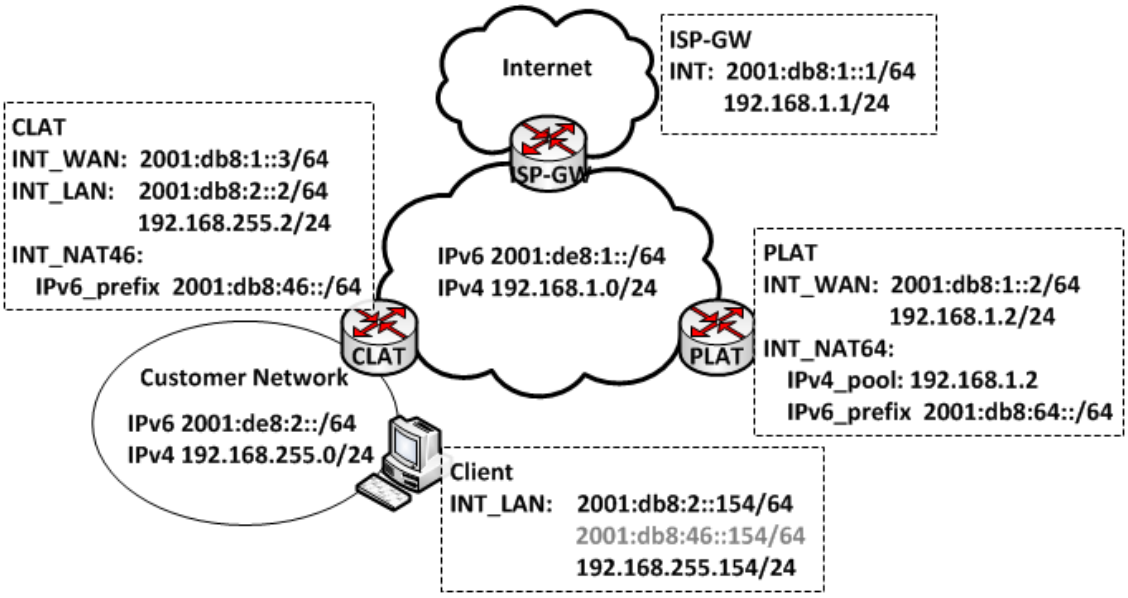
download sourcecode: (http://www.litech.org/tayga/tayga-0.9.2.tar.bz2)

```
$./configure
$make
$sudo make install
```

11.4 Configuration

เนื่องจาก TAYGA เป็น stateless translation และไม่ได้ถูกเขียนมาเพื่อใช้เป็น NAT46 โดยเฉพาะ การนำมาใช้งานจริงจำเป็นจะต้องทำการจับคู่ IPv4 address ของ client ในเครือข่ายผู้ใช้งานกับ IPv6 address แบบ manual ซึ่งไม่เหมาะกับการให้บริการเมื่อมี client จำนวนมาก และนอกจากนี้ ในเครือข่ายผู้ใช้งานที่ใช้ TAYGA เป็น CLAT นั้นต้องการ IPv6 prefix 2 ชุดด้วยกัน ชุดแรก /64 สำหรับใช้งาน IPv6 native ชุดที่สอง /96 ใช้สำหรับ NAT46 เนื่องจาก TAYGA ดำเนินการ NAT แบบ stateless จึงไม่

สามารถแยกแยะได้ว่า IPv6 address สำหรับ NAT46 ออกจาก Native จึงต้องกำหนดให้ใช้งาน IPv6 prefix 2 ชุด หากไม่ใช้งาน IPv6 prefix 2 ชุดก็จะไม่สามารถเชื่อมต่อ IPv6 Native ได้



รูปที่ 11.3 รูปแบบเครือข่ายที่ใช้ทดสอบ 464xlat

11.4.1 PLAT configuration (ecdysis Linux live CD)

ตั้งค่า IP address

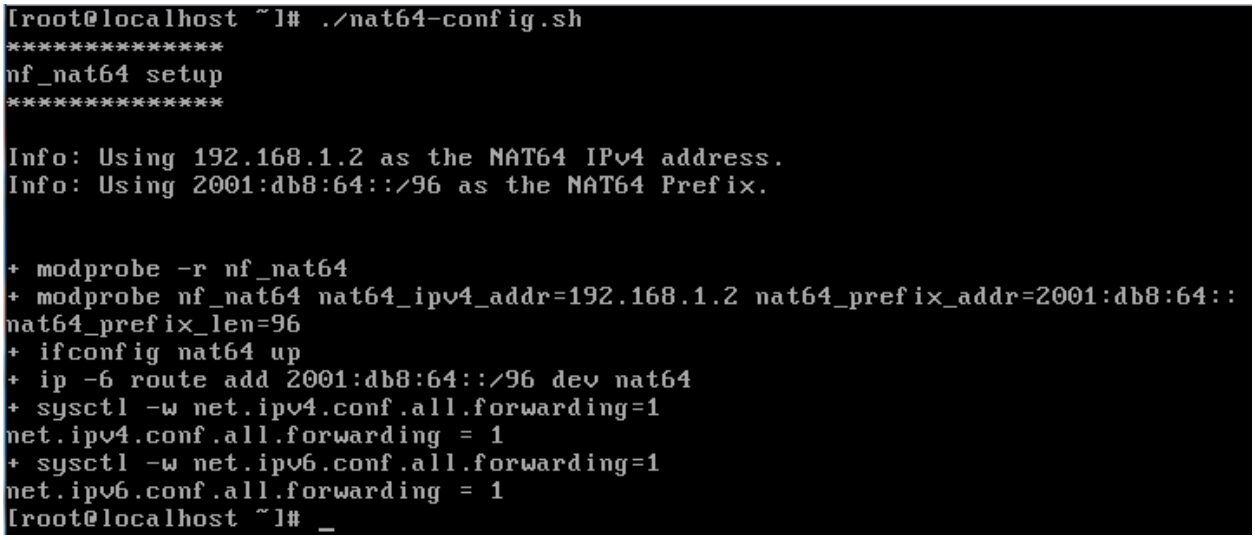
```
$ip addr add 192.168.1.2/24 broadcast 192.168.1.255 dev WAN
$ip addr add 2001:db8:1::2/64 dev WAN
$ip -6 route add 2001:db8:46::/64 via 2001:db8:1::3   [route to CLAT]
```

แก้ไขไฟล์คอนฟิกสำหรับใช้งาน /root/nat64-config.sh

```
IPV4_ADDR=“192.168.1.2”
PREFIX_ADDR=“2001:db8:64::”
PREFIX_LEN=“96”
```

รัน ecdysis (หากการตั้งค่าไม่ถูกต้องหรือไม่ได้ตั้งค่า IP โปรแกรมจะแจ้งเตือน)

```
$./nat64-config.sh
```



รูปที่ 11.4 ผลลัพธ์จากการรัน ecdysis

ทดสอบ ecdysis NAT64

$ping6 2001:db8:64::192.168.1.2

(2001:db8:64:: คือ NAT64 prefix, 192.168.1.2 คือ Destination IPv4 address)

11.4.2 CLAT configuration

ตั้งค่า IP address

```
$ip addr add 2001:db8:1::3/64 dev WAN
$ip addr add 192.168.255.2/24 broadcast 192.168.255.255 dev LAN
$ip addr add 2001:db8:2::2/64 dev LAN
$ip -6 route add 2001:db8:64::/64 via 2001:db8:1::2   [route to PLAT]
```

แก้ไขไฟล์คอนฟิกสำหรับใช้งาน /usr/local/etc/tayga.conf

```
tun-device CLAT
ipv4-addr 192.168.255.1
prefix 2001:db8:46::/96
data-dir /var/db/tayga
#ห้าม map 192.168.255.1  กับ IPv6 อื่นๆ
#dynamic-pool 192.168.255.0/24 ใช้ map แบบ static แทน
map 192.168.255.2 2001:db8:46::2
map 192.168.255.154 2001:db8:46::154
```

ตั้งค่าสำหรับ tayga

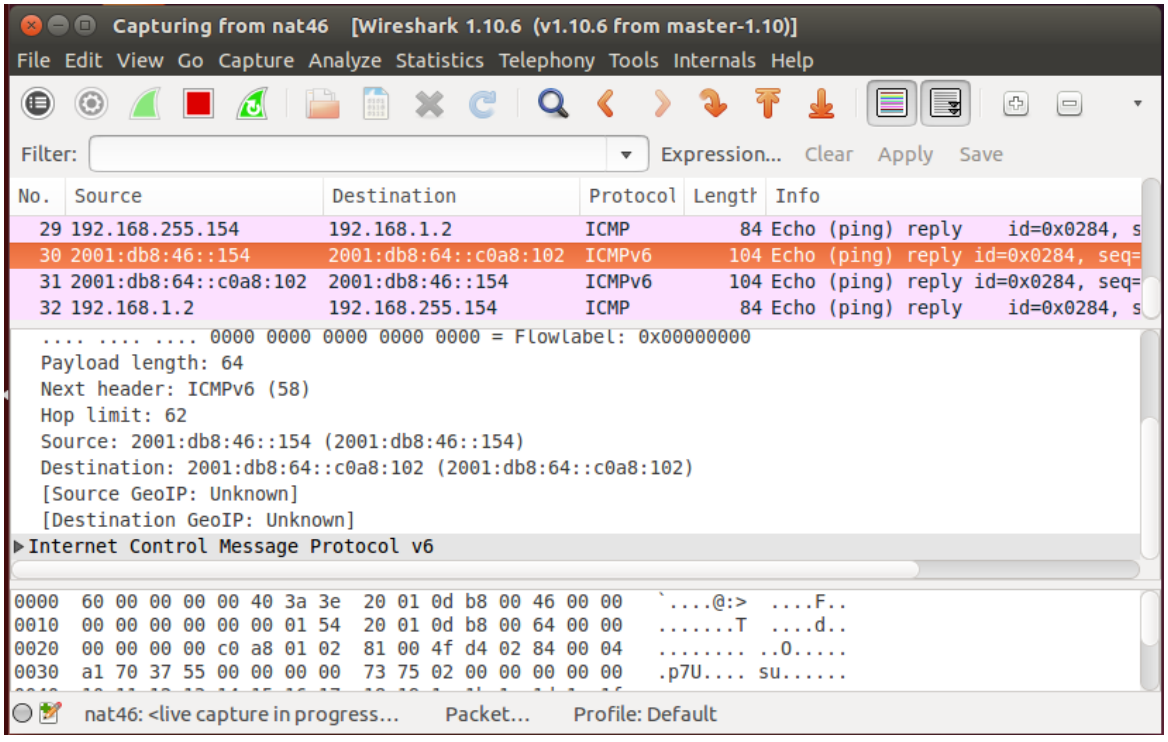
```
$tayga --mktun
$sysctl -w net.ipv4.conf.all.forwarding=1
$sysctl -w net.ipv6.conf.all.forwarding=1
$ip link set dev CLAT up
[$ip addr add 192.168.255.2 dev CLAT]
$ip -4 route add default dev CLAT
$ip -6 route add 2001:db8:46::/64 dev CLAT
$tayga
```

ทดสอบ nat46 (tayga)

```
$ping 192.168.1.2
```

11.5 การทดสอบ

ทดสอบโดยคำสั่ง ping ไปยังเครื่องปลายทาง 192.168.1.2 (ซึ่งเป็น Wan Interface ของ Plat) แล้วใช้ wireshark ตรวจสอบการรับส่งข้อมูล โดย wireshark แสดงให้เห็นว่า ICMP ถูกแปลงเป็น ICMPv6 ที่ CLAT แล้วส่งต่อไปยัง PLAT เมื่อ ICMPv6 ถูกส่งมายัง PLAT ก็จะถูกแปลงกลับไปเป็น ICMP เช่นเดิม เพื่อส่งไปยังเครื่องปลายทางต่อไป



รูปที่ 11.5 ผลลัพธ์การดักจับ ICMP packet ด้วย wireshark

หัวข้อที่ 12 osTicket

12.1 ความรู้และทฤษฎีที่เกี่ยวข้อง

osTicket เป็นซอฟแวร์ แบบ Open Source ที่เป็นระบบ Ticket Support ซอฟแวร์ตัวนี้สามารถโหลดมาใช้งานได้ฟรี แต่เป็นเว็บแอพพลิเคชั่น นั่นหมายถึงว่าคุณต้องมีเว็บเซิร์ฟเวอร์ และมีความรู้ความเข้าใจกับการปรับแต่งค่าต่างๆเล็กน้อยเพื่อให้โปรแกรมได้ทำงานได้ตรงตามความต้องการ osTicket มีคุณสมบัติค่อนข้างครบถ้วน

12.2 การติดตั้ง

12.2.1 ความต้องการของระบบ

Required Software: HTTP server running Microsoft® IIS or Apache
PHP version 5.3 or greater
mysqli extension for PHP
MySQL database version 5.0 or greater

12.2.2 การเตรียมความพร้อมก่อนการติดตั้ง

ตัวเซิร์ฟเวอร์นั้นใช้ระบบปฏิบัติการ Ubuntu 14.04.1 LTS โดยจะต้องติดตั้ง LAMP และ phpMyAdmin ให้พร้อมก่อนดังนี้

1. การอัพเดต Repository

การอัพเดต Repository ของ Ubuntu เพื่อให้รายชื่อ Package ต่างๆ ของระบบนั้นเป็นรุ่นล่าสุด สามารถทำได้โดยการรันคำสั่งดังต่อไปนี้

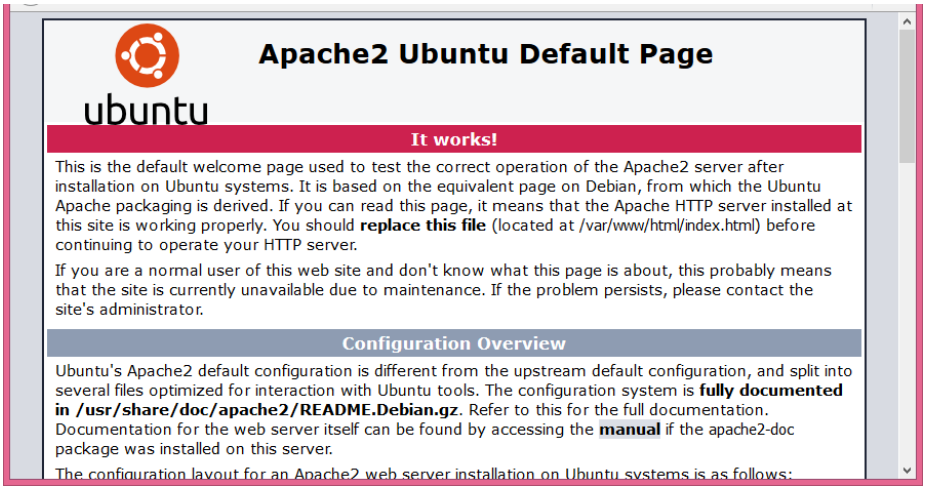
```
# apt-get update
```

2. การติดตั้งl Apache

Apache เป็น Web Service ที่จำเป็นสำหรับการรัน PHP Website ในการติดตั้งให้รันคำสั่งดังต่อไปนี้

```
# apt-get install apache2
```

เมื่อติดตั้งเสร็จแล้ว สามารถทดสอบการทำงานของบริการ Apache ได้โดยการป้อนหมายเลย IPv6 ลงไปในช่อง URL ของ browser ดังเช่น http://[2001:db8:x::20c:29ff:fe1a:d686] ก็จะได้ผลลัพธ์ดังรูปด่านล่าง



รูปที่ 12.1 Default Page ของ Apache บน Ubuntu

3. การติดตั้ง MySQL

MySQL เป็นระบบการบริหารและจัดการฐานข้อมูลสำหรับเว็บไซต์ตัวหนึ่ง ที่นิยมใช้กันอย่างแพร่หลาย โดยสามารถติดตั้งได้ดังนี้

```
# apt-get install mysql-server mysql-client
```

โดยระหว่างการติดตั้งจะมีหน้าจอขึ้นมาถามรหัสผ่านของชื่อผู้ใช้งาน root ซึ่งสามารถตั้งค่าได้ตามต้องการ และเมื่อการติดตั้งเสร็จสมบูรณ์แล้ว เราสามารถทดสอบการทำงานได้ดังนี้

```
# mysql -u root -p
Enter password:
mysql> exit
#
```

เมื่อพิมพ์คำสั่งบรรทัดแรกไปตัว MySQL ก็จะถามรหัสผ่าน ให้ใส่รหัสผ่าน ที่ได้ตั้งไว้ หากรหัสผ่านถูกต้องก็จะเข้าสู่ Prompt ของ MySQL และสามารถพิมพ์คำสั่ง exit เพื่อออกจากโปรแกรม

4. การติดตั้ง PHP

PHP เป็นภาษาที่ใช้ในการสร้างหน้าเว็บแบบ Dynamic การติดตั้งสามารถทำได้ โดยการรันคำสั่งดังต่อไปนี้

```
# apt-get install php5
```

เมื่อติดตั้งเสร็จแล้วสามารถตรวจสอบได้ว่า PHP ได้ทำการติดตั้งลงไปแล้ว ดังคำสั่งดังด้านล่าง ซึ่งก็จะปรากฏรุ่นของโปแกรมที่ได้ติดตั้งลงไป

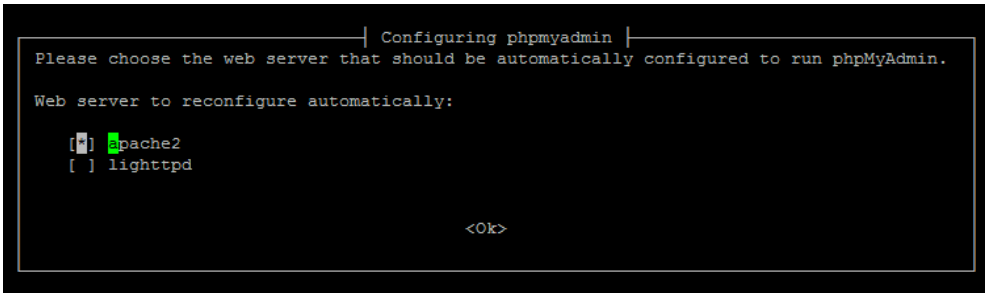
```
# php -v
```

5. การติดตั้ง phpMyAdmin

phpMyAdmin เป็นเครื่องมือที่ช่วยให้นักพัฒนาเว็บไซต์สามารถบริหาร และจัดการฐานข้อมูล MySQL ได้โดยผ่านหน้าเว็บ ซึ่งจะทำให้สะดวกกว่า การใช้งานผ่าน Prompt ในการติดตั้งสามารถทำได้ดังต่อไปนี้

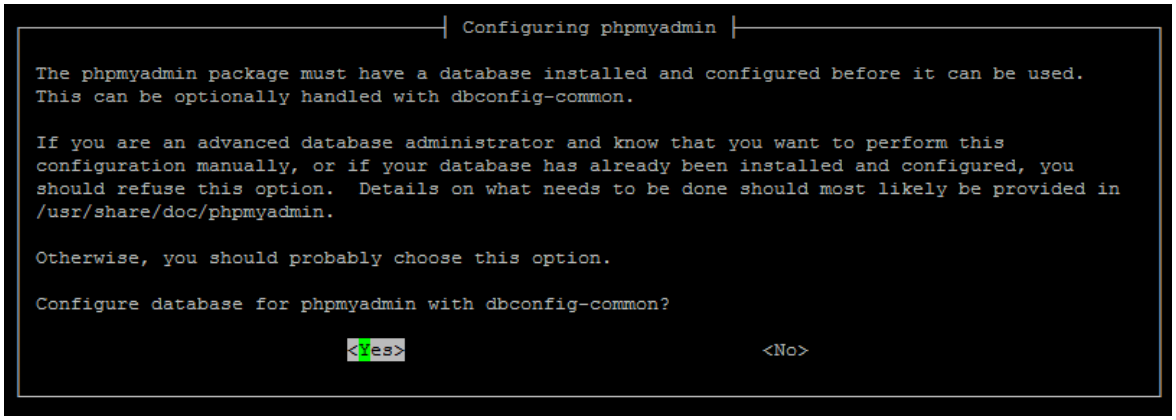
```
# apt-get install phpmyadmin
```

ระหว่างการติดตั้งจะมีการถามว่าจะใช้ Web Service ตัวใดในการรัน phpMyAdmin ให้เลือก apache2 ดังรูปด้านล่าง



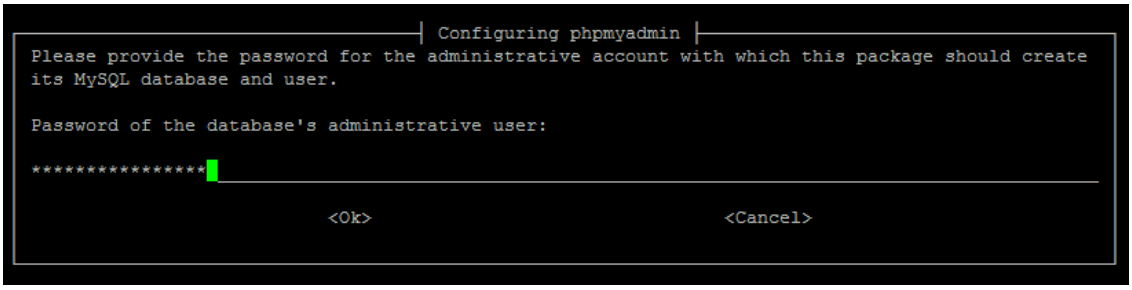
รูปที่ 12.2 การตั้งค่า phpmyadmin

จากนั้นจะมีหน้าต่างถามต่อไป ให้ตอบ Yes เพื่อทำการสร้างฐานข้อมูลสำหรับตัว phpMyAdmin ดังรูปด้านล่าง



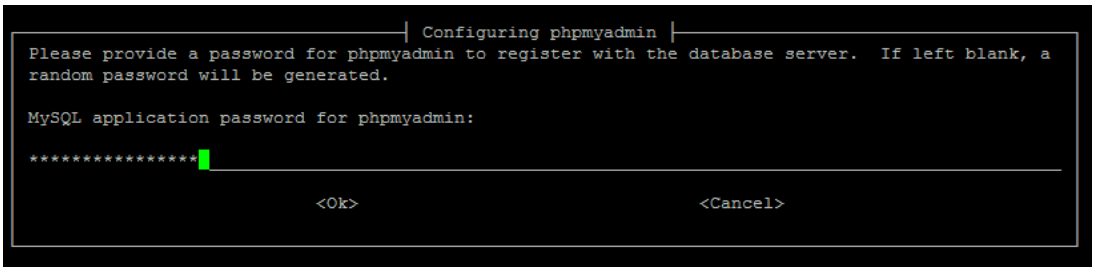
รูปที่ 12.3 การตั้งค่า phpmyadmin: configure database for phpmyadmin

เสร็จแล้วจะมีหน้าต่างขึ้นมาถามรหัสผ่านของชื่อผู้ใช้งาน root ที่โปรแกรมจะใช้ สำหรับการเข้าถึงฐานข้อมูล MySQL เพื่อสร้างข้อมูลของตัวเอง



รูปที่ 12.4 การตั้งค่า phpmyadmin: Password of database's administrative user

จากนั้นก็จะเป็นถามรหัสผ่านของชื่อผู้ใช้งาน phpmyadmin ที่กำลังจะสร้าง ขึ้นมาใหม่สำหรับการใช้งาน phpMyAdmin โดยจะต้องกรอกสองครั้ง เพื่อยืนยันความถูกต้องของรหัสผ่าน



รูปที่ 12.5 การตั้งค่า phpmyadmin: MySQL application password สำหรับ phpmyadmin

12.2.3 ขั้นตอนการติดตั้ง osTicket

ในการติดตั้ง osTicket รุ่น 1.9.5.1 สามารถทำได้ดังต่อไปนี้

1. การสร้างฐานข้อมูลสำหรับ osTicket

ขั้นแรกจะเป็นการสร้างฐานข้อมูล osticket โดยมีชื่อผู้ใช้งานคือ osticket และรหัสผ่านคือ xxxxxxxx ซึ่งสามารถทำได้ดังคำสั่งต่อไปนี้

```
# mysql -u root -p
mysql> CREATE DATABASE osticket CHARACTER SET utf8 COLLATE
utf8_bin;
mysql> GRANT ALL PRIVILEGES on osticket.* TO osticket@localhost
IDENTIFIED BY 'xxxxxxxx';
mysql > FLUSH PRIVILEGES;
```

จากนั้นสามารถตรวจสอบสิทธิของผู้ใช้งาน osticket และรายชื่อฐานข้อมูล ที่ได้สร้างไว้ดังคำสั่งต่อไปนี้

```
mysql > SHOW GRANTS FOR osticket@localhost;
mysql> SHOW DATABASES;
mysql > Exit
```

2. การติดตั้งแพ็กเกจ PHP ที่จำเป็นสำหรับ osTicket

osTicket นั้นต้องการแพ็กเกจ php5-imap สำหรับการใช้งานระบบอีเมล์ โดยสามารถติดตั้งได้ดังนี้

```
# apt-get install php5-imap
# php5enmod imap
# service apache2 reload
```

3. การดาวน์โหลดไฟล์ติดตั้ง osTicket

ทำการดาวน์โหลดไฟล์ osTicket-v1.9.5.1.zip จากเว็บไซต์หลัก และแตกไฟล์ ไปที่ /var/www/osticket ดังคำสั่งต่อไปนี้

```
# cd /opt/
# wget http://www.osticket.com/sites/default/files/download/osTicket-v1.9.5.1.zip
# cp -r osTicket-v1.8.1.2.zip  /var/www/
# cd /var/www/
# mkdir osticket
# unzip osTicket-v1.9.5.1.zip -d osticket
```

4. การสร้าง shortcut จากโฟลเดอร์โปรแกรมไปยังโฟลเดอร์ root ของ Apache

ในขั้นตอนนี้จะทำการสร้าง shortcut จากโฟลเดอร์ upload ของ osTicket ไปยังชื่อโฟลเดอร์ tickets ซึ่งตั้งอยู่บนโฟลเดอร์ root ของ Apache คือ /var/www/html โดยสามารถทำได้ดังคำสั่งต่อไปนี้

```
# ln -s /var/www/osticket/upload /var/www/html/tickets
```

5. การสร้างไฟล์คอนฟิกครั้งแรกสำหรับ osTicket

ให้ทำการคัดลอกตัวอย่างไฟล์คอนฟิก ost-sampleconfig.php ไปเป็น ost-config.php สำหรับใช้งานจริง และทำการกำหนดสิทธิของไฟล์ ให้สามารถแก้ไขได้ผ่านหน้าเว็บ ดังคำสั่งต่อไปนี้

```
# cd /var/www/html/tickets
# cp include/ost-sampleconfig.php include/ost-config.php
# chmod 666 include/ost-config.php
```

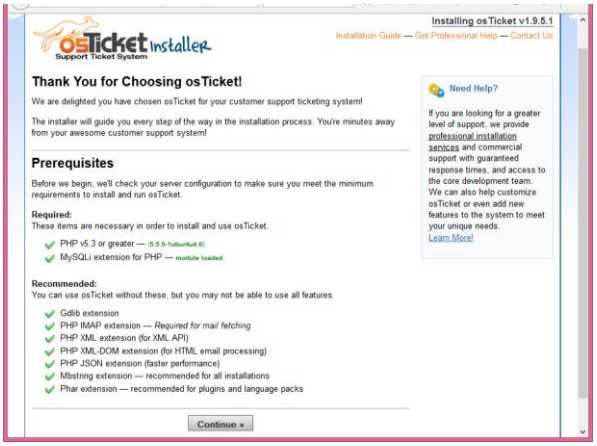
6. การเริ่มบริการ Apache ใหม่

หลังจากจัดเตรียมไฟล์ติดตั้งของ osTicket เสร็จเรียบร้อยแล้ว ให้ทำการเริ่มบริการ Apache ใหม่ เพื่อให้มีการอัพเดตข้อมูลหน้าเว็บ osTicket ดังคำสั่งต่อไปนี้

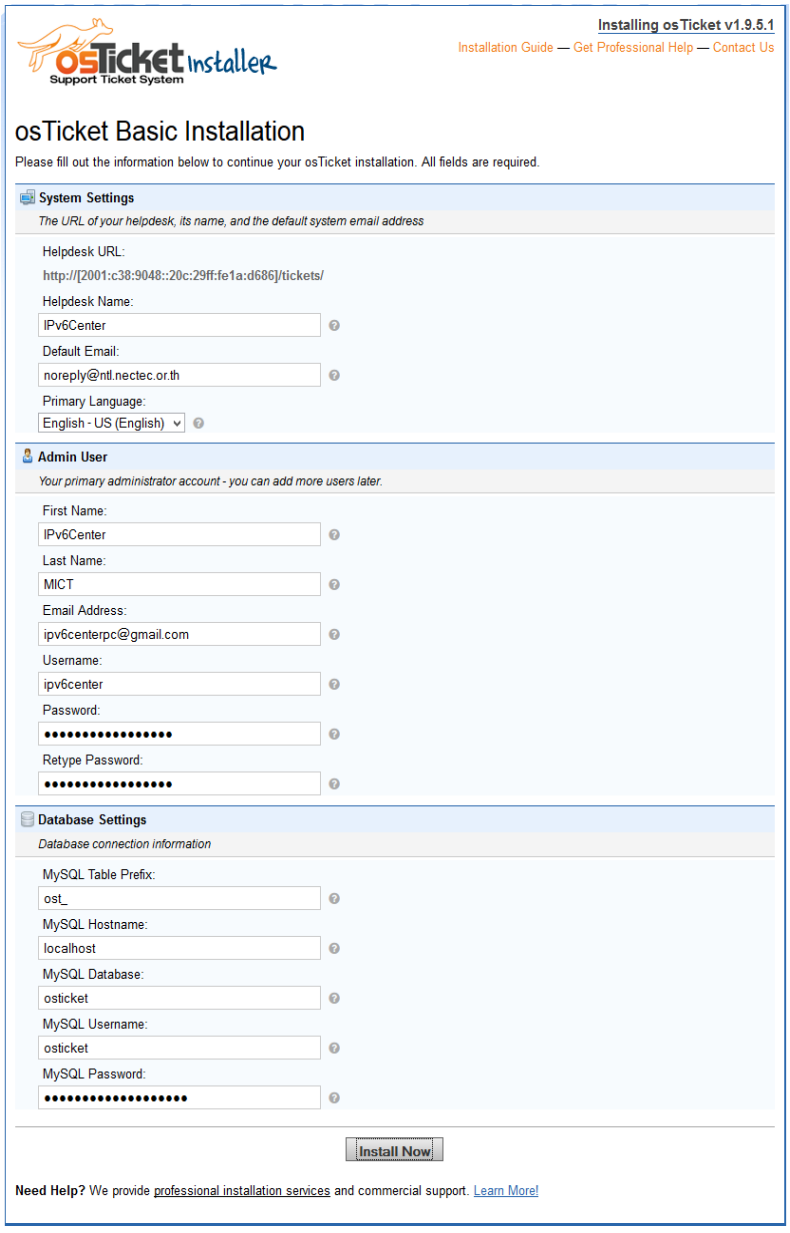
```
# /etc/init.d/apache2 restart
```

7. การติดตั้ง osTicket ผ่านหน้าเว็บ

ในการเริ่มต้นขั้นตอนการติดตั้ง osTicket นั้นสามารถทำได้โดยการกรอก URL ดังด้านล่าง http://[2001:db8:x::20c:29ff:fe1a:d686]/tickets/setup/ โดยจะปรากฏหน้าเว็บแรกดังรูปด้านล่าง ให้คลิก Continue เพื่อเริ่มการติดตั้ง



รูปที่ 12.6 การติดตั้ง osTicket

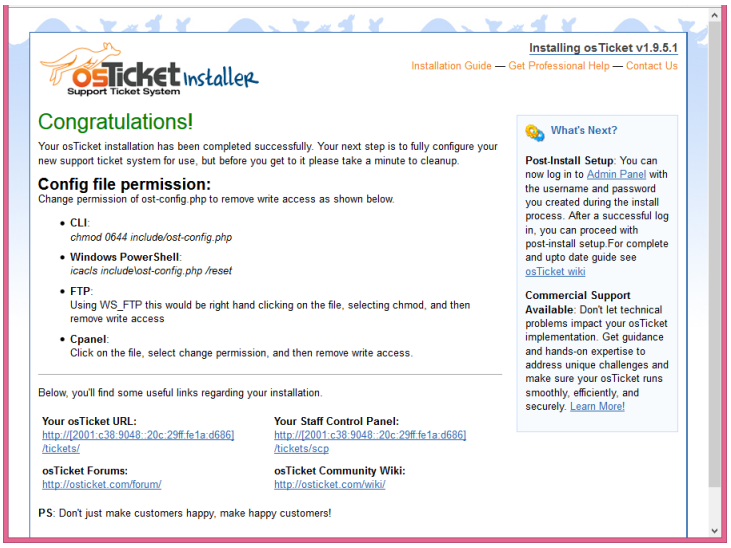


รูปที่ 12.7 การติดตั้ง osTicket: กำหนดข้อมูลสำหรับ osTicket

โดยในการติดตั้ง osTicket จะต้องกรอกข้อมูลทั้งหมด 3 ส่วน ดังต่อไปนี้

1) System Settings เป็นการตั้งค่าพื้นฐานของระบบ
   - Helpdesk URL: เป็นลิงค์หน้า Helpdesk ของ osTicket
   - Helpdesk Name: เป็นชื่อของ Helpdesk
   - Default Email: เป็นอีเมล์ของระบบที่ใช้ในการส่งข้อมูลแจ้งเตือนต่างๆ
   - Primary Language: เป็นภาษาหลักของ osTicket
2) Admin User เป็นการตั้งค่าบัญชีผู้ดูแลระบบ
   - First Name: เป็นชื่อแรกของบัญชีผู้ดูแลระบบ
   - Last Name: เป็นนามสกุลของบัญชีผู้ดูแลระบบ
   - Email Address: เป็นอีเมล์ของบัญชีผู้ดูแลระบบ
   - Username: เป็นชื่อผู้ใช้ของบัญชีผู้ดูแลระบบ
   - Password: เป็นรหัสผ่านของบัญชีผู้ดูแลระบบ
   - Retype Password: เป็นรหัสผ่านของบัญชีผู้ดูแลระบบ
3) Database Settings เป็นการตั้งค่าการเชื่อมต่อฐานข้อมูล
   - MySQL Table Prefix: เป็นคำนำหน้าของตารางสำหรับ osTicket
   - MySQL Hostname: เป็นชื่อโฮสต์ของ MySQL Server
   - MySQL Database: เป็นชื่อฐานข้อมูลที่ได้สร้างไว้ก่อนหน้านี้
   - MySQL Username: เป็นชื่อผู้ใช้สำหรับฐานข้อมูลข้างต้น
   - MySQL Password: เป็นรหัสผ่านสำหรับฐานข้อมูลข้างต้น

โดยเมื่อกรอกข้อมูลครบถ้วนแล้ว ให้คลิกปุ่ม Install Now เพื่อทำการติดตั้ง หลังการติดตั้งเสร็จสมบูรณ์ก็จะปรากฏหน้าเว็บดังรูปต่อไปนี้



รูปที่ 12.8 การติดตั้ง osTicket : เริ่มการติดตั้ง osTicket

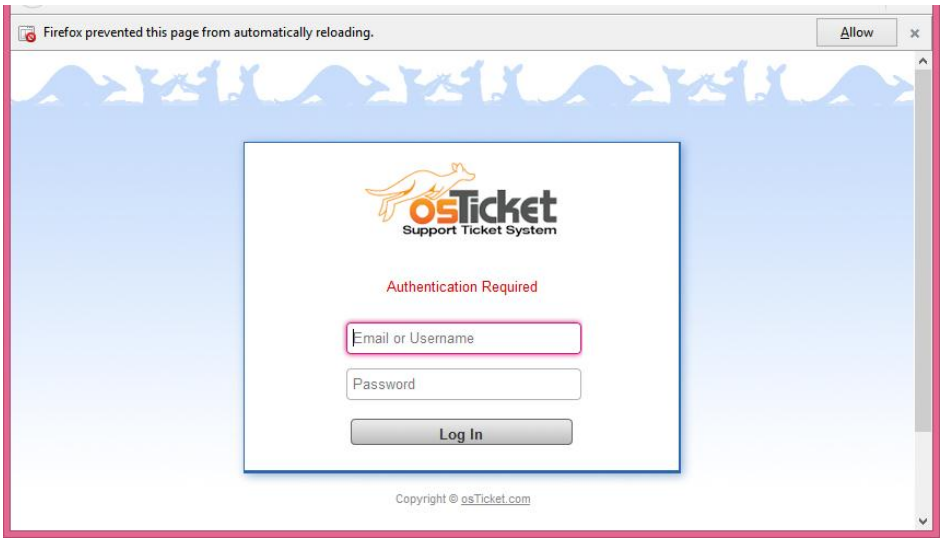
8. การป้องกันการติดตั้ง osTicket ซ้ำจากผู้ใช้คนอื่น

เพื่อป้องการผู้ไม่ประสงค์ดีเข้ามาแก้ไขข้อมูลในไฟล์คอนฟิกของ osTicket จึงต้องทำการกำหนดสิทธิให้คนที่ไม่ใช่เจ้าของไฟล์ทำได้เพียงอ่านของมูลเพียงอย่างเดียว และทำการเปลี่ยนชื่อโฟลเดอร์ setup เป็นชื่ออื่นเพื่อป้องกันการติดตั้งซ้ำ

```
# chmod 0644 include/ost-config.php
# cd /var/www/html/tickets
# mv setup setup-old-150310
```

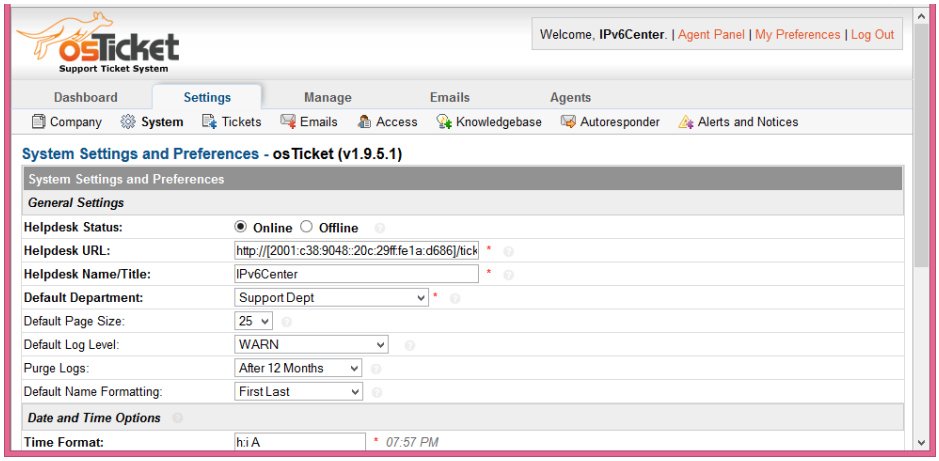
9. การเข้าสู่ระบบเพื่อใช้งาน osTicket

ในการ Log In เพื่อเริ่มต้นใช้งาน osTicket ให้กรอก URL ดังด้านล่างลงไปใน browser http://[2001:db8:x::20c:29ff:fe1a:d686]/tickets/scp/ จากนั้นให้กรอกอีเมล์หรือชื่อผู้ใช้พร้อมทั้งรหัสผ่านที่ได้กำหนดไปในการติดตั้ง แล้วให้คลิกปุ่ม Log In เพื่อเข้าสู่ระบบ



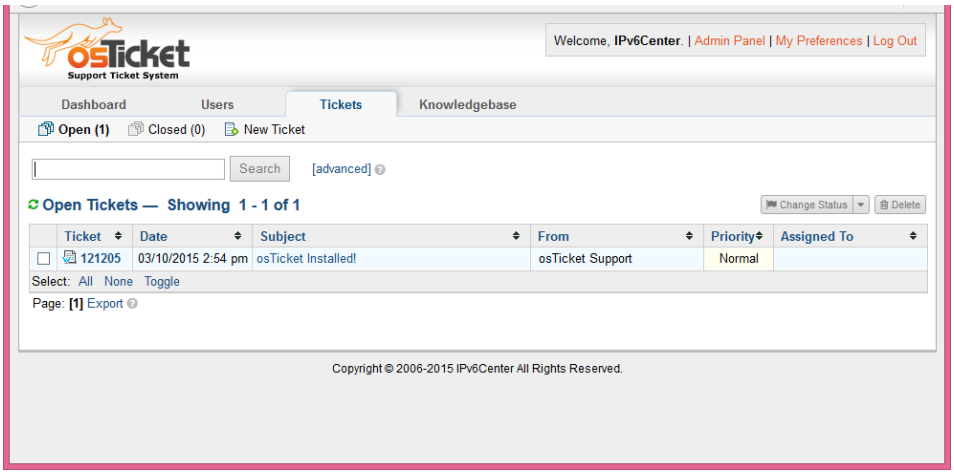
รูปที่ 12.9 การใช้งาน osTicket: Log in ไม่ถูกต้อง

โดยหากข้อมูลล๊อกอินถูกต้องก็จะปรากฏหน้าเว็บของบัญชีผู้ดูแลระบบดังรูปต่อไปนี้



รูปที่ 12.10 การใช้งาน osTicket: หน้าเว็บของบัญชีผู้ดูแลระบบ

สำหรับหน้าเว็บของการใช้งาน Ticket นั้นให้คลิกที่เมนู Agent Panel บริเวณมุมบนขวาจะปรากฏหน้าเว็บขึ้นมาดังรูปต่อไปนี้



รูปที่ 12.11 การใช้งาน osTicket: Agent Panel

อ้างอิง

1) http://engineerbabu.com/2014/09/how-to-install-lamp-in-ubuntu/
2) http://engineerbabu.com/2014/09/install-phpmyadmin-ubuntu-14-04-lts/
3) http://lwathcrunch.blogspot.com/2014/02/install-osticket-in-your-ubuntu.html

หัวข้อที่ 13 การตั้งค่า IPv6 สำหรับ Router Wireless Access Point และ Printer

13.1 การตั้งค่า IPv6 สำหรับ Router

หัวข้อนี้จะกล่าวถึงข้อมูลการตั้งค่า IPv6 สำหรับ Gateway Router ของศูนย์ประสานงานและปฏิบัติการ IPv6 โดย Gateway Router ใช้เป็น Cisco Router 1841 จากข้อมูลด้านล่าง ด้านซ้ายคือ configuration ที่ใช้งานบน Gateway Router ส่วนด้านขวาคือคำอธิบายการตั้งค่า

Configuration	Description
Building configuration... Current configuration : 1828 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec service password-encryption ! hostname GDC151384 ! boot-start-marker boot-end-marker ! logging buffered 4096 debugging enable password 7 03075A1F2606315A180A1C0B031719 ! aaa new-model ! ! ! aaa session-id common ip cef ! !	
ip domain name ns.ipv6.testbed.local	กำหนด DNS server IPv4
ip name-server 8.8.8.8	กำหนด DNS server IPv6
ip name-server 2001:4860:4860::8888	กำหนด DNS server IPv6
ip name-server 2001:db8:x::3	กำหนด DNS server IPv6
ip auth-proxy max-nodata-conns 3 ip admission max-nodata-conns 3 !	
ipv6 unicast-routing	เปิดใช้งาน IPv6 unicast-routing
ipv6 dhcp pool dhcp-pool	กำหนดข้อมูลสำหรับ dhcp-pool

dns-server 2001:4860:4860::8888	กำหนด DNS server IPv6
!	
ipv6 dhcp pool IPv6centerPool	กำหนดข้อมูลสำหรับ IPv6centerPool
prefix-delegation pool IPv6centerPrefix lifetime 86400 86400	กำหนด IPv6 prefix = IPv6centerPrefix
dns-server 2001:db8:x::3	กำหนด DNS server IPv6
!	
!	
!	
username ipv6 password 7	
03075A1F2606315A180A1C0B031719	
!	
!	
ip ssh authentication-retries 5	
!	
!	
interface FastEthernet0/0	ตั้งค่า WAN-to-CAT
description WAN-to-CAT	คำอธิบาย interface
ip address x.x.x.x 255.255.255.252	ตั้งค่า IPv4 address
duplex auto	
speed auto	
ipv6 address 2001:db8:x:x::9931:2/64	ตั้งค่า IPv6 address
!	
interface FastEthernet0/1	ตั้งค่า LAN-to-CUSTOMER
description LAN-to-CUSTOMER	คำอธิบาย interface
ip address x.x.x.x 255.255.255.240	ตั้งค่า IPv4 address
duplex auto	
speed auto	
ipv6 address 2001:db8:x::1/64	ตั้งค่า IPv6 address
ipv6 enable	
ipv6 dhcp server IPv6centerPool	ตั้งค่า IPv6 DHCP โดยเรียกใช้ pool: IPv6centerPool
!	
ip forward-protocol nd	
ip route 0.0.0.0 0.0.0.0 x.x.x.x	กำหนด IPv4 default route
!	
!	
no ip http server	
no ip http secure-server	
!	
!	
!	
ipv6 route 2001:db8:x:x::/64 2001:db8:x::165	กำหนด IPv6 routing ภายในสำหรับ AP
ipv6 route 2001:db8:x:x:FFFF::/96 2001:db8:x::2	กำหนด IPv6 routing ภายในสำหรับ NAT64
ipv6 route 2001:db8:x:x::/64 2001:db8:x::2	กำหนด IPv6 routing ภายในสำหรับ NAT64

ipv6 route 2001:db8:x:x::/64 2001:db8:x::164 ipv6 route ::/0 2001:db8:x:x:10::9931:1 ipv6 local pool IPv6centerPrefix 2001:db8:x::/64 64 ! ! control-plane ! ! line con 0 line aux 0 line vty 0 4 password 7 130616062B05143C7D272D3D212701 logging synchronous transport input ssh ! scheduler allocate 20000 1000 end	กำหนด IPv6 routing ภายในสำหรับ AP: Native กำหนด IPv6 default route กำหนด IPv6 prefix สำหรับ IPv6centerPrefix กำหนดสิทธิการล๊อกอินรูปแบบต่างๆ

13.2 การตั้งค่า IPv6 สำหรับ Wireless Access Point

Wireless Access Point ของศูนย์ประสานงานและปฏิบัติการ IPv6 ใช้เป็น Linksys WRT54GL ซึ่งติดตั้ง firmware ของ OpenWRT 10.03.1 โดยการตั้งค่าสำหรับ Wireless Access Point ให้สามารถใช้งาน IPv6 ได้มีรายละเอียดดังต่อไปนี้

13.2.1 ติดตั้ง package IPv6 และ RADVD สำหรับ OpenWRT

1) ดาวน์โหลด package radvd_1.8.3-1_brcm47xx.ipk และ kmod-ipv6_2.6.32.27-1_brcm47xx.ipk ที่ http://downloads.openwrt.org/backfire/10.03.1/brcm47xx/packages/

2) คัดลอกไฟล์ไปยัง Wireless Access Point ด้วยคำสั่ง

```
scp radvd_1.8.3-1_brcm47xx.ipk root@192.168.2.1:/tmp
scp kmod-ipv6_2.6.32.27-1_brcm47xx.ipk root@192.168.2.1:/tmp
```

3) ล๊อกอินเข้าสู่ OpenWRT เพื่อทำการติดตั้ง package IPv6 และ RADVD

```
ssh root@192.168.2.1
$cd /tmp
$opkg install kmod-ipv6_2.6.32.27-1_brcm47xx.ipk
$opkg install radvd_1.8.3-1_brcm47xx.ipk
```

13.2.2 ตั้งค่า IPv6 สำหรับ WAN และ LAN Interface

1) ตั้งค่า IPv6 แบบ Dual Stack

$vi /etc/config/network (แก้ไขไฟล์ดังต่อไปนี้)

```
config 'interface' 'lan'
        option 'type' 'bridge'
        option 'ifname' 'eth0.0'
        option 'proto' 'static'
        option 'ipaddr' '192.168.1.1'
        option 'netmask' '255.255.255.0'
        option 'ip6addr' '2001:db8:x:x::2/64'

config 'interface' 'wan'
        option 'ifname' 'eth0.1'
        option '_orig_ifname' 'eth0.1'
        option '_orig_bridge' 'false'
        option 'proto' 'static'
        option 'ipaddr' 'x.x.x.165'
        option 'netmask' '255.255.255.240'
        option 'gateway' 'x.x.x.x.161'
        option 'dns' '8.8.8.8'
        option 'ip6addr' '2001:db8:x::165/64'
        option 'ip6gw' '2001:db8:x::1'
        option 'dns' '2001:db8:x::3'
```

$vi /etc/sysctl.conf (อนุญาตให้ forward IPv6)

```
net.ipv6.conf.all.forwarding=1
```

$vi /etc/config/radvd (ตั้งค่า RADVD เพื่อประกาศ IPv6 prefix, Gateway,DNS)

```
config interface
        option interface                'lan'
        option AdvSendAdvert            1
        option AdvManagedFlag           0
        option AdvOtherConfigFlag       0
        list client                     ''
        option AdvLinkMTU               1452
        option ignore                   0 #default 1
```

```
config prefix
        option interface        'lan'
        # If not specified, a non-link-local prefix of the interface is used
        list prefix             ''
        option AdvOnLink        1
        option AdvAutonomous    1
        option AdvRouterAddr    0
        option prefix           '2001:db8:x:x::/64'
        option ignore           0 #defaut 1

config route
        option interface        'lan'
        list prefix             ''
        option ignore           1

config rdnss
        option interface        'lan'
        # If not specified, the link-local address of the interface is used
        list addr               '2001:db8:x:x::2'
        option ignore           0 #default 1

config dnssl
        option interface        'lan'
        list suffix             ''
        option ignore           1
```

2) ตั้งค่า IPv6 แบบ Native

$vi /etc/config/network (แก้ไขไฟล์ดังต่อไปนี้)

```
config 'interface' 'lan'
        option 'type' 'bridge'
        option 'ifname' 'eth0.0'
        option 'proto' 'static'
        option 'netmask' '255.255.255.0'
        option 'ipaddr' '192.168.2.1'                   #ประกาศเพื่อให้ Mobile สามารถเชื่อมต่อเครือข่ายได้
        option 'ip6addr' '2001:db8:x:x::164/64'
        option 'dns' '2001:db8:x::3'
```

```
config 'interface' 'wan'
        option 'ifname' 'eth0.1'
        option 'proto' 'static'
        option 'ip6addr' '2001:db8:x::164/64'
        option 'ip6gw' '2001:db8:x::1'
        option 'dns' '2001:db8:x::3'
```

$vi /etc/sysctl.conf (อนุญาตให้ forward IPv6)

```
net.ipv6.conf.all.forwarding=1
```

$vi /etc/config/radvd (ตั้งค่า RADVD เพื่อประกาศ IPv6 prefix, Gateway,DNS)

```
config interface
        option interface        'lan'
        option AdvSendAdvert    1
        option AdvManagedFlag   0
        option AdvOtherConfigFlag 0
        list client             ''
        option AdvLinkMTU       1452
        option ignore           0 #default 1

config prefix
        option interface        'lan'
        # If not specified, a non-link-local prefix of the interface is used
        list prefix             ''
        option AdvOnLink        1
        option AdvAutonomous    1
        option AdvRouterAddr    0
        option prefix           '2001:db8:x:x::/64'
        option ignore           0 #defaut 1

config route
        option interface        'lan'
        list prefix             ''
        option ignore           1
```

```
config rdnss
        option interface        'lan'
        # If not specified, the link-local address of the interface is used
        list addr               '2001:db8:x::3'
        option ignore           0 #default 1

config dnssl
        option interface        'lan'
        list suffix             ''
        option ignore           1
```

13.3 การตั้งค่า IPv6 สำหรับ Printer

13.3.1 การตั้งค่า IPv6: Stateless Address บน Canon Printer

1. กดปุ่ม [Menu].
2. กดปุ่ม [◄—] or [+►] เพื่อเลือก <SYSTEM SETTINGS> แล้วกด [OK].
3. กดปุ่ม [◄—] or [+►] เพื่อเลือก <NETWORK SETTINGS> แล้วกด [OK].
4. กดปุ่ม [◄—] or [+►] เพื่อเลือก <TCP/IP SETTINGS> แล้วกด [OK].
5. กดปุ่ม [◄—] or [+►] เพื่อเลือก <IPv6 SETTINGS> แล้วกด [OK].
6. กดปุ่ม [◄—] or [+►] เพื่อเลือก <STATELESS ADD SET> แล้วกด [OK].
7. กดปุ่ม [◄—] or [+►] เพื่อเลือก <ON> แล้วกด [OK].

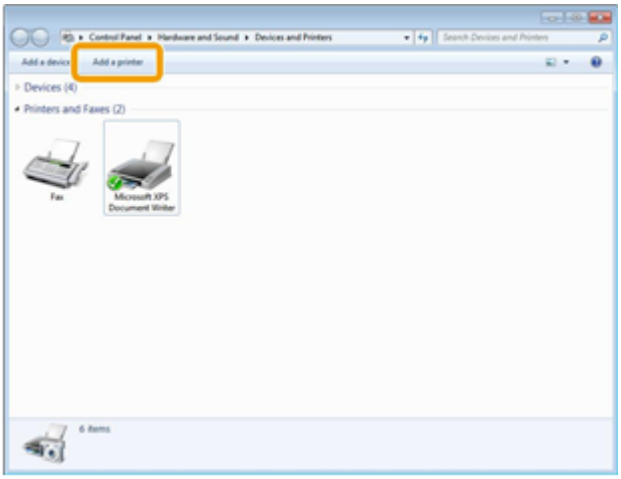
13.3.2 การติดตั้ง MF Drivers เพื่อใช้งานผ่าน Web Services on Devices (WSD) Network บน Windows 7

- **ติดตั้ง MF Drivers**

  1 แสดง Printers.

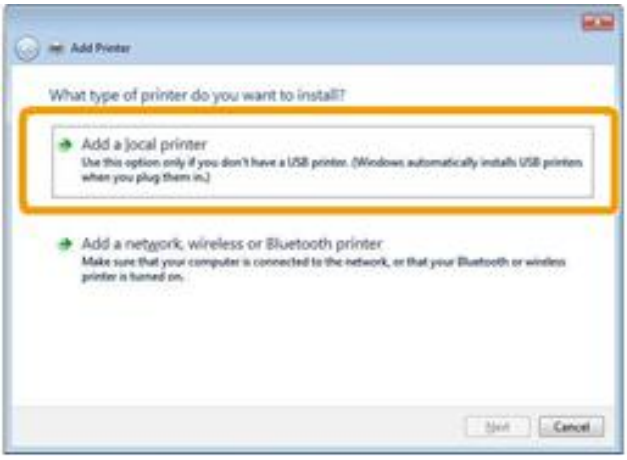
  คลิกเลือก [Start] แล้วเลือก [Devices and Printers].

  2 คลิก [Add a printer]



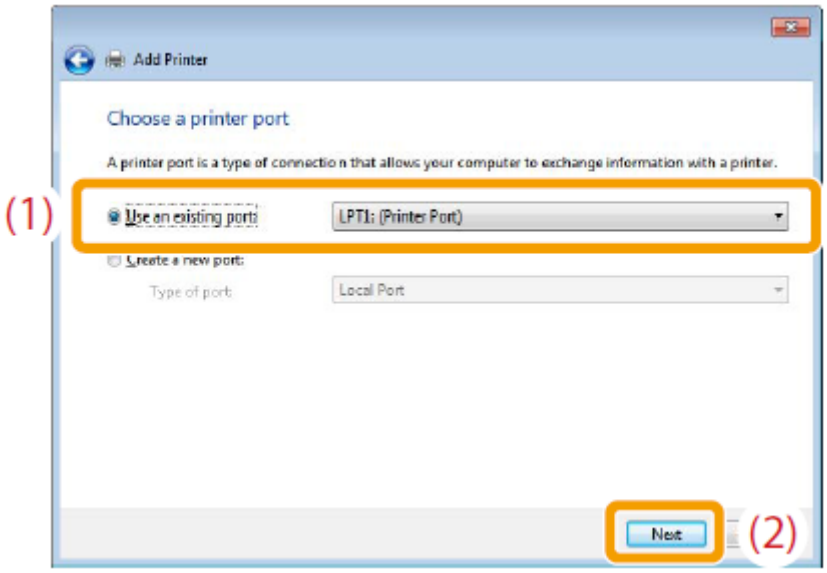
รูปที่ 13.1 ติดตั้ง MF Drivers

3 คลิก [Add a local printer].



รูปที่ 13.2 ติดตั้ง MF Drivers (2)

4 เลือก LPT1: (Printer Port) ใน [Use an existing port] แล้วคลิก [Next].



รูปที่ 13.3 ติดตั้ง MF Drivers (3)

5 คลิก [Have Disk].

รูปที่ 13.4 ติดตั้ง MF Drivers (4)

6 ใส่แผ่น Canon Software CD-ROM.

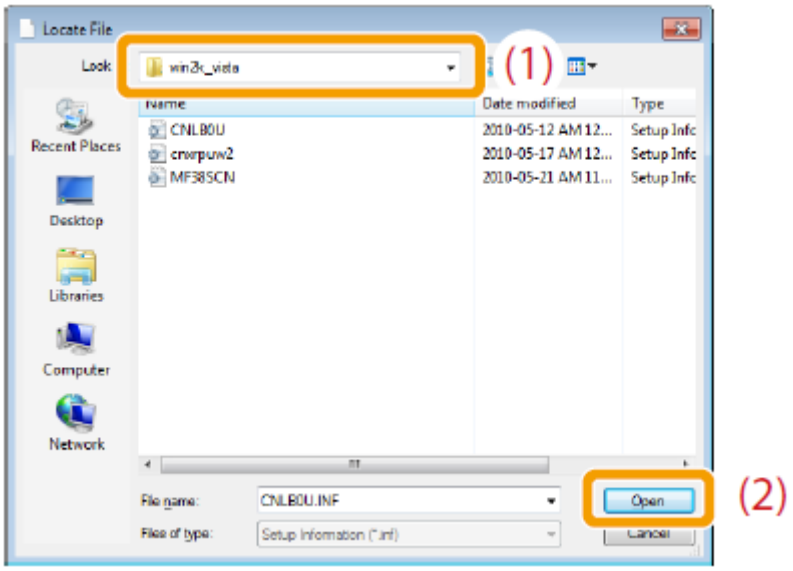
7 คลิก [Browse].

รูปที่ 13.5 ติดตั้ง MF Drivers (5)

8 เปิดโฟลเดอร์ [DRIVERS].

• สำหรับ 32-bit: [DRIVERS] -> [us_eng] -> [32bit] -> [win2k_vista] ใน CD-ROM, แล้วคลิก [Open].

• สำหรับ 64-bit: [DRIVERS] -> [us_eng] -> [x64] -> [Driver] ใน CD-ROM, แล้วคลิก [Open].

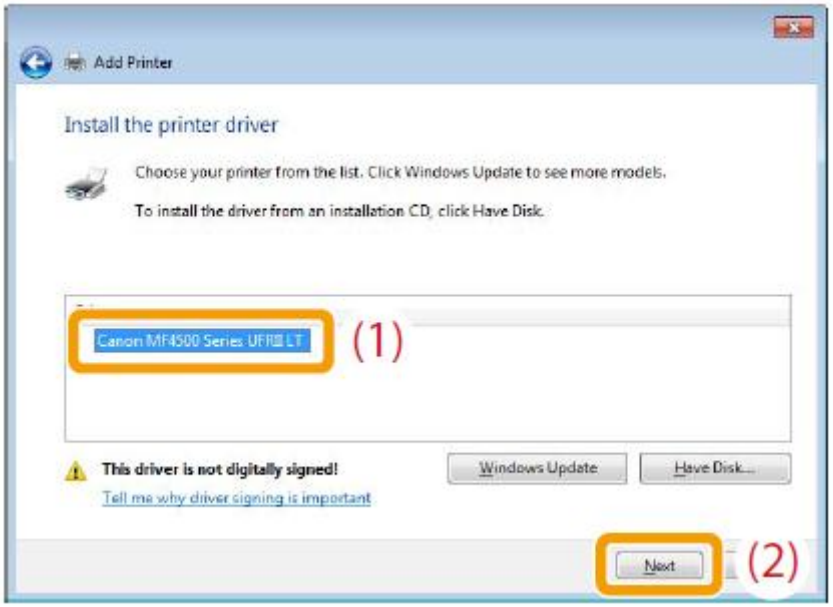


รูปที่ 13.6 ติดตั้ง MF Drivers (6)

9 คลิก [OK].

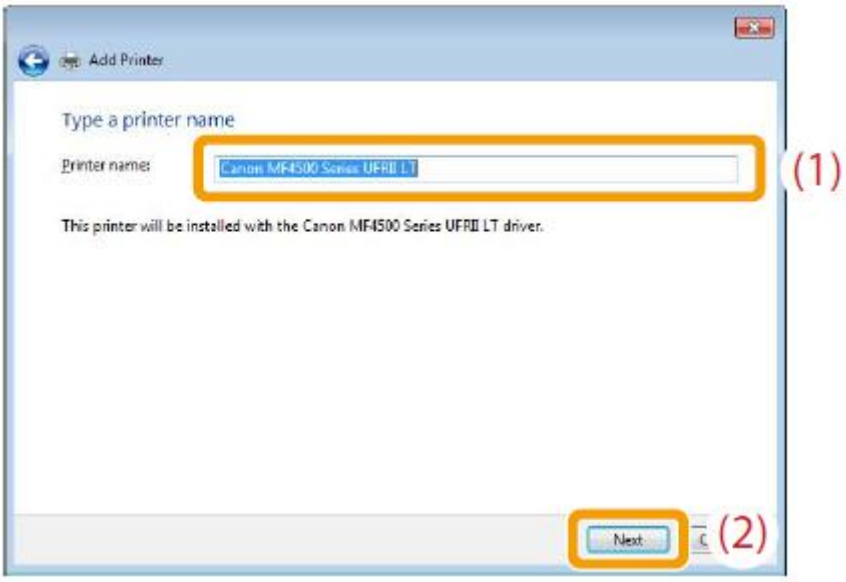
รูปที่ 13.7 ติดตั้ง MF Drivers (7)

10 เลือก [Canon XXXX Series UFRII LT] แล้วคลิก [Next].



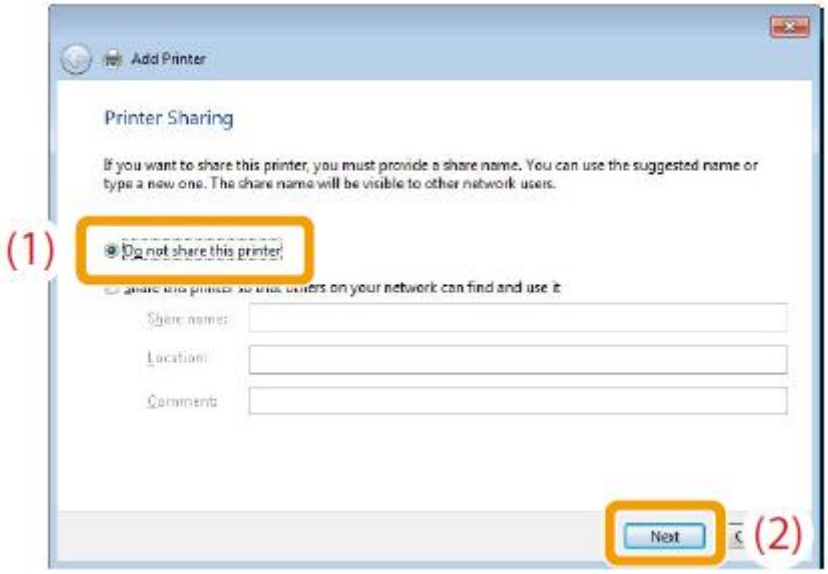
รูปที่ 13.8 ติดตั้ง MF Drivers (8)

11 กำหนดชื่อ Printer แล้ว [Next].



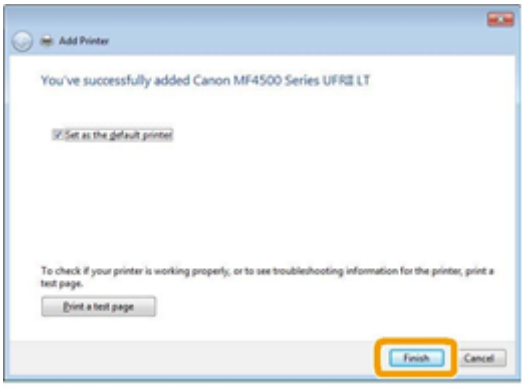
รูปที่ 13.9 ติดตั้ง MF Drivers (9)

12 เลือก [Do not share this printer] แล้วคลิก [Next].



รูปที่ 13.10 ติดตั้ง MF Drivers (10)

13 คลิก [Finish].



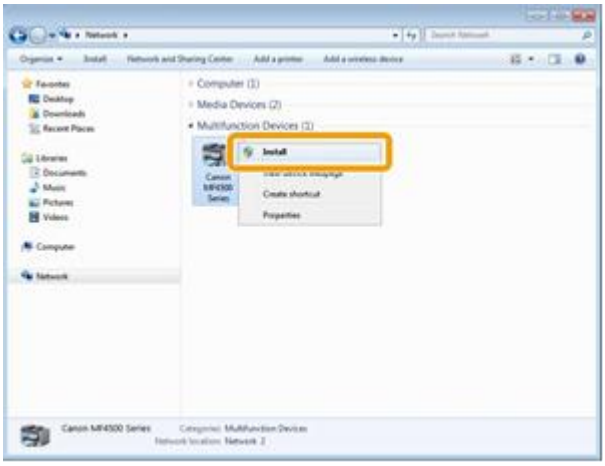
รูปที่ 13.11 ติดตั้ง MF Drivers (11)

- **ตั้งค่า WSD**

1 แสดง Printers ใน Network.

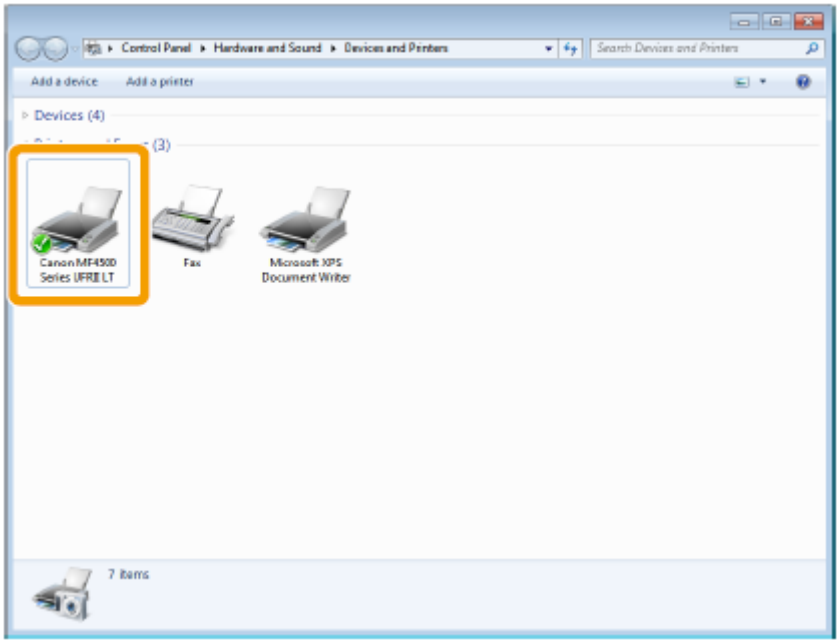
เลือก [Start] -> [Computer] แล้ว [Network].

2 Right-click ที่ machine icon, แล้วเลือก [Install] จาก pop-up menu.



รูปที่ 13.12 ติดตั้ง WSD

⟶ เมื่อติดตั้งเสร็จจะปรากฏไอคอนปริ้นเตอร์ดังภาพ



รูปที่ 13.13 ผลลัพธ์จากการติดตั้ง WSD

3 จากนั้นลบไอคอนปริ้นเตอร์ที่ติดตั้งโดย MF Driver ในหัวข้อ

(1) Right-click ที่ไอคอนปริ้นเตอร์แล้วเลือก [Remove device] จาก pop-up menu.

(2) คลิก [Yes].