



ใบรับรองวิทยานิพนธ์
บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์

วิทยาศาสตร์มหาบัณฑิต (วิทยาการคอมพิวเตอร์)

ปริญญา

วิทยาการคอมพิวเตอร์

วิทยาการคอมพิวเตอร์

สาขา

ภาควิชา

เรื่อง การศึกษาการใช้งานจริงของไอพีแอดเดรสเวอร์ชัน 4 ที่มีการจัดสรรภายใน
มหาวิทยาลัยเกษตรศาสตร์

A Study of IPv4 Addresses Allocation and Utilization within Kasetsart University

นามผู้วิจัย นางสาวแสงดาว พรทวีโชคสกุล

ได้พิจารณาเห็นชอบโดย

อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก

(ผู้ช่วยศาสตราจารย์สุพุมล กิตติสิน, Ph.D.)

อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม

(อาจารย์พนิดา พงษ์ไพบูลย์, Ph.D.)

หัวหน้าภาควิชา

(ผู้ช่วยศาสตราจารย์ศิริกร จันทร์นวล, M.S.)

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์รับรองแล้ว

(รองศาสตราจารย์กัญจนา ชีระกุล, D.Agr)

คณบดีบัณฑิตวิทยาลัย

วันที่ เดือน พ.ศ.

ลิขสิทธิ์ มหาวิทยาลัยเกษตรศาสตร์

วิทยานิพนธ์

เรื่อง

การศึกษาการใช้งานจริงของไอพีแอดเดรสเวอร์ชัน 4 ที่มีการจัดสรรภายใน
มหาวิทยาลัยเกษตรศาสตร์

A Study of IPv4 Addresses Allocation and Utilization within Kasetsart University

โดย

นางสาวแสงดาว พรทวีโชคสกุล

เสนอ

บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์
เพื่อความสมบูรณ์แห่งปริญญาวิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)
พ.ศ. 2555

ลิขสิทธิ์ มหาวิทยาลัยเกษตรศาสตร์

แสงดาว พรทวีโชคสกุล 2555: การศึกษาการใช้งานจริงของไอพีแอดเดรสเวอร์ชัน 4 ที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์ ปริญญาวิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์) สาขาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก: ผู้ช่วยศาสตราจารย์สุพุมล กิตติสิน, Ph.D. 96 หน้า

งานวิจัยนี้ศึกษาการใช้งานจริงของไอพีแอดเดรสเวอร์ชัน 4 ที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์ โดยใช้งานวิจัยของ John Heidemann และคณะ เป็นต้นแบบในการออกแบบการสำรวจ โดยทำการทดลองเพื่อให้เข้าใจลักษณะการใช้งานไอพีแอดเดรสภายในมหาวิทยาลัย ซึ่งมหาวิทยาลัยเกษตรศาสตร์ได้รับไอพีแอดเดรส class B block -- 158.108.0.0/16 สำหรับการใช้งานโดยที่คอมพิวเตอร์ส่วนมากจะใช้ private address ด้านหลังไฟร์วอลล์

งานวิจัยนี้ได้ทำการศึกษาภายใต้บล็อก /24 ($2^8 = 256$) โดยมีการใช้ทั้ง Active Probing และ Passive Probing ในการสำรวจที่ Internet Control Message Protocol (ICMP) และ Transmission Control Protocol (TCP) ของพอร์ตต่าง ๆ ผลการสำรวจพบว่ามีไอพีแอดเดรสที่มีการใช้งานจริงประมาณ 49.80 % โดยการสำรวจด้วย โพรโทคอล TCP สำรวจพบจำนวนปริมาณไอพีแอดเดรสที่มีการใช้งานจริงมากกว่าการสำรวจด้วยโพรโทคอล ICMP และจากผลการสำรวจนำมาวิเคราะห์หาค่า Availability, ค่า Volatility และค่า Uptime สามารถคาดการณ์ลักษณะการใช้งานของไอพีแอดเดรสเป็น 5 กลุ่มดังนี้ กลุ่ม Always – stable จะเป็นกลุ่มไอพีแอดเดรสที่มีการใช้งานตลอดเวลาและสม่ำเสมอและทำงานอย่างต่อเนื่องสูงสุด ซึ่งจะเป็นกลุ่มของเครื่องแม่ข่ายเป็นส่วนมากมีจำนวน ร้อยละ 3.95 กลุ่ม Sometimes - stable จะเป็นกลุ่มไอพีแอดเดรสที่มีการใช้งานในระยะเวลาสั้นและทำงานอย่างต่อเนื่องรองลงมาจำนวนร้อยละ 10.04 กลุ่ม Intermittent จะเป็นกลุ่มไอพีแอดเดรสที่มีการใช้งานบ่อย แต่ใช้งานในช่วงเวลาสั้น ๆ มีจำนวนร้อยละ 16.49 กลุ่ม Underutilized จะเป็นไอพีแอดเดรสที่มีการใช้งานในบางครั้งมีจำนวนร้อยละ 19.32 และกลุ่มสุดท้ายกลุ่ม Unclassifiable จะเป็นกลุ่มไอพีแอดเดรสที่ไม่ได้รับการจัดสรร หรือไม่มีการใช้งานผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีจำนวนร้อยละร้อยละ 50.20

Sangdao Prontaweechoksakul 2012: A Study of IPv4 Addresses Allocation and Utilization within Kasetsart University. Master of Science (Computer Science), Major Field: Computer Science, Department of Computer Science. Thesis Advisor: Assistant Professor Sukumal Kritisin, Ph.D. 96 pages.

This research is a study on IPv4 address allocation and utilization at Kasetsart University. Referenced the previous study of Visible Internet by Heidemann, et al., we did a few experiments in order to understand IP addresses usage characteristics within the university. Kasetsart University was assigned a class B block address -- 158.108.0.0/16 for its domain. The university consists of five campuses throughout Thailand. Many campus computers are using private address behind firewalls.

The research has studied /24 ($2^8 = 256$) blocks which are allocated to departments or organizations of the university. We used both active and Passive Probing which used Internet Control Message Protocol (ICMP) and Transmission Control Protocol (TCP) on various ports. The experimental results show that only 49.80% of allocated IP addresses are used and to find IP addresses, using TCP is more visible than using ICMP. We also analyzed the address characteristics, such as, availability, volatility, and uptime. The evaluations show that, IP addresses as the following characteristics: 3.95 % is always stable; 10.04 % is sometimes stable; 16.49 % is intermittent; 19.32 % is underutilized; and finally 50.20 % is unclassifiable.

Student's signature

Thesis Advisor's signature

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ดีด้วยความช่วยเหลืออย่างดียิ่งของ ผู้ช่วยศาสตราจารย์ ดร. สุขุมล กิตติสิน ประธานกรรมการที่ปรึกษา และดร.พนิดา พงษ์ไพบูลย์ ที่ได้สั่งสอนให้คำแนะนำ วิธีการและขั้นตอนในการดำเนินงาน ชี้แนะแนวทางแก้ไขปัญหาและตรวจแก้ข้อบกพร่องต่างๆ ในงานวิจัยมาโดยตลอด

ขอกราบขอบพระคุณ คุณพ่อ คุณแม่ ที่ได้ให้กำลังใจ ให้การสนับสนุน และความช่วยเหลืออย่างที่สุดมาโดยตลอดจนสำเร็จการศึกษา ขอขอบพระคุณคณาจารย์ทุกท่านที่ให้การอบรม สั่งสอนวิชาความรู้ต่างๆมาจนสำเร็จการศึกษา

ขอขอบคุณโครงการทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย หรือทุน TGIST ที่ให้ทุนการศึกษาสนับสนุนการเรียนในระดับบัณฑิตศึกษา

ขอขอบคุณภาควิชาวิทยาการคอมพิวเตอร์ ที่ได้สนับสนุนด้านอุปกรณ์ และสถานที่ตลอดระยะเวลาในการทำวิทยานิพนธ์

แสงดาว พรทวีโชคสกุล

เมษายน 2555

สารบัญ

	หน้า
สารบัญ	(1)
สารบัญตาราง	(2)
สารบัญภาพ	(3)
คำอธิบายสัญลักษณ์และคำย่อ	(5)
คำนำ	1
วัตถุประสงค์	3
การตรวจเอกสาร	4
อุปกรณ์และวิธีการ	22
อุปกรณ์	22
วิธีการ	22
ผลและวิจารณ์	31
ผล	31
วิจารณ์	54
สรุปและข้อเสนอแนะ	57
สรุป	57
ข้อเสนอแนะ	59
เอกสารและสิ่งอ้างอิง	60
ภาคผนวก	62
ภาคผนวก ก รายละเอียดผลการทดลอง	63
ภาคผนวก ข ผลงานตีพิมพ์	82
ประวัติการศึกษา และการทำงาน	96

สารบัญตาราง

ตารางที่		หน้า
1	การเปรียบเทียบจำนวนไอพีแอดเดรส	31
2	การเปรียบเทียบจำนวนไอพีแอดเดรสโดยใช้ โปรโทคอล ICMP และ โปรโทคอล TCP	33
3	การเปรียบเทียบจำนวนไอพีแอดเดรสสำรวจโดย โปรโทคอล TCP ที่คำสั่งต่างกัน	34
4	การเปรียบเทียบจำนวนไอพีแอดเดรสโดยใช้ Active Probing และ Passive Probing	36
5	การเปรียบเทียบผลการสำรวจจำนวนไอพีแอดเดรสด้วยวิธี Active Probing กับการจัดสรรไอพีแอดเดรสของมหาวิทยาลัยเกษตรศาสตร์	37
6	การแบ่งประเภทการบริการ	43
7	การแบ่งประเภทลักษณะการใช้งานจริงของไอพีแอดเดรสโดยใช้ Active Probing	53
ตารางผนวกที่		
ก1	ชุดข้อมูลที่ได้จากการทดลองสำรวจจำนวนไอพีแอดเดรสวิธี Active Probing	64
ก2	ชุดข้อมูลที่ได้จากการทดลองสำรวจจำนวนไอพีแอดเดรสวิธี Passive	64
ก3	ข้อมูลการจัดสรรไอพีแอดเดรสของมหาวิทยาลัยเกษตรศาสตร์	73

สารบัญญภาพ

ภาพที่		หน้า
1	การเชื่อมต่อของเครือข่าย	8
2	การสแกนแบบ Ping	13
3	การสแกนแบบ TCP SYN กรณีเครื่องปลายทางปิดพอร์ต	14
4	การสแกนแบบ TCP SYN กรณีเครื่องปลายทางเปิดพอร์ต	14
5	การสแกนแบบ TCP connect() กรณีเครื่องปลายทางปิดพอร์ต	15
6	การสแกนแบบ TCP connect() กรณีเครื่องปลายทางเปิดพอร์ต	15
7	การสแกนแบบ ACK Scan กรณีเครื่องปลายทางปิดพอร์ต	16
8	การสแกนแบบ ACK Scan กรณีเครื่องปลายทางเปิดพอร์ต	16
9	ผลการสำรวจจำนวนไอพีแอดเดรสที่สำรวจด้วยโปรโตคอล ICMP และ โปรโตคอล TCP	32
10	ผลการสำรวจจำนวนไอพีแอดเดรสที่สำรวจด้วย โปรโตคอล TCP ที่ option ต่างกัน	34
11	ผลการสำรวจจำนวนไอพีแอดเดรสที่สำรวจด้วย Active Probing และ Passive Probing	36
12	ผลการสำรวจปริมาณการใช้งานโปรแกรมประยุกต์ในแต่ละประเภท	44
13	แผนภาพค่า Availability ของไอพีแอดเดรสภายใน มหาวิทยาลัยเกษตรศาสตร์	46
14	แผนภาพค่า Volatility ของแต่ละไอพีแอดเดรสภายใน มหาวิทยาลัยเกษตรศาสตร์	47
15	แผนภาพค่า Uptime ของแต่ละไอพีแอดเดรสภายใน มหาวิทยาลัยเกษตรศาสตร์	49
16	การกระจายตัวของไอพีแอดเดรส	50
17	การกระจายตัวของไอพีแอดเดรส	51
18	การกระจายตัวของไอพีแอดเดรส	52

สารบัญภาพ (ต่อ)

ภาพผนวกที่		หน้า
ก1	จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดสำรวจด้วย Active Probing	65
ก2	จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโพรโทคอล ICMP	66
ก3	จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโพรโทคอล TCP	68
ก4	จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโพรโทคอล TCP - ACK	69
ก5	จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโพรโทคอล TCP - SYN	71

คำอธิบายสัญลักษณ์และคำย่อ

ICMP	= Internet Control Message Protocol
TCP	= Transmission Control Protocol
Nmap	= Network Mapper
UDP	= User Datagram Protocol
DDOS	= Distributed denial of service
IP	= Internet Protocol
NAT	= Network Address Translation
FTP	= File Transfer Protocol
SSH	= Secure Shell

การศึกษาการใช้งานจริงของ ไอพีแอดเดรสเวอร์ชัน 4 ที่มีการจัดสรรภายใน มหาวิทยาลัยเกษตรศาสตร์

A Study of IPv4 Addresses Allocation and Utilization within Kasetsart University

คำนำ

ในปัจจุบันระบบการสื่อสารข้อมูลผ่านเครือข่ายคอมพิวเตอร์เข้ามามีบทบาทในชีวิตประจำวันมากขึ้น ทั้งด้านการติดต่อสื่อสาร การค้นหาข้อมูล การทำธุรกรรม หรือการพักผ่อน ไม่ว่าจะเป็นหน่วยงานของรัฐเอกชน หรือมหาวิทยาลัยก็ใช้งานระบบการสื่อสารข้อมูลผ่านเครือข่ายคอมพิวเตอร์ และใช้เป็นสื่อกลางในการดำเนินชีวิต โดยมีได้จำกัดอยู่ภายในวงการศึกษา บริษัท หรือสำนักงานเท่านั้น แต่แพร่กระจายออกไปยังผู้ใช้งานตามบ้านเรือน ซึ่งส่งผลให้ระบบการสื่อสารข้อมูลผ่านเครือข่ายคอมพิวเตอร์เพิ่มจำนวนมากขึ้นอย่างรวดเร็วและในอนาคตจำนวนผู้ใช้งานก็อาจเพิ่มจำนวนมากขึ้น ถือได้ว่าการสื่อสารข้อมูลผ่านเครือข่ายคอมพิวเตอร์เป็นรูปแบบการสื่อสารที่มีความสำคัญ ช่วยให้เราสามารถติดต่อสื่อสาร และแลกเปลี่ยนข้อมูลได้อย่างรวดเร็วและกว้างขวาง สามารถรับรู้ข้อมูลข่าวสาร เหตุการณ์ ความเปลี่ยนแปลงของสถานการณ์ที่เกิดขึ้นได้อย่างทันเวลา

ระบบการสื่อสารข้อมูลผ่านเครือข่ายคอมพิวเตอร์มีการเจริญเติบโตอย่างรวดเร็ว และมีความจำเป็นในการดำเนินกิจกรรมของหน่วยงานหรือองค์กรทั้งของรัฐบาลและเอกชน เป็นเหตุให้มีการใช้งานระบบเครือข่ายคอมพิวเตอร์มากขึ้น ปัจจัยที่สำคัญที่ทำให้เครื่องคอมพิวเตอร์สามารถใช้งานการสื่อสารข้อมูลผ่านเครือข่ายได้คือหมายเลขประจำตัวของเครื่องที่เชื่อมต่อในระบบเครือข่าย ที่เรียกว่า ไอพีแอดเดรส (IP address) ไอพีแอดเดรสที่ใช้กันส่วนใหญ่ในปัจจุบันเป็นประเภทไอพีแอดเดรสเวอร์ชัน 4 (IPv4) ซึ่งมีขนาดเพียง 32 บิต ทำให้ไม่เพียงพอสำหรับการใช้งานในอนาคต เนื่องจากไอพีแอดเดรสเวอร์ชัน 4 (IPv4) ทำให้การกำหนดค่าไอพีแอดเดรส (IP address) ไม่เพียงพอกับเครื่องคอมพิวเตอร์และเครือข่ายใหม่ ๆ ที่มีมากขึ้น หรือถ้าเป็นระบบเครือข่ายภายในองค์กร หรือหน่วยงานการทราบจำนวนของไอพีแอดเดรส (IP address) ช่วยทำให้การจัดสรร ไอพีแอดเดรส (IP address) มีประสิทธิภาพมากขึ้น สามารถจัดสรรได้เพียงพอกับความ

ต้องการของแต่ละองค์กร และสามารถคาดการณ์แนวโน้มในการพัฒนาเครือข่ายให้สามารถรองรับการใช้งานได้อย่างมีประสิทธิภาพ และคุ้มค่าต่อการลงทุน

การใช้ระบบเครือข่ายของมหาวิทยาลัยเกษตรศาสตร์เป็นต้นแบบในการสำรวจและวิเคราะห์ปริมาณไอพีแอดเดรสที่ใช้งานจริง เนื่องจากเครือข่ายของมหาวิทยาลัยเกษตรศาสตร์เชื่อมโยงระบบคอมพิวเตอร์ของหน่วยงานทุกหน่วยงาน ภายในมหาวิทยาลัยเกษตรศาสตร์เข้าด้วยกัน และการใช้งานภายในมหาวิทยาลัยมีความหลากหลาย ทั้งงานทางด้านการเรียน การสอน งานวิจัย งานสนับสนุนการบริหาร รวมทั้งใช้เป็นระบบสื่อสารระหว่างบุคคลและหน่วยงาน ซึ่งกลุ่มผู้ใช้งานก็ครอบคลุมทุกเพศ ทุกวัย ทั้งนักเรียน นิสิต อาจารย์ นักวิจัย นักวิชาการ ข้าราชการ พนักงาน และบุคลากรภายนอกมหาวิทยาลัย

วัตถุประสงค์

เพื่อศึกษาการใช้ประโยชน์ของไอพีแอดเดรส (IP Address) ที่มีการจัดสรร และสำรวจปริมาณไอพีแอดเดรสที่มีการใช้งานจริงภายในเครือข่ายมหาวิทยาลัยเกษตรศาสตร์ รวมทั้งวิเคราะห์ผลการสำรวจ คาดการณ์ลักษณะการใช้งานไอพีแอดเดรสภายในองค์กร หรือหน่วยงานของมหาวิทยาลัย และเพื่อให้เข้าใจประสิทธิภาพของวิธีการสำรวจข้อมูลทั้ง Active Probing และ Passive Probing

ประโยชน์ที่คาดว่าจะได้รับ

การบริหารจัดการเครือข่ายมีประสิทธิภาพมากขึ้น ทำให้สามารถจัดสรรปริมาณการใช้งานไอพีแอดเดรสได้อย่างเหมาะสม เพียงพอกับความต้องการของแต่ละองค์กร หรือหน่วยงาน และใช้งานได้อย่างเต็มประสิทธิภาพ นอกจากนี้ทำให้ทราบถึงปริมาณการใช้งาน ไอพีแอดเดรสที่ถูกใช้งานจริง เพื่อคาดการณ์แนวโน้มในการพัฒนาเครือข่ายให้สามารถรองรับการใช้งานได้อย่างมีประสิทธิภาพ

ขอบเขตและข้อจำกัด

1. ศึกษาและรวบรวมข้อมูลเกี่ยวกับ IPv4 Address
2. สำรวจปริมาณไอพีแอดเดรสด้วยวิธี Active Probing โดยใช้รูปแบบโปรโตคอล ICMP และ โปรโตคอล TCP
3. วิเคราะห์ข้อมูลทางสถิติของไอพีแอดเดรสที่มีการใช้งาน เพื่อคาดการณ์ลักษณะการใช้งานไอพีแอดเดรสภายในองค์กร หรือหน่วยงานของมหาวิทยาลัยเกษตรศาสตร์
4. สำรวจ และเปรียบเทียบผลการสำรวจไอพีแอดเดรสของวิธี Active Probing กับ Passive Probing ภายในภาควิชาวิทยาการคอมพิวเตอร์

การตรวจเอกสาร

ทฤษฎีที่เกี่ยวข้อง

การศึกษาการใช้งานจริงของไอพีแอดเดรสที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์ ผู้วิจัยได้ศึกษาข้อมูลของเครือข่ายมหาวิทยาลัยเกษตรศาสตร์ และค้นคว้าเอกสารเกี่ยวกับไอพีแอดเดรสและโพรโทคอล รวมทั้งทฤษฎีที่เกี่ยวข้องกับการสำรวจไอพีแอดเดรสดังนี้

1. เครือข่ายมหาวิทยาลัยเกษตรศาสตร์

มหาวิทยาลัยเกษตรศาสตร์ ได้พัฒนาเครือข่ายคอมพิวเตอร์ที่เรียกว่า เครือข่ายนนทรี หรือนนนทรีเน็ต เป็นระบบที่เชื่อมโยงระบบคอมพิวเตอร์ของหน่วยงานทุกหน่วยงาน ภายในมหาวิทยาลัยเกษตรศาสตร์เข้าด้วยกัน และรองรับการใช้งานภายในมหาวิทยาลัย ทั้งงานทางด้านการเรียน การสอน งานวิจัย งานสนับสนุนการบริหาร รวมทั้งใช้เป็นระบบสื่อสารระหว่างบุคคล และหน่วยงานทั้งที่บางเขนและกำแพงแสน มหาวิทยาลัยเกษตรศาสตร์ได้บริหารจัดการเครือข่ายนนทรีอย่างเป็นระบบ โดยวางรหัสไอพีแอดเดรส ครอบคลุมทุกหน่วยงานและสามารถรองรับการใช้งานได้อย่างทั่วถึง ทั้งนักเรียน นิสิต และบุคลากรของมหาวิทยาลัย โดยเครือข่ายนนทรีมีหมายเลขไอพีแอดเดรสอยู่ภายใต้คลาสบี (Class B) คือ 158.108.x.x โดเมนชื่อว่า ku.ac.th และหมายเลข Autonomous System (AS) คือ AS9411 โดยมีสำนักบริการคอมพิวเตอร์เป็นผู้ดูแลและบริหาร

2. ไอพีแอดเดรส (IP Address)

IP Address เป็นหมายเลขประจำตัวของเครื่องที่เชื่อมต่อในเครือข่ายอินเทอร์เน็ต (Internet) โดย IP Address ของแต่ละเครื่องจะไม่ซ้ำกัน และไม่ผูกติดกับตัวฮาร์ดแวร์ (Hardware) จึงสามารถถูกกำหนดใหม่หรือแก้ไขได้ IP Address เป็นตัวเลขขนาด 32 บิต (Bit) แบ่งออกเป็น 4 ชุด ชุดละ 4 บิต (Bit) และคั่นแต่ละชุดด้วยจุด (.) ซึ่งค่าตัวเลขแต่ละชุดจะเริ่มตั้งแต่ 0 ถึง 255 (2^8) เช่น IP Address 158.108.21.1 หรือ 10.0.0.1 ซึ่งปัจจุบันเรียกรูปแบบดังกล่าวว่า IP version 4 หรือ IPv4

การกำหนดค่า IP Address ถูกกำหนดเป็น 2 ส่วนย่อยคือ ค่าของหมายเลขเครื่องลูกข่าย (Host Address) และค่าของหมายเลขเครือข่าย (Network Address) เช่น 158.108.21.71 และ 158.108.21.118 หมายความว่าเครื่องทั้งสองมีหมายเลขเครือข่ายเหมือนกันคือ 158.108.21 แสดงว่าเครื่องทั้งสองอยู่ในเครือข่ายเดียวกัน แต่มีหมายเลขเครื่องลูกข่ายแตกต่างกันคือ 71 และ 118

การแบ่งส่วน IP Address จะเป็นไปตามการแบ่งระดับชั้นของเครือข่าย เรียกว่า Network class เพื่อให้สามารถแจกจ่าย IP Address ให้กับเครือข่ายต่าง ๆ ได้อย่างเหมาะสม บางเครือข่ายมีจำนวนเครื่องลูกข่ายมาก บางเครือข่ายมีเครื่องลูกข่ายน้อยแต่มีเครือข่ายย่อย ๆ ถ้าไม่มีการจัดลำดับของเครือข่ายให้ดี IP Address จะถูกใช้งานอย่างสิ้นเปลืองและใช้งานได้ไม่เต็มจำนวนที่มี ลำดับชั้นของเครือข่ายแบ่งเป็น 5 ลำดับคือ

Class A เป็น IP Address ที่เริ่มตั้งแต่ 0 – 127 จะกำหนดให้กับเครือข่ายที่มีขนาดใหญ่ เครือข่าย 1 เครือข่ายสามารถมีเครื่องลูกข่ายได้กว่า 16 ล้านเครื่อง IP Address จะอยู่ในลักษณะ net.host.host.host

Class B เป็น IP Address ที่เริ่มตั้งแต่ 128 – 191 จะกำหนดให้กับเครือข่ายที่มีขนาดใหญ่แต่เล็กกว่า Class A ในแต่ละเครือข่ายของ Class B สามารถมีเครื่องลูกข่ายได้ 2^{16} Address ซึ่งเท่ากับ 64,516 เครื่อง IP Address จะอยู่ในลักษณะ net.net.host.host

Class C เป็น IP Address ที่เริ่มตั้งแต่ 192 – 223 จะกำหนดให้กับเครือข่ายที่เป็นองค์กรทั่วไป ซึ่งเป็นองค์กรขนาดกลางถึงขนาดเล็ก ในแต่ละเครือข่ายมีเครื่องลูกข่ายไม่เกิน 2^8 Address ซึ่งเท่ากับ 254 เครื่อง IP Address จะอยู่ในลักษณะ net.net.net.host

Class D เป็นการกำหนด IP Address สำรองไว้สำหรับส่งข้อมูลแบบ Multicast คือ การส่งข้อมูลจากที่หนึ่งให้กับกลุ่มผู้รับอื่น ๆ ซึ่งไม่มีการส่งข้อมูลให้ใช้งานทั่วไป

Class E เป็น IP Address พิเศษที่ใช้สำหรับงานทดสอบและพัฒนา ไม่มีการกำหนดให้ใช้งานทั่วไป

3. การแบ่งเครือข่ายย่อย (Subnet)

Subnet หรือ Sub Network เป็นการกำหนด IP Address แบบแยกส่วนของโครงสร้างเครือข่าย เพื่อแบ่งเครือข่ายออกเป็นเครือข่ายย่อย ๆ และทำให้การกำหนดใช้งาน IP Address ที่ได้รับมาสามารถแบ่งออกเป็นส่วน ๆ เหมาะกับจำนวนเครื่องในแต่ละเครือข่าย เช่น หน่วยงานมีเครือข่าย 3 เครือข่าย แต่ละเครือข่ายมี IP Address Class C คือ 192.168.1.0 192.168.2.0 และ 192.168.3.0 แต่ละเครือข่ายสามารถเชื่อมต่อกับเครื่องลูกข่ายได้สูงสุดถึง 254 เครื่อง เนื่องจากใช้ 8 บิตสุดท้ายเป็นตัวกำหนด Host Address ซึ่งในความเป็นจริง 8 บิตสุดท้ายสามารถมี IP Address ที่แตกต่างกัน 256 Address แต่เอาออกไป 2 Address คือ 0 กับ 255 ซึ่งไว้สำหรับควบคุมการทำงานของเครือข่าย การมีหมายเลขที่ใช้กำหนด Subnet ขึ้นมา ทำให้สามารถแบ่งเครือข่ายที่มีขนาดเล็กกว่า Class C และ ไม่สูญเสีย Class C ซึ่งสามารถใช้ IP Address ได้อย่างมีประสิทธิภาพ โดยการกำหนด Subnet มีดังต่อไปนี้

Subnet in decimal format : 192.168.1.0 /24

หมายความว่า 24 บิตแรกใน IP Address เป็นการระบุเครือข่าย (Network Address) ส่วน 8 บิตหลังเป็นการระบุเครื่องลูกข่าย (Host Address) แปลง Subnet ให้อยู่ในรูปแบบ Binary format ดังนี้

Subnet in binary format : 11000000.10101000. 00000001.00000000 / 24

หมายความว่า มีเครื่องลูกข่าย (Host Address) ภายใน Subnet นี้ทั้งหมด 2^8 คือ 256 เครื่อง โดยที่แต่ละเครื่องมี IP Address ดังนี้

IP Address in this subnet : 11000000. 10101000. 00000001.xxxxxxxxxx (x = 0,

1)

จากตัวอย่างนำเครื่องลูกข่าย (Host Address) จำนวน 8 บิตมาแบ่งออกเป็น 2 ส่วนเพื่อแบ่งเครือข่ายออกเป็นเครือข่ายย่อย ๆ เช่น ใช้ข้อมูล 2 บิตทางซ้ายเป็นตัวกำหนดเครือข่ายย่อย และใช้ 6 บิตทางขวาเป็นตัวกำหนดเครื่องลูกข่าย ดังนั้น IP Address 1 ชุดสามารถแบ่งเป็นเครือข่ายย่อยได้ 4

เครือข่ายโดยแต่ละเครือข่ายจะมีเครื่องลูกข่ายจำนวน 64 เครื่อง ซึ่งเรียกการแบ่งเครือข่ายย่อยนี้ว่า Subnet แต่ในแต่ละ Subnet จะต้องมีการจอง Host Address ไว้ 2 ตำแหน่งคือ Host Address ที่มีค่าเป็น 0 หกทุกบิต และ 1 หกทุกบิต ดังนั้นในทุก Subnet จะมีการเอาออกไป 2 Address จึงทำให้เหลือจำนวนเครือข่ายย่อย 2 เครือข่ายและมีจำนวนเครื่องลูกข่าย 62 เครื่อง

ในการแบ่งเครือข่ายย่อย (Subnet) อุปกรณ์ Router จะต้องทราบข้อมูลการแบ่ง Subnet ว่าใช้ข้อมูลกี่บิตเป็น เครือข่ายย่อยและกี่บิตเป็นเครื่องลูกข่าย (Host Address) จึงจะส่งข้อมูลให้เครือข่ายได้อย่างถูกต้อง เรียกข้อมูลการแบ่งเครือข่ายย่อย (Subnet) ว่า Subnet Mask โดยกำหนดให้ค่าของ Network Address และ Subnet Address มีค่าเป็น 1 ส่วน Subnet Mask ของ Host Address จะมีค่าเป็น 0

Subnet Mask in binary format : 11111111.11111111.11111111.11000000

Subnet Mask in decimal format : 255.255.255.192

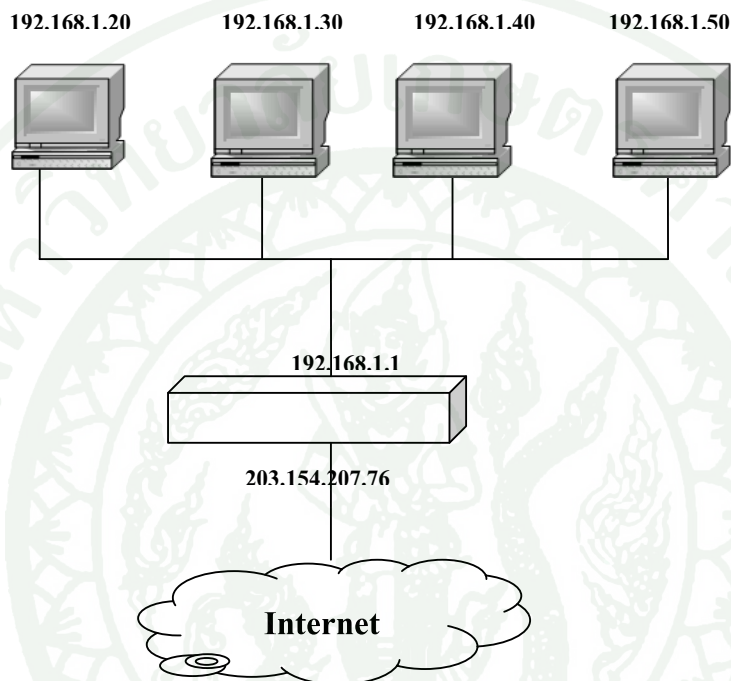
4. Network Address Translation (NAT)

ในการติดต่อสื่อสารเครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่ออยู่ในเครือข่ายต้องมีการระบุหมายเลข IP Address ของเครื่องเพื่อระบุตำแหน่งต้น/ปลายทางในการเชื่อมต่อ ดังนั้นหมายเลขแต่ละหมายเลขจะต้องไม่ซ้ำกัน โดยการจัดสรร IP Address จะได้จาก ISP หรือหน่วยงานที่เกี่ยวข้อง ซึ่งมีการจำกัดให้มีการกำหนดหมายเลข IP Address ให้อยู่ในช่วงต่อไปนี้

Class	IP Address
A	0.0.0.0 – 127.255.255.255
B	128.0.0.0 – 191.255.255.255
C	192.0.0.0 – 223.255.255.255

IP Address ที่อยู่ในช่วงดังกล่าวจะเป็น ไอพีปลอม หรือ Private IP Address ซึ่งการกำหนดให้เป็น Private IP Address จะทำให้เครื่องที่อยู่นอกเครือข่ายไม่สามารถเข้าถึงเครื่องลูกข่ายภายในเครือข่ายได้ เพราะ ไม่ทราบ IP Address แต่ถ้าต้องการติดต่อกับเครื่องที่อยู่ภายนอกเครือข่าย ก็จะต้องผ่านกระบวนการแปลง Address ที่เรียกว่า Network Address Translation (NAT) [RFC

4787] นอกจาก Private IP Address แล้วก็ยังมี ไอพีจริง หรือ Public IP Address เป็นไอพีที่เครื่องทุกเครื่องที่มีการติดต่อสื่อสารกับเครือข่ายสามารถเข้าถึงได้



ภาพที่ 1 การเชื่อมต่อของเครือข่าย

จากภาพที่ 1 จะเห็นได้ว่าสามารถใช้ ไอพีแท้ หรือ Public IP Address เพียงตัวเดียว ในการเชื่อมต่อคอมพิวเตอร์ 4 เครื่องไปยังเครือข่ายอื่นๆ ได้ โดยทั้ง 4 เครื่องดังกล่าวก็จะมี IP Address ของตัวเอง เป็น ไอพีปลอม หรือ Private IP Address ที่ใช้ในการจำแนกอีกทีหนึ่งว่าเครื่องไหนเป็นเครื่องไหน โดยการทำงานคือเมื่อมีการติดต่อสื่อสารกับเครือข่ายภายนอก NAT จะมีการกำหนดหมายเลข IP ชั่วคราวให้ใช้งาน และเมื่อมีการรับส่งข้อมูลระหว่างเครือข่ายภายนอกกับเครื่องภายในเครือข่าย NAT จะทำการแปลง ไอพีแท้ หรือ Public IP Address ให้เป็น ไอพีปลอม หรือ Private IP Address ในการรับข้อมูลจากเครือข่ายภายนอก แต่ถ้าเป็นการส่งข้อมูลออกไปยังเครือข่ายภายนอก NAT จะทำการแปลงไอพีปลอม หรือ Private IP Address ให้เป็นไอพีแท้ หรือ Public IP Address

Network Address Translation (NAT) มี 2 ประเภท คือ Static NAT และ Dynamic NAT โดย Static NAT เป็นการ map ค่าไอพีปลอม หรือ Private IP Address ไปเป็น ไอพีแท้ หรือ Public IP Address ตามที่กำหนดไว้ใน NAT Table ส่วน Dynamic NAT เป็นการ map ค่า ไอพีปลอม หรือ Private IP Address ไปเป็น ไอพีแท้ หรือ Public IP Address จะทำเฉพาะในเวลาเครื่องภายในเครือข่ายต้องการติดต่อกับเครื่องภายนอก

5. ประเภทของโพรโทคอล

Internet Control Message Protocol (ICMP) เป็นโพรโทคอลที่สามารถทำหน้าที่ตรวจสอบการเชื่อมต่อและช่วยเหลือในการตั้งค่าโครงสร้างอัตโนมัติของโฮสต์ หน้าที่หลักของโพรโทคอล ICMP (Internet Control Message Protocol) คือการแจ้งหรือแสดงข้อความจากระบบ เพื่อบอกให้ผู้ใช้ทราบว่าเกิดอะไรขึ้นในระหว่างที่มีการส่งแพ็กเก็ตในเครือข่ายโพรโทคอล ICMP ใช้การส่งแบบคอนเน็กชันเลสส์ (Connectionless) ซึ่งหมายถึงการรับ - ส่งข้อมูลที่ฝ่ายรับและฝ่ายส่งไม่ได้ประสานงานกันก่อนคือ ฝ่ายรับจะไม่ทราบว่าจะมีแพ็กเก็ตส่งมาหาตัวเอง ดังนั้น โอกาสที่แพ็กเก็ตจะส่งไม่ถึงปลายทางจึงเป็นไปได้สูง ในการส่งผ่านข้อมูลนั้น ซึ่งปัญหาส่วนมากที่พบคือส่งไปไม่ได้ หรือปลายทางรับข้อมูลไม่ได้ เป็นต้น นอกจากนี้โพรโทคอล ICMP ยังถูกเรียกใช้งานจากเครื่องเซิร์ฟเวอร์และเราเตอร์ (Router) อีกด้วย เพื่อแลกเปลี่ยนข้อมูลที่ใช้ควบคุม ส่วนรูปแบบการทำงานของโพรโทคอล ICMP นั้นจะทำงานคู่กับโพรโทคอล IP ในระดับเดียวกัน และข้อความต่างๆ ที่แจ้งให้ทราบจะถูกผนึกอยู่ภายในข้อมูลของ IP (IP datagram) อีกทีหนึ่ง ข้อความที่โพรโทคอล ICMP ส่งนั้นแบ่งออกได้ 2 แบบคือ ICMP error message หรือข้อความแจ้งข้อผิดพลาด และ ICMP query หรือข้อความเรียกขอข้อมูลเพิ่มเติม ตัวอย่างกลไกการทำงานของโพรโทคอล ICMP เช่น เมื่อมีการส่งผ่านข้อมูลจากผู้ไปยังปลายทางที่ไม่ถูกต้อง หรือขณะนั้นเครื่องปลายทางเกิดปัญหาจนไม่สามารถรับข้อมูลได้ที่ router จะส่งข้อความแจ้งเป็น ICMP message ที่ชื่อ destination unreachable ให้กับผู้ส่งข้อมูล นอกจากนี้ตัวข้อมูลที่แจ้งข้อความก็จะมีส่วนของข้อมูล IP datagram ที่เกิดปัญหาคือ ดังนั้นเมื่อผู้ส่งข้อมูลได้รับข้อความแจ้งแล้วก็จะทราบได้ว่าจุดที่เกิดปัญหานั้นอยู่ที่ใด

ดังนั้นโพรโทคอล ICMP จึงกลายมาเป็นเครื่องมืออย่างหนึ่งในการช่วยทดสอบเครือข่าย เช่น คำสั่ง Ping ที่เรามักใช้ทดสอบว่าเครื่องเซิร์ฟเวอร์ที่ให้บริการหรืออุปกรณ์ที่ต่ออยู่ในเครือข่ายอินเทอร์เน็ตนั้นยังทำงานเป็นปกติหรือไม่ คำสั่ง Ping มีการเรียกใช้งานโพรโทคอล ICMP แจ้งเป็น

ข้อความให้ทราบอีกต่อหนึ่ง โพรโทคอล ICMP เป็นโพรโทคอลที่ช่วยเหลือระบบ ให้ทำงานได้อย่างมีประสิทธิภาพ ช่วยทำให้การดูแลเครือข่าย หรือการแสดงสถานะของเครือข่ายที่โหนดต่าง ๆ เป็นไปอย่างถูกต้อง และแจ้งสถานะของตนเองได้

Transmission Control Protocol (TCP) เป็นโพรโทคอลที่มีการรับส่งข้อมูลแบบ stream oriented protocol หมายความว่า การรับส่งข้อมูลจะไม่คำนึงถึงปริมาณข้อมูลที่จะส่งไป แต่จะแบ่งข้อมูลเป็นส่วนย่อย ๆ ก่อน แล้วจึงจะส่งไปยังปลายทางอย่างต่อเนื่องเป็นลำดับข้อมูล ในกรณีที่ข้อมูลส่วนใดส่วนหนึ่งสูญหายไป ก็จะส่งข้อมูลส่วนนั้นใหม่อีกครั้ง สำหรับปลายทางก็จะทำหน้าที่จัดเรียงส่วนของข้อมูล datagram ใหม่ให้ต่อเนื่องกันและประกอบกับเป็นข้อมูลทั้งหมดได้ ซึ่งจะแยกข้อมูลที่ไม่ว่างออก ดังนั้นแอปพลิเคชันหรือโปรเซสใดที่อาศัยการส่งผ่านข้อมูลด้วยโพรโทคอล TCP จะต้องใช้หน่วยความจำและขนาดของช่องสัญญาณ (bandwidth) มากกว่า UDP

การติดต่อระหว่างกันจะต้องเป็นแบบ connection-oriented ก็คือต้องมีการสร้างการติดต่อกันเป็น session ทั้ง 2 ด้านเสียก่อน แล้วจึงจะรับส่งข้อมูลไปได้พร้อมกัน (full duplex) เหมือนกับการใช้โทรศัพท์ติดต่อกัน เมื่อผู้ติดต่อต้นทางเรียกให้ฝ่ายตรงข้ามรับสายแล้ว จึงเริ่มการสนทนา เช่น พูดคำว่า “สวัสดี” หรือ “ฮัลโล” กันก่อนเพื่อให้แน่ใจว่าฝ่ายตรงข้ามพร้อมจะติดต่อด้วย จากนั้นจึงเริ่มต้นติดต่อกัน และเมื่อต้องการจะเลิกการติดต่อก็จะมีการพูดคำว่า “สวัสดี” ให้ฝ่ายตรงข้ามทราบว่าเลิกการติดต่อและวางสายไป ซึ่งในระหว่างการติดต่อกันนั้น แม้ว่าฝ่ายใดฝ่ายหนึ่งหรือทั้งสองฝ่ายจะเงียบไป คือไม่พูดอะไรเวลานาน ๆ แต่การเชื่อมโยงระหว่างทั้งสองด้านยังคงมีอยู่ไม่ขาดไป จนกว่าฝ่ายใดฝ่ายหนึ่งจะวางสาย เช่นเดียวกับการติดต่อกันด้วยกลไกโพรโทคอล TCP เมื่อแอปพลิเคชันต้องการส่งผ่านข้อมูลจะใช้โพรโทคอลที่เหมาะสมในชั้น Process layer ติดต่อไปและมีการสร้างช่องส่งข้อมูลผ่าน port ที่กำหนดเพื่อส่งผ่านข้อมูลไปยังโพรโทคอล TCP ในระหว่างการรับส่งข้อมูลนี้ โพรโทคอล TCP จะเพิ่มขบวนการสอบทานข้อมูลเพื่อให้ข้อมูลมีความถูกต้องไม่ผิดพลาดไปจากเดิม โดยการส่งสัญญาณสอบทานข้อมูล (acknowledgement) และส่งข้อมูลให้ใหม่อีกครั้ง ถ้าปลายทางไม่ได้รับหรือเกิดความผิดพลาดขึ้น ความน่าเชื่อถือของการส่งผ่านข้อมูลโดยโพรโทคอล TCP จะมีมากกว่า แต่ก็ต้องอาศัยทรัพยากรของระบบมากกว่าในการทำงานเช่นกัน

User Datagram Protocol (UDP) เป็นวิธีการสื่อสารหรือโพรโทคอลที่จำกัดจำนวนการบริการ เมื่อข่าวสารมีการแลกเปลี่ยน ระหว่างคอมพิวเตอร์ในเครือข่ายที่ใช้ Internet Protocol (IP) โดย UDP เป็นตัวเลือกหนึ่งของ Transmission Control Protocol (TCP) และใช้ร่วมกับ IP บางครั้ง

เรียกว่า UDP/IP ซึ่ง UDP เหมือนกับ TCP ในการใช้ IP ในการคั่นหน่วยข้อมูล (เรียกว่า datagram) จากคอมพิวเตอร์หนึ่งไปยังอีกเครื่องหนึ่งแต่ต่างจาก TCP โดย UDP ไม่ให้การบริการสำหรับการแบ่งข่าวสารเป็นแพ็กเก็ต และประกอบขึ้นใหม่เมื่อถึงปลายทาง UDP ไม่ให้ชุดของแพ็กเก็ตที่ข้อมูลมาถึง หมายความว่า โปรแกรมประยุกต์ที่ใช้ UDP ต้องมีความสามารถในการสร้างความมั่นใจว่าข่าวสารที่มาถึงอยู่ในลำดับที่ถูกต้อง UDP ให้ 2 บริการที่ไม่มีใน TCP โดยเลขของ IP คือ Port number เพื่อช่วยแยกแยะการขอของผู้ใช้ และความสามารถ checksum เพื่อตรวจสอบการมาถึงข้อมูล ในแบบจำลองการสื่อสาร Open System Interconnection (OSI) UDP เหมือนกับ TCP คือ อยู่ทีเลเยอร์ 4 Transport Layer

6. เทคนิคการค้นหาการบริการ (Service Discovery Techniques)

Active Probing จะค้นหาการบริการโดยการส่ง แพ็กเก็ต ไปยังแต่ละโฮสต์และติดตามการตอบสนอง (response) Active Probing จะเกี่ยวข้องกับโฮสต์ที่กำลังให้บริการอยู่ ดังนั้นผลลัพธ์ที่ได้จากการสำรวจจะได้รับผลกระทบจากไฟร์วอลล์ การค้นหาโฮสต์ที่ทำงานเป็นการค้นหาโดยการสำรวจพอร์ตเป้าหมาย หรือ การบริการ (service) ทั้งหมดของแต่ละโฮสต์บนเครือข่าย การค้นหาโฮสต์สามารถค้นหาการบริการได้อย่างรวดเร็วโดยการตรวจสอบสถานะของโฮสต์ และข้ามแอดเดรสที่ไม่ได้ใช้งาน

Passive Probing จะตรวจพบการบริการบนเครือข่ายโดยการสังเกตการจราจร (traffic) ที่เกิดขึ้นโดยเครื่องแม่ข่าย และเครื่องลูกข่าย ที่ผ่านจุดสังเกตและโดยทั่วไปจะมองไม่เห็นโฮสต์ที่กำลังให้บริการอยู่ ซึ่งการสำรวจการใช้งานแบบนี้จะไม่รบกวนการทำงานของระบบเครือข่าย ซึ่งจะมีการตรวจจับทั้งโปรโตคอล TCP และโปรโตคอล UDP

7. การตรวจสอบสถานะของโฮสต์

Ping คือโปรแกรมที่เป็นเครื่องมือเกี่ยวกับเครือข่ายคอมพิวเตอร์ ใช้ทดสอบว่าโฮสต์ (Host) ปลายทางได้เชื่อมต่อกับ IP Address อยู่หรือไม่ โปรแกรม Ping ทำงานโดยการส่งข้อมูล Internet Control Message Protocol ประเภท "echo request" ไปยังโฮสต์ปลายทาง และรอคอยการตอบรับเป็นข้อมูล "echo response" กลับมา โปรแกรม Ping สามารถประมาณเวลาเดินทางโดยเฉลี่ยของ

ข้อมูลไปกลับ โดยคำนวณจากช่วงเวลาและอัตราเร็วในการตอบรับ เป็นหน่วยมิลลิวินาที และอัตรา การสูญเสียข้อมูลระหว่างโฮสต์เป็นเปอร์เซ็นต์ โดยมีรูปแบบคำสั่งดังนี้

ping [target]

Nmap (Network Mapper) เป็นโปรแกรม open source ที่ใช้สแกนเครือข่ายและตรวจสอบ ความปลอดภัย ซึ่ง Nmap ถูกพัฒนาให้สามารถทำการสแกนเครือข่ายขนาดใหญ่ได้อย่างรวดเร็ว โดยการสแกน ip address เพื่อที่จะรายงาน port, application, OS หรือไฟร์วอลล์

รูปแบบการใช้งานคำสั่ง Nmap สามารถสรุปได้ดังต่อไปนี้

nmap [Scan Type (s)] [Options] {target specification}

Wireshark หรือที่รู้จักกันในชื่อเดิมว่า Ethereal เป็นโปรแกรมวิเคราะห์ข้อมูลบนเครือข่าย (Network Protocol Analyzer) ลักษณะเดียวกันกับโปรแกรม Microsoft Network Monitor หรือ Sniffer แตกต่างกันว่า Wireshark นั้นเป็นซอฟต์แวร์แบบโอเพนซอร์ส (Open Source) จึงใช้งานได้ โดยไม่มีค่าใช้จ่าย โดย Wireshark มีทั้งเวอร์ชันสำหรับระบบปฏิบัติการ Windows และ Unix และมี เวอร์ชัน 32-bit และ 64-bit ให้เลือกใช้งาน Wireshark สามารถทำการวิเคราะห์ข้อมูลบนเครือข่าย ได้หลากหลายรูปแบบ และมีฟีเจอร์สำคัญๆ ให้ใช้งานครบถ้วน เช่น การดูรายละเอียดต่างๆ ของ ข้อมูลที่แคปเจอร์จากระบบเครือข่าย สามารถทำการวิเคราะห์ข้อมูลได้ทั้งแบบเรียลไทม์และจาก ไฟล์ที่ได้จากแคปเจอร์ Wireshark เป็นซอฟต์แวร์แบบโอเพนซอร์ส จึงสามารถใช้งานได้ฟรีโดยไม่ ต้องเสียค่าลิขสิทธิ์ และมีต้นฉบับ (Source Code) สำหรับให้ผู้ที่สนใจนำไปพัฒนาต่อยอดได้

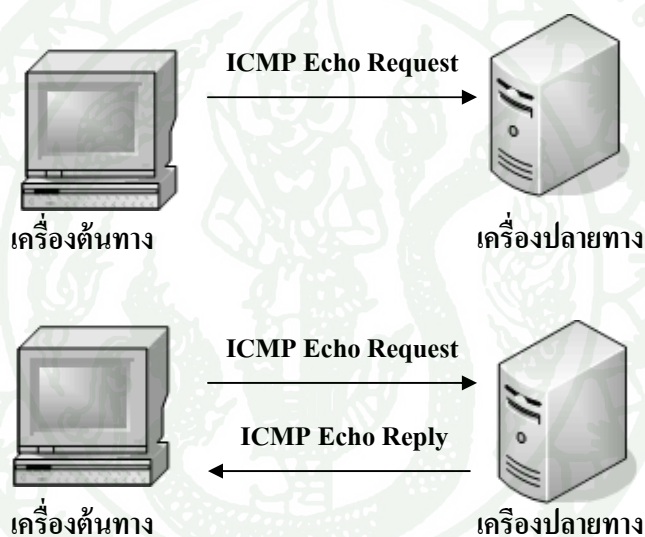
8. ประเภทของการสแกน

8.1 Ping Scan [-sP]

การสแกนแบบ Ping (Ping scan) เป็นการสแกนที่มีความรวดเร็วสูง เพื่อค้นหาโฮสต์ เพราะว่าไม่ต้องกำหนดพอร์ตที่ใช้ในการสแกน ไม่เหมือนกับการสแกนพอร์ตที่ทำให้เกิดการ แพ็กเก็ต เจ็ต จำนวนมากส่งถึงกันระหว่างเครื่องต้นทางกับเครื่องปลายทาง โดยการสแกนแบบ Ping เกิด

แพ็กเก็ต เพียงสองเลขอร์เท่านั้น ซึ่งเป็นประโยชน์มากกับเครื่องคอมพิวเตอร์ที่กำลังทำงานอยู่ หรือใช้เป็นตัวนำทางที่จะให้ โพรโทคอล ICMP สามารถผ่านด่านกั้นการบุกรุกได้

การทำงานของสแกนแบบ Ping เป็นการส่ง ICMP echo request จากเครื่องที่มีการติดตั้งโปรแกรม Nmap ไปยังเครื่องคอมพิวเตอร์ปลายทาง จากนั้นเครื่องปลายทางที่ทำงานอยู่จะส่ง ICMP echo reply กลับมา แต่ก็มีบางไอพีแอดเดรสที่ไม่ได้ทำงานบนเครือข่ายหรือ โพรโทคอล ICMP ที่ส่งไปถูกกรองด้วยไฟร์วอลล์ก็จะมี response ส่งไปถึง

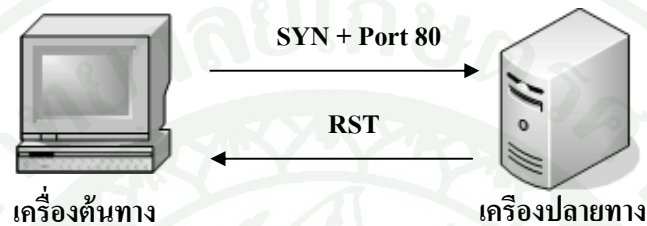


ภาพที่ 2 การสแกนแบบ Ping

8.2 TCP SYN Scan [-sS]

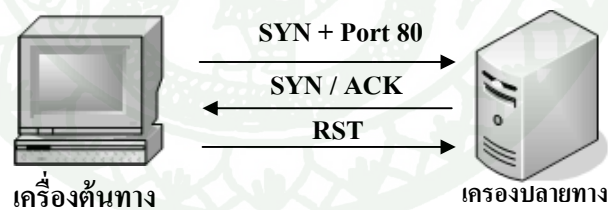
การสแกนแบบ TCP SYN เป็นการสแกนพอร์ตแบบ TCP – SYN อาศัยเทคนิคที่เรียกว่า Half Open คือใช้วิธีการระบุพอร์ต เพื่อให้ Nmap สามารถได้ข้อมูลเกี่ยวกับพอร์ตที่เปิดให้บริการก่อนที่จะกระบวนกร TCP handshake จะเสร็จสมบูรณ์ เทคนิคนี้จะทำให้โฮสต์ (Host) เป้าหมายส่วนใหญ่ยังไม่ทันได้บันทึกเหตุการณ์ไว้ใน Log จึงเป็นการสแกนที่ไม่ทิ้งร่องรอย

การทำงานของสแกนแบบ TCP SYN คือเครื่องต้นทางจะทำการส่ง SYN แฟ็กเก็ต และพอร์ตที่ต้องการทราบการให้บริการไปยังเครื่องปลายทาง ถ้าพอร์ตที่ต้องการทราบข้อมูลป้อนอยู่ responses ที่ได้รับการสแกนแบบ TCP SYN คือเครื่องปลายทางจะส่ง RST แฟ็กเก็ต กลับมา



ภาพที่ 3 การสแกนแบบ TCP SYN กรณีเครื่องปลายทางปิดพอร์ต

ถ้าส่ง SYN แฟ็กเก็ต และพอร์ตที่ต้องการทราบการให้บริการแล้วปรากฏว่าเครื่องปลายทางเปิดพอร์ตดังกล่าว เครื่องปลายทางก็จะส่ง SYN / ACK ตอบกลับมา จากนั้นเครื่องที่มี Nmap ก็จะส่ง RST แฟ็กเก็ต กลับไปยังเครื่องปลายทาง เพื่อทำการ reset session และก็ทำให้การ handshake ไม่เสร็จสมบูรณ์



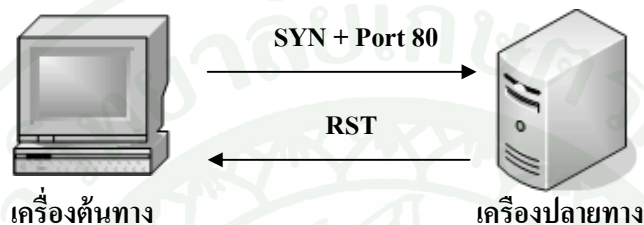
ภาพที่ 4 การสแกนแบบ TCP SYN กรณีเครื่องปลายทางเปิดพอร์ต

8.3 TCP connect() Scan [-sT]

การสแกนแบบ TCP connect() เป็นวิธีการพื้นฐานของโปรแกรม Port Scanner ซึ่งเป็นการจำลองกระบวนการร้องขอ (Request) เพื่อการติดต่อขอใช้บริการจากเครื่องลูกข่าย แต่วิธีการนี้จะง่ายต่อการตรวจจับโดยโฮสต์ (Host) ปลายทาง และถูกบันทึกเข้าสู่ Log

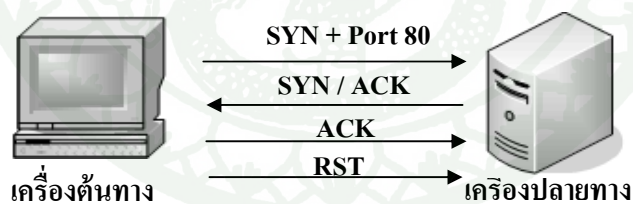
การทำงานของสแกนแบบ TCP connect() คือเครื่องต้นทางจะทำการส่ง SYN แฟ็กเก็ต และพอร์ตที่ต้องการทราบการให้บริการไปยังเครื่องปลายทาง ถ้าพอร์ตที่ต้องการทราบข้อมูล

ปิดอยู่ responses ที่ได้รับจากการสแกนแบบ TCP SYN คือเครื่องปลายทางจะส่ง RST แฉกเกิดกลับมา ซึ่งเหมือนกับการสแกนแบบ TCP SYN



ภาพที่ 5 การสแกนแบบ TCP connect() กรณีเครื่องปลายทางปิดพอร์ต

ถ้าส่ง SYN แฉกเกิด และพอร์ตที่ต้องการทราบการให้บริการแล้วปรากฏว่าเครื่องปลายทางเปิดพอร์ตดังกล่าว เครื่องปลายทางก็จะส่ง SYN / ACK ตอบกลับมา จากนั้นเครื่องที่มี Nmap ก็จะส่ง ACK แฉกเกิด ซึ่งเป็นการทำ TCP three-way handshake เสร็จสมบูรณ์ จากนั้นก็จะส่ง RST แฉกเกิด กลับไปยังเครื่องปลายทางทันทีเพื่อทำการปิดการเชื่อมต่อ

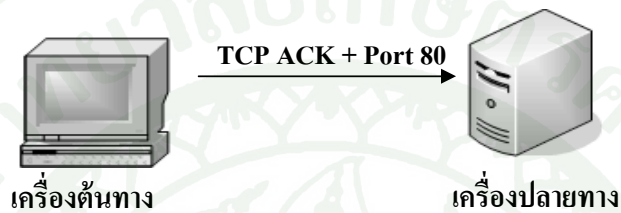


ภาพที่ 6 การสแกนแบบ TCP connect() กรณีเครื่องปลายทางเปิดพอร์ต

8.4 ACK Scan [-sA]

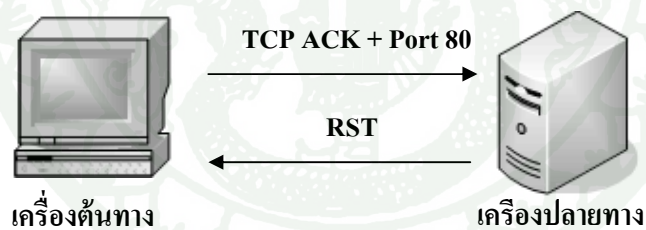
การสแกนแบบ ACK Scan เป็นเทคนิคที่ใช้ค้นหาบริการที่เปิดให้บริการอยู่แต่ปฏิเสธการตอบสนองต่อ ICMP Ping เพื่อตรวจสอบว่า firewall สามารถกรอง แฉกเกิด อะไรไว้บ้าง โดยการสแกนแบบนี้จะใช้ TCP แฉกเกิด ที่มี flag เป็น ACK ส่งไปยังพอร์ตเครื่องปลายทาง ถ้าพอร์ตเปิดอยู่ เครื่องปลายทางจะส่ง RST กลับมา แต่ถ้าปิดอยู่ก็จะไม่สนใจ แฉกเกิด นั้น

การทำงานของสแกนแบบ ACK Scan คือเครื่องต้นทางจะทำการส่ง TCP ACK และพอร์ตที่ต้องการทราบการให้บริการไปยังเครื่องปลายทาง เพื่อที่ต้องการ remote port ถ้าไม่มี responses หรือ มีข้อความ ICMP ว่าไม่พบโฮสต์ปลายทางตอบกลับมา แสดงว่าพอร์ตดังกล่าวถูกดักจับการบุกรุก (filtered)



ภาพที่ 7 การสแกนแบบ ACK Scan กรณีเครื่องปลายทางปิดพอร์ต

ถ้าเครื่องปลายทางส่ง RST แพ็กเก็ต กลับมา แสดงว่าการเชื่อมต่อระหว่างเครื่อง Nmap ต้นทางกับเครื่องปลายทางที่ถูก remote port จัดอยู่ในประเภทไม่ถูกดักจับการบุกรุก (unfiltered)



ภาพที่ 8 การสแกนแบบ ACK Scan กรณีเครื่องปลายทางเปิดพอร์ต

9. ตัวเลือก (option) ของโปรแกรม Nmap ที่ใช้สำหรับการสแกน

9.1 PA [portlist]

การทำงานคือจะทำการสุ่ม TCP ACK ส่งไปยังเครื่องปลายทาง ถ้าเครื่องปลายทางทำงานอยู่ก็จะทำการส่ง RST แพ็กเก็ต กลับมา แต่ถ้าเครื่องปลายทางไม่ได้ทำงาน หรือพอร์ตถูกดักจับการบุกรุกก็จะไม่มี response ตอบกลับมา แสดงว่าโฮสต์ดังกล่าวเป็น Host down

ถ้าใช้ -PA ในรูปแบบการสแกนแบบ TCP ACK เครื่องต้นทางจะทำการส่ง TCP ACK พร้อมพอร์ตที่ต้องการทราบการให้บริการไปยังเครื่องปลายทาง และเครื่องปลายทางก็จะส่ง RST แพ็กเก็ต กลับมา แต่ถ้าไม่มีการส่ง response ตอบกลับมา แสดงว่าไอพีแอดเดรสปลายทางไม่ได้ใช้งานหรือเครื่องปลายทางอยู่หลัง firewall

ถ้าใช้ -PA ในรูปแบบการสแกนแบบ TCP connect() คือเครื่องต้นทางจะทำการส่ง SYN แพ็กเก็ต และพอร์ตที่ต้องการทราบการให้บริการไปยังเครื่องปลายทาง ถ้าพอร์ตที่ต้องการทราบข้อมูลป้อนอยู่ responses ที่ได้รับจากการสแกนแบบ TCP SYN คือเครื่องปลายทางจะส่ง RST แพ็กเก็ต กลับมา

ถ้าใช้ -PA ในรูปแบบการสแกนแบบ TCP connect() คือเครื่องต้นทางจะทำการส่ง SYN แพ็กเก็ต และพอร์ตที่ต้องการทราบการให้บริการแล้วปรากฏว่าเครื่องปลายทางเปิดพอร์ตดังกล่าว เครื่องปลายทางก็จะส่ง SYN / ACK ตอบกลับมา จากนั้นเครื่องที่มี Nmap ก็จะส่ง ACK แพ็กเก็ต ซึ่งเป็นการทำ TCP three-way handshake เสร็จสมบูรณ์ จากนั้นก็จะส่ง RST แพ็กเก็ต กลับไปยังเครื่องปลายทางทันทีเพื่อทำการปิดการเชื่อมต่อ

9.2 PS [portlist] เหมือนกับกระบวนการของ TCP SYN scan

ถ้าใช้ -PS ในรูปแบบการสแกนแบบ TCP SYN คือเครื่องต้นทางจะทำการส่ง SYN แพ็กเก็ต และพอร์ตที่ต้องการทราบการให้บริการไปยังเครื่องปลายทาง ถ้าพอร์ตที่ต้องการทราบข้อมูลป้อนอยู่ responses ที่ได้รับจากการสแกนแบบ TCP SYN คือเครื่องปลายทางจะส่ง RST แพ็กเก็ต กลับมา

ถ้าใช้ -PS ในรูปแบบ TCP SYN คือ ถ้าส่ง SYN แพ็กเก็ต และพอร์ตที่ต้องการทราบการให้บริการแล้วปรากฏว่าเครื่องปลายทางเปิดพอร์ตดังกล่าว เครื่องปลายทางก็จะส่ง SYN / ACK ตอบกลับมา จากนั้นเครื่องที่มี Nmap ก็จะส่ง RST แพ็กเก็ต กลับไปยังเครื่องปลายทาง

ถ้าใช้ -PS ในรูปแบบการสแกนแบบ TCP connect() คือเครื่องต้นทางจะทำการส่ง SYN แพ็กเก็ต และพอร์ตที่ต้องการทราบการให้บริการแล้วปรากฏว่าเครื่องปลายทางเปิดพอร์ตดังกล่าว เครื่องปลายทางก็จะส่ง SYN / ACK ตอบกลับมา จากนั้นเครื่องที่มี Nmap ก็จะส่ง ACK

แพ็กเก็ต ซึ่งเป็นการทำ TCP three-way handshake เสร็จสมบูรณ์ จากนั้นก็จะส่ง RST แพ็กเก็ต กลับไปยังเครื่องปลายทางทันทีเพื่อทำการปิดการเชื่อมต่อ

10. เทคนิคในการสแกน

เรื่องเวลา

- T[0-5] : กำหนดเวลาในการสำรวจ
- --scan-delay/--max-scan-delay <time> : ปรับเปลี่ยน delay ของการสำรวจ
อื่นๆ
- n (No DNS resolution) : เป็นการช่วยให้ประหยัดเวลาในการ Probe เพราะไม่ต้องไปติดต่อกับ DNS หรือ Domain Server หากเราไม่ต้องการรู้ว่า IP ดังกล่าวจะจดทะเบียน Domain name ว่าจะไร

11. ลักษณะการทำงานของโปรแกรม Nmap

การใช้ Nmap ตรวจสอบว่า host อยู่ในสถานะ online หรือ offline คือเป็นการตรวจสอบในแง่ของการค้นหาโฮสต์ (Host discovery) โปรแกรม Nmap จะสามารถตอบเราได้ว่าโฮสต์ตัวนั้น up (online) หรือ down (offline) ซึ่งการจะตัดสินใจว่า up หรือ down ก็จะขึ้นกับโปรโตคอลที่เราเลือกใช้

การใช้ Nmap ทำการ สแกนพอร์ตจะได้ผลลัพธ์ 3 รูปแบบคือ

- open : ให้บริการอยู่
- filtered : หมายถึงโดน Firewall กันไว้หรือมีอุปสรรคอื่นๆ ที่ block พอร์ตนั้นไว้ หรือกรณีอื่นๆ ที่ไม่สามารถตัดสินใจได้ว่า Open หรือ Close
- close : ตอนนี้ไม่มี Application ใดๆ รอฟังการบริการจากพอร์ต แต่ว่าพอร์ตดังกล่าวนี้จะถูกใช้งานเมื่อไรก็ได้

งานวิจัยที่เกี่ยวข้อง

นอกจากทฤษฎีที่เกี่ยวข้องที่กล่าวมาข้างต้นแล้วนั้น ผู้วิจัยยังได้ศึกษางานวิจัยเกี่ยวกับการสำรวจไอพีแอดเดรส และการวิเคราะห์ลักษณะการใช้งานโดยมีงานวิจัยที่เกี่ยวข้องดังนี้

งานวิจัยเรื่อง Understanding Passive and Active Service Discovery ของ Bartlett *et al.* (2007) ได้ทำการศึกษาการค้นหาคำบริการ (service discovery) 2 วิธีการคือ Active Probing และ Passive Probing โดยเปรียบเทียบความถูกต้องของการสำรวจของทั้งสองวิธีการ ซึ่งผลการทดลองพบว่า การค้นหาด้วย Passive Probing พบไอพีแอดเดรสประมาณ 99% แต่การค้นหาแบบ Active Probing จะสำรวจพบประมาณ 98% แสดงให้เห็นว่าข้อจำกัดทางด้านความเป็นส่วนตัว ปลอดภัยมีผลกระทบต่อ การสำรวจ โดยการสำรวจ Passive จะพบการบริการจำนวนมากทั้งการบริการที่เป็นระยะแฝง (intermittent) และการบริการที่มีป้องกัน แม้ว่าการให้บริการเหล่านี้จะถูกป้องกันด้วยไฟร์วอลล์ ส่วนค้นหาแบบ Active Probing จะไม่สามารถสำรวจพบ

งานวิจัยเรื่อง Census and survey of the visible Internet ของ Heidemann *et al.* (2008) ได้ทำการสำรวจไอพีแอดเดรสโดยแบ่งการสำรวจออกเป็น 2 แบบคือการสำรวจประชากร (census) และการสำรวจแบบสุ่มตัวอย่าง (survey) ซึ่งทั้งสองแบบจะทำการแบ่งลักษณะของ IPv4 Address ออกเป็น 2 ลักษณะคือ Visible Internet คือ โพรโทคอล ICMP สามารถมองเห็น และ Invisible Internet (เช่น IPv4 Address ที่ซ่อนอยู่หลัง firewall) คือ โพรโทคอล ICMP ไม่สามารถมองเห็น แต่โพรโทคอลอื่นสามารถเห็นได้เช่น โพรโทคอล TCP โดยการสำรวจจะทำการวิเคราะห์ข้อมูลที่ได้จากการสำรวจ มีการแบ่งรูปแบบการตอบกลับ (respond) ออกเป็น 3 รูปแบบคือ Positive acknowledgement (แสดงถึงการมีโฮสต์อยู่จริงที่ IP Address นั้น), Negative acknowledgement (คือไม่สามารถเข้าถึงโฮสต์นั้นได้ ณ เวลานั้น หมายถึง Host Down หรือว่า IP Address ไม่ได้ใช้งาน) และ No reply คือขาดการตอบรับ โดยการสำรวจจะทำการตรวจสอบสถานะของโฮสต์เป็นตัววัดปริมาณ IP Address ที่ใช้งานจริง ซึ่งจะทำการตรวจสอบสถานะของ Host โดยตรวจสอบ IP Address ด้วยชุดคำสั่ง Ping และ Nmap ในงานวิจัยนี้ได้ทำการเลือกโพรโทคอลที่ใช้ในการสำรวจคือโพรโทคอล ICMP และโพรโทคอล TCP เพื่อนำมาเปรียบเทียบผลการสำรวจว่าโพรโทคอลใดสามารถที่จะตอบสนองต่อการสำรวจได้มากกว่ากัน ซึ่งจากการสำรวจก็พบว่าจำนวนโฮสต์ที่ตอบสนองต่อ โพรโทคอล ICMP มีมากกว่าโพรโทคอล TCP แสดงว่าโพรโทคอล TCP ถูกกรองโดย firewall มากกว่า นอกจากนี้โพรโทคอล TCP ยังก่อให้เกิดความรำคาญต่อผู้ที่ถูกตรวจสอบง่าย

กว่า (คิดว่าเป็น Distributed denial of service) จึงตัดสินใจเลือกโปรโตคอล ICMP เป็นโปรโตคอลที่ใช้ในการสำรวจ

งานวิจัยเรื่อง Active Probing to Classify Internet Address Blocks ของ Cai *et al.* (2008) ได้ทำการสำรวจศักยภาพของ Active Probing และ external classification ของการใช้ block address โดยงานวิจัยนี้มีการตั้งสมมุติฐานไว้ 3 สมมุติฐานคือ จำนวนไอพีแอดเดรสที่มีการตอบสนองกับการสำรวจ (probe) ภายนอกมีเท่าไร บางรูปแบบของการ probe ซ้ำนั้นสามารถบอกได้ถึงการใช้งานไอพีแอดเดรสที่แตกต่างกันหรือไม่ และไอพีแอดเดรสที่ต่อเนื่องกันหรือใกล้เคียงกันจะเป็นไอพีแอดเดรสที่มีการใช้งานในวัตถุประสงค์เหมือนกัน ซึ่งในงานวิจัยก่อนหน้านี้จะศึกษาประสิทธิภาพของการสำรวจด้วย โปรโตคอล ICMP และโปรโตคอล TCP โดยจะแสดงการตรวจสอบในเรื่องของการใช้ไอพีแอดเดรส โดยงานวิจัยนี้จะขยายบน 2 สมมุติฐานโดยใช้ผลการสำรวจเพื่อศึกษา address allocation และเพื่อสรุปการใช้งานไอพีแอดเดรส โดยมีขั้นตอนในการสำรวจจะแบ่งเป็น 4 ขั้นตอนคือ การสำรวจ (Survey) จะทำการ probe ส่วนของ Internet address space บ่อยๆ โดยเลือก 24,000 /24 block (ประมาณ 1% ของพื้นที่ที่ไอพีแอดเดรสมีการครอบครอง) และใช้ ICMP echo request แฝกเกิด ส่งไป probe แบบ active ในแต่ละไอพีแอดเดรสใน block ทุก 11 นาทีในรอบสัปดาห์ การวิเคราะห์รูปแบบ (Pattern Analysis) จะทำการวิเคราะห์การใช้งานของแต่ละไอพีแอดเดรสบน survey replies ซึ่งเราจะระบุหลายตัววัดเพื่อบอกลักษณะไอพีแอดเดรส สิ่งแรกคือแต่ละไอพีแอดเดรสจะถูกพิจารณาสถานะที่เป็น up เมื่อมีการตอบสนอง (respond) กับ Ping และจะระบุเป็น up duration, การจัดเป็นกลุ่ม (Clustering) จะทำการจัดกลุ่มไอพีแอดเดรสที่ใกล้เคียงกันมีการใช้เหมือนกัน ใน block ซึ่งการทดลองปัจจุบันจะใช้สำหรับแบ่งกลุ่มที่แตกต่างกัน เพื่อสำรวจความเป็นไปได้ของ block ทั้งหมดที่ความยาว prefix จาก /29 ถึง /24 (กลุ่มของ 8 ถึง 256 address) และการจัดแบ่งประเภท (Classification) จะแยก block จากการจัดกลุ่มออกได้ 5 ประเภทคือ server และ block ที่เป็น stable, intermittent (เป็นช่วงๆ ไม่ต่อเนื่อง), underutilized (ไม่ทำประโยชน์), หรือ unclassifiable (ไม่สามารถแบ่งแยกได้)

งานวิจัยเรื่อง Understanding Address Usage in the Visible Internet ของ Cai *et al.* (2009) จะทำการปรับปรุงอัลกอริทึมการจัดกลุ่มเพื่อประมาณการว่าไอพีแอดเดรสมีการใช้งานอย่างไรจะแสดงให้เห็นว่าไอพีแอดเดรสที่อยู่ติดกันบ่อยๆ จะมีลักษณะคล้ายกันและมีการใช้งานสำหรับวัตถุประสงค์เดียวกัน ในงานวิจัยนี้เริ่มต้นสำรวจศักยภาพของการจัดกลุ่มของการสำรวจด้วย Active Probing เพื่ออ้างถึงการใช้งานไอพีแอดเดรส โดยงานวิจัยจะทำ 3 สมมุติฐานคือ Active

address จำนวนมากจะตอบสนองต่อการสำรวจ ไอพีแอดเดรสที่อยู่ติดกันจะมีการใช้งานที่เหมือนกันบ่อยๆ และรูปแบบการตอบสนองต่อการสำรวจจะบอกถึงไอพีแอดเดรสมีการใช้งาน ซึ่งผลการทดลองพบว่าไอพีแอดเดรสจำนวนมากตอบสนองกับ Active Probing และเป็นไอพีแอดเดรสที่ต่อเนื่อง แสดงว่าเป็นการใช้งานคล้าย ๆ กัน

งานวิจัยเรื่อง Understanding Block-level Address Usage in the Visible Internet ของ Cai *et al.* (2010) ได้มีการประยุกต์ block level โดยการจับกลุ่มเพื่อให้ข้อมูลที่ทำให้การสำรวจเกิดประเด็นว่าเครือข่ายมีการจัดการอย่างไร ซึ่งมีการกำหนดสมมติฐานไว้ 3 สมมติฐานคือไอพีแอดเดรสที่ตอบสนองต่อการสำรวจจะเป็นไอพีแอดเดรสที่มีการใช้งาน ไอพีแอดเดรสที่อยู่ติดกันจะมีการใช้งานเหมือนกันหรือคล้ายกัน และรูปแบบของการตอบสนองจะบอกถึงลักษณะการใช้งานไอพีแอดเดรส จากสมมติฐานดังกล่าวสามารถพัฒนาอัลกอริทึมเพื่อระบุ block ของหมายเลขไอพีแอดเดรสที่มีการใช้งานอย่างสอดคล้องกัน จากการสำรวจดังกล่าวพบว่าหลาย block มีการใช้งานเพียงเล็กน้อย (ประมาณ 1 ใน 5 ของ /24 แสดงให้เห็นว่าน้อยกว่า 10% ของการใช้ประโยชน์) การพัฒนาอัลกอริทึมเป็นการเพิ่มความสามารถในการจัดการพื้นที่ว่างของ IPv4 address ให้มีประสิทธิภาพ ซึ่งไอพีแอดเดรสปัจจุบันใกล้ที่จะถูกจัดสรรเต็มแล้ว การปรับปรุงประสิทธิภาพ IPv4 เป็นการวัดต้นทุนเพื่อเปรียบเทียบกับเปลี่ยนแปลงไปเป็น IPv6 การศึกษางานวิจัยนี้ก็เพื่อปรับปรุงวิธีการใหม่เพื่อแบ่งแยกการใช้งานไอพีแอดเดรสและนำไปประยุกต์ใช้กับวิธีการอื่นๆ

อุปกรณ์และวิธีการ

การศึกษการใช้งานจริงของไอพีแอดเดรสที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์ มีวัตถุประสงค์เพื่อให้ทราบจำนวนของไอพีแอดเดรสที่มีการถูกใช้งาน และสามารถจัดสรรจำนวนไอพีแอดเดรสให้เหมาะสมกับองค์กร หรือหน่วยงาน รวมทั้งสามารถคาดการณ์แนวโน้มในการพัฒนาเครือข่ายให้สามารถรองรับการใช้งานได้อย่างมีประสิทธิภาพ

อุปกรณ์

Software:

- 1.1 โปรแกรม Nmap (Network Mapper) สำหรับสแกนเครือข่าย ตรวจสอบสถานะของโฮสต์
- 1.2 โปรแกรม Wireshark สำหรับดักจับข้อมูล และวิเคราะห์ระบบเครือข่าย
- 1.3 Operating System: Ubuntu

วิธีการ

จุดมุ่งหมายสำคัญของงานวิจัยนี้คือ เพื่อศึกษการใช้งานประโยชน์ของไอพีแอดเดรสเวอร์ชัน 4 ที่มีการจัดสรรภายในเครือข่ายมหาวิทยาลัยเกษตรศาสตร์ โดยการสำรวจปริมาณไอพีแอดเดรสด้วยวิธีการ Active Probing และ Passive Probing, วิเคราะห์ผลการสำรวจ คาดการณ์ลักษณะการใช้งานไอพีแอดเดรสภายในองค์กร หรือหน่วยงานของมหาวิทยาลัยดังรายละเอียดต่อไปนี้

1. ประชากรและกลุ่มตัวอย่าง

- 1.1 ประชากร ที่ใช้ในการวิจัยเป็นไอพีแอดเดรส (IP address) ภายในเครือข่ายมหาวิทยาลัยเกษตรศาสตร์ ซึ่งหมายเลขไอพีแอดเดรส (IP address) อยู่ภายใต้คลาสบี (Class B) คือ 158.108.0.0/16

1.2 กลุ่มตัวอย่าง ที่ใช้ในการวิจัยเป็นไอพีแอดเดรส (IP address) ภายในเครือข่ายมหาวิทยาลัยเกษตรศาสตร์ กลุ่มตัวอย่างจะเลือกจากหมายเลขไอพีแอดเดรสใน block ของ 256 address หรือ /24 prefix

2. การเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูลในการสำรวจปริมาณไอพีแอดเดรส (IP address) ได้ทำการสำรวจและวิเคราะห์ข้อมูลภายใต้สภาพแวดล้อมการใช้งานคอมพิวเตอร์ของเครือข่ายมหาวิทยาลัยเกษตรศาสตร์ ซึ่งการรวบรวมข้อมูล มีขั้นตอนการเก็บรวบรวมข้อมูลคือ การเตรียมการทดลอง วันเวลาในการทดลอง ขั้นตอนการทดลองและการเก็บรวบรวมข้อมูล ซึ่งมีรายละเอียดดังนี้

2.1 การเตรียมการสำรวจ คือ การเตรียมความพร้อมของเครื่องมือ จัดเตรียมเครื่องคอมพิวเตอร์ให้มีสภาพพร้อมใช้งาน ได้แก่ เครื่องคอมพิวเตอร์เป็นระบบปฏิบัติการยูนิกซ์ ติดตั้งโปรแกรม Nmap และ Wireshark พร้อมต่อเชื่อมระบบเครือข่าย ขนาดของหน่วยเก็บข้อมูลมีพื้นที่จำนวนมากสำหรับเก็บข้อมูลที่ได้จากการสำรวจ

2.2 การออกแบบการสำรวจ

2.2.1 การเลือกใช้โปรโตคอลในการสำรวจ คือ ทุกโหนดต้องรู้จักโปรโตคอลรูปแบบการร้องขอ (request) ของโปรโตคอลที่ใช้ในการสำรวจ และรูปแบบการตอบกลับ (respond) ต้องมีความแน่นอน รวมทั้งรูปแบบการสำรวจจะต้องไม่มีอันตราย ต้องพยายามออกแบบไม่ให้ฝ่ายที่ถูกตรวจสอบคิดว่าถูกโจมตี หรือ DDOS (Distributed denial of service) Attack คือการระดมส่งข้อมูลในรูปแบบที่ควบคุมได้โดยผู้ควบคุมการโจมตีไปยังเหยื่อหรือเป้าหมายที่ต้องการ ซึ่งการโจมตีรูปแบบนี้ก่อให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่จนผู้อื่นไม่สามารถใช้งานได้ตามปกติ หรือทำให้ระบบที่ถูกโจมตีไม่มีทรัพยากรเหลือพอที่จะให้บริการผู้ใช้ธรรมดาได้ เพื่อให้สามารถสำรวจได้ข้อมูลทั้งหมด และถูกต้อง

2.2.2 การวิเคราะห์ข้อมูลที่ได้จากการสำรวจ มีการแบ่งรูปแบบการตอบกลับ (respond) ออกเป็น 3 รูปแบบคือ Positive acknowledgement (แสดงถึงการมีโฮสต์อยู่จริงที่ไอพี

แอดเดรสนั้น) Negative acknowledgement (คือไม่สามารถเข้าถึงโฮสต์นั้นได้ ณ เวลานั้น หมายถึง Host Down หรือว่าไอพีแอดเดรสไม่ได้ใช้งาน) และ No reply คือขาดการตอบรับ (ซึ่งอาจเกิดได้จากหลายสาเหตุ เช่น การไหลของข้อมูล (traffic) มีความแออัดเกินไป หรือเป็นผลจากการถูกกรองข้อมูลด้วยไฟร์วอลล์)

2.2.3 ความถี่ในการส่งการร้องขอ (Request) จะต้องส่งการร้องขอไปสำรวจในรูปแบบของการสุ่มแต่ละช่วงเวลา เพื่อลดความผิดพลาดของการรบกวนระบบเครือข่ายของมหาวิทยาลัย ซึ่งทำให้ได้ผลการสำรวจไม่ถูกต้อง และการร้องขอที่เกิดขึ้นจะต้องไม่อยู่ในรูปแบบของการบุกรุก หรือโจมตีเครือข่าย ถ้าหากการสำรวจในครั้งแรกล้มเหลว ต้องมีการส่งการร้องขออีกครั้ง เพื่อได้ผลการสำรวจที่น่าเชื่อถือมากขึ้น

2.3 ขั้นตอนการสำรวจด้วยวิธี Active Probing

2.3.1 เลือกโปรโตคอลที่จะใช้ในการสำรวจสถานะของโฮสต์ เพื่อหาปริมาณของไอพีแอดเดรส ซึ่งในการสำรวจครั้งนี้จะใช้โปรโตคอล ICMP และ โปรโตคอล TCP เพราะว่าโปรโตคอล ICMP สามารถตรวจสอบสถานะของโฮสต์ได้อย่างรวดเร็ว และมีความถูกต้องสูง ส่วนโปรโตคอล TCP ใช้ในการสแกนพอร์ต เพื่อช่วยให้ได้รับข้อมูลในการสำรวจได้ถูกต้อง แม่นยำมากยิ่งขึ้น เนื่องจากโปรโตคอล TCP สามารถตรวจพบบางไอพีแอดเดรสที่ออนไลน์ แต่ไม่สามารถตรวจพบได้ด้วยโปรโตคอล ICMP เพราะว่าไอพีแอดเดรสบางไอพีได้บล็อกการ Ping ไว้ แต่การสำรวจด้วยโปรโตคอล TCP ใช้เวลาในการสำรวจมากกว่าการใช้ โปรโตคอล ICMP โดยมีการเลือกสแกนพอร์ต ดังนี้ พอร์ต 21 (ftp) 22 (ssh) 25(smtp) 53 (domain) 80 (http) 110 (pop3) 135 (epmap) 137 (netbios) 139 (netbios) 443 (https) 445 (microsoft-ds) 458 (appleqtcp) 587 (submission) 1433 (ms-sql-s) 1434 (ms-sql-m) 1214 (kazaa) 3306 (mysql) 6346(gnutella) 1863 (msnp)

2.3.2 เลือกเครื่องมือที่ใช้ในการสำรวจสถานะของโฮสต์ ในการสำรวจครั้งนี้ได้เลือกใช้โปรแกรม Nmap สำหรับการสำรวจด้วยวิธีการ Active Probing ซึ่งใช้สำหรับสแกนเครือข่าย ตรวจสอบสถานะของโฮสต์ และปริมาณไอพีแอดเดรส เพราะว่าเป็นโปรแกรมที่สามารถตรวจสอบสถานะของโฮสต์ได้หลายรูปแบบ สามารถระบุลักษณะของการสำรวจได้ตามต้องการ เช่น ชนิดของโปรโตคอลที่ใช้สำรวจ เทคนิคการสแกนค้นหาโฮสต์ ระบุพอร์ต การจัดการ

เกี่ยวกับเวลาที่ใช้ในการสำรวจ และสามารถรับ input ได้หลายรูปแบบ และสามารถนำหลายทางเลือก (option) มารวมกันภายในคำสั่งเดียวได้ นอกจากนี้ Nmap ยังสามารถปรับระดับความเร็วให้เหมาะสมกับเครือข่ายที่ใช้งานได้อย่างอัตโนมัติ

2.3.3 เลือกตัวเลือก (option) ของโปรแกรม Nmap ที่เหมาะสมสำหรับการสำรวจปริมาณไอพีแอดเดรสด้วยวิธีการ Active Probing โดยการสำรวจได้ใช้คำสั่งคือ

```
nmap -sP -n [target]
nmap -PA [portlist] -n [target]
nmap -PS [portlist] -n [target]
```

พอร์ตที่ใช้ในการสำรวจคือ พอร์ต 21 (ftp) 22 (ssh) 25(smtp) 53 (domain) 80 (http) 110 (pop3) 135 (epmap) 137 (netbios) 139 (netbios) 443 (https) 445 (microsoft-ds) 458 (appleqt) 587 (submission) 1433 (ms-sql-s) 1434 (ms-sql-m) 1214 (kazaa) 3306 (mysql) 6346(gnutella) 1863 (msnp) เพราะว่าสภาพแวดล้อมของมหาวิทยาลัยเกษตรศาสตร์การใช้งานเครือข่ายส่วนมากเป็นการทำงานของนิสิต อาจารย์ พนักงานภายในมหาวิทยาลัย ดังนั้นการใช้งานจะเป็นการใช้งานเว็บไซต์ การส่งข้อมูลผ่านระบบเครือข่าย และระบบปฏิบัติการที่ใช้ส่วนมากจะเป็นระบบปฏิบัติการวินโดวส์

2.3.4 กำหนดระยะเวลาในการส่งการร้องขอ (request) เพื่อทำการสำรวจ โดยทำการสำรวจภายในมหาวิทยาลัยเกษตรศาสตร์ โดยการสำรวจทุกๆ 5 ชั่วโมงสำหรับรอบแรก ทั้งการ Ping โดยโปรโตคอล ICMP เพื่อค้นหาสถานะของโฮสต์และการสแกนพอร์ต ด้วยโปรโตคอล TCP เพื่อค้นหาว่าไอพีแอดเดรสที่มีการบล็อกการ Ping และทำการสำรวจอีกครั้งทุก 20 นาทีโดยทำการสำรวจทีละ 10 บล็อก บล็อกละ 256 หมายเลขไอพีแอดเดรส โดยเลือกเฉพาะบล็อกที่พบไอพีแอดเดรสที่ตอบสนองต่อการสำรวจในรอบแรก ใช้ระยะเวลา 7 วันในการเก็บข้อมูล แสดงข้อมูลการสำรวจตามตารางผนวกที่ ก1 ชุดข้อมูลที่ได้จากการทดลองสำรวจจำนวนไอพีแอดเดรสด้วยวิธี Active Probing

2.3.5 เริ่มทำการสำรวจไอพีแอดเดรสทั้งหมดภายในมหาวิทยาลัยเกษตรศาสตร์ในกรณีที่ทำการสำรวจด้วยวิธี Active Probing ซึ่งจากชุดข้อมูลที่ได้จากการทดลองสำรวจจำนวนไอพีแอดเดรสด้วยวิธี Active Probing ตามตารางผนวกที่ ก1 นั้นจะเห็นได้ว่าการสำรวจของเราจะมีการแบ่งการสำรวจตามรูปแบบของ prefix length เช่น /24 ก็จะทำการสำรวจทีละ 256 หมายเลขไอพี

แอดเดรส /25 ทำการสำรวจทีละ 128 หมายเลขไอพีแอดเดรส /26 ทำการสำรวจทีละ 64 หมายเลขไอพีแอดเดรส /27 ทำการสำรวจทีละ 32 หมายเลขไอพีแอดเดรส /28 ทำการสำรวจทีละ 16 หมายเลขไอพีแอดเดรส และ /16 ทำการสำรวจทีเดียวทั้งหมดทั้ง Class B โดยจะสำรวจทุก 20 นาทีทีละ 10 บล็อกที่มีการตอบสนองการสำรวจในรอบแรก โดยการสำรวจรอบแรกนั้นจะทำการสำรวจทุกไอพีแอดเดรสในทุก 5 ชั่วโมง ซึ่งช่วงเวลาที่กำหนดให้มีการสำรวจจะแบ่งเป็น 3 ช่วงต่อวันคือ 8 โมงเช้า บ่าย 3 โมง และ 2 ทุ่ม

2.3.6 จัดเก็บข้อมูลที่ได้จากการสำรวจจะทำการเขียนคำสั่ง (script) ที่ใช้สำหรับการสำรวจสถานะของโฮสต์ภายในเครือข่ายมหาวิทยาลัยเกษตรศาสตร์ เพื่อทำการสำรวจปริมาณของไอพีแอดเดรสให้เป็นไปอย่างอัตโนมัติ โดยภายในคำสั่งจะมีองค์ประกอบในการแปลงข้อมูลของการสำรวจด้วย Nmap ให้เป็นไฟล์ที่มีนามสกุล .txt เพื่อให้สามารถเข้าใจได้ง่าย และสะดวกต่อการรวบรวมข้อมูลหรือนำไปวิเคราะห์มากยิ่งขึ้น

2.3.7 รวบรวมผลการทดลองทั้งหมดที่สำรวจได้ นำมาวิเคราะห์หาจำนวนของไอพีแอดเดรสที่มีการตอบสนองต่อการสำรวจ ค่า Availability หรือ A(address) ค่า Volatility หรือ V(address) และ ค่า Uptime หรือ U(address) ของแต่ละแอดเดรสวิธีการสำรวจด้วย Active Probing

2.4 ขั้นตอนการสำรวจด้วยวิธี Passive Probing

2.4.1 เลือกเครื่องมือที่ใช้ในการสำรวจสถานะของโฮสต์ ในการสำรวจครั้งนี้ได้เลือกใช้โปรแกรม Wireshark ในการสำรวจด้วยวิธี Passive Probing เพื่อตรวจจับ traffic ที่เกิดขึ้นในเครือข่าย สามารถทำการวิเคราะห์ข้อมูลบนเครือข่ายได้หลากหลายรูปแบบ และมีฟีเจอร์ต่างๆ เช่น การดูรายละเอียดของข้อมูลที่ต้องการวิเคราะห์ด้วยการดักจับข้อมูลตัวนั้น (Capture) สามารถทำการวิเคราะห์ข้อมูลได้ทั้งแบบการเชื่อมต่อแบบทันทีและบันทึกลงไฟล์ที่ทำการดักจับ

2.4.2 กำหนดระยะเวลาในการส่งการร้องขอ (request) เพื่อทำการสำรวจ โดยการสำรวจครั้งนี้ได้ทำการสำรวจด้วยวิธีการ Passive Probing จะทำการสำรวจภายในภาควิชาวิทยาการคอมพิวเตอร์ ใช้ระยะเวลาในการเก็บข้อมูลทั้งหมด 7 วัน แสดงข้อมูลการสำรวจตามตารางผนวกที่ ก2 ชุดข้อมูลที่ได้จากการทดลองสำรวจจำนวนไอพีแอดเดรส Passive

2.4.3 เริ่มทำการสำรวจไอพีแอดเดรสภายในภาควิชาวิทยาการคอมพิวเตอร์เท่านั้น ใน x.x.21.0/24 และ x.x.16.0/24 โดยการใช้ Wireshark ตรวจสอบ traffic ที่เข้ามายังเครื่องต้นทาง ซึ่งจะเก็บทั้งข้อมูล TCP –SYN, SYN-ACK และ RST แพ็กเก็ต และจะนำมาพิจารณาหา SYN-ACK flags set เพื่อหาไอพีแอดเดรสที่มีการตอบสนองต่อการสำรวจแบบ Passive Probing ซึ่งทำการตั้งเครื่องไว้ที่ห้องปฏิบัติการคอมพิวเตอร์ที่ภาควิชาวิทยาการคอมพิวเตอร์และทำการเก็บข้อมูลที่เกิดขึ้นไว้ตลอดระยะเวลา 7 วันจากนั้นนำข้อมูลมาวิเคราะห์เพื่อดู traffic ที่เข้ามายังเครื่อง

2.4.4 จัดเก็บข้อมูลที่ได้จากการสำรวจ และนำมาวิเคราะห์ข้อมูลที่ได้จากการสำรวจ ด้วยวิธีการ Passive Probing โดยทำการเก็บข้อมูลในรูปแบบ file

3. ขั้นตอนการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลสำหรับวิธีการ Active Probing ได้ทำการวิเคราะห์ข้อมูล 2 กลุ่มคือการวิเคราะห์ข้อมูลกลุ่มประชากร และกลุ่มตัวอย่างมี 3 ประเด็นคือ (1) การวิเคราะห์จำนวนไอพีแอดเดรสจากการสำรวจโดยใช้โปรโตคอลต่างกัน ได้แก่ โปรโตคอล ICMP และ โปรโตคอล TCP (2) การวิเคราะห์จำนวนไอพีแอดเดรสจากการสำรวจโดยใช้โปรโตคอลประเภทเดียวกัน แต่ใช้คำสั่งในการสำรวจต่างกัน และ (3) การวิเคราะห์การกระจายตัวของไอพีแอดเดรส ส่วนการวิเคราะห์ข้อมูลสำหรับวิธีการ Passive Probing นั้นได้ทำการวิเคราะห์จำนวนไอพีแอดเดรสที่มีการสำรวจได้ภายในภาควิชาวิทยาการคอมพิวเตอร์ โดยมีรายละเอียดดังต่อไปนี้

การทดลอง

การวิเคราะห์ข้อมูลกลุ่มตัวอย่างเป็นการนำกลุ่มตัวอย่างเพื่อนำมาสำรวจ จากนั้นนำข้อมูลทุกครั้งของกลุ่มสำรวจนำมาวิเคราะห์เพื่อหาค่าเฉลี่ยที่มีความแน่นอน แม่นยำ และมีประสิทธิภาพ โดยนำมาวิเคราะห์ตามประเด็นต่อไปนี้

3.1 การวิเคราะห์จำนวนไอพีแอดเดรสจากการสำรวจโดยใช้โปรโตคอลต่างกัน

ในการสำรวจปริมาณไอพีแอดเดรสได้ทำการสำรวจโดยใช้ โปรโตคอล ICMP และ โปรโตคอล TCP เพื่อสำรวจสถานะของโฮสต์ (Host) จากนั้นนำข้อมูลกลุ่มตัวอย่างที่ได้จากการ

สำรวจของทั้งสองโพรโทคอลมาเปรียบเทียบปริมาณไอพีแอดเดรสที่สำรวจได้ เพื่อให้ได้ข้อมูลจากการสำรวจที่มีความแม่นยำ ถูกต้องและมีประสิทธิภาพ เพราะว่าโพรโทคอลแต่ละโพรโทคอลให้ประสิทธิภาพในการสำรวจที่ต่างกัน เช่น โพรโทคอล ICMP สามารถตรวจสอบสถานะของโฮสต์ (Host) ได้อย่างรวดเร็ว และมีความถูกต้องสูง ส่วน โพรโทคอล TCP จะนำมาสำรวจซ้ำเพื่อช่วยให้ได้รับข้อมูลในการสำรวจได้ถูกต้อง แม่นยำมากยิ่งขึ้น แต่การสำรวจด้วย โพรโทคอล TCP ใช้เวลาในการสำรวจมากกว่าการใช้ โพรโทคอล ICMP

3.2 การวิเคราะห์จำนวนไอพีแอดเดรสจากการสำรวจโดยใช้โพรโทคอลประเภทเดียวกันแต่ใช้คำสั่งในการสำรวจต่างกัน

การสำรวจปริมาณไอพีแอดเดรสได้ทำการสำรวจโดยใช้ โพรโทคอล TCP ที่มีคำสั่งในการสำรวจที่ต่างกันคือ Nmap -PA [portlist] -n [target] และ Nmap -PS [portlist] -n [target] เพื่อสำรวจสถานะของโฮสต์ ซึ่งการสำรวจด้วย โพรโทคอล TCP จะถูกกรองจากไฟลต์วอลล์ ดังนั้นต้องใช้คำสั่งในการสำรวจที่มีความสามารถในการที่จะผ่านไฟลต์วอลล์ได้ จากนั้นนำข้อมูลกลุ่มตัวอย่างที่ได้จากการใช้คำสั่งทั้งสองมาเปรียบเทียบปริมาณไอพีแอดเดรสที่สำรวจได้ เพื่อให้ได้ข้อมูลที่มีความถูกต้อง แม่นยำมากที่สุด

3.3 การวิเคราะห์การใช้งานของไอพีแอดเดรส

การวิเคราะห์การใช้งานตัวของไอพีแอดเดรสจะแบ่งการวิเคราะห์คือการประเมินลักษณะการใช้งานจากค่า Availability (A) ค่า Volatility (V) และ ค่า Uptime (U) ของแต่ละแอดเดรส โดยค่า Availability เป็นค่าความน่าจะเป็นที่บ่งบอกถึงลักษณะการใช้งานของไอพีแอดเดรส ค่า Volatility เป็นค่าความน่าจะเป็นที่บ่งบอกถึงสถานะของโฮสต์ของไอพีแอดเดรส และค่า Uptime เป็นค่าความน่าจะเป็นที่บ่งบอกถึงระยะเวลาการใช้งานของไอพีแอดเดรส

3.4 การวิเคราะห์จำนวนไอพีแอดเดรสที่ได้จากการสำรวจด้วยวิธี Passive Probing

ในการสำรวจปริมาณไอพีแอดเดรสด้วยวิธี Passive Probing ได้ทำการตรวจจับแพคเกจที่ผ่านเข้ามายังเครื่องต้นทางโดยจะพิจารณาหา SYN-ACK flags set ที่ได้จากสำรวจทั้งหมด จากนั้นดูไอพีแอดเดรสและนำข้อมูลของจำนวนไอพีแอดเดรสมาใช้เป็นผลการสำรวจ ซึ่งผลการ

สำรวจดังกล่าวจะนำมาใช้ในการเปรียบเทียบกับการสำรวจด้วยวิธี Active Probing เพื่อให้ได้ข้อมูลของการสำรวจที่ครอบคลุมทุกไอพีแอดเดรสที่มีการใช้งาน

4. ตัววัดข้อมูล

ในการวิเคราะห์ข้อมูลที่ได้จากการสำรวจ ผู้วิจัยจะวิเคราะห์รูปแบบการตอบกลับ (response) ซึ่งแบ่งออกเป็น 3 รูปแบบคือ Positive response คือการมีโฮสต์อยู่จริงที่ไอพีแอดเดรส นั้น Negative respond คือไม่สามารถเข้าถึงโฮสต์ได้ (unreachable) หรือว่าไอพีแอดเดรสไม่ได้ถูกใช้งาน และ No reply คือขาดการตอบรับ เนื่องจากข้อมูลถูกรองด้วยไฟร์วอลล์

ผู้วิจัยวิเคราะห์ข้อมูลของแต่ละไอพีแอดเดรส เพื่อศึกษาลักษณะการใช้งานไอพีแอดเดรส ซึ่งตัววัดที่ใช้วิเคราะห์ได้แก่ ค่า Availability หรือ $A(\text{address})$ เป็นค่าความน่าจะเป็นที่บ่งบอกถึงลักษณะการใช้งานของไอพีแอดเดรส โดยคำนวณได้จากผลรวมของระยะเวลาที่โฮสต์ตอบสนองต่อการสำรวจ (probe) ทั้งหมดหารด้วยเวลาที่สำรวจทั้งหมด ดังสมการที่ (1) ค่า Volatility หรือ $V(\text{address})$ เป็นค่าความน่าจะเป็นที่บ่งบอกถึงสถานะของโฮสต์ของไอพีแอดเดรส โดยคำนวณได้จากจำนวนครั้งที่โฮสต์ตอบสนองต่อการสำรวจหารด้วยครึ่งหนึ่งของจำนวนการสำรวจ ดังสมการที่ (3) และ ค่า Uptime หรือ $U(\text{Address})$ เป็นค่าความน่าจะเป็นที่บ่งบอกถึงระยะเวลาการใช้งานของไอพีแอดเดรส โดยคำนวณได้จากระยะเวลาที่โฮสต์ตอบสนองอย่างต่อเนื่อง หารด้วยจำนวนครั้งที่โฮสต์ตอบสนองต่อการสำรวจ ดังสมการที่ (4)

$$A(\text{address}) = \frac{1}{N_p} \left(\sum_{i=1}^N r_i \right) \quad (1)$$

โดยที่ N_p เป็นจำนวนครั้งของการสำรวจทั้งหมด

r_i เป็น positive หรือ negative response ของแต่ละครั้งของการสำรวจคำนวณได้ดังสมการที่ (2)

$$r_i(\text{address}) = 1 \text{ or } 0, \forall i \in [1, N_p] \quad (2)$$

$$V(\text{address}) = 2 \frac{N_u}{N_p} \quad (3)$$

โดยที่ N_u เป็นจำนวนครั้งของการที่โฮสต์ตอบสนองต่อการสำรวจ

$$U(address) = \frac{A(address)}{N_u} \quad (4)$$

ผู้วิจัยนำค่า Availability (A) ค่า Volatility (V) และค่า Uptime (U) ของแต่ละไอพีแอดเดรส มาทำการประเมินลักษณะการใช้งานของไอพีแอดเดรส ซึ่งจากงานวิจัยของ Xue Cai และคณะมีการกำหนดขอบเขตของแต่ละค่าสำหรับใช้ประเมินลักษณะการใช้งาน ซึ่งผู้วิจัยได้นำขอบเขตดังกล่าวมาใช้ และปรับค่าขอบเขตของค่า Volatility และ Uptime ให้เหมาะสมกับสภาพแวดล้อมในการสำรวจ ทำให้ได้ค่าดังต่อไปนี้ $A_H = 0.95$ สำหรับค่า Availability สูง คือไอพีแอดเดรสมีการใช้งานและทำงานอย่างต่อเนื่องสูงสุด $A_L = 0.10$ สำหรับค่า Availability ต่ำ คือการใช้งานค่อนข้างน้อยหรือใช้งานในบางโอกาส $V = 0.004$ สำหรับค่า Volatility ต่ำ คือไอพีแอดเดรสมีการเปลี่ยนสถานะของโฮสต์น้อยครั้ง สถานะคงที่ หรือไม่มีการเปลี่ยนสถานะคือสถานะของโฮสต์เป็นออนไลน์ตลอดเวลา และ $U = 0.95$ สำหรับค่า Uptime สูง $U = 0.048$ สำหรับค่า Uptime ต่ำ คือไอพีแอดเดรสมีระยะเวลาการใช้งานที่ไม่แน่นอน แล้วแต่โอกาส นอกจากนี้ Xue Cai และคณะได้แบ่งลักษณะการใช้งานไอพีแอดเดรส ออกเป็น 5 กลุ่ม พร้อมเงื่อนไขที่จะใช้ในการประเมินลักษณะการใช้งานของไอพีแอดเดรส ดังนี้ กลุ่ม Always – stable จะเป็นกลุ่มไอพีแอดเดรสที่มีการใช้งานตลอดเวลาและสม่ำเสมอและทำงานอย่างต่อเนื่องสูงสุด ซึ่งจะเป็นกลุ่มของเครื่องแม่ข่ายเป็นส่วนใหญ่ กลุ่ม Sometimes - stable จะเป็นกลุ่มไอพีแอดเดรสที่มีการใช้งานในระยะเวลาสั้นและทำงานอย่างต่อเนื่องรองลงมา กลุ่ม Intermittent จะเป็นกลุ่มไอพีแอดเดรสที่มีการใช้งานบ่อย แต่ใช้งานในช่วงเวลาสั้น ๆ กลุ่ม Underutilized จะเป็นไอพีแอดเดรสที่มีการใช้งานในบางครั้ง และกลุ่ม Unclassifiable จะเป็นกลุ่มไอพีแอดเดรสที่ไม่ได้รับการจัดสรร หรือไม่มีการใช้งาน ซึ่งแต่ละกลุ่มมีเงื่อนไขดังต่อไปนี้

Always - stable: ($A \geq 0.95$ หรือ $U \geq 0.95$) และ ($V \leq 0.004$)

Sometimes – stable: ($U \geq 0.048$) และ ($A \geq 0.1$) และ ($A < 0.95$ หรือ $V > 0.004$)

Intermittent: ($U < 0.048$) และ ($A > 0.1$) และ ($A < 0.95$ หรือ $V > 0.004$)

Underutilized: ($A < 0.10$) และ ($A > 0.00$)

Unclassifiable: ($A=0.00$) และ ($V=0.00$) และ ($U=0.00$)

ผลและวิจารณ์

ผล

ในการสำรวจจำนวนไอพีแอดเดรสที่ใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์ ได้ทำการสำรวจไอพีแอดเดรสเพื่อเป็นข้อมูลทางสถิติของจำนวนไอพีแอดเดรสโดยใช้วิธีการสำรวจแบบ Active Probing ซึ่งเลือกใช้โปรโตคอลในการสำรวจ คือ โปรโตคอล ICMP และโปรโตคอล TCP ได้ทำการสำรวจที่พอร์ต 21 (ftp) 22 (ssh) 25(smtp) 53 (domain) 80 (http) 110 (pop3) 135 (epmap) 137 (netbios) 139 (netbios) 443 (https) 445 (microsoft-ds) 458 (appleqt) 587 (submission) 1433 (ms-sql-s) 1434 (ms-sql-m) 1214 (kazaa) 3306 (mysql) 6346(gnutella) 1863 (msnp) เพื่อใช้ในการดูแลรักษาการใช้งาน และการให้บริการ นอกจากนี้ยังใช้วิธี Passive Probing ในการสำรวจไอพีแอดเดรสที่มีการใช้งานจริงภายในภาควิชาวิทยาการคอมพิวเตอร์ ซึ่งผลการสำรวจปรากฏดังนี้

1. ผลการทดลองการสำรวจจำนวนไอพีแอดเดรสที่ใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์ ด้วยวิธี Active Probing

จากการสำรวจจำนวนไอพีแอดเดรสที่ใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์จากการสำรวจจำนวนไอพีแอดเดรสทั้งหมดจำนวน 65,536 แอดเดรส สามารถแยกเป็น 2 กลุ่ม คือ กลุ่มไอพีแอดเดรสที่ตอบสนอง และกลุ่มไอพีแอดเดรสที่ไม่ตอบสนองดังตารางที่ 1 และภาพผนวกที่ ก 1 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดสำรวจด้วย Active Probing ซึ่งผลการทดลองแสดงว่าไอพีแอดเดรสภายในมหาวิทยาลัยเกษตรศาสตร์ได้มีการใช้งานเพียง 49.80% เท่านั้นยังเหลือจำนวนไอพีแอดเดรสอีก 50.20% ให้สามารถใช้งานได้

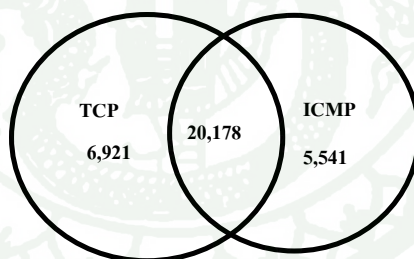
ตารางที่ 1 การเปรียบเทียบจำนวนไอพีแอดเดรส

ประเภท	จำนวนไอพีแอดเดรส	%
ไอพีแอดเดรสที่ใช้สำรวจ	65,536	100.00
ไอพีแอดเดรสที่ไม่ตอบสนอง	32,896	50.20
ไอพีแอดเดรสที่ตอบสนอง	32,640	49.80

ผลการสำรวจที่พบได้มีการนำมาเปรียบเทียบข้อมูลความถูกต้อง เพื่อตรวจสอบความถูกต้องในการทำการทดลองโดยการเปรียบเทียบข้อมูลกับข้อมูลการจัดสรรไอพีแอดเดรสของมหาวิทยาลัยเกษตรศาสตร์จากตารางผนวกที่ ก3 ที่มีการจัดสรรให้กับภาค ส่วนต่างๆ ภายในมหาวิทยาลัย จะพบว่าข้อมูลที่สำรวจพบมีความเกี่ยวข้องกับข้อมูลการจัดสรรไอพีแอดเดรส

1.1 การเปรียบเทียบจำนวนไอพีแอดเดรสโดยใช้ โพรโทคอล ICMP และ โพรโทคอล TCP

ผลการทดลองเปรียบเทียบปริมาณของไอพีแอดเดรสที่พบจากการสำรวจในแต่ละวิธีการทั้งการตรวจสอบด้วยโพรโทคอล ICMP และการตรวจสอบด้วยโพรโทคอล TCP จากการทดลองทำการสำรวจจำนวนไอพีแอดเดรสพบว่าจำนวนโฮสต์ที่ตอบสนองต่อการสำรวจด้วยโพรโทคอล TCP มีจำนวนมากกว่าจำนวนโฮสต์ที่ตอบสนองต่อการสำรวจด้วยโพรโทคอล ICMP แสดงดังภาพที่ 9 และ ภาพผนวกที่ ก1



ภาพที่ 9 ผลการสำรวจจำนวนไอพีแอดเดรสที่สำรวจด้วยโพรโทคอล ICMP และ โพรโทคอล TCP

จากภาพที่ 9 และ ภาพผนวกที่ ก1 การทดลองสำรวจจำนวนไอพีแอดเดรสที่ใช้งาน พบว่าจำนวนโฮสต์ที่ตอบสนองต่อการสำรวจทั้ง โพรโทคอล ICMP และ โพรโทคอล TCP มีจำนวน 20,178 โฮสต์ คิดเป็นร้อยละ 61.82 จำนวนโฮสต์ที่ตอบสนองต่อ โพรโทคอล ICMP แต่ไม่ตอบสนองต่อ โพรโทคอล TCP จำนวน 5,541 โฮสต์คิดเป็น ร้อยละ 16.98 และจำนวนโฮสต์ที่ตอบสนองต่อโพรโทคอล TCP แต่ไม่ตอบสนองต่อโพรโทคอล ICMP จำนวน 6,921 โฮสต์คิดเป็นร้อยละ 21.20 ดังปรากฏข้อมูลตามตารางที่ 2 สำหรับภาพผนวกที่ ก1 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดสำรวจด้วยวิธี Active Probing โดยใช้โพรโทคอล ICMP และโพรโทคอล TCP ในแกน x แสดงจำนวนจำนวนไอแอดเดรสใน 1 บล็อกจำนวน 256 ไอพีแอดเดรส แกน y แสดง

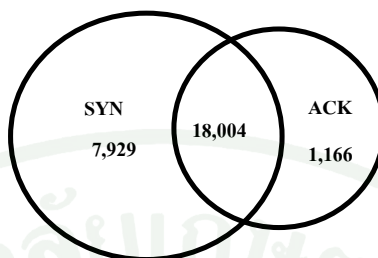
จำนวนบล็อก 256 บล็อกของ /24 ซึ่งจุดสีทั้งหมดที่ plot ลงบนพื้นนั้นจะแสดงถึงจำนวนไอพีแอดเดรสทั้งหมดที่มีการใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์จากชุดข้อมูลทั้งหมดในตารางภาคผนวกที่ ก1 จุดสีฟ้าแสดงถึงไอพีแอดเดรสที่มีการสำรวจพบด้วยโปรโตคอล ICMP เพียงอย่างเดียวจุดสีชมพูแสดงถึงไอพีแอดเดรสที่มีการสำรวจพบด้วยโปรโตคอล TCP เพียงอย่างเดียว และจุดสีเขียวแสดงถึง ไอพีแอดเดรสที่มีการสำรวจพบทั้งโปรโตคอล ICMP และ TCP

ตารางที่ 2 การเปรียบเทียบจำนวนไอพีแอดเดรสโดยใช้ โปรโตคอล ICMP และ โปรโตคอล TCP

ประเภท	จำนวนไอพีแอดเดรส	%
ไอพีแอดเดรสที่ใช้สำรวจ	65,536	
ไอพีแอดเดรสที่ไม่ตอบสนอง	32,896	
ไอพีแอดเดรสที่ตอบสนอง	32,640	100.00
ไอพีแอดเดรสที่ตอบสนองต่อ ICMP	25,719	78.79
ไอพีแอดเดรสที่ตอบสนองต่อ TCP	27,099	83.02
ไอพีแอดเดรสที่ตอบสนองต่อทั้ง ICMP และ TCP	20,178	61.82
ไอพีแอดเดรสที่ตอบสนองต่อ ICMP อย่างเดียว	5,541	16.98
ไอพีแอดเดรสที่ตอบสนองต่อ TCP อย่างเดียว	6,921	21.20

1.2 การเปรียบเทียบจำนวนไอพีแอดเดรสสำรวจโดย โปรโตคอล TCP ที่คำสั่งต่างกัน

ผลการทดลองเปรียบเทียบปริมาณของไอพีแอดเดรสที่พบจากการสำรวจในแต่ละวิธีการทั้งการตรวจสอบด้วย TCP-SYN option และการตรวจสอบด้วย TCP - ACK option จากการทดลองทำการสำรวจจำนวนไอพีแอดเดรสพบว่า จำนวนโฮสต์ที่ตอบสนองต่อการสำรวจด้วย TCP-SYN option มีจำนวนมากกว่าจำนวนโฮสต์ที่ตอบสนองต่อการสำรวจด้วย TCP - ACK option แสดงดังภาพที่ 10 และภาพผนวกที่ ก3



ภาพที่ 10 ผลการสำรวจจำนวนไอพีแอดเดรสที่สำรวจด้วย โพรโทคอล TCP ที่ option ต่างกัน

จากภาพที่ 10 และภาพผนวกที่ ก3 การทดลองสำรวจจำนวนไอพีแอดเดรสที่ใช้งาน พบว่า จำนวนโฮสต์ที่ตอบสนองต่อการสำรวจทั้ง TCP-SYN และ TCP - ACK option มีจำนวน 18,004 โฮสต์ คิดเป็นร้อยละ 66.44 จำนวนโฮสต์ที่ตอบสนองต่อ TCP-SYN option แต่ไม่ตอบสนองต่อ TCP - ACK option จำนวน 7,929 โฮสต์คิดเป็นร้อยละ 29.26 และจำนวนโฮสต์ที่ตอบสนองต่อ TCP - ACK option แต่ไม่ตอบสนองต่อ TCP-SYN option จำนวน 1,166 โฮสต์ คิดเป็นร้อยละ 4.3 ดังปรากฏข้อมูลตามตารางที่ 3 สำหรับภาพผนวกที่ ก3 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมด ที่สำรวจพบโดยโพรโทคอล TCP โดยใช้รูปแบบ TCP-SYN และ TCP-ACK ในแกน x แสดงจำนวนจำนวนไอพีแอดเดรสใน 1 บล็อกจำนวน 256 ไอพีแอดเดรส แกน y แสดงจำนวนบล็อก 256 บล็อกของ /24 ซึ่งจุดสีทั้งหมดที่ plot ลงบนพื้นนั้นจะแสดงถึงจำนวนไอพีแอดเดรสทั้งหมดที่มีการใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์ที่สามารถสำรวจพบด้วยโพรโทคอล TCP จากชุดข้อมูลทั้งหมดในตารางภาคผนวกที่ ก1 จุดสีม่วงแสดงถึงไอพีแอดเดรสที่มีการสำรวจพบด้วยโพรโทคอล TCP ในรูปแบบ TCP - SYN เพียงอย่างเดียว จุดสีเหลืองแสดงถึงไอพีแอดเดรสที่มีการสำรวจพบด้วยโพรโทคอล TCP ในรูปแบบ TCP-ACK เพียงอย่างเดียว และจุดสีชมพูแสดงถึงไอพีแอดเดรสที่มีการสำรวจพบทั้งรูปแบบ TCP - SYN และ TCP -ACK

ตารางที่ 3 การเปรียบเทียบจำนวนไอพีแอดเดรสสำรวจโดย โพรโทคอล TCP ที่คำสั่งต่างกัน

ประเภท	จำนวนไอพีแอดเดรส	%
ไอพีแอดเดรสที่ใช้สำรวจ	65,536	
ไอพีแอดเดรสที่ไม่ตอบสนอง	32,896	
ไอพีแอดเดรสที่ตอบสนอง	27,099	100.00

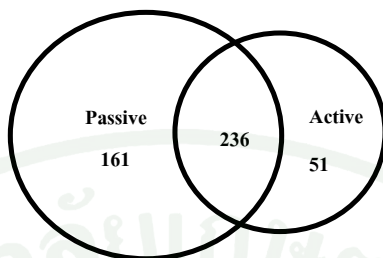
ตารางที่ 3 (ต่อ)

ประเภท	จำนวนไอพีแอดเดรส	%
ไอพีแอดเดรสที่ตอบสนองต่อ TCP-SYN	25,933	95.69
ไอพีแอดเดรสที่ตอบสนองต่อ TCP - ACK	19,170	70.74
ไอพีแอดเดรสที่ตอบสนองต่อทั้ง TCP-SYN และ TCP - ACK	18,004	66.44
ไอพีแอดเดรสที่ตอบสนองต่อ TCP-SYN	7,929	29.26
ไอพีแอดเดรสที่ตอบสนองต่อ TCP - ACK	1,166	4.3

จากผลการทดลองการสำรวจจำนวนไอพีแอดเดรสที่ใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์พบว่าไอพีแอดเดรสที่มีการใช้งานจริงประมาณร้อยละ 49.80 โดยการสำรวจด้วย โพรโทคอล TCP สำรวจพบจำนวนไอพีแอดเดรสที่มีการใช้งานจริงมากกว่าการสำรวจด้วย โพรโทคอล ICMP เพราะว่าภายในเครือข่ายของมหาวิทยาลัยเกษตรศาสตร์อาจมีการบล็อกหรือป้องกันการใช้คำสั่ง Ping ด้วย โพรโทคอล ICMP ในบางไอพีแอดเดรสจึงทำให้ผลการสำรวจด้วย โพรโทคอล TCP สำรวจพบจำนวนไอพีแอดเดรสที่มากกว่าการสำรวจด้วย โพรโทคอล ICMP

1.4 การเปรียบเทียบจำนวนไอพีแอดเดรสโดยใช้ Active Probing และ Passive Probing ในภาควิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์

ผลการทดลองเปรียบเทียบปริมาณของไอพีแอดเดรสที่พบจากการสำรวจในแต่ละวิธีการทั้งการตรวจสอบด้วย Active Probing และการตรวจสอบด้วย Passive Probing จากการทดลองทำการสำรวจจำนวนไอพีแอดเดรสตามชุดข้อมูลการทดลองที่ตารางผนวกที่ ก2 ระยะเวลา 7 วัน ภายในภาควิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์ ที่ x.x.16.0./24 และ x.x.21.0./24 พบว่า จำนวนโฮสต์ที่ตอบสนองต่อการสำรวจด้วย Passive Probing มีจำนวนมากกว่าจำนวนโฮสต์ที่ตอบสนองต่อการสำรวจด้วย Active Probing แสดงดังภาพที่ 11



ภาพที่ 11 ผลการสำรวจจำนวนไอพีแอดเดรสที่สำรวจด้วย Active Probing และ Passive Probing

จากภาพที่ 11 การทดลองสำรวจจำนวนไอพีแอดเดรสที่ใช้งานภายในภาควิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์ พบว่าจำนวนโฮสต์ที่ตอบสนองต่อการสำรวจทั้ง Active Probing และ Passive Probing มีจำนวน 236 โฮสต์ คิดเป็นร้อยละ 52.68 จำนวนโฮสต์ที่ตอบสนองต่อ Passive Probing แต่ไม่ตอบสนองต่อ Active Probing จำนวน 161 โฮสต์คิดเป็นร้อยละ 35.94 และจำนวนโฮสต์ที่ตอบสนองต่อ Active Probing แต่ไม่ตอบสนองต่อ Passive Probing จำนวน 51 โฮสต์ คิดเป็นร้อยละ 11.38 ดังปรากฏข้อมูลตามตารางที่ 4 ซึ่งแสดงให้เห็นว่าภายในภาควิชาวิทยาการคอมพิวเตอร์มีการใช้งานไอพีแอดเดรสไปเป็นจำนวนมาก และเหลือไอพีแอดเดรสที่ยังไม่ถูกใช้งานเพียง 12.5%

ตารางที่ 4 การเปรียบเทียบจำนวนไอพีแอดเดรสโดยใช้ Active Probing และ Passive Probing

ประเภท	จำนวนไอพี แอดเดรส	%
ไอพีแอดเดรสที่ใช้สำรวจ	512	
ไอพีแอดเดรสที่ไม่ตอบสนอง	64	
ไอพีแอดเดรสที่ตอบสนอง	448	100 %
ICMP or TCP (Active Probing)	287	64.04 %
Passive Probing	397	88.62 %
ไอพีแอดเดรสที่ตอบสนองทั้ง Active และ Passive	236	52.68 %
ไอพีแอดเดรสที่ตอบสนองต่อ Active อย่างเดียว	51	11.38 %
ไอพีแอดเดรสที่ตอบสนองต่อ Passive อย่างเดียว	161	35.94 %

ผลการทดลองการสำรวจจำนวนไอพีแอดเดรสที่ใช้งานจริงภายในภาควิชาวิทยาการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์พบว่าไอพีแอดเดรสที่มีการใช้งานจริงประมาณร้อยละ 87.5 จากการสำรวจด้วย Active Probing และ Passive Probing โดยการสำรวจด้วย Passive Probing พบไอพีแอดเดรสคิดเป็นร้อยละ 88.62% และการสำรวจด้วยวิธีการ Active Probing พบไอพีแอดเดรสคิดเป็นร้อยละ 64.04% ซึ่งใช้การสำรวจทั้งโปรโทคอล ICMP และโปรโทคอล TCP จากผลการทดลองแสดงให้เห็นว่าการสำรวจด้วยวิธีการ Passive Probing สำรวจพบจำนวนไอพีแอดเดรสที่มีการใช้งานจริงมากกว่าการสำรวจด้วย Active Probing จะเห็นได้ว่าการสำรวจด้วยวิธีการ Active Probing เพียงอย่างเดียวไม่สามารถสำรวจได้ครอบคลุมถึงแม้จะใช้หลายโปรโทคอลในการสำรวจก็ตาม

1.5 การเปรียบเทียบผลการสำรวจจำนวนไอพีแอดเดรสด้วยวิธี Active Probing กับการจัดสรรไอพีแอดเดรสของมหาวิทยาลัยเกษตรศาสตร์

ตารางที่ 5 การเปรียบเทียบผลการสำรวจจำนวนไอพีแอดเดรสด้วยวิธี Active Probing กับการจัดสรรไอพีแอดเดรสของมหาวิทยาลัยเกษตรศาสตร์

Subnetwork	ไอพีแอดเดรสที่สำรวจ	Subnetwork	ไอพีแอดเดรสที่สำรวจ
158.108.1.0/24	/	158.108.243.64/27	/
158.108.1.0/25	/	158.108.243.96/27	/
158.108.1.128/25	/	158.108.243.128/27	/
158.108.2.0/24	/	158.108.243.160/27	/
158.108.2.0/27	/	158.108.243.192/27	/
158.108.2.32/27	/	158.108.243.224/27	/
158.108.2.64/26	/	158.108.244.0/22	/
158.108.2.128/25	/	158.108.48.0/25	/
158.108.3.0/24	/	158.108.48.128/25	/
158.108.3.0/25	/	158.108.49.0/27	/
158.108.3.128/25	/	158.108.49.32/27	/
158.108.4.0/24	/	158.108.49.64/26	/
158.108.4.0/25	/	158.108.49.128/25	/

ตารางที่ 5 (ต่อ)

Subnetwork	ไอพีแอดเดรสที่สำรวจ	Subnetwork	ไอพีแอดเดรสที่สำรวจ
158.108.4.128/26	/	158.108.50.0/24	/
158.108.4.192/27	/	158.108.51.0/24	/
158.108.4.224/27	/	158.108.52.0/24	/
158.108.5.0/24	/	158.108.53.0/24	/
158.108.5.0/27	/	158.108.54.0/24	/
158.108.5.32/27	/	158.108.55.0/24	/
158.108.5.64/26	/	158.108.56.0/25	/
158.108.5.128/26	/	158.108.57.0/27	/
158.108.5.194/27	/	158.108.57.32/27	/
158.108.5.224/27	/	158.108.57.64/26	/
158.108.6.0/24	/	158.108.57.128/25	/
158.108.6.0/25	/	158.108.58.0/24	/
158.108.6.128/25	/	158.108.59.0/24	X
158.108.7.0/24	/	158.108.60.0/24	/
158.108.8.0/24	/	158.108.61.0/24	X
158.108.8.0/27	/	158.108.62.0/24	X
158.108.8.32/27	/	158.108.63.0/24	X
158.108.8.64/29	/	158.108.64.0/24	/
158.108.8.72/29	/	158.108.65.0/24	X
158.108.8.80/28	/	158.108.66.0/24	/
158.108.8.96/27	/	158.108.67.0/24	X
158.108.8.128/25	/	158.108.68.0/23	/
158.108.9.0/24	/	158.108.69.0/24	/
158.108.9.0/28	/	158.108.70.0/23	/
158.108.9.16/28	/	158.108.71.0/24	/
158.108.9.32/27	/	158.108.72.0/24	X
158.108.9.64/26	/	158.108.73.0/24	X

ตารางที่ 5 (ต่อ)

Subnetwork	ไอพีแอดเดรสที่สำรวจ	Subnetwork	ไอพีแอดเดรสที่สำรวจ
158.108.9.128/27	/	158.108.74.0/25	/
158.108.9.160/27	/	158.108.74.128/25	/
158.108.9.192/27	/	158.108.75.0/24	X
158.108.9.224/27	/	158.108.76.0/24	/
158.108.10.0/24	/	158.108.77.0/24	X
158.108.10.0/26	/	158.108.78.0/24	/
158.108.10.64/26	/	158.108.79.0/25	/
158.108.10.128/26	/	158.108.80.0/24	/
158.108.10.192/26	/	158.108.81.0/24	/
158.108.11.0/24	/	158.108.82.0/24	X
158.108.11.0/27	/	158.108.83.0/24	/
158.108.11.32/27	/	158.108.89.0/24	/
158.108.11.64/27	/	158.108.92.0/24	/
158.108.11.96/27	/	158.108.95.0/24	/
158.108.11.128/27	/	158.108.84.0/24	/
158.108.11.160/27	/	158.108.85.0/24	/
158.108.11.192/27	/	158.108.86.0/24	/
158.108.11.224/27	/	158.108.87.0/24	/
158.108.12.0/24	/	158.108.88.0/25	/
158.108.13.0/24	/	158.108.88.128/25	/
158.108.13.0/26	/	158.108.90.0/24	/
158.108.13.64/27	/	158.108.91.0/24	/
158.108.13.96/27	/	158.108.93.0/25	/
158.108.13.128/26	/	158.108.93.128/25	/
158.108.13.192/27	/	158.108.94.0/24	/
158.108.13.224/27	/	158.108.95.0/24	/
158.108.14.0/24	/	158.108.96.0/24	/

ตารางที่ 5 (ต่อ)

Subnetwork	ไอพีแอดเดรสที่สำรวจ	Subnetwork	ไอพีแอดเดรสที่สำรวจ
158.108.15.0/24	/	158.108.160.0/24	/
158.108.128.0/21	/	158.108.160.0/27	/
158.108.136.0/22	/	158.108.160.32/27	/
158.108.140.0/23	/	158.108.160.64/26	/
158.108.142.0/24	/	158.108.160.128/26	/
158.108.143.0/24	/	158.108.160.192/27	/
158.108.208.0/23	/	158.108.160.224/27	/
158.108.210.0/23	/	158.108.161.0/24	/
158.108.212.0/25	/	158.108.161.0/26	/
158.108.212.128/25	/	158.108.161.64/28	/
158.108.213.0/25	/	158.108.161.80/28	/
158.108.213.128/25	/	158.108.161.96/28	/
158.108.240.0/23	/	158.108.161.112/28	/
158.108.242.0/27	/	158.108.161.128/25	/
158.108.242.32/27	/	158.108.162.0/24	/
158.108.242.64/27	/	158.108.163.0/24	/
158.108.242.96/27	/	158.108.163.0/25	/
158.108.242.128/27	/	158.108.163.0/25	/
158.108.242.160/27	/	158.108.164.0/24	X
158.108.242.192/27	/	158.108.165.0/24	X
158.108.242.224/27	/	158.108.166.0/24	/
158.108.243.0/27	/	158.108.167.0/24	X
158.108.243.32/27	/	158.108.168.0/24	/
158.108.16.0/26	/	158.108.24.0/24	/
158.108.16.64/26	/	158.108.25.0/26	/
158.108.16.128/26	/	158.108.25.64/27	/
158.108.16.192/26	/	158.108.25.97/27	/

ตารางที่ 5 (ต่อ)

Subnetwork	ไอพีแอดเดรสที่สำรวจ	Subnetwork	ไอพีแอดเดรสที่สำรวจ
158.108.17.0/24	/	158.108.25.129/26	/
158.108.18.0/25	/	158.108.25.192/27	/
158.108.18.128/25	/	158.108.25.225/27	/
158.108.19.0/24	/	158.108.26.0/25	/
158.108.20.0/27	/	158.108.26.128/25	/
158.108.20.32/27	/	158.108.27.0/25	/
158.108.20.64/27	/	158.108.27.128/25	/
158.108.20.96/27	/	158.108.28.0/25	/
158.108.20.128/25	/	158.108.28.128/25	/
158.108.21.0/26	/	158.108.29.0/25	/
158.108.21.65/26	/	158.108.29.128/27	/
158.108.21.129/26	/	158.108.29.192/27	/
158.108.21.193/26	/	158.108.29.224/27	/
158.108.22.0/24	/	158.108.30.0/24	X
158.108.23.0/24	/	158.108.31.0/24	/

ผลการเปรียบเทียบผลการสำรวจจำนวนไอพีแอดเดรสด้วยวิธี Active Probing กับการจัดสรรไอพีแอดเดรสของมหาวิทยาลัยเกษตรศาสตร์ตามตารางผนวกที่ ก3 พบว่าการสำรวจสามารถพบไอพีแอดเดรสที่มีการจัดสรรได้ตามที่มีการจัดสรร และมี subnetwork บางส่วนสามารถสำรวจพบเช่น 158.108.69.0/24, 158.108.71.0/24, 158.108.96.0/24, 158.108.168.0/24 และจากตารางที่ 5 สัญลักษณ์ “/” แสดงว่าผู้วิจัยสำรวจพบไอพีแอดเดรส สัญลักษณ์ “X” แสดงว่าผู้วิจัยสำรวจไม่พบไอพีแอดเดรส และเมื่อทำการเปรียบเทียบกับ ตารางผนวกที่ ก3 พบว่าเป็น subnetwork ที่ว่างไม่มีการใช้งาน

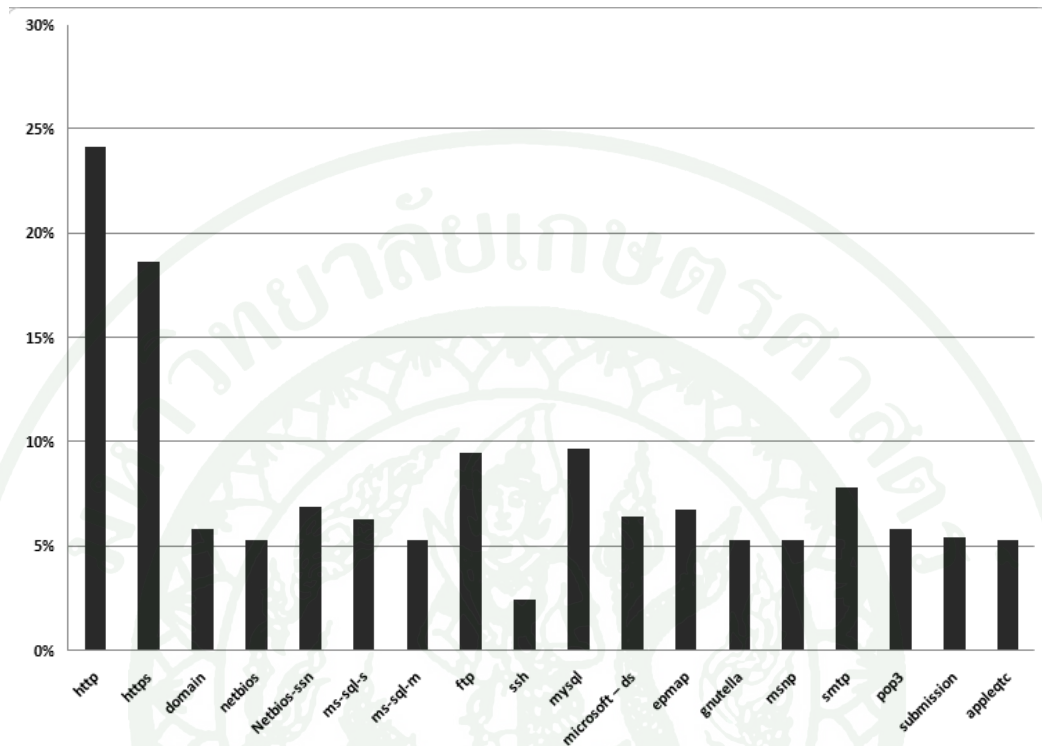
2. ผลการทดลองจำนวนไอพีแอดเดรสที่มีการใช้งานบริการ (Service)

การค้นหาการบริการ (Service) เป็นการทำการสำรวจพอร์ตที่ต้องการทราบการเปิดให้บริการโดยการสำรวจได้ทำการสำรวจพอร์ตดังต่อไปนี้พอร์ต 21 (ftp) 22 (ssh) 25(smtp) 53 (domain) 80 (http) 110 (pop3) 135 (epmap) 137 (netbios) 139 (netbios) 443 (https) 445 (microsoft-ds) 458 (appleqt) 587 (submission) 1433 (ms-sql-s) 1434 (ms-sql-m) 1214 (kaza) 3306 (mysql) 6346(gnutella) 1863 (msnp) ภายในมหาวิทยาลัยเกษตรศาสตร์ โดยการสำรวจด้วยวิธี Active Probing อย่างเดียว เพื่อนำข้อมูลมาจัดกลุ่มเป็นประเภทของการใช้งานในด้านโปรแกรมประยุกต์ (Application) รวมทั้งทราบจำนวนการใช้งาน

ข้อมูลที่ได้จากการสำรวจพอร์ตสามารถนำมาแบ่งประเภทการบริการได้ดังตารางที่ 6 โดยทำการแบ่งเป็นประเภทการบริการจากกลุ่มของพอร์ตที่อยู่ในประเภทเดียวกัน ซึ่งแต่ละประเภทในด้านโปรแกรมประยุกต์จะแสดงจำนวนการใช้งานภายในมหาวิทยาลัยเกษตรศาสตร์ดังตารางที่ 6 และ ภาพที่ 12

ตารางที่ 6 การแบ่งประเภทการบริการ

ประเภท	หมายเลขพอร์ต		จำนวนไอพี แอดเดรส	การใช้งานคิดเป็น %
Web	Port 80	http	15,821	24.14%
	Port 443	https	12,243	18.68%
DNS	Port 53	domain	3,821	5.83%
Betbios	Port 137	netbios	3,499	5.33%
	Port 139	Netbios-ssn	4,538	6.92%
Window Server	Port 1433	ms-sql-s	4,113	6.28%
	Port 1434	ms-sql-m	3,499	5.34%
FTP	Port 21	ftp	6,208	9.47%
SSH	Port 22	ssh	1,602	2.44%
My SQL	Port 3306	mysql	6,332	9.66%
Microsoft Windows	Port 445	microsoft – ds	4,214	6.43%
	Port 135	epmap	4,445	6.78%
Bittorrent	Port 6346	gnutella	3,499	5.34%
Chat	Port 1863	msnp	3,501	5.34%
Email	Port 25	smtp	5,135	7.84%
	Port 110	pop3	3,817	5.82%
	Port 587	submission	3,545	5.41%
Streaming	Port 458	appleqt	3,499	5.34%



ภาพที่ 12 ผลการสำรวจปริมาณการใช้งานโปรแกรมประยุกต์ในแต่ละประเภท

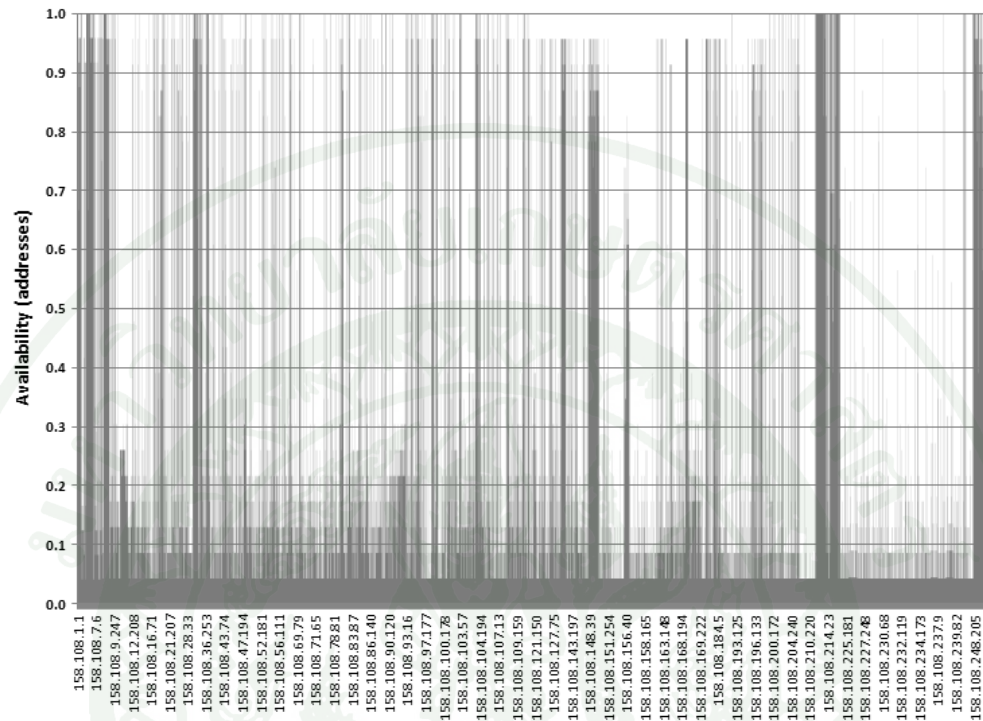
จากภาพที่ 12 พบว่าภายในมหาวิทยาลัยเกษตรศาสตร์มีการใช้งานดังนี้ โปรแกรมประเภทเว็บไซต์ จดหมายอิเล็กทรอนิกส์ (E-mail) NetBios ซึ่งบ่งบอกถึงการใช้งานที่เป็นระบบปฏิบัติการ Windows โปรแกรมฐานข้อมูลประเภท My SQL โปรแกรมประเภทการสนทนาออนไลน์ โปรแกรมประเภท Bittorrent โปรแกรมประเภทการแลกเปลี่ยนข้อมูล (FTP) Window Server DNS โปรแกรมประเภท และโปรแกรมประเภทวิดีโอร้อยละ โดยประเภทการใช้งานที่กล่าวมาข้างต้นนั้นแสดงได้จากผลการสำรวจพบพอร์ตที่มีการใช้งาน แต่ผลการทดลองดังกล่าวอาจไม่ครอบคลุมประเภทการใช้งานทั้งหมด เนื่องจากพอร์ตที่ใช้สำรวจเป็นพอร์ตที่เรากำหนดขึ้นจากการเลือก และคาดคะเนว่าเป็นกลุ่มการใช้งานที่ได้รับความนิยมและทั่วไป

3. ผลการทดลองการประเมินลักษณะของแต่ละไอพีแอดเดรส

การประเมินลักษณะของแต่ละไอพีแอดเดรสจากการสำรวจด้วยวิธี Active Probing ใช้การประเมินลักษณะโดยพิจารณาจากค่า Availability ค่า Volatility และ ค่า Uptime ของแต่ละแอดเดรส

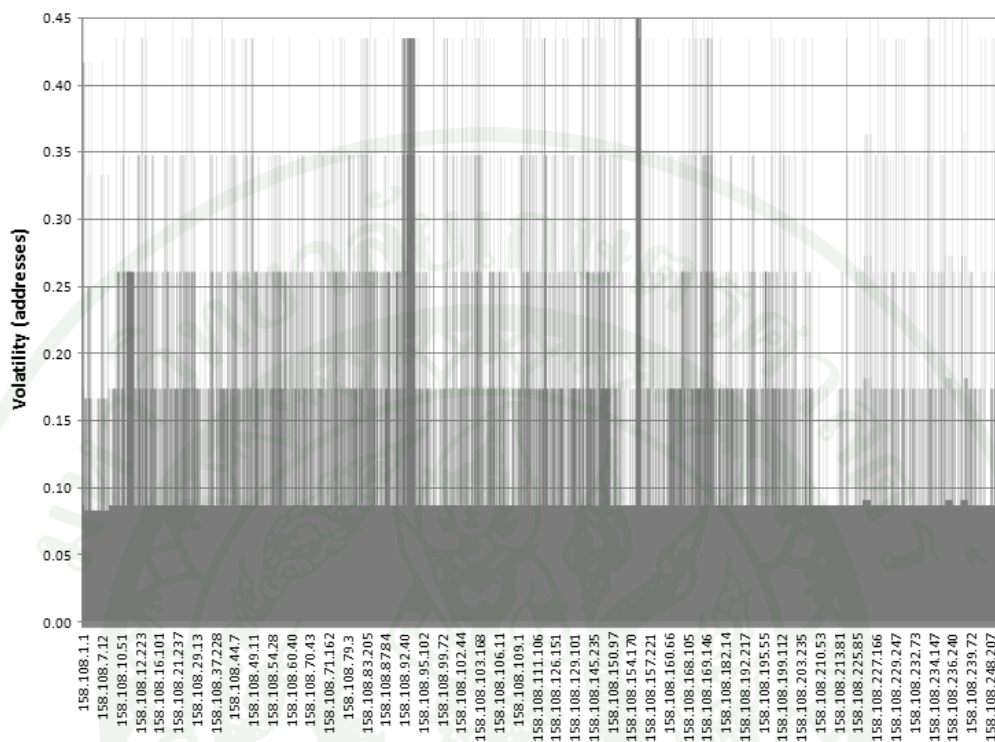
3.1 ค่า Availability เป็นค่าความน่าจะเป็นที่บ่งบอกถึงการพร้อมใช้งานของไอพีแอดเดรสภายในมหาวิทยาลัยเกษตรศาสตร์ เปรียบเสมือนแสดงให้เห็นถึงลักษณะการใช้งาน โดยถ้าค่า Availability สูงแสดงว่าไอพีแอดเดรสดังกล่าวมีการใช้งานจำนวนมาก แต่ถ้า Availability ต่ำ ไอพีแอดเดรสถูกใช้งานน้อย และถ้า Availability เป็น 0 ไอพีแอดเดรสไม่ถูกใช้งาน

จากภาพที่ 13 ในแกน x แสดงแต่ละไอพีแอดเดรสที่มีการสำรวจพบทั้งหมดซึ่งจะอยู่ในช่วง $x.x.0.0 - x.x.255.255$ แกน y แสดงค่า Availability ของแต่ละไอพีแอดเดรส โดยถ้าหากค่า Availability มีค่ามากกว่า 0.75 แต่น้อยกว่าหรือเท่ากับ 1 ($0.75 < A \leq 1.00$) แสดงว่าไอพีแอดเดรสถูกใช้งานมาก ถ้าค่า Availability มีค่ามากกว่า 0.25 แต่น้อยกว่าหรือเท่ากับ 0.75 ($0.25 < A \leq 0.75$) แสดงว่าไอพีแอดเดรสถูกใช้งานบางครั้ง ถ้าค่า Availability มีค่ามากกว่า 0.00 แต่น้อยกว่าหรือเท่ากับ 0.25 ($0.00 < A \leq 0.25$) แสดงว่าไอพีแอดเดรสถูกใช้งานน้อย และถ้าค่า Availability มีค่าเป็นศูนย์แสดงว่าไอพีแอดเดรสไม่มีการใช้งาน จากการสำรวจพบว่ากลุ่มไอพีแอดเดรสมีค่า Availability สูงอยู่ในช่วง 0.751 - 1.00 ซึ่งเป็นกลุ่มไอพีแอดเดรสกลุ่มที่มีการใช้งานและทำงานอย่างต่อเนื่อง เนื่องจากเป็นไอพีแอดเดรสที่ได้รับการจัดสรรให้กับหน่วยงานที่ให้บริการทางด้านการคอมพิวเตอร์ เช่น ศูนย์บริการคอมพิวเตอร์ ห้องปฏิบัติการคอมพิวเตอร์ และอื่น ๆ ซึ่งหน่วยงานเหล่านี้จะมีเครื่องแม่ข่ายที่การทำงานอย่างต่อเนื่องอยู่เป็นจำนวนมาก ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 19.14 ส่วนกลุ่มไอพีแอดเดรสที่มีค่า Availability อยู่ในช่วง 0.251 - 0.75 ซึ่งแสดงว่าไอพีแอดเดรสกลุ่มนี้มีการใช้งานบ่อย แต่เป็นการทำงานที่ไม่ต่อเนื่อง ซึ่งการใช้งานไอพีแอดเดรสกลุ่มนี้จะอยู่ในกลุ่มที่เป็นการจัดสรรไอพีแอดเดรสให้กับหน่วยงาน หรือสถานที่ที่นิสิต นักศึกษาเช่น ตึกกิจกรรมนักศึกษา ห้องเรียน โดยผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 5.47 และกลุ่มไอพีแอดเดรสมีค่า Availability อยู่ในช่วง 0.001 - 0.25 ซึ่งแสดงว่าไอพีแอดเดรสกลุ่มดังกล่าวมีการใช้งานค่อนข้างน้อย หรือใช้งานในบางโอกาส เช่น Video Conference Tele Conference หรือมีการจัดสรรให้กับหน่วยงานที่มีการใช้งานคอมพิวเตอร์ในระดับทั่วไป เช่น สำนักทะเบียน บัณฑิตศึกษา คณะอุตสาหกรรมเกษตร และอื่น ๆ ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็น ร้อยละ 56.25 และสุดท้ายกลุ่มไอพีแอดเดรสที่มีค่า Availability เท่ากับ 0.00 ซึ่งแสดงว่าไอพีแอดเดรสกลุ่มดังกล่าวเป็นไอพีแอดเดรสที่ไม่มีการถูกใช้งานในองค์กร หน่วยงานภายในมหาวิทยาลัย ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 19.14



ภาพที่ 13 แผนภาพค่า Availability ของไอพีแอดเดรสภายในมหาวิทยาลัยเกษตรศาสตร์

3.2 ค่า Volatility เป็นค่าความน่าจะเป็นที่บ่งบอกถึงสถานะของโฮสต์ของไอพีแอดเดรสภายในมหาวิทยาลัยเกษตรศาสตร์ เช่น เปลี่ยนสถานะของโฮสต์จากออนไลน์เป็นออฟไลน์ในช่วงเวลาสั้น ๆ โดยถ้าค่า Volatility สูงแสดงว่าไอพีแอดเดรสดังกล่าวมีการเปลี่ยนสถานะจาก online ไปเป็น offline บ่อย แต่ถ้า Volatility ต่ำ ไอพีแอดเดรสจะมีการเปลี่ยนสถานะไม่บ่อย และถ้า Volatility เป็น 0 ไอพีแอดเดรสไม่มีการเปลี่ยนสถานะ



ภาพที่ 14 แผนภาพค่า Volatility ของแต่ละไอพีแอดเดรสภายในมหาวิทยาลัยเกษตรศาสตร์

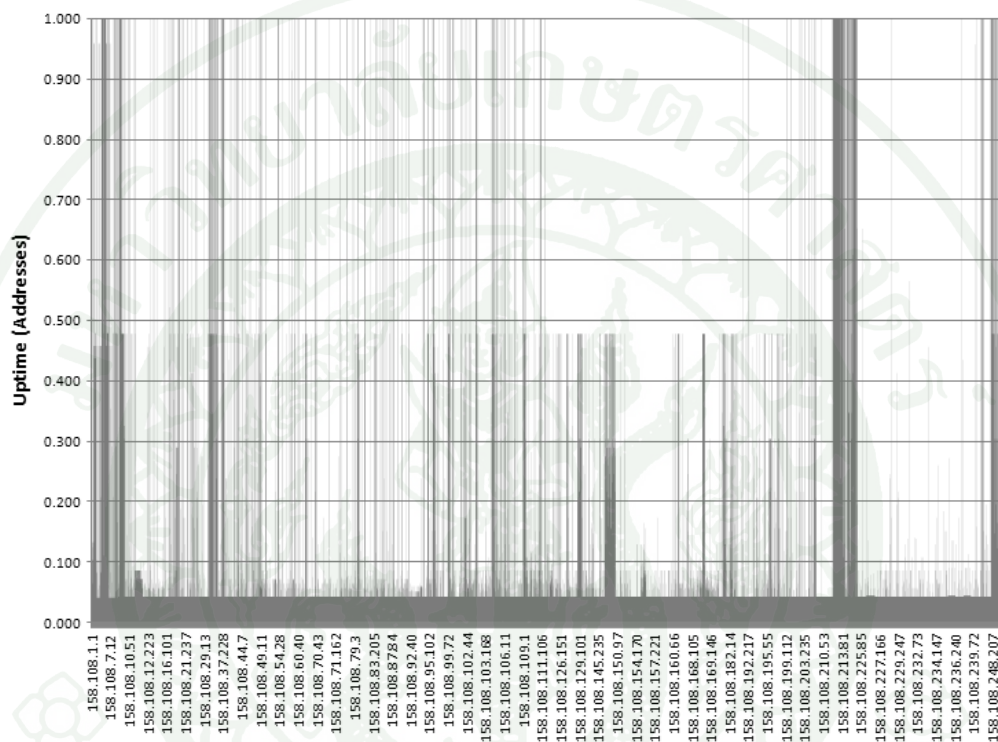
จากภาพที่ 14 ในแกน x แสดงแต่ละไอพีแอดเดรสที่มีการสำรวจพบทั้งหมดซึ่งจะอยู่ในช่วง $x.x.0.0 - x.x.255.255$ แกน y แสดงค่า Volatility ของแต่ละไอพีแอดเดรส แอดเดรส โดยถ้าหากค่า Volatility มีค่ามากกว่า 0.35 แต่น้อยกว่าหรือเท่ากับ 0.45 ($0.35 < V \leq 0.45$) แสดงว่าไอพีแอดเดรสมีการเปลี่ยนสถานะจาก online ไปเป็น offline บ่อยครั้ง ถ้าค่า Volatility มีค่ามากกว่า 0.15 แต่น้อยกว่าหรือเท่ากับ 0.35 ($0.15 < V \leq 0.35$) แสดงว่าไอพีแอดเดรสมีการเปลี่ยนสถานะจาก online ไปเป็น offline ในบางครั้งเท่านั้น ถ้าค่า Volatility มีค่ามากกว่า 0.00 แต่น้อยกว่าหรือเท่ากับ 0.15 ($0.00 < V \leq 0.15$) แสดงว่าไอพีแอดเดรสไม่ค่อยมีการเปลี่ยนสถานะจาก online ไปเป็น offline สถานะคงที่ และถ้าค่า Volatility มีค่าเป็นศูนย์แสดงว่าไอพีแอดเดรสไม่มีการเปลี่ยนสถานะคือ offline อยู่ จากการสำรวจพบว่ากลุ่มไอพีแอดเดรสมีค่า Volatility อยู่ในช่วง 0.351 – 0.45 ซึ่งเป็นกลุ่มไอพีแอดเดรสที่มีสถานะของโฮสต์เป็นออนไลน์ (online) ในช่วงเวลาสั้น ๆ และเกิดการเปลี่ยนสถานะเป็นออฟไลน์บ่อยครั้ง ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 1.95 รองลงมาเป็นกลุ่มไอพีแอดเดรสมีค่า Volatility อยู่ในช่วง 0.151 – 0.35 เป็นกลุ่มไอพีแอดเดรสที่มีสถานะของโฮสต์เป็นออนไลน์ในช่วงเวลายาวนาน แล้วจึงเปลี่ยนสถานะเป็นออฟไลน์ในบางช่วงเวลา หรือบางครั้ง ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ

35.55 ถัดมาเป็นกลุ่มไอพีแอดเดรสที่มีค่า Volatility อยู่ในช่วง 0.001 – 0.15 ซึ่งแสดงว่าไอพีแอดเดรสกลุ่มนี้มีการเปลี่ยนสถานะของโฮสต์น้อยครั้ง สถานะคงที่ หรือไม่มีการเปลี่ยนสถานะคือสถานะของโฮสต์เป็นออนไลน์ตลอดเวลาผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 43.36 และสุดท้ายกลุ่มไอพีแอดเดรสที่มีค่า Volatility เท่ากับ 0.00 ซึ่งแสดงว่าไอพีแอดเดรสกลุ่มนี้ไม่มีการใช้งาน สถานะของโฮสต์จึงไม่ปรากฏส่งผลให้ค่า Volatility เท่ากับ 0.00 ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 19.14

3.3 ค่า Uptime เป็นค่าความน่าจะเป็นที่บ่งบอกถึงระยะเวลาการใช้งานของไอพีแอดเดรสภายในมหาวิทยาลัยเกษตรศาสตร์ โดยถ้าค่า Uptime สูงแสดงว่าไอพีแอดเดรสดังกล่าวมีระยะเวลาในการ online เป็นเวลานาน แต่ถ้า Uptime ต่ำ ไอพีแอดเดรสระยะเวลาในการ online เป็นเวลาสั้น ๆ และถ้า Uptime เป็น 0 ไอพีแอดเดรสไม่มีระยะเวลาในการ online

จากภาพที่ 15 ในแกน x แสดงแต่ละไอพีแอดเดรสที่มีการสำรวจพบทั้งหมดซึ่งจะอยู่ในช่วง $x.x.0.0 - x.x.255.255$ แกน y แสดงค่า Uptime ของแต่ละไอพีแอดเดรส โดยถ้าหากค่า Uptime มีค่ามากกว่า 0.75 แต่น้อยกว่าหรือเท่ากับ 1 ($0.75 < U \leq 1.00$) แสดงว่าไอพีแอดเดรสมีระยะเวลาการใช้งานยาวนาน ถ้าค่า Uptime มีค่ามากกว่า 0.25 แต่น้อยกว่าหรือเท่ากับ 0.75 ($0.25 < U \leq 0.75$) แสดงว่าไอพีแอดเดรสมีระยะเวลาการใช้งานสั้น ๆ แต่บ่อยครั้ง ถ้าค่า Uptime มีค่ามากกว่า 0.00 แต่น้อยกว่าหรือเท่ากับ 0.25 ($0.00 < U \leq 0.25$) แสดงว่าไอพีแอดเดรสมีระยะเวลาการใช้งานที่ไม่แน่นอนตามโอกาส และถ้าค่า Uptime มีค่าเป็นศูนย์แสดงว่าไอพีแอดเดรสไม่มีระยะเวลาการใช้งาน จากผลการสำรวจพบว่ากลุ่มไอพีแอดเดรสมีค่า Uptime อยู่ในช่วง 0.751 – 1.00 ซึ่งเป็นกลุ่มไอพีแอดเดรสกลุ่มที่มีระยะเวลาการใช้งานตลอดเวลา หรือยาวนาน เนื่องจากเป็นเครื่องแม่ข่ายที่มีการทำงานในระยะเวลาที่ยาวนาน และต่อเนื่อง ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 8.20 รองลงมาเป็นกลุ่มไอพีแอดเดรสมีค่า Uptime อยู่ในช่วง 0.251 – 0.75 แสดงว่าไอพีแอดเดรสกลุ่มดังกล่าวมีระยะเวลาการใช้งานในช่วงสั้น ๆ แต่มีการใช้งานบ่อยครั้ง ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 10.16 ลำดับถัดมาเป็นกลุ่มไอพีแอดเดรสมีค่า Uptime อยู่ในช่วง 0.001 – 0.25 แสดงว่ากลุ่มไอพีแอดเดรสกลุ่มนี้มีระยะเวลาการใช้งานที่ไม่แน่นอน แล้วแต่โอกาส เพราะว่าไอพีแอดเดรสกลุ่มนี้จะถูกใช้งานในบางครั้งเท่านั้น เช่น Video Conference หรือ Tele Conference ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 62.50 และลำดับสุดท้ายกลุ่มไอพีแอดเดรสที่มีค่า Uptime เท่ากับ 0.00 แสดงว่าไอพีแอดเดรสกลุ่มนี้ไม่มี

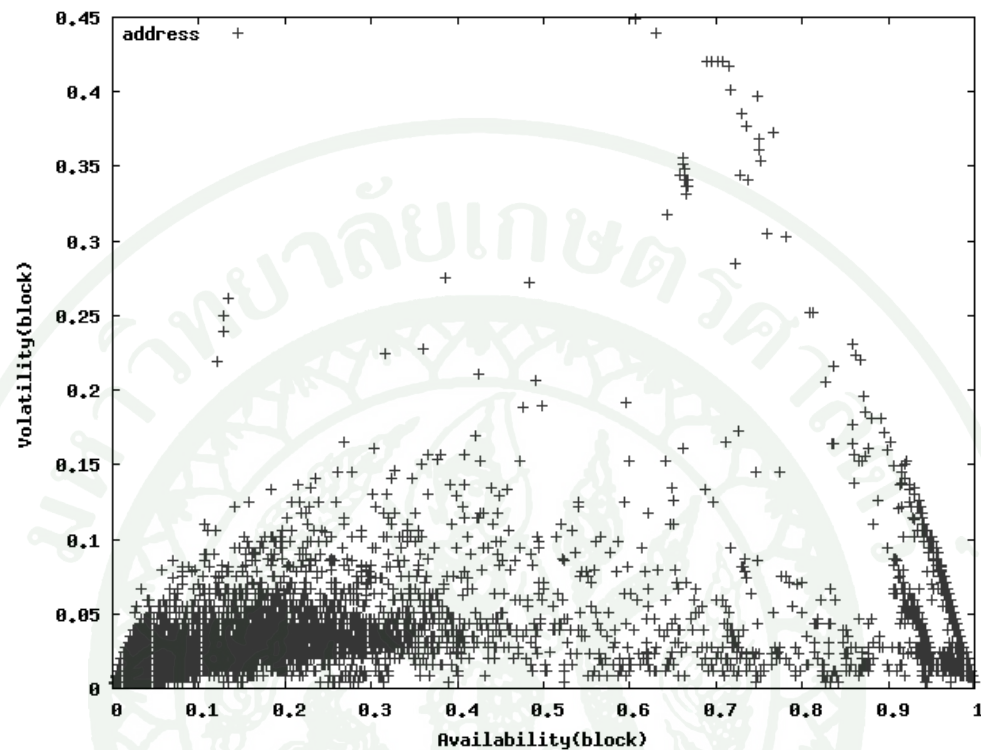
การใช้งาน จึงไม่ปรากฏระยะเวลาในการใช้งาน ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 19.14



ภาพที่ 15 แผนภาพค่า Uptime ของแต่ละไอพีแอดเดรสภายในมหาวิทยาลัยเกษตรศาสตร์

4. ผลการทดลองการกระจายตัว และความหนาแน่นของไอพีแอดเดรสภายในมหาวิทยาลัยเกษตรศาสตร์

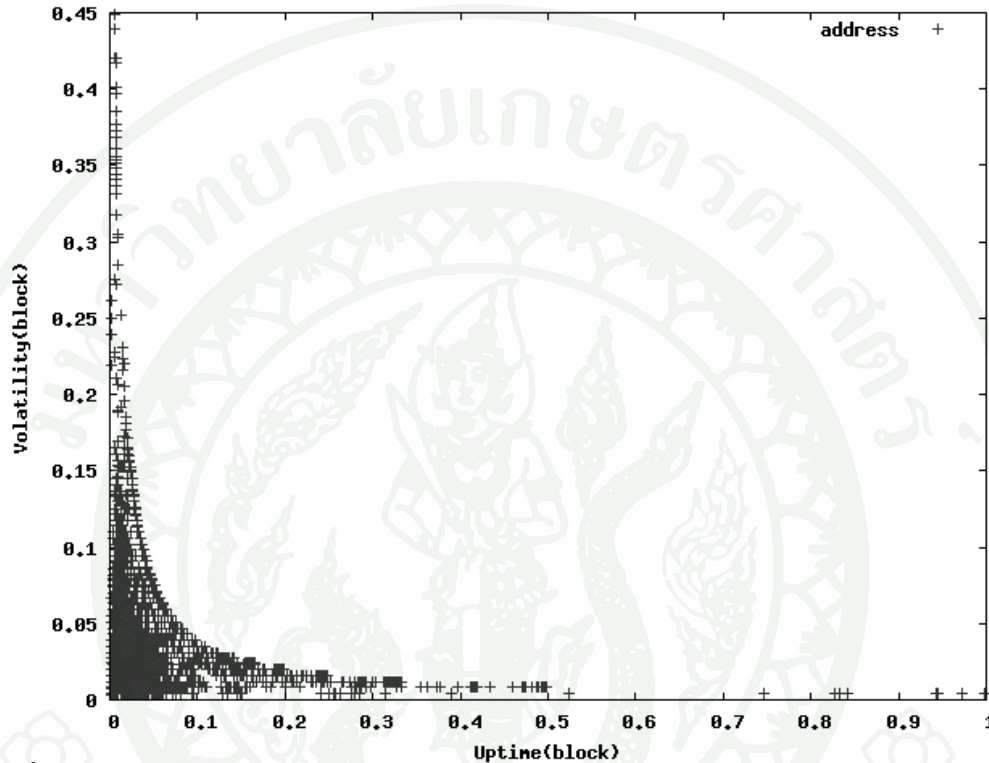
4.1 ความหนาแน่นของไอพีแอดเดรสตามระนาบของ Availability กับ Volatility



ภาพที่ 16 การกระจายตัวของไอพีแอดเดรส

จากภาพที่ 16 การกระจายตัวของไอพีแอดเดรสโดยการพล็อต (A, V) โดยในแกน x แสดงค่า Availability ของแต่ละไอพีแอดเดรส แกน y แสดงค่า Volatility ของแต่ละไอพีแอดเดรส เพื่อแสดงความเกี่ยวข้องของค่า Availability และ ค่า Volatility ในการจัดกลุ่มลักษณะการใช้งานของไอพีแอดเดรสโดยที่ $(A, V) = (0.95, 0.004)$ พบว่ามี Availability สูงและมีค่า Volatility ต่ำ แสดงว่ามีการใช้งานไอพีแอดเดรสอย่างสม่ำเสมอ ซึ่งจัดอยู่ในกลุ่ม Always – stable โดยเครื่องคอมพิวเตอร์กลุ่มนี้จะเป็นเครื่องแม่ข่าย (server) $(A, V) = (0.05, 0.004)$ แสดงว่ามีการใช้งานในกลุ่ม Underutilized รวมทั้งการกระจายตัวของ $(A, V) = (0.1-0.8, 0.045 - 0.4)$ แสดงว่ามีการใช้งานอยู่ในกลุ่มของ Sometimes – stable หรือ Intermittent ซึ่งจากภาพจะเห็นได้ว่าความหนาแน่นของไอพีแอดเดรสส่วนมากจะอยู่ที่ค่า Availability ต่ำและ ค่า Volatility ต่ำ แสดงว่าไอพีแอดเดรสมีการใช้งานน้อย และไม่ค่อยมีการเปลี่ยนสถานะจาก online ไปเป็น offline

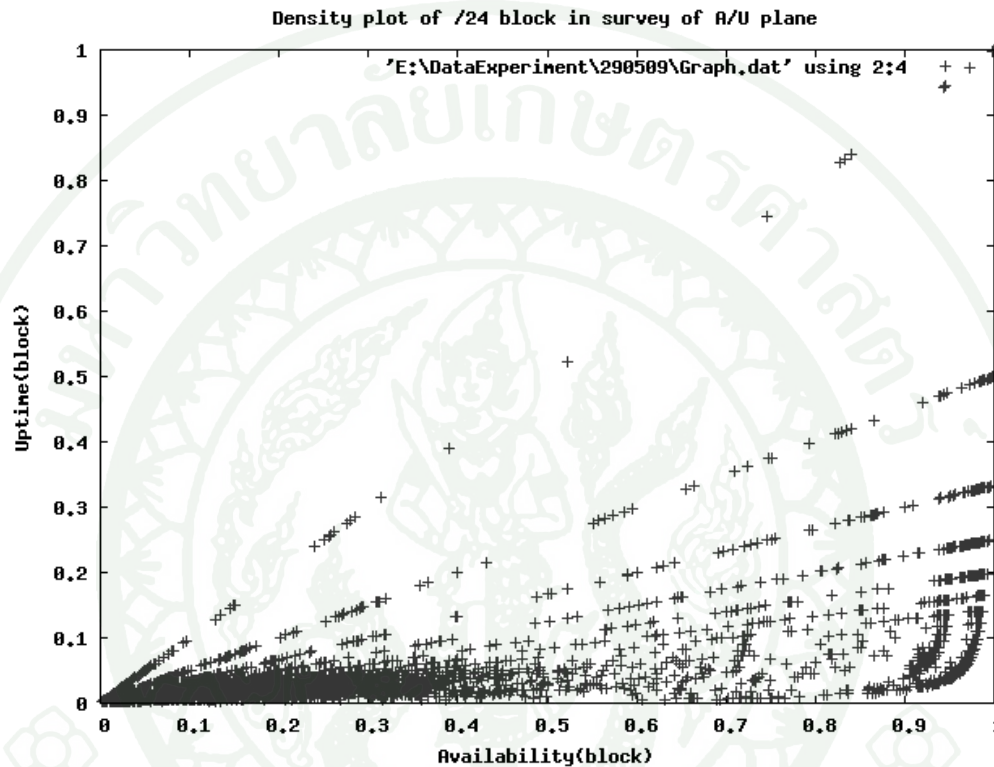
4.2 ความหนาแน่นของไอพีแอดเดรสตามระนาบของ Uptime กับ Volatility



ภาพที่ 17 การกระจายตัวของไอพีแอดเดรส

จากภาพที่ 17 การกระจายตัวของไอพีแอดเดรสโดยการพล็อต (U, V) ในแกน x แสดง ค่า Uptime ของแต่ละไอพีแอดเดรส แกน y แสดงค่า Volatility ของแต่ละไอพีแอดเดรส เพื่อแสดงความเกี่ยวข้องของค่า Uptime และ ค่า Volatility ในการจัดกลุ่มลักษณะการใช้งานของไอพีแอดเดรสโดยที่ $(U,V) = (0.95,0.004)$ พบว่า มี Uptime สูงและมีค่า Volatility ต่ำ แสดงว่ามีการใช้งานไอพีแอดเดรสตลอดเวลาและสถานะของโฮสต์ค่อนข้างคงที่จัดอยู่ในกลุ่ม Always – stable โดยเครื่องคอมพิวเตอร์กลุ่มนี้จะเป็นเครื่องแม่ข่าย (server) $(U,V) = (0.05,0.004)$ แสดงว่ามีการใช้งานในกลุ่ม Underutilized รวมทั้งการกระจายตัวของ $(U, V) = (0.1-0.8,0.045 - 0.4)$ แสดงว่ามีการใช้งานอยู่ในกลุ่มของ Sometimes – stable หรือ Intermittent ซึ่งจากภาพจะเห็นได้ว่าความหนาแน่นของไอพีแอดเดรสส่วนมากจะอยู่ที่ค่า Uptime ต่ำและ ค่า Volatility ต่ำ แสดงว่าไอพีแอดเดรสมีระยะเวลาที่ online น้อย และไม่ค่อยมีการเปลี่ยนสถานะจาก online ไปเป็น offline

4.3 ความหนาแน่นของไอพีแอดเดรสตามระนาบของ Availability กับ Uptime



ภาพที่ 18 การกระจายตัวของไอพีแอดเดรส

จากภาพที่ 18 การกระจายตัวของไอพีแอดเดรสโดยการพล็อต (A, U) ในแกน x แสดง ค่า Availability ของแต่ละไอพีแอดเดรส แกน y แสดงค่า Uptime ของแต่ละไอพีแอดเดรส เพื่อแสดงความเกี่ยวข้องของค่า Availability และ ค่า Uptime ในการจัดกลุ่มลักษณะการใช้งานของไอพีแอดเดรสโดยที่ $(A,U) = (0.95,0.95)$ พบว่ามีค่า Availability สูงและค่า Uptime สูงแสดงว่ามีการใช้งานอย่างสม่ำเสมอและตลอดเวลาหรือระยะเวลายาวนานจัดอยู่ในกลุ่ม Always – stable โดยคอมพิวเตอร์กลุ่มนี้จะเป็นเครื่องแม่ข่าย (server) อย่างแน่นอน $(A,U) = (0.05,0.05)$ แสดงว่ามีการใช้งานในกลุ่ม Underutilized รวมทั้งการกระจายตัวของ $(A, U) = (0.1-0.8, 0.1-0.8)$ แสดงว่ามีการใช้งานอยู่ในกลุ่มของ Sometimes – stable หรือ Intermittent ซึ่งจากภาพจะเห็นได้ว่าความหนาแน่นของไอพีแอดเดรสส่วนมากจะอยู่ที่ค่า Availability ต่ำและ ค่า Uptime ต่ำ แสดงว่าไอพีแอดเดรสมีการใช้งานที่น้อย และระยะเวลาที่ไอพีแอดเดรสอยู่ในสถานะ online ก็น้อย

จากการพล็อต (A, V, U) การกระจายตัวของไอพีแอดเดรสสามารถนำความเกี่ยวข้องดังกล่าวมาประเมินเป็นลักษณะการใช้งานไอพีแอดเดรสได้ดังนี้ กลุ่ม Always – stable จะเป็นไอพีแอดเดรสที่มีการใช้งานตลอดเวลาและสม่ำเสมอและทำงานอย่างต่อเนื่องสูงสุด โดยที่ (A, V, U) = (0.95, 0.004, 0.095) คิดเป็นร้อยละ 2.79 กลุ่ม Sometimes – stable จะเป็นไอพีแอดเดรสที่มีการใช้งานในระยะเวลาสั้นและทำงานอย่างต่อเนื่องรองลงมาโดยที่ (A, V, U) = (0.1-0.8, 0.045 – 0.4, 0.1-0.8) คิดเป็นร้อยละ 1.90 กลุ่ม Intermittent จะเป็นไอพีแอดเดรสที่มีการใช้งานน้อย แต่ใช้งานในช่วงเวลาสั้น ๆ โดยที่ (A, V, U) = (0.1-0.8, 0.045 – 0.4, 0.1-0.8) คิดเป็นร้อยละ 5.90 กลุ่ม Underutilized จะเป็นไอพีแอดเดรสที่มีการใช้งานในบางครั้ง โดยที่ (A, V, U) = (0.05, 0.004, 0.05) คิดเป็นร้อยละ 11.58 และกลุ่ม Unclassifiable จะเป็นไอพีแอดเดรสที่ไม่ได้รับการจัดสรร หรือไม่มีการใช้งาน ซึ่ง (A, V, U) = (0.00, 0.000, 0.000) คิดเป็นร้อยละ 77.83

5. ผลการแบ่งประเภทลักษณะการใช้งานของไอพีแอดเดรส

การแบ่งประเภทลักษณะการใช้งานของไอพีแอดเดรสเป็นการนำค่าของ Availability, Volatility และ Uptime มาพิจารณาในการแยกลักษณะการใช้งาน

ผลการแบ่งลักษณะการใช้งานจะแสดงให้เห็นในตารางที่ 7 ซึ่งไอพีแอดเดรสของมหาวิทยาลัยเกษตรศาสตร์สามารถแบ่งประเภทลักษณะการใช้งานจริงของไอพีแอดเดรสส่วนใหญ่ได้เป็น Underutilized ไอพีแอดเดรสที่มีการใช้งานในบางครั้ง คิดเป็นร้อยละ 19.32 รองลงมาคือ Intermittent คิดเป็นร้อยละ 16.49% แต่จะเห็นได้ว่าไอพีแอดเดรสจำนวนมากจะอยู่ในประเภท Unclassifiable ซึ่งเป็นไอพีแอดเดรสที่ใช้งานน้อยมาก หรือไม่มีการใช้งาน

ตารางที่ 7 การแบ่งประเภทลักษณะการใช้งานจริงของไอพีแอดเดรสโดยใช้ Active Probing

ประเภท	จำนวนไอพีแอดเดรส	จำนวนไอพีแอดเดรส (%)
Always – stable	2,590	3.95 %
Sometimes – stable	6,581	10.04 %
Intermittent	10,808	16.49 %
Underutilized	12,661	19.32 %
Unclassifiable	32,896	50.20 %

วิจารณ์

1. วิจารณ์ผลการทดลอง Active Probing สามารถค้นหาไอพีแอดเดรสที่มีการใช้งาน

การสำรวจจำนวนไอพีแอดเดรสด้วยวิธี Active Probing โดยใช้โปรโตคอล ICMP และ TCP เพื่อแสดงว่าการเนื่องจากถ้าใช้เพียงโปรโตคอลเดียวในการสำรวจจะทำให้ผลการสำรวจไม่ครอบคลุม

ผลการทดลองพบว่าการสำรวจไอพีแอดเดรสที่พบได้ทั้งหมด โปรโตคอล ICMP สำรวจขาดไป 21.21% ส่วนโปรโตคอล TCP สำรวจขาดไป 16.98% ซึ่งจากผลการทดลองนี้ แสดงให้เห็นว่าจำเป็นต้องใช้ทั้งสองโปรโตคอลทำการสำรวจร่วมกัน เพื่อที่จะได้ข้อมูลที่ครอบคลุมเนื่องจากบางโปรโตคอลอาจมีการถูกบล็อกการสำรวจ

2. วิจารณ์ผลการทดลองเปรียบเทียบความถูกต้องของโปรโตคอล ICMP และ TCP

การเปรียบเทียบความถูกต้องของโปรโตคอล ICMP และโปรโตคอล TCP เพื่อแสดงว่าการสำรวจด้วยโปรโตคอล ICMP และโปรโตคอล TCP การสำรวจในรูปแบบใดสามารถแสดงถึงประสิทธิภาพในการสำรวจ

ผลการทดลองพบว่าการสำรวจจำนวนไอพีแอดเดรสด้วยโปรโตคอล TCP สามารถค้นหาไอพีแอดเดรสได้มากกว่าการสำรวจด้วยโปรโตคอล ICMP ประมาณ 4% แสดงให้เห็นว่าประสิทธิภาพในการสำรวจของโปรโตคอล TCP มีมากกว่า แต่อาจเกิดจากในช่วงเวลาของการทำการทดลอง การสำรวจทำการรบกวนระบบเครือข่ายของมหาวิทยาลัย เครื่องที่ทำการสำรวจจึงถูกบล็อกการ Ping จึงทำให้การสำรวจด้วยโปรโตคอล ICMP สำรวจได้จำนวนไอพีแอดเดรสน้อยกว่าการสำรวจด้วยโปรโตคอล TCP จึงส่งผลต่อประสิทธิภาพของการสำรวจด้วยโปรโตคอล ICMP ก็ได้

3. วิจัยผลการทดลองจำนวนไอพีแอดเดรสที่มีการใช้งานบริการ

การสำรวจจำนวนไอพีแอดเดรสที่มีการใช้งานบริการ (Service) เพื่อแสดงให้เห็นว่าภายในมหาวิทยาลัยมีการใช้งานไอพีแอดเดรสในรูปแบบใด

ผลการทดลองพบว่ามีการใช้งานในรูปแบบเว็บไซต์สูงสุด แต่จากผลการสำรวจไม่พบการใช้งานบางโปรแกรม ซึ่งอาจเป็นเพราะการสำรวจมีการระบุพอร์ตเพื่อสำรวจการใช้งานที่ไม่ถูกต้อง หรือไม่ได้สำรวจพอร์ตอื่นที่เกี่ยวข้องดังนั้นทำให้ไม่พบโปรแกรมที่เราต้องการ รวมทั้งการสำรวจโปรแกรมที่ไม่ได้นิยมใช้งานในปัจจุบัน ซึ่งทำให้ได้รับผลการทดลองที่ไม่ถูกต้องทั้งหมด

4. วิจัยผลการประเมินลักษณะของแต่ละไอพีแอดเดรสจากการหาค่า Availability ค่า Volatility และ ค่า Uptime ของแต่ละแอดเดรส

การการประเมินลักษณะของแต่ละไอพีแอดเดรสจากการหาค่า Availability ค่า Volatility และ ค่า Uptime ของแต่ละแอดเดรสในการประเมินเราได้นำขนาดบล็อกของ /24 มาใช้ประเมินลักษณะซึ่งส่งผลให้ได้ลักษณะของไอพีแอดเดรสไม่ครอบคลุมตามลักษณะการใช้งานจริงตามสภาพแวดล้อมของมหาวิทยาลัย

ผลการทดลองพบว่าลักษณะไอพีแอดเดรสของขนาดบล็อก /24 พบว่าลักษณะการใช้งานไอพีแอดเดรสส่วนใหญ่มีการใช้งานค่อนข้างน้อย หรือใช้งานในบางโอกาส ซึ่งจากผลการทดลองนี้สามารถบอกถึงลักษณะการใช้งานของไอพีแอดเดรสทั้งหมดได้ เพราะผลการทดลองประเมินลักษณะของไอพีแอดเดรสก็บอกว่าไอพีแอดเดรสส่วนมากของมหาวิทยาลัยเกษตรศาสตร์มีการใช้งานค่อนข้างน้อย และบางโอกาสเท่านั้น

5. วิจัยผลการทดลองเปรียบเทียบระหว่าง Active Probing และ Passive Probing

การสำรวจจำนวนไอพีแอดเดรสจะใช้วิธีการสำรวจทั้ง Active Probing และ Passive Probing ในการสำรวจ เนื่องจากการสำรวจด้วยวิธีใดวิธีหนึ่งจะให้ผลการทดลองไม่ครอบคลุมจำนวนไอพีแอดเดรสที่มีการใช้งานจริงทั้งหมด แม้ว่าการสำรวจด้วย Active Probing จะใช้หลายโปรโตคอลและหลายรูปแบบของการสำรวจก็ตาม

ผลการทดลองพบว่าการสำรวจด้วย Passive Probing สามารถหาไอพีแอดเดรสพบประมาณ 80% ส่วนของ Active Probing พบประมาณ 60% ซึ่งแสดงให้เห็นว่า Passive Probing สามารถค้นพบไอพีแอดเดรสที่มีการใช้งานในลักษณะ Intermittent พบ ซึ่งทำให้ผลการสำรวจมีความครอบคลุมการใช้งานจริงได้มากขึ้น

6. วิเคราะห์ผลการทดลองโดยรวม

ผลการทดลองโดยรวมพบว่ามหาวิทยาลัยเกษตรศาสตร์มีการใช้งานไอพีแอดเดรสจริงเพียง 49.80% เท่านั้น ซึ่งยังคงเหลือไอพีแอดเดรสอีกเป็นจำนวนมากให้ใช้สำหรับภายในมหาวิทยาลัย โดยการเลือกใช้โปรโตคอลมีผลต่อการสำรวจ เนื่องจากถ้าใช้เพียงโปรโตคอลเดียวในการสำรวจจะทำให้ผลการสำรวจไม่ครอบคลุม เพราะว่าอาจถูกบล็อกหรือป้องกันโปรโตคอลที่ใช้ในการสำรวจเพื่อป้องกันเครือข่ายให้ปลอดภัยจากการถูกโจมตีผ่านทางโปรโตคอลเช่นโปรโตคอล ICMP ที่สามารถถูกบล็อกคำสั่ง Ping ที่ใช้ในการสำรวจไอพีแอดเดรส จึงส่งผลกระทบต่อผลการสำรวจทำให้ไม่พบไอพีแอดเดรสที่มีการใช้งานจริง และการสำรวจพอร์ตทำให้เห็นถึงรูปแบบการใช้งานที่มีความหลากหลาย รวมทั้งการประเมินลักษณะการใช้งานก็พบว่าไอพีแอดเดรสส่วนมากของมหาวิทยาลัยเกษตรศาสตร์มีการใช้งานในลักษณะ underutilized และ Intermittent เป็นส่วนมากเท่านั้น นอกจากนี้การสำรวจต้องการ การสำรวจด้วยวิธีการทั้ง Active Probing และ Passive Probing เพื่อช่วยเพิ่มประสิทธิภาพในการสำรวจมากขึ้น เนื่องจากผลการสำรวจจะครอบคลุมมากขึ้น

สรุปและข้อเสนอแนะ

สรุป

การศึกษาการใช้งานจริงของไอพีแอดเดรสที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์ มีวัตถุประสงค์ เพื่อศึกษาการใช้ประโยชน์ของไอพีแอดเดรสที่มีการจัดสรร และสำรวจปริมาณไอพีแอดเดรสที่มีการใช้งานจริงภายในเครือข่ายมหาวิทยาลัยเกษตรศาสตร์ รวมทั้งวิเคราะห์ผลการสำรวจ คำนวณลักษณะการใช้งานไอพีแอดเดรสภายในองค์กร หรือหน่วยงานของมหาวิทยาลัย สำหรับนำไปพัฒนาการจัดการไอพีแอดเดรส และเพื่อให้เข้าใจประสิทธิภาพของวิธีการสำรวจข้อมูลทั้ง Active Probing และ Passive Probing

ผู้วิจัยทำการสำรวจปริมาณไอพีแอดเดรสที่ขนาดบล็อก /24 โดยการใช้วิธี Active Probing เลือกรูปแบบโปรโตคอล Internet Control Message Protocol (ICMP) และ Transmission Control Protocol (TCP) ที่พอร์ต 21 (ftp) 22 (ssh) 25(smtp) 53 (domain) 80 (http) 110 (pop3) 135 (epmap) 137 (netbios) 139 (netbios) 443 (https) 445 (microsoft-ds) 458 (appleqt) 587 (submission) 1433 (ms-sql-s) 1434 (ms-sql-m) 1214 (kazaa) 3306 (mysql) 6346(gnutella) 1863 (msnp) สำรวจภายในมหาวิทยาลัยเกษตรศาสตร์ และใช้วิธี Active Probing และ Passive Probing สำรวจจำนวนไอพีแอดเดรสภายในภาควิชาวิทยาการคอมพิวเตอร์ โดยใช้งานวิจัยของ John Heidemann และคณะเป็นต้นแบบในการออกแบบการสำรวจ จากนั้นนำผลการสำรวจมาวิเคราะห์ดูแนวโน้มการใช้งานว่าการใช้งานไอพีแอดเดรสส่วนใหญ่ใช้งานด้านใด

ผลการสำรวจพบว่าไอพีแอดเดรสที่มีการใช้งานจริงประมาณร้อยละ 49.80 แสดงว่ามหาวิทยาลัยเกษตรศาสตร์ยังคงมีไอพีแอดเดรสอีกเป็นจำนวนมากที่เหลือสำหรับการใช้งาน โดยการสำรวจด้วยโปรโตคอล TCP สำรวจพบจำนวนปริมาณไอพีแอดเดรสที่มีการใช้งานจริงมากกว่าการสำรวจด้วยโปรโตคอล ICMP และจากผลการสำรวจนำมาวิเคราะห์หาค่า Availability ซึ่งเป็นค่าความน่าจะเป็นที่บ่งบอกถึงลักษณะการใช้งานของไอพีแอดเดรส ค่า Volatility ซึ่งเป็นค่าความน่าจะเป็นที่บ่งบอกถึงสถานะของโฮสต์ของไอพีแอดเดรส และค่า Uptime ซึ่งเป็นค่าความน่าจะเป็นที่บ่งบอกถึงระยะเวลาการใช้งานของไอพีแอดเดรส จากนั้นนำค่าดังกล่าวมาคำนวณลักษณะการใช้งานของไอพีแอดเดรสโดยแบ่งออกเป็น 5 กลุ่มดังนี้ กลุ่ม Always – stable จะเป็นกลุ่มไอพีแอดเดรสที่มีการใช้งานตลอดเวลาและสม่ำเสมอและทำงานอย่างต่อเนื่องสูงสุด ซึ่งจะเป็นกลุ่มของ

เครื่องแม่ข่ายเป็นส่วนมาก ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 3.95 กลุ่ม Sometimes - stable จะเป็นกลุ่มไอพีแอดเดรสที่มีการใช้งานในระยะเวลานานและทำงานอย่างต่อเนื่องรองลงมา ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 10.04 กลุ่ม Intermittent จะเป็นกลุ่มไอพีแอดเดรสที่มีการใช้งานบ่อย แต่ใช้งานในช่วงเวลาสั้น ๆ ผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 16.49 กลุ่ม Underutilized จะเป็นไอพีแอดเดรสที่มีการใช้งานในบางครั้งผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 19.32 และกลุ่มสุดท้ายกลุ่ม Unclassifiable จะเป็นกลุ่มไอพีแอดเดรสที่ไม่ได้รับการจัดสรร หรือไม่มีการใช้งานผลการสำรวจไอพีแอดเดรสกลุ่มนี้มีปริมาณคิดเป็นร้อยละ 50.20

นอกจากนี้การสำรวจด้วยวิธีการทั้ง Active Probing และ Passive Probing ภายในภาควิชาวิทยาการคอมพิวเตอร์ ยังแสดงให้เห็นว่าควรทำการสำรวจทั้งสองวิธี เนื่องจากการสำรวจด้วยวิธี Active Probing เพียงอย่างเดียวก็ไม่สามารถหาไอพีแอดเดรสได้ครบถ้วน หรือการใช้เพียงวิธีการ Passive Probing อย่างเดียวก็ไม่สามารถได้ไอพีแอดเดรสครบถ้วนเช่นกัน และทั้งสองวิธีก็มีข้อเสียในการสำรวจที่แตกต่างกัน ดังนั้นจึงต้องมีการใช้ทั้งสองวิธีเพื่อช่วยเพิ่มประสิทธิภาพในการสำรวจมากขึ้น เนื่องจากผลการสำรวจจะครอบคลุมมากขึ้น

สำหรับการศึกษาการใช้งานจริงของไอพีแอดเดรสที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์ที่นำเสนอสามารถสรุป ข้อเด่นและข้อด้อยได้ดังนี้

ข้อเด่น

1. การทำการทดลองมีการสำรวจโดยใช้ทั้งโปรโตคอล ICMP และโปรโตคอล TCP
2. วิธีการสำรวจใช้หลายชุดคำสั่งในการสำรวจ
3. วิธีการสำรวจใช้ทั้ง Active Probing และ Passive Probing

ข้อด้อย

1. การสำรวจด้วยวิธีการ Passive Probing ทำการสำรวจเพียงภายในภาควิชาวิทยาการคอมพิวเตอร์เท่านั้น ไม่ได้ทำการสำรวจข้อมูลทั้งหมดภายในมหาวิทยาลัย จึงทำให้ไม่ได้ข้อมูลที่ใช้งานจริงทั้งหมด
2. พอร์ตที่ทำการค้นหาการให้บริการใช้การกำหนดพอร์ตที่ต้องการ แต่ไม่ได้ทำการสำรวจพอร์ตที่มีการเปิดใช้งานจริงทั้งหมด

ข้อเสนอแนะ

1. งานวิจัยนี้มุ่งเน้นการสำรวจไอพีแอดเดรสที่มีการใช้จริงด้วยวิธีการ Active Probing ดังนั้นจึงควรใช้การสำรวจแบบ Passive Probing สำรวจเพิ่มในส่วนของภาควิชาอื่น ๆ และหน่วยงานในมหาวิทยาลัยให้ครอบคลุมทั้งมหาวิทยาลัย เพื่อจะได้ข้อมูลที่ถูกต้องในเรื่องของการใช้งานจริงไอพีแอดเดรส
2. การเลือกช่วงเวลาในการทดลองจะต้องเลือกให้เหมาะสมกับสภาพแวดล้อมที่ใช้สำรวจ เพราะการเลือกช่วงเวลามีผลกระทบทำให้ได้ผลการสำรวจที่ไม่ครอบคลุมการใช้งานไอพีแอดเดรสทั้งหมด เนื่องจากได้ทำการสำรวจไอพีแอดเดรสในช่วงเวลาปิดภาคเรียน ซึ่งการเรียนการสอนจะมีการเปิดบางส่วนเท่านั้น
3. ภายในมหาวิทยาลัยเกษตรศาสตร์มีการใช้ Network Address Translation (NAT) ในการเชื่อมต่อเครือข่าย ส่งผลให้ผลการทดลองแสดงการใช้งานที่เพิ่มมากขึ้น เมื่อเทียบกับระบบเครือข่ายที่ไม่มีการใช้ NAT
4. ถ้าทำการสำรวจจากภายนอกมหาวิทยาลัยจะมีการถูกปิดกั้นการสำรวจด้วย firewall ดังนั้นจะต้องเลือกวิธีการและรูปแบบที่เหมาะสมใหม่สำหรับการสำรวจ
5. เนื่องจากในการทำการทดลองมีการส่งแพ็กเก็ตออกไปสำรวจเป็นจำนวนมากเกิดการรบกวนการทำงานของระบบเครือข่ายของมหาวิทยาลัย และการสำรวจดังกล่าวถูกมองว่าเป็นการโจมตีระบบเครือข่าย ทำให้ต้องมีการออกแบบการสำรวจให้ดีขึ้นไม่ส่งผลกระทบต่อการทำงานของระบบเครือข่าย

เอกสารและสิ่งอ้างอิง

- Huffaker, B., Plummer, D., Moore, D., and Claffy, K. C. 2002. Topology Discovery by Active Probing. In **Proceedings of the Symposium on Applications and the Internet**.
- Muhlbauer, W., Maennel, O., Uhlig, S., Feldmann, A., and Roughan, M. 2006. Building an AS-topology model that captures route diversity. pp. 195–204. In **Proceedings of the ACM SIGCOMM Conference**
- Dimitropoulos, X., Krioukov, D., Fomenkov, M., Huffaker, B., Hyun, Y., and Riley, G. 2007. AS relationships. pp. 29–40. **Inference and validation ACM Computer Communication Review**.
- Bartlett, G., Heidemann, J., and Papadopoulos, C. 2007. Understanding Passive and Active Service Discovery. In **Proceedings of IMC'07, October 24 – 26, 2007, San Diego, California, USA**.
- Heidemann, J., Pradkin Y., Govindan R., Papadopoulos C., Bartlett G., and Bannister, J. 2008. Census and Survey of the Visible Internet. In **Proceedings of IMC'08, October 20 – 22, 2008, Vouliagmeni, Greece**.
- Cai, X. and Heidemann, J. 2008. Active Probing to Classify Internet Address Blocks. ANT Censuses of the Internet Address Space project. **USC/ISI Technical Report ISI-TR-653, USC/Information Sciences Institute**.
- Cai, X. and Heidemann, J. 2009. Understanding Address Usage in the Visible Internet. ANT Censuses of the Internet Address Space project. **USC/ISI Technical Report ISI-TR-656, USC/Information Sciences Institute**.

Cai, X. and Heidemann, J. 2010. Understanding Block-level Address Usage in the Visible Internet. In **Proceedings of SIGCOMM'10, August 30 – September 3, 2010, New Delhi, India.**

Lyon, G. 1997. **Nmap**. Available Source: <http://Nmap.org/>, June 1997.

Heidemann, J., Pradkin, Y., Govindan, R., Papadopoulos, C., Bartlett, G. and Bannister, J. 2007. **ANT Census of the Internet Address Space**. Available Source: <http://www.isi.edu/ant/address/>, November 2007.



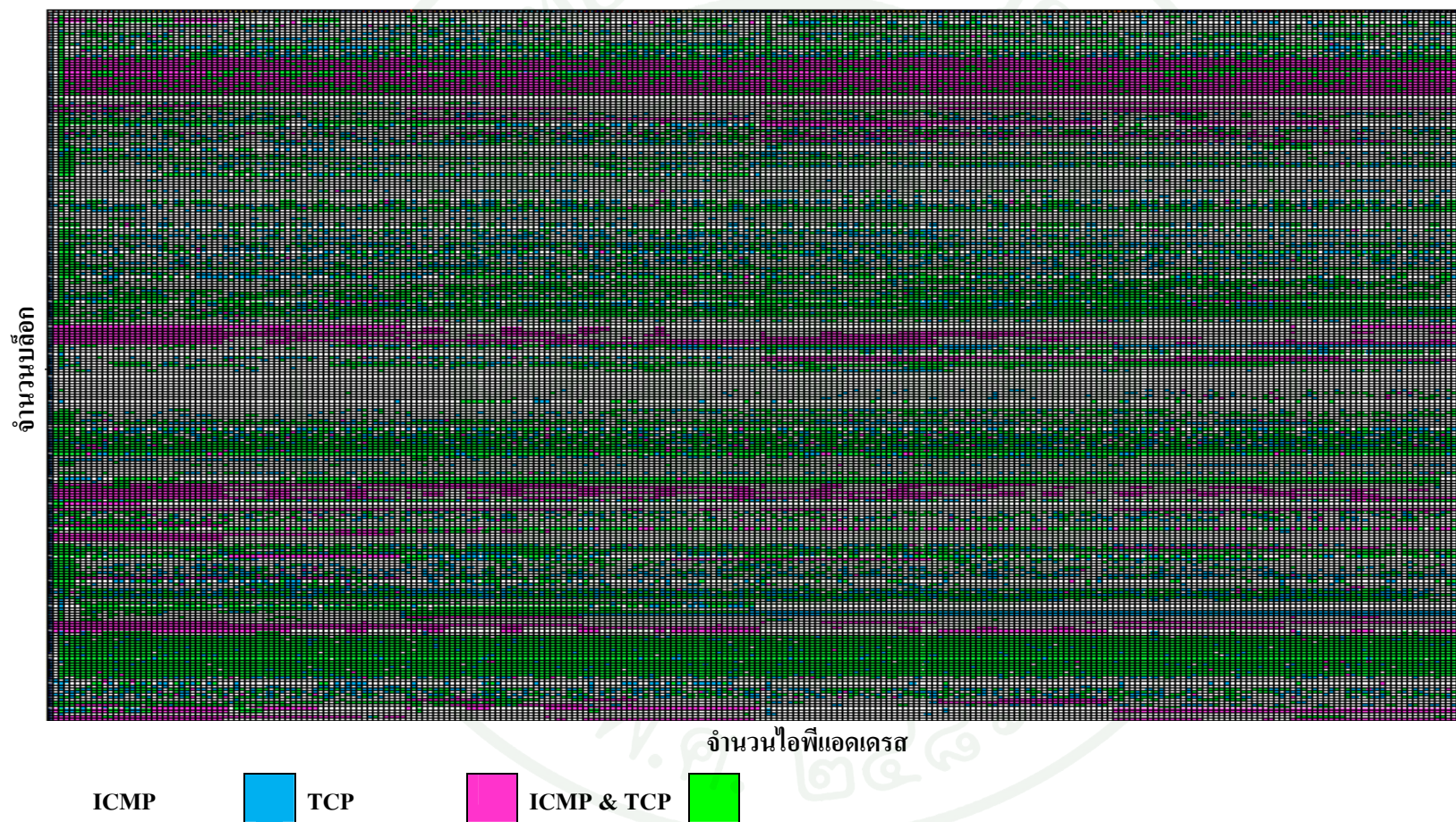


ตารางผนวกที่ ก1 ชุดข้อมูลที่ได้จากการทดลองสำรวจจำนวนไอพีแอดเดรสด้วยวิธี Active Probing

ชุดข้อมูล	เริ่มการสำรวจ	ระยะ เวลา	Prefix length	Active Probings	จำนวนไอพี แอดเดรสที่พบ
การทดลองที่ 1	03 กุมภาพันธ์ 2552	3 วัน	/24	ทุก 20 นาที	12,912
การทดลองที่ 2	05 กุมภาพันธ์ 2552	5 วัน	/24	ทุก 20 นาที	15,763
การทดลองที่ 3	29 เมษายน 2552	7 วัน	/24	ทุก 20 นาที	14,532
การทดลองที่ 4	16 มิถุนายน 2552	7 วัน	/24	ทุก 20 นาที	13,359
การทดลองที่ 5	11 สิงหาคม 2552	7 วัน	/24	ทุก 20 นาที	19,128
การทดลองที่ 6	17 สิงหาคม 2552	7 วัน	/25	ทุก 20 นาที	11,931
การทดลองที่ 7	24 สิงหาคม 2552	7 วัน	/26	ทุก 20 นาที	13,671
การทดลองที่ 8	07 กันยายน 2552	7 วัน	/27	ทุก 20 นาที	13,280
การทดลองที่ 9	15 กันยายน 2552	7 วัน	/28	ทุก 20 นาที	13,766
การทดลองที่ 10	21 กันยายน 2552	7 วัน	/16	ทุก 5 ชั่วโมง	13,827
การทดลองที่ 11	28 กันยายน 2552	7 วัน	/25	ทุก 5 ชั่วโมง	11,032
การทดลองที่ 12	05 ตุลาคม 2552	7 วัน	/17	ทุก 5 ชั่วโมง	12,057
การทดลองที่ 13	12 ตุลาคม 2552	7 วัน	/18	ทุก 5 ชั่วโมง	10,992

ตารางผนวกที่ ก2 ชุดข้อมูลที่ได้จากการทดลองสำรวจจำนวนไอพีแอดเดรสด้วยวิธี Passive

ชุดข้อมูล	เริ่มการสำรวจ	ระยะเวลา
การทดลองที่ 1	5 กันยายน 2552	7 วัน
การทดลองที่ 2	28 กันยายน 2552	7 วัน
การทดลองที่ 3	6 ตุลาคม 2552	7 วัน
การทดลองที่ 4	28 มกราคม 2553	7 วัน
การทดลองที่ 5	5 กุมภาพันธ์ 2553	7 วัน



ภาพผนวกที่ 1 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดสำรวจด้วย Active Probing

จำนวนบล็อก



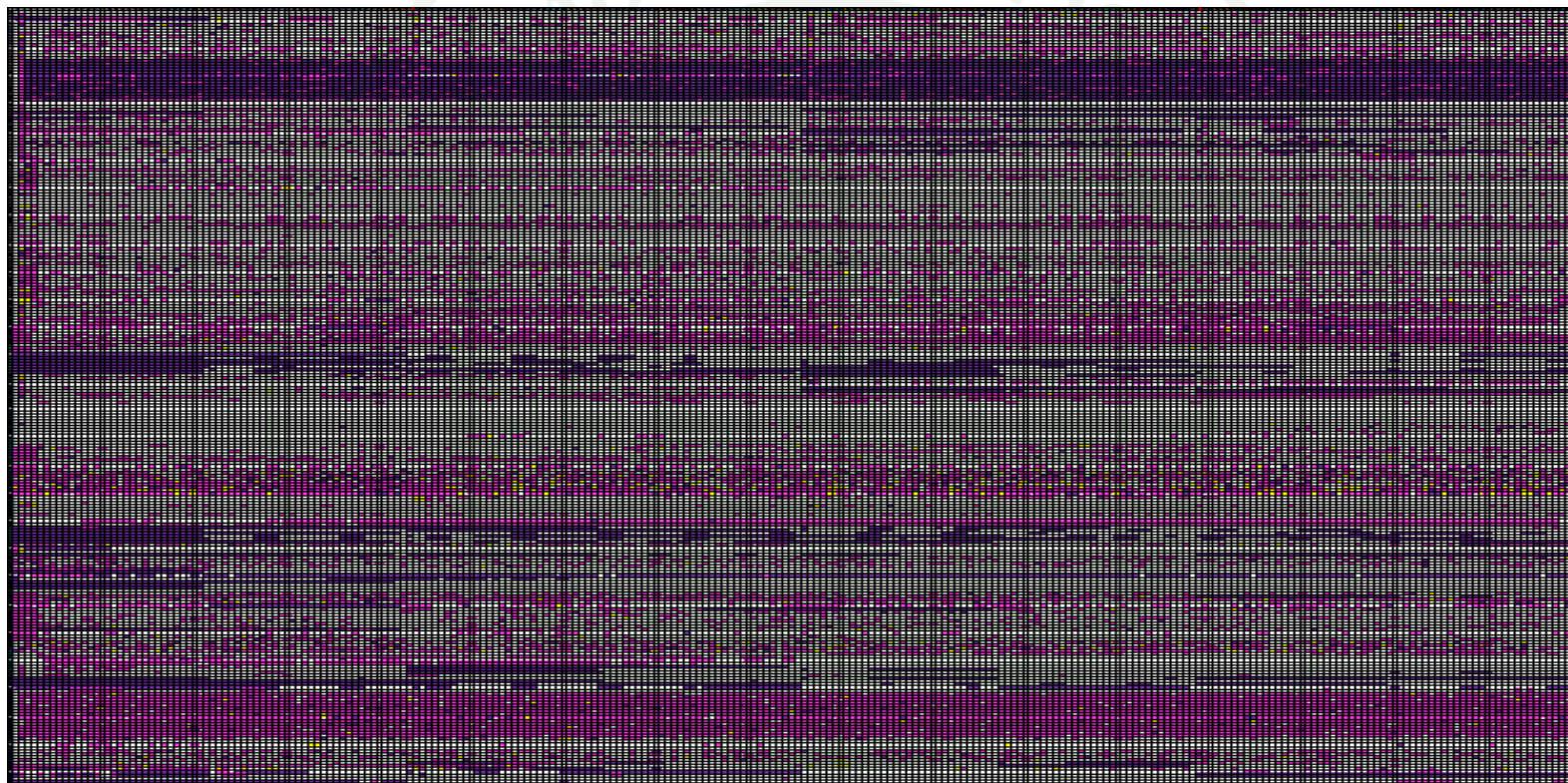
จำนวนไอพีแอดเดรส



ภาพผนวกที่ 2 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโปรโตคอล ICMP

จากภาพผนวกที่ ก2 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโพรโทคอล ICMP ในแกน x แสดงจำนวนจำนวนไอแอดเดรสใน 1 บล็อกจำนวน 256 หมายเลขไอพีแอดเดรส แกน y แสดงจำนวนบล็อก 256 บล็อกของ /24 ซึ่งจุดสีทั้งหมดที่ plot ลงบนพื้นนั้นจะแสดงถึงจำนวนไอพีแอดเดรสที่มีการใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์โดยการสำรวจพบด้วยโพรโทคอล ICMP เพียงอย่างเดียว โดยการสำรวจเราได้นำชุดข้อมูลจากการทดลองที่ 1, 2, 3, 4, 5, 6, 7, 8, 9 และ 11 ที่ทำการสำรวจทั้งหมดมา plot เป็นจุดสีเพื่อแสดงจำนวนไอพีแอดเดรสที่สำรวจพบ จุดสีเขียวแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /24 คือทำการสำรวจทีละ 256 หมายเลขไอพีแอดเดรส จุดสีม่วงแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /25 คือทำการสำรวจทีละ 128 หมายเลขไอพีแอดเดรส จุดสีแดงแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /26 คือทำการสำรวจทีละ 64 หมายเลขไอพีแอดเดรส จุดสีเหลืองแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /27 คือทำการสำรวจทีละ 32 หมายเลขไอพีแอดเดรส จุดสีฟ้าแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /28 คือทำการสำรวจทีละ 16 หมายเลขไอพีแอดเดรส จุดสีส้มแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 และ /25 จุดสีเทาแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 /25 และ /26 จุดสีน้ำเงินแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 /25 /26 และ /27 สุดท้ายจุดสีชมพูแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 /25 /26 /27 และ /28 จะเห็นได้ว่าถ้าทำการสำรวจด้วยขนาดของบล็อกที่เล็กลงจะทำให้สามารถพบไอพีแอดเดรสเพิ่มมากขึ้นจากการสำรวจด้วยขนาดของบล็อกที่ขนาดเดียวตลอด

จำนวนบล็อก



SYN



ACK



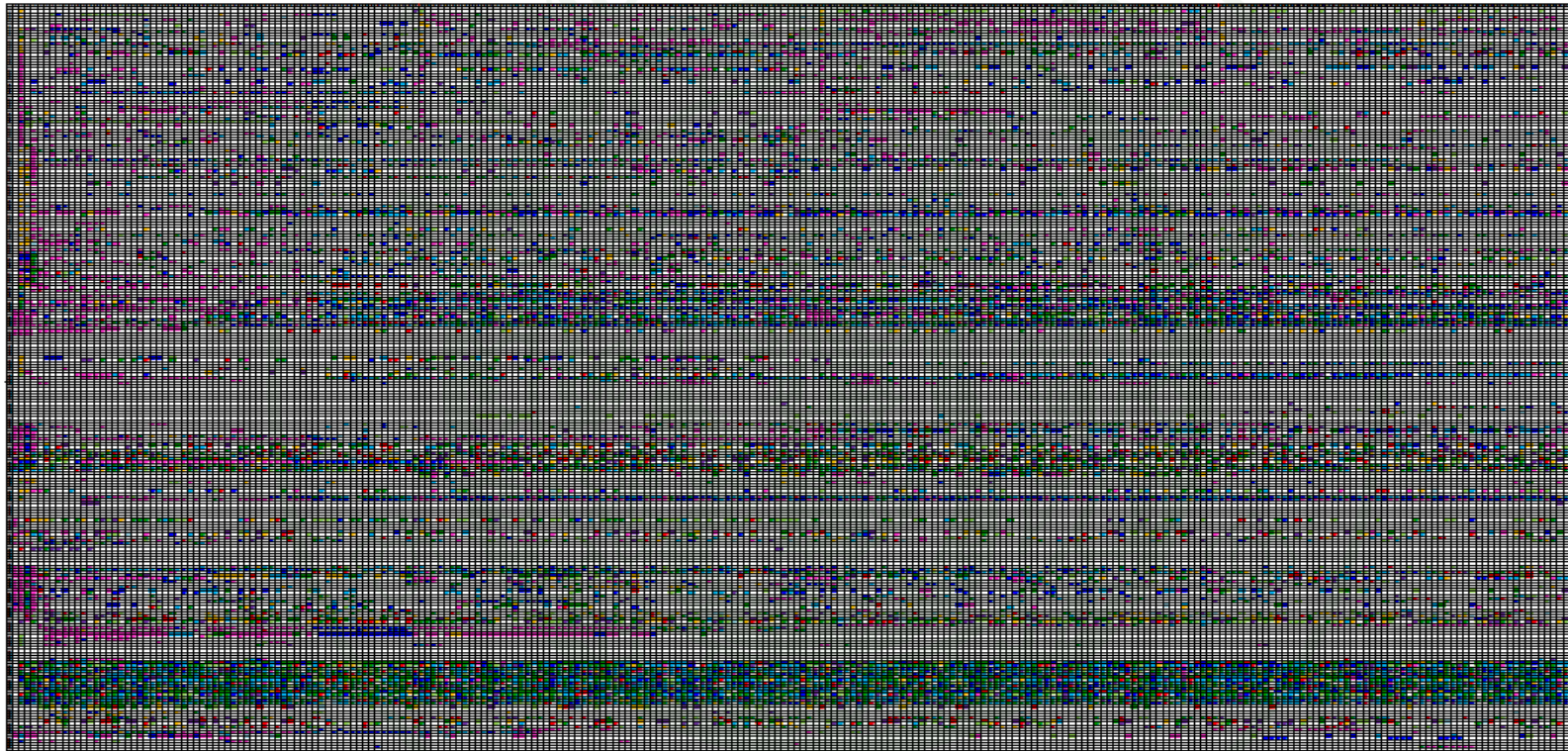
ACK & SYN



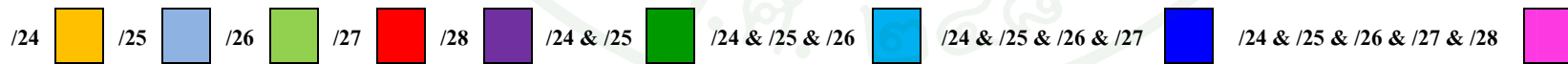
จำนวนไอพีแอดเดรส

ภาพผนวกที่ ก3 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโปรโตคอล TCP

จำนวนบล็อก



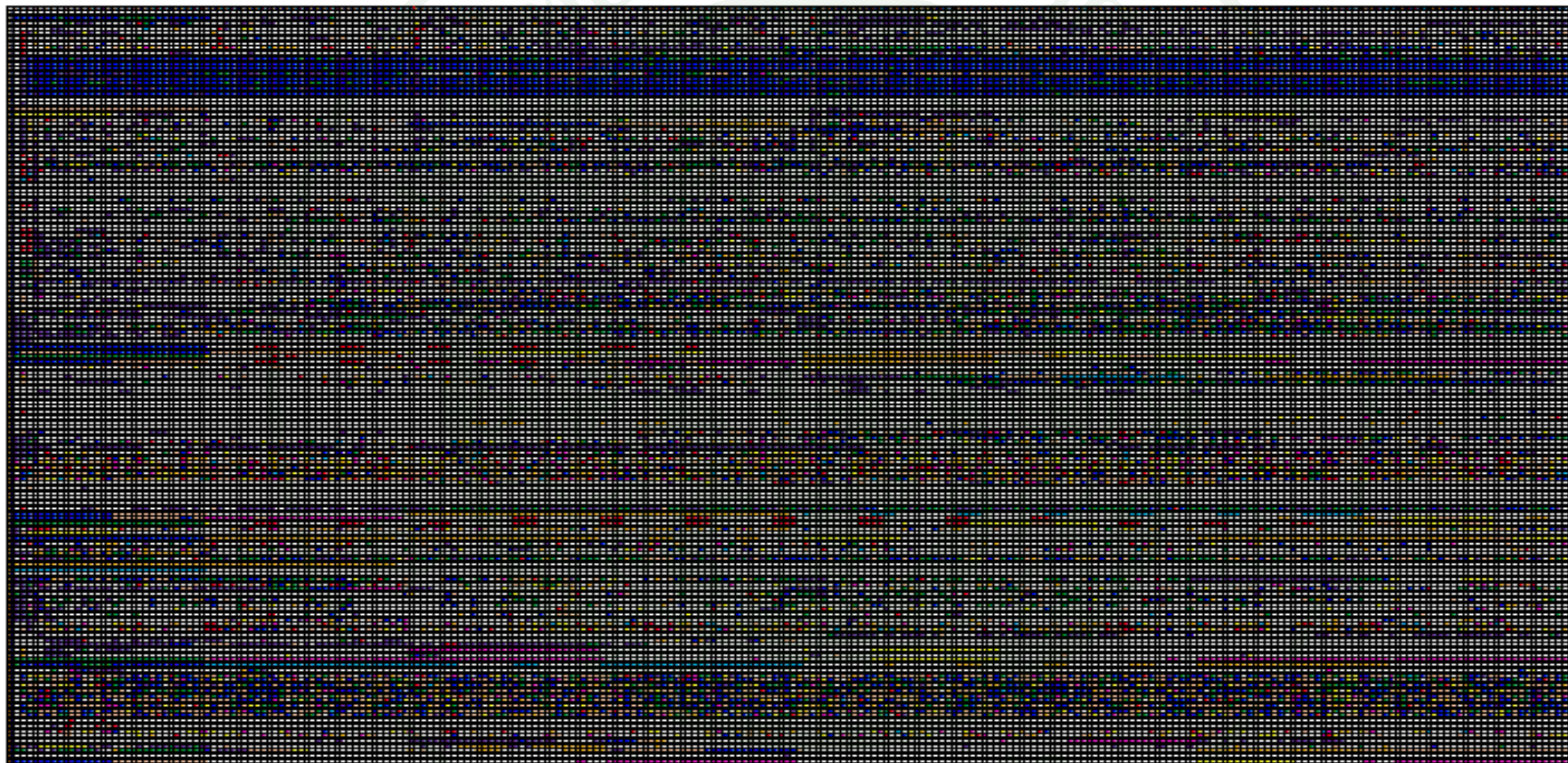
จำนวนไอพีแอดเดรส



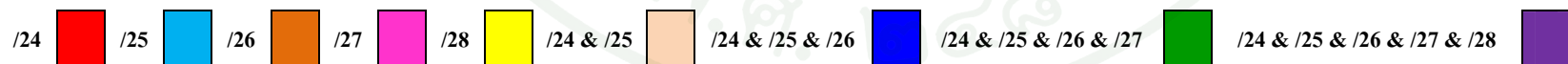
ภาพผนวกที่ ก4 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโปรโตคอล TCP - ACK

จากภาพผนวกที่ ก4 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโพรโทคอล TCP ในรูปแบบ TCP - ACK ในแกน x แสดงจำนวนจำนวนไอพีแอดเดรสใน 1 บล็อกจำนวน 256 หมายเลขไอพีแอดเดรส แกน y แสดงจำนวนบล็อก 256 บล็อกของ /24 ซึ่งจุดสีทั้งหมดที่ plot ลงบนพื้นนั้นจะแสดงถึงจำนวนไอพีแอดเดรสที่มีการใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์ โดยการสำรวจพบด้วยโพรโทคอล ICMP เพียงอย่างเดียว โดยการสำรวจเราได้นำชุดข้อมูลจากการทดลองที่ 1, 2, 3, 4, 5, 6, 7, 8, 9 และ 11 ที่ทำการสำรวจทั้งหมดมา plot เป็นจุดสีเพื่อแสดงจำนวนไอพีแอดเดรสที่สำรวจพบ จุดสีเหลืองแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /24 คือทำการสำรวจทีละ 256 หมายเลขไอพีแอดเดรส จุดสีฟ้าแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /25 คือทำการสำรวจทีละ 128 หมายเลขไอพีแอดเดรส จุดสีเขียวแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /26 คือทำการสำรวจทีละ 64 หมายเลขไอพีแอดเดรส จุดสีแดงแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /27 คือทำการสำรวจทีละ 32 หมายเลขไอพีแอดเดรส และจุดสีม่วงแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /28 คือทำการสำรวจทีละ 16 หมายเลขไอพีแอดเดรส จุดสีเขียวแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 และ /25 จุดสีฟ้าแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 /25 และ /26 จุดสีน้ำเงินแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 /25 /26 และ /27 สุดท้ายจุดสีชมพูแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 /25 /26 /27 และ /28 จะเห็นได้ว่าทำการสำรวจด้วยขนาดของบล็อกที่เล็กลงจะทำให้สามารถพบไอพีแอดเดรสเพิ่มมากขึ้นจากการสำรวจด้วยขนาดของบล็อกที่ขนาดเดียวตลอด

จำนวนบล็อก



จำนวนไอพีแอดเดรส



ภาพผนวกที่ ก5 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโปรโตคอล TCP - SYN

จากภาพผนวกที่ ก5 จำนวนไอพีแอดเดรสที่มีการใช้งานทั้งหมดที่สำรวจพบโดยโปรโตคอล TCP ในรูปแบบ TCP - SYN ในแกน x แสดงจำนวนจำนวนไอพีแอดเดรสใน 1 บล็อกจำนวน 256 หมายเลขไอพีแอดเดรส แกน y แสดงจำนวนบล็อก 256 บล็อกของ /24 ซึ่งจุดสีทั้งหมดที่ plot ลงบนพื้นนั้นจะแสดงถึงจำนวนไอพีแอดเดรสที่มีการใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์ โดยการสำรวจพบด้วยโปรโตคอล ICMP เพียงอย่างเดียว โดยการสำรวจเราได้นำชุดข้อมูลจากการทดลองที่ 1, 2, 3, 4, 5, 6, 7, 8, 9 และ 11 ที่ทำการสำรวจทั้งหมดมา plot เป็นจุดสีเพื่อแสดงจำนวนไอพีแอดเดรสที่สำรวจพบ จุดสีแดงแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /24 คือทำการสำรวจทีละ 256 หมายเลขไอพีแอดเดรส จุดสีฟ้าแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /25 คือทำการสำรวจทีละ 128 หมายเลขไอพีแอดเดรส จุดสีน้ำตาลแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /26 คือทำการสำรวจทีละ 64 หมายเลขไอพีแอดเดรส จุดสีชมพูแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /27 คือทำการสำรวจทีละ 32 หมายเลขไอพีแอดเดรส และจุดสีเหลืองแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ /28 คือทำการสำรวจทีละ 16 หมายเลขไอพีแอดเดรส จุดสีส้มแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 และ /25 จุดสีน้ำเงินแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 /25 และ /26 จุดสีเขียวแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 /25 /26 และ /27 สุดท้ายจุดสีม่วงแสดงถึงไอพีแอดเดรสที่พบจากการสำรวจ ทั้ง /24 /25 /26 /27 และ /28 จะเห็นได้ว่าถ้าทำการสำรวจด้วยขนาดของบล็อกที่เล็กลงจะทำให้สามารถพบไอพีแอดเดรสเพิ่มมากขึ้นจากการสำรวจด้วยขนาดของบล็อกที่ขนาดเดียวตลอด

ตารางผนวกที่ 3 ข้อมูลการจัดสรรไอพีแอดเดรสของมหาวิทยาลัยเกษตรศาสตร์

Network	subnetwork#1	subnetwork#2	Description
158.108.0.0/20			
	158.108.1.0/24		
		158.108.1.0/25	Free
		158.108.1.128/25	Tele Conference
	158.108.2.0/24		
		158.108.2.0/27	Caching Server
		158.108.2.32/27	VMWARE
		158.108.2.64/26	Server Farm
		158.108.2.128/25	Development Server
	158.108.3.0/24		
		158.108.3.0/25	Free
		158.108.3.128/25	ETO Academic Services Building
	158.108.4.0/24		
		158.108.4.0/25	CPC Staff
		158.108.4.128/26	Server Farm Oracle Server
		158.108.4.192/27	Free
		158.108.4.224/27	NOC Server
	158.108.5.0/24		
		158.108.5.0/27	Server Farm E-meeting
		158.108.5.32/27	Server Farm KUWIN
		158.108.5.64/26	VoIP System & IP telephone
		158.108.5.128/26	Server Farm Webhost
		158.108.5.194/27	Network Server Farm Zone1
		158.108.5.224/27	Network Server Farm Zone2
	158.108.6.0/24		
		158.108.6.0/25	Classroom 2nd Floor

ตารางผนวกที่ ก3 (ต่อ)

Network	subnetwork#1	subnetwork#2	Description
			Multimedia
		158.108.6.128/25	Operation Server Farm
	158.108.7.0/24		Staff OCS New
	158.108.8.0/24		
		158.108.8.0/27	Student Activity Building
		158.108.8.32/27	Insee Football Stadium
		158.108.8.64/29	Modem Device
		158.108.8.72/29	Free
		158.108.8.80/28	Free
		158.108.8.96/27	Department of Apply Economic
		158.108.8.128/25	NOC Development Server
	158.108.9.0/24		
		158.108.9.0/28	Student Admin board
		158.108.9.16/28	Vedio Conference
		158.108.9.32/27	KU-Press
		158.108.9.64/26	Savings Co-Operation
		158.108.9.128/27	KU Book Center
		158.108.9.160/27	Royal Project Foundation
		158.108.9.192/27	History Building
		158.108.9.224/27	Security Building Gate#2 & Sell tree
	158.108.10.0/24		
		158.108.10.0/26	X'MBA Department
		158.108.10.64/26	KU-SLUSE Flr.3 Wittayaborikarn bld.
		158.108.10.128/26	International MBA Department

ตารางผนวกที่ ก3 (ต่อ)

Network	subnetwork#1	subnetwork#2	Description
		158.108.10.192/26	X'MBA Department
	158.108.11.0/24		
		158.108.11.0/27	Office of Agriculture Museum and Culture
		158.108.11.32/27	Women Dormitory
		158.108.11.64/27	Vehical Department
		158.108.11.96/27	Sport Office
		158.108.11.128/27	Environment College
		158.108.11.160/27	Sport Science
		158.108.11.192/27	Vehical Department
		158.108.11.224/27	Bio-Control
	158.108.12.0/24		E-student(KFC)
	158.108.13.0/24		
		158.108.13.0/26	Home economics
		158.108.13.64/27	KU'Service Office
		158.108.13.96/27	Bug Museum
			Language
		158.108.13.128/26	center(Witayaborikarn Bld. Flr.3)
		158.108.13.192/27	Nursery
		158.108.13.224/27	Bio-Technology
			Faculty of Business
	158.108.14.0/24		Administration
	158.108.15.0/24		Faculty of Economic
158.108.224.0/20			Office of Computer Service Area

ตารางผนวกที่ ก3 (ต่อ)

Network	subnetwork#1	subnetwork#2	Description
158.108.128.0/20			
	158.108.128.0/21		KUWIN
	158.108.136.0/22		KUWIN-WPA
	158.108.140.0/23		Management KUWIN
	158.108.142.0/24		KUWIN-Register
	158.108.143.0/24		Nopparat Hospital
158.108.208.0/21			
	158.108.208.0/23		Modem Teacher & Staff KU
	158.108.210.0/23		Modem Student KU
	158.108.212.0/25		Modem E-Mail Usage KU
	158.108.212.128/25		Free
	158.108.213.0/25		Thai National Grid Center
	158.108.213.128/25		Free
158.108.240.0/21			
	158.108.240.0/23		Staff VPN
	158.108.242.0/27		BOX-VPN(Doypui)
	158.108.242.32/27		BOX-VPN(Kanchanaburi)
	158.108.242.64/27		BOX-VPN(ResearchX)
	158.108.242.96/27		BOX-VPN(Tupkwang)
	158.108.242.128/27		BOX-VPN(Siracha Research)
	158.108.242.160/27		BOX-VPN(Lopburi)
	158.108.242.192/27		BOX-VPN(RaiSuwan)
	158.108.242.224/27		BOX-VPN(Trat)
	158.108.243.0/27		BOX-VPN(Sakon1)
	158.108.243.32/27		BOX-VPN(Sakon2)
	158.108.243.64/27		BOX-VPN()
	158.108.243.96/27		BOX-VPN()

ตารางผนวกที่ ก3 (ต่อ)

Network	subnetwork#1	subnetwork#2	Description
	158.108.243.128/27		BOX-VPN()
	158.108.243.160/27		BOX-VPN()
	158.108.243.192/27		BOX-VPN()
	158.108.243.224/27		BOX-VPN()
	158.108.244.0/22		Nisit VPN
158.108.48.0/20	158.108.48.0/24	158.108.48.0/25	Study Center Building 2 (LH2)
		158.108.48.128/25	Service LIB
	158.108.49.0/24	158.108.49.0/27	Study Center Building 3 (LH3)
		158.108.49.32/27	Sirinthorn Center(LIB)
		158.108.49.64/26	ว่าง
		158.108.49.128/25	ว่าง
	158.108.50.0/24	158.108.50.0/24	Registration Department
	158.108.51.0/24	158.108.51.0/24	Extension Department
	158.108.52.0/24	158.108.52.0/24	Agriculture Department
	158.108.53.0/24	158.108.53.0/24	Fisheries Department
	158.108.54.0/24	158.108.54.0/24	Human Department
	158.108.55.0/24	158.108.55.0/24	Graduate Department
	158.108.56.0/24	158.108.56.0/25	Man Dormarity and Student Affiars
	158.108.57.0/24	158.108.57.0/27	Hokky club(158.108.57.0/27)
		158.108.57.32/27	Chulaporn-pool
		158.108.57.64/26	ว่าง
		158.108.57.128/25	ว่าง
	158.108.58.0/24	158.108.58.0/24	LH4
	158.108.59.0/24		ว่าง

ตารางผนวกที่ ก3 (ต่อ)

Network	subnetwork#1	subnetwork#2	Description
	158.108.60.0/24		ว่าง
	158.108.61.0/24		ว่าง
	158.108.62.0/24		ว่าง
	158.108.63.0/24		ว่าง
158.108.64.0/20			
	158.108.64.0/24	158.108.64.0/24	Agro-Industries Department
	158.108.65.0/24		ว่าง
	158.108.66.0/24	158.108.66.0/24	Kasetsart University School
	158.108.67.0/24		ว่าง
	158.108.68.0/23		Forest Faculty
	158.108.70.0/23		Satit School
	158.108.72.0/24		ว่าง
	158.108.73.0/24		ว่าง
	158.108.74.0/24	158.108.74.0/25	Veterinary College
		158.108.74.128/25	
	158.108.75.0/24	158.108.75.0/24	TEST-CPC-FLOOR3
	158.108.76.0/24	158.108.76.0/24	Social Department
	158.108.77.0/24		
	158.108.78.0/24	158.108.78.0/24	Education Department
	158.108.79.0/24	158.108.79.0/25	Human Ratchanakarin
		158.108.79.128/27	KU Dairy plant
158.108.80.0/22			
	158.108.80.0/24	158.108.80.0/24	Library's Network
	158.108.81.0/24	158.108.81.0/24	Research of Department
	158.108.82.0/24		ว่าง
	158.108.83.0/24	158.108.83.0/24	VET Medical
	158.108.89.0/24	158.108.89.0/24	LH1

ตารางผนวกที่ ก3 (ต่อ)

Network	subnetwork#1	subnetwork#2	Description
	158.108.92.0/24	158.108.92.0/24	Office of Library
	158.108.95.0/24	158.108.95.0/24	RECOFTC
	158.108.84.0/24	158.108.84.0/24	Local 50 Year Building
	158.108.85.0/24	158.108.85.0/24	CNC
	158.108.86.0/24	158.108.86.0/24	Fishies Department
	158.108.87.0/24	158.108.87.0/24	Architecture Department
	158.108.88.0/24	158.108.88.0/25	KAPI
		158.108.88.128/25	Agro-Industry bld.3
	158.108.90.0/24	158.108.90.0/24	Local 50 Year Building
	158.108.91.0/24	158.108.91.0/24	Satit International Program
	158.108.93.0/24	158.108.93.0/25	SCI tool center
		158.108.93.128/25	Radiation Center
	158.108.94.0/24	158.108.94.0/24	Food Department
	158.108.95.0/24	158.108.95.0/24	RECOFTC
158.108.160.0/21	158.108.160.0/24		
		158.108.160.0/27	50 Year Building Floor3
		158.108.160.32/27	50 Year Building Floor4
		158.108.160.64/26	50 Year Building Floor6
		158.108.160.128/26	50 Year Building Floor8
		158.108.160.192/27	Temp For Floor1
		158.108.160.224/27	50 Year Building Floor10
	158.108.161.0/24		
		158.108.161.0/26	50 Year Building Floor7
		158.108.161.64/28	Car Park 50Y
		158.108.161.80/28	Free
		158.108.161.96/28	Free
		158.108.161.112/28	Free

ตารางผนวกที่ ก3 (ต่อ)

Network	subnetwork#1	subnetwork#2	Description
		158.108.161.128/25	Free
	158.108.162.0/24		Netday
	158.108.163.0/24		
		158.108.163.0/25	Coordinate station Campus
		158.108.163.0/25	Free
	158.108.164.0/24		Free
	158.108.165.0/24		Free
	158.108.166.0/24		Research and Development Building
	158.108.167.0/24		Free
158.108.16.0/20	158.108.16.0/24	158.108.16.0/26	Computer Science Floor1
		158.108.16.64/26	Computer Science Floor3
		158.108.16.128/26	Computer Science Floor1
		158.108.16.192/26	Computer Science Floor3
	158.108.17.0/24	158.108.17.0/24	Bot Science
	158.108.18.0/24	158.108.18.0/25	Stat Science
		158.108.18.128/25	Lab-Stat
	158.108.19.0/24	158.108.19.0/24	Micro Science
	158.108.20.0/24	158.108.20.0/27	Chem1
		158.108.20.32/27	Chem2
		158.108.20.64/27	Chem3
		158.108.20.96/27	Chem Floor5
		158.108.20.128/25	Chem Floor3
	158.108.21.0/24	158.108.21.0/26	SCL CS_F3
		158.108.21.65/26	SCL CS_F3
		158.108.21.129/26	SMC to SCL
		158.108.21.193/26	CS

ตารางผนวกที่ ก3 (ต่อ)

Network	subnetwork#1	subnetwork#2	Description
	158.108.22.0/24	158.108.22.0/24	Math Science
	158.108.23.0/24	158.108.23.0/24	Zoo Science
	158.108.24.0/24	158.108.24.0/24	Physic Science
	158.108.25.0/24	158.108.25.0/26	Chem1 Science
		158.108.25.64/27	Chem2 Science
		158.108.25.97/27	Chem3 Science
		158.108.25.129/26	Chem4 Science
		158.108.25.192/27	Chem5 Science
		158.108.25.225/27	Chem6 Science
	158.108.26.0/24	158.108.26.0/25	BioChem Science
		158.108.26.128/25	Gene Science
	158.108.27.0/24	158.108.27.0/25	Rad Science
		158.108.27.128/25	ScOff Science
	158.108.28.0/24	158.108.28.0/25	Environment Science
		158.108.28.128/25	General Science
	158.108.29.0/24	158.108.29.0/25	Lab-CmSrv
		158.108.29.128/27	Lab-Sot
		158.108.29.192/27	Chem7 Science
		158.108.29.224/27	Chem8 Science
	158.108.30.0/24		
	158.108.31.0/24		



ผลงานตีพิมพ์

แสงดาว พรทวีโชคสกุล, สุขุมล กิตติสิน และ พนิดา พงษ์ไพบูลย์. 2552. การศึกษาการใช้งานจริงของ ไอพีแอดเดรสที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์, น. 73-78. ใน รายงานการประชุมทางวิชาการวิทยาการคอมพิวเตอร์และวิศวกรรมคอมพิวเตอร์แห่งชาติครั้งที่ 13 (NCSEC 2009). กรุงเทพฯ.

Prontaweechoksakul, S., Kitisin, S. and Pongpaibool, P. 2011. A Study of IP Address Usage with Active and Passive Probing within Kasetsart University. In **Proceedings of ICSEC 2011, September 7 – 9, 2011, Bangkok, Thailand.**

การศึกษาการใช้งานจริงของ ไอพีแอดเดรสที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์

A study of IP addresses allocation utilization within Kasetsart University

แสงดาว พรทวีโชคกุล¹ สุขุมล ฤทธิสิน² และ พนิดา พงษ์ไพบูลย์³

^{1,2}ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

เลขที่ 50 ถนนพหลโยธิน แขวงลาดยาว เขตจตุจักร กรุงเทพมหานคร 10900 โทรศัพท์: 02-562-5444

E-mail:gs064183@ku.ac.th, sukumali@ku.ac.th

³ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

เลขที่ 112 ถนนพหลโยธิน ต.คลองหนึ่ง อ.คลองหลวง จ.ปทุมธานี 12120 โทรศัพท์: 02-564-6900 ต่อ 2566 E-mail: panita@necetec.or.th

บทคัดย่อ

การศึกษาการใช้งานจริงของไอพีแอดเดรสที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์มีวัตถุประสงค์เพื่อให้ทราบข้อมูลสถิติของไอพีแอดเดรสที่มีการใช้งานจริง และคาดการณ์ลักษณะการใช้งานของไอพีแอดเดรสของเน็ตเวิร์ก อาจารย์ พนักงาน และบุคลากรภายในมหาวิทยาลัย ผู้วิจัยทำการสำรวจไอพีแอดเดรสของ /24 บล็อก จำนวน 207 บล็อก โดยการสำรวจได้เลือกสำรวจเฉพาะบล็อกที่มีการจัดสรรให้กับหน่วยงานหรือองค์กรภายในมหาวิทยาลัย ซึ่งใช้ Internet Control Message Protocol (ICMP) และ Transmission Control Protocol (TCP) ที่พอร์ต 21 (ftp) 22 (ssh) 80 (http) 443 (https) 3306 (MySQL) 445 (microsoft-ds) และ 139 (netbios). ผลการสำรวจพบว่าไอพีแอดเดรสที่มีการใช้งานจริงประมาณ 27.42 % โดยการสำรวจด้วย ICMP สำรวจพบจำนวนไอพีแอดเดรสที่มีการใช้งานจริงมากกว่าการสำรวจด้วย TCP และจากผลการสำรวจนำมาวิเคราะห์หาค่า Availability ค่า Volatility และค่า Uptime จากนั้นนำค่าดังกล่าวมาคาดการณ์ลักษณะการใช้งานของไอพีแอดเดรสได้ดังนี้กลุ่ม Always - stable คือมีการใช้งานอย่างต่อเนื่อง คิดเป็น 0.7 % โดยเครื่องคอมพิวเตอร์กลุ่มนี้เป็นเครื่องแม่ข่าย (server) กลุ่ม Sometimes - stable มีการใช้งานอย่างต่อเนื่องในบางครั้ง คิดเป็น 8.86 % กลุ่ม Intermittent มีการใช้งานอย่างสม่ำเสมอ คิดเป็น 4.04 % กลุ่ม Underutilized มีการใช้งานไม่เต็มประสิทธิภาพคิดเป็น คิดเป็น 14.32 % และ Unclassifiable ไม่สามารถจำแนกลักษณะการใช้งานได้ คิดเป็น 72.85 %

คำสำคัญ: IPv4, การสำรวจไอพีแอดเดรส, การจัดสรรไอพีแอดเดรส

Abstract

This paper studies address allocation utilization within Kasetsart University. We propose to count number of IP addresses in use and their usage characteristics within the university. We 207 / 24 blocks which are allocated to departments or organizations within the university. Our experiments use Internet Control Message Protocol (ICMP) and Transmission Control Protocol (TCP) on port 21 (ftp) 22

(ssh) 80 (http) 443 (https) 3306 (MySQL) 445 (microsoft-ds) and 139 (netbios). Our experiment results show that the only 27.42% of allocated IP addresses are in use. ICMP method can find more visible IP address than the TCP method. We also analyze the address characteristics, such as, availability, volatility, and uptime. Evaluations show IP addresses have the following characteristics: 0.7% is always stable; 8.86% is sometimes stable; 4.04% is intermittent; 14.32% is underutilized; and finally 72.85% is unclassifiable.

Keywords: Internet address allocation, Utilization, Survey, IPv4, Internet Measurement

1. บทนำ

การสำรวจไอพีแอดเดรสที่ใช้งานจริงก่อนหน้านี้ทำการสำรวจด้วยการสำรวจโครงสร้าง (topology) [1] โดยใช้การวัดโครงสร้างและข้อมูลรอบเวลาการเดินทาง (RTT) ซึ่งผลที่ได้จากวิธีการนี้จะเห็นภาพรวมความสัมพันธ์ระหว่างรอบเวลาการเดินทางกับโครงสร้าง ต่อมาได้ทำการศึกษาโครงสร้าง และเน้นในในระดับ Autonomous System (AS) และ router topology โดยให้ความสำคัญกับความสัมพันธ์ของ AS และ interdomain routing [2,3,4] แต่ในเรื่องความสัมพันธ์ก็จะเกี่ยวข้องกับสถิติประชากรของ edge host และการใช้ IPv4 address space โดยในปัจจุบันมีผู้วิจัยพยายามที่จะศึกษาลักษณะการใช้งานไอพีแอดเดรสที่เครื่องลูกข่ายจึงได้ทำการสำรวจไอพีแอดเดรสด้วย ICMP และ TCP [5,6,8] โดยเสนอหลักการสำรวจแบบการสำรวจประชากร (census) คือการสำรวจไอพีแอดเดรสทั้งหมด และ การสำรวจแบบสุ่มตัวอย่าง (random survey) คือการเลือกตัวอย่างบางไอพีแอดเดรสขึ้นมาสำรวจ แต่ก็มีหลายปัจจัยที่มีผลต่อการสำรวจ เช่น จำนวนของไอพีแอดเดรสที่มีจำนวนมาก และไอพีแอดเดรสที่ซ่อนอยู่หลังไฟร์วอลล์ ส่งผลให้การสำรวจมีความคลาดเคลื่อน ซึ่งจากงานวิจัยดังกล่าวได้นำมาเป็นต้นแบบในการสำรวจปริมาณไอพีแอดเดรสที่มีการใช้งานภายในมหาวิทยาลัยเกษตรศาสตร์ โดยสำรวจแบบการสำรวจประชากร แต่จะมีแบ่งข้อมูลออกเป็นกลุ่มย่อย เพื่อให้ใช้เวลาในการสำรวจไม่มาก และนำ

ผลการสำรวจวิเคราะห์ปริมาณไอพีแอดเดรสที่ใช้งาน โดยแยกตามประเภทการใช้งาน และคาดการณ์ลักษณะการใช้งานไอพีแอดเดรสภายในมหาวิทยาลัย

การศึกษารูปแบบการใช้งานจริงของไอพีแอดเดรสที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์ ทำให้ทราบสถิติของไอพีแอดเดรสที่มีการใช้งานจริง และคาดการณ์ลักษณะการใช้งานไอพีแอดเดรสของนิสิต อาจารย์ พนักงาน และบุคลากรภายในมหาวิทยาลัย ผู้วิจัยสำรวจไอพีแอดเดรสของ /24 บล็อก จำนวน 207 บล็อก โดยการสำรวจได้เลือกสำรวจเฉพาะบล็อกที่มีการจัดสรรให้กับหน่วยงานหรือองค์กรภายในมหาวิทยาลัย ซึ่งใช้ ICMP และ TCP ที่พอร์ต 21 (ftp) 22 (ssh) 80 (http) 443 (https) 3306 (MySQL) 445 (microsoft-ds) และ 139 (netbios) จากนั้นนำผลการสำรวจมาวิเคราะห์ดูแนวโน้มการใช้งานว่าใช้งานไอพีแอดเดรสส่วนใหญ่ใช้งานด้านใด

2. วิธีการดำเนินการวิจัย

ผู้วิจัยได้สำรวจปริมาณไอพีแอดเดรสที่มีการใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์ และลักษณะการใช้งานไอพีแอดเดรสโดยมีขั้นตอนดังนี้

2.1 วิธีการสำรวจ

ผู้วิจัยทำการเลือกโพรโตคอลที่จะใช้ในการสำรวจสถานะของโฮสต์ เพื่อหาปริมาณของไอพีแอดเดรส โดยโพรโตคอลที่ผู้วิจัยเลือกใช้ในการสำรวจคือ ICMP และ TCP เพราะ ICMP สามารถตรวจสอบสถานะของโฮสต์ได้อย่างรวดเร็วและมีความถูกต้อง ส่วน TCP ใช้ในการสแกนพอร์ต เพื่อช่วยให้ได้รับข้อมูลในการสำรวจที่ถูกต้องแม่นยำมากขึ้น เนื่องจาก TCP สามารถตรวจพบบางไอพีแอดเดรสที่โฮสต์อยู่ในสถานะออนไลน์ แต่ไม่สามารถตรวจพบได้ด้วย ICMP เพราะไอพีแอดเดรสบางไอพีได้รับเลือกการ ping ไว้ แต่การสำรวจด้วย TCP ใช้เวลาในการสำรวจมากกว่าการใช้ ICMP จึงได้มีการเลือกสแกนพอร์ตเฉพาะพอร์ตที่มีการใช้งานค่อนข้างมาก ได้แก่ พอร์ต 21 (ftp) 22 (ssh) 80 (http) 443 (https) 3306 (MySQL) พอร์ต 445 (microsoft-ds) และ 139 (netbios) ซึ่งการสำรวจจะเน้นรูปแบบการสำรวจที่ต่อเนื่องไม่เินควาย และออกแบบไม่ให้เครื่องมือที่ตรวจสอบประเมินได้ว่าถูกโจมตี เพื่อให้สามารถสำรวจได้ข้อมูลที่ถูกต้อง

นอกจากนี้ผู้วิจัยเลือกเครื่องมือที่ใช้ในการสำรวจสถานะของโฮสต์คือโปรแกรม nmap [9] ซึ่งใช้สำหรับสแกนเครือข่าย ตรวจสอบสถานะของโฮสต์ และปริมาณไอพีแอดเดรส เพราะว่าเป็นโปรแกรมที่สามารถตรวจสอบสถานะของโฮสต์ได้หลายรูปแบบ สามารถระบุลักษณะของการสำรวจได้ตามต้องการ เช่น ชนิดของโพรโตคอลที่ใช้สำรวจ เทคนิคการสแกนค้นหาโฮสต์ ระบุพอร์ต การจัดการเกี่ยวกับเวลาที่ใช้ในการสำรวจ สามารถปรับ input ได้หลายรูปแบบ สามารถนำหลายตัวเลือก (option) มารวมกันภายในคำสั่งเดียวได้ และสามารถปรับระดับความเร็วให้เหมาะสมกับเครือข่ายที่ใช้งานได้อัตโนมัติ ในการ

เลือกตัวเลือก(option) ของโปรแกรม nmap ที่เหมาะสมสำหรับการสำรวจปริมาณไอพีแอดเดรสใช้ 3 คำสั่งคือ nmap -p -n [target] เป็นการส่ง ICMP ping เพื่อค้นหาโฮสต์ nmap -PA [portlist] -n [target] เป็นการส่ง TCP ACK เพื่อค้นหาโฮสต์ที่เปิดให้บริการในช่วงพอร์ตที่สนใจ โดยการทำงานของเครื่องต้นทางจะส่ง TCP ACK พร้อมพอร์ตที่ต้องการทราบการให้บริการไปยังเครื่องปลายทาง ถ้าเครื่องปลายทางเปิดอยู่ ก็จะส่ง RST packet กลับมา แต่ถ้าในกรณีที่ไม่มีการส่ง response คอยกลับมา แสดงว่าไอพีแอดเดรสปลายทางไม่ได้ใช้งาน หรือเครื่องปลายทางอยู่หลังไฟร์วอลล์ และ nmap -PS [portlist] -n [target] เป็นการส่ง TCP SYN เพื่อค้นหาโฮสต์ที่เปิดให้บริการในช่วงพอร์ตที่สนใจ โดยการทำงานของเครื่องต้นทางจะทำการส่ง SYN packet และพอร์ตที่ต้องการทราบการให้บริการไปยังเครื่องปลายทาง ถ้าเครื่องปลายทางเปิดอยู่ก็จะส่ง SYN / ACK คอยกลับมาจากนั้นเครื่องเครื่องต้นทางก็จะส่ง RST packet กลับไปยังเครื่องปลายทาง ในการทดลองได้เลือกพอร์ตที่ใช้ในการสำรวจคือ พอร์ต 21 (ftp) 22 (ssh) 80 (http) 443 (https) 3306 (MySQL) 445 (microsoft-ds) และ 139 (netbios) เพราะว่าสภาพแวดล้อมของมหาวิทยาลัยเกษตรศาสตร์การใช้งานเครือข่ายส่วนมากเป็นการใช้งานของนิสิต อาจารย์ พนักงานภายในมหาวิทยาลัย ดังนั้นการใช้งานจะเป็นการใช้งานเว็บไซต์ การส่งข้อมูลผ่านระบบเครือข่าย และระบบปฏิบัติการที่ใช้ส่วนมากจะเป็นระบบปฏิบัติการวินโดวส์

ในการสำรวจผู้วิจัยได้สำรวจไอพีแอดเดรสของ /24 บล็อกจำนวน 207 บล็อกที่ได้รับการจัดสรรให้กับหน่วยงานหรือองค์กรภายในมหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตบางเขน ซึ่งกำหนดระยะเวลาในการส่งการร้องขอ (request) โดยทำการสำรวจทุก ๆ 20 นาทีทำการ ping โดย ICMP เพื่อค้นหาสถานะของโฮสต์ และสแกนพอร์ตโดย TCP เพื่อค้นหาบางไอพีแอดเดรสที่บล็อกการ ping จากนั้นจึงเก็บข้อมูลที่ได้ออกจากการสำรวจโดยบันทึกลงใน log file และนำมาวิเคราะห์

2.2 การเก็บรวบรวมข้อมูล

การรวบรวมข้อมูลไอพีแอดเดรส ผู้วิจัยเขียนคำสั่ง (script) ที่ใช้สำหรับสำรวจสถานะของโฮสต์ภายในเครือข่ายเพื่อสำรวจปริมาณของไอพีแอดเดรสที่เป็นไปอย่างอัตโนมัติ ภายในคำสั่ง (script) จะมีองค์ประกอบในการแปลงข้อมูลของการสำรวจด้วย nmap ให้เป็นไฟล์ที่มียนามสกุล .txt เพื่อให้สามารถเข้าใจได้ง่าย และสะดวกต่อการรวบรวมข้อมูลหรือนำไปวิเคราะห์ จากนั้นรวบรวมผลการทดลองทั้งหมดที่สำรวจได้ นำมาหาจำนวนของไอพีแอดเดรสที่ตอบสนองต่อการสำรวจ และวิเคราะห์การใช้งานจริงของแต่ละไอพีแอดเดรสโดยใช้ตัววัดดังนี้ค่า Availability (A) ค่า Volatility (V) ค่า Uptime (U) ของแต่ละแอดเดรส

2.3 ตัววัดข้อมูล

ในการวิเคราะห์ข้อมูลที่ได้ออกจากการสำรวจ ผู้วิจัยจะวิเคราะห์รูปแบบการตอบกลับ (response) ซึ่งแบ่งออกเป็น 3 รูปแบบคือ Positive

response คือการมีโฮสต์อยู่จริงที่ไอพีแอดเรสนั้น, Negative respond คือ ไม่สามารถเข้าถึงโฮสต์ได้ (unreachable) หรือว่าไอพีแอดเรสไม่ได้ถูกใช้งาน และ No reply คือขาดการตอบรับ เนื่องจากข้อมูลถูกรองด้วยไฟร์วอลล์

ผู้วิจัยวิเคราะห์ข้อมูลของแต่ละไอพีแอดเรส เพื่อศึกษาลักษณะการใช้งานไอพีแอดเรส ซึ่งตัววัดที่ใช้วิเคราะห์ได้แก่ ค่า Availability หรือ A(address) เป็นผลรวมของระยะเวลาที่โฮสต์ตอบสนองต่อการสำรวจ (probe) ทั้งหมดหารด้วยเวลาที่สำรวจทั้งหมด คำนวณได้ดังสมการที่ (1) ค่า Volatility หรือ V(address) เป็นจำนวนครั้งที่โฮสต์ตอบสนองต่อการสำรวจ (probe) หารด้วยครั้งหนึ่งของจำนวนการสำรวจ (probe) คำนวณได้ดังสมการที่ (3) และ ค่า Uptime หรือ U(Address) เป็นระยะเวลาที่โฮสต์ตอบสนองอย่างต่อเนื่อง หารด้วยจำนวนครั้งที่โฮสต์ตอบสนองต่อการสำรวจ (probe) คำนวณได้ดังสมการที่ (4)

$$A(address) = \frac{1}{N_p} \left(\sum_{i=1}^N r_i \right) \quad (1)$$

โดยที่ N_p เป็นจำนวนครั้งของการสำรวจ (probe) ทั้งหมด
 r_i เป็น positive หรือ negative response ของแต่ละครั้งของการสำรวจ (probe) คำนวณได้ดังสมการที่ (2)

$$r_i(address) = 1 \text{ or } 0, \forall i \in [1, N_p] \quad (2)$$

$$V(address) = \frac{N_u}{N_p / 2} \quad (3)$$

โดยที่ N_u เป็นจำนวนครั้งของการที่โฮสต์ตอบสนองต่อการสำรวจ (probe)

$$U(address) = \frac{A(address)}{N_u} \quad (4)$$

หลังจากที่วิเคราะห์ข้อมูล ผู้วิจัยนำค่า Availability (A) ค่า Volatility (V) และค่า Uptime (U) ของแต่ละแอดเรส มาทำการประเมินลักษณะการใช้งานของไอพีแอดเรส ซึ่งจาก Xue Cai และคณะ [5] มีการกำหนดขอบเขตของแต่ละค่าสำหรับใช้ประเมินลักษณะการใช้งาน ซึ่งผู้วิจัยได้นำขอบเขตดังกล่าวมาใช้ และปรับค่าขอบเขตของค่า Volatility และ Uptime ให้เหมาะสมกับสภาพแวดล้อมในการสำรวจ ทำให้ได้ค่าดังต่อไปนี้ $A_u = 0.95$ สำหรับค่า Availability สูง คือ ไอพีแอดเรสมีสภาพการใช้งานอย่างมาก $A_u = 0.10$ สำหรับค่า Availability ต่ำ คือ ไอพีแอดเรสมีสภาพการใช้งานน้อย $V = 0.004$ สำหรับค่า Volatility ต่ำ คือ ไอพีแอดเรสมีการเปลี่ยนแปลงสถานะ (up หรือ down)

ไม่บ่อย และ $U = 0.026$ สำหรับค่า Uptime ต่ำ คือ ไอพีแอดเรสมีการใช้งานไม่ค่อยเนื่อง นอกจากนี้ Xue Cai และคณะ [7] ได้แบ่งลักษณะการใช้งานไอพีแอดเรส ออกเป็น 5 กลุ่ม พร้อมเงื่อนไขที่จะใช้ในการประเมินลักษณะการใช้งานของไอพีแอดเรส ดังนี้ Always - stable มีการใช้งานอย่างต่อเนื่อง ซึ่งเป็นกลุ่มของเครื่องแม่ข่าย (server) ค่า Sometimes - stable มีการใช้งานอย่างต่อเนื่องในบางครั้ง Intermittent มีการใช้งานอย่างสม่ำเสมอ Underutilized มีการใช้งานไม่เต็มประสิทธิภาพ และ Unclassifiable ไม่สามารถจำแนกลักษณะการใช้งานได้ ซึ่งแต่ละกลุ่มมีเงื่อนไขดังต่อไปนี้

Always - stable: $A \geq 0.95$ และ $V < 0.004$ หรือ $U \geq 0.95$

Sometimes - stable: $U > 0.026$ และ $A \geq 0.95$ และ

$A < 0.95$ หรือ $V > 0.004$

Intermittent: $U < 0.026$ และ $A \geq 0.95$ และ $A < 0.95$ หรือ $V > 0.004$

Underutilized: $A < 0.10$

Unclassifiable: $A = 0.00$ และ $U = 0.00$

3. ผลการดำเนินงาน

ในการสำรวจปริมาณไอพีแอดเรสที่ใช้งานจริงภายในมหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตบางเขน ได้ทำการสำรวจไอพีแอดเรสของ /24 บล็อก จำนวน 207 บล็อก โดยการสำรวจได้เลือกสำรวจเฉพาะบล็อกที่มีการจัดสรรให้กับหน่วยงานหรือองค์กรภายในมหาวิทยาลัย โดยสำรวจที่พอร์ต 21 (ftp) 22 (ssh) 80 (http) 443 (https) 3306 (MySQL) 445 (microsoft-ds) และ 139 (netbios) โดยทดลองสำรวจปริมาณไอพีแอดเรส ใช้เวลาสำรวจ 7 วัน ตั้งแต่วันที่ 29 เมษายน พ.ศ. 2552 เวลา 13:20 น. ถึงวันที่ 6 พฤษภาคม พ.ศ. 2552 เวลา 15:20 น. มีการสำรวจเกิดขึ้นทั้งหมด 511 ครั้ง สำรวจทุก 20 นาที คิดตั้งคำสั่ง (script) ไว้ในเครื่องคอมพิวเตอร์จำนวน 3 เครื่องภายในภาควิชาวิทยาการคอมพิวเตอร์มหาวิทยาลัยเกษตรศาสตร์ ซึ่งแต่ละเครื่องคิดตั้งคำสั่งที่แตกต่างกันไว้เครื่องละ 1 คำสั่ง และทำการสำรวจที่เวลาเดียวกัน โดยมีผลการสำรวจดังต่อไปนี้

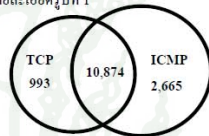
ตารางที่ 1: การเปรียบเทียบปริมาณไอพีแอดเรสโดยใช้ ICMP

โพรโตคอล และ TCP โพรโตคอล

ประเภท	จำนวนไอพีแอดเรส	%
ไอพีแอดเรสที่ใช้สำรวจ	52,992	
ไอพีแอดเรสที่ไม่ตอบสนอง	38,460	
ไอพีแอดเรสที่ตอบสนอง	14,532	100.00
ไอพีแอดเรสที่ตอบสนองต่อ ICMP	13,539	93.2
ไอพีแอดเรสที่ตอบสนองต่อ TCP	11,867	81.7

ไอพีแอดเรสที่ตอบสนองต่อทั้ง ICMP และ TCP	10,874	74.8
ไอพีแอดเรสที่ตอบสนองต่อ ICMP อย่างเดียว	2,665	18.3
ไอพีแอดเรสที่ตอบสนองต่อ TCP อย่างเดียว	993	6.8
ไอพีแอดเรสที่ตอบสนองต่อทั้ง TCP-SYN และ TCP - ACK	10557	
ไอพีแอดเรสที่ตอบสนองต่อ TCP-SYN	1096	
ไอพีแอดเรสที่ตอบสนองต่อ TCP - ACK	214	

จากตารางที่ 1 เปรียบเทียบปริมาณของไอพีแอดเรสที่พบจากการสำรวจในแต่ละวิธีการทั้งการตรวจสอบด้วย ICMP และการตรวจสอบด้วย TCP จากการทดลองทำการสำรวจปริมาณไอพีแอดเรสพบว่า จำนวนไอพีแอดเรสที่ตอบสนองต่อการสำรวจด้วย ICMP โปรโตคอลมีจำนวนมากกว่าจำนวนไอพีแอดเรสที่ตอบสนองต่อการสำรวจด้วย TCP โปรโตคอล ดังรายละเอียดรูปที่ 1



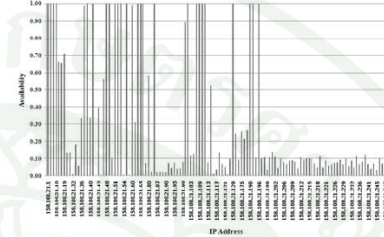
รูปที่ 1: ผลการสำรวจปริมาณไอพีแอดเรสที่สำรวจด้วย ICMP และ TCP โปรโตคอล

จากรูปที่ 1 การทดลองสำรวจปริมาณไอพีแอดเรสที่ใช้งานพบว่าจำนวนไอพีแอดเรสที่ตอบสนองต่อการสำรวจทั้ง ICMP โปรโตคอลและ TCP โปรโตคอลมีจำนวน 10,874 ไอพีแอดเรส คิดเป็น 74.8% จำนวนไอพีแอดเรสที่ตอบสนองต่อ ICMP โปรโตคอลแต่ไม่ตอบสนองต่อ TCP โปรโตคอลจำนวน 2,665 ไอพีแอดเรสคิดเป็น 18.3% และจำนวนไอพีแอดเรสที่ตอบสนองต่อ TCP โปรโตคอลแต่ไม่ตอบสนองต่อ ICMP โปรโตคอลจำนวน 993 ไอพีแอดเรสคิดเป็น 6.8%

จากการสำรวจพอร์ต 21 (ftp) 22 (ssh) 80 (http) 443 (https) 3306 (MySQL) 445 (microsoft-ds) และ 139 (netbios) พบว่าภายในมหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตบางเขนมีการใช้งานพอร์ตที่สำรวจดังนี้พอร์ต 21 (ftp) คิดเป็น 10.05% 22(ssh) คิดเป็น 10.78% 80(http) คิดเป็น 35.85% 443(https) คิดเป็น 22.28% 3306(MySQL) คิดเป็น 76.12% 445 (microsoft-ds) คิดเป็น 4.24% และ 139 (netbios) คิดเป็น 2.28%

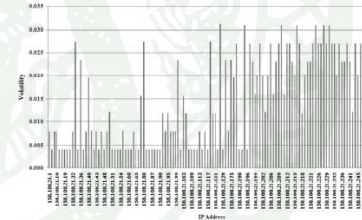
จากผลการสำรวจปริมาณไอพีแอดเรสที่มีการใช้งานได้นำเอาผลการสำรวจมาประเมินลักษณะของแต่ละไอพีแอดเรสจากการหาค่า Availability ค่า Volatility และค่า Uptime ของแต่ละแอดเรส โดยได้นำค่า Availability ค่า Volatility และค่า Uptime ของแต่ละแอดเรสในบล็อก 158.108.21.0/24 ซึ่งเป็นบล็อกของภาควิชาวิทยาการ

คอมพิวเตอร์มาเป็นตัวอย่างในการประเมินลักษณะไอพีแอดเรส ผลการประเมินมีดังต่อไปนี้



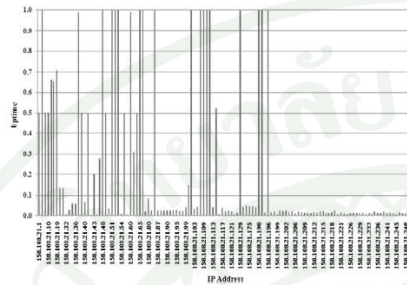
รูปที่ 2: แผนภาพค่า Availability ของแต่ละไอพีแอดเรสภายในภาควิชาวิทยาการคอมพิวเตอร์

จากรูปที่ 2 จะเห็นได้ว่าไอพีแอดเรสจะมี Availability อยู่ในช่วง 0.1 – 0.95 คิดเป็น 29.27% บอกได้ว่าไอพีแอดเรสกลุ่มดังกล่าวมีการใช้งานระดับปานกลางไอพีแอดเรสจำนวนหนึ่งที่มีค่า Availability มากกว่า 0.95 หมายความว่าไอพีแอดเรสกลุ่มนี้มีการใช้งานอย่างมาก คิดเป็น 22.76% เป็นกลุ่มของเครื่องแม่ข่าย และกลุ่มไอพีแอดเรสที่มีค่า Availability อยู่ใกล้เคียง 0 แสดงว่าไอพีแอดเรสกลุ่มนี้มีการใช้งานค่อนข้างน้อย คิดเป็น 47.97%



รูปที่ 3: แผนภาพค่า Volatility ของแต่ละไอพีแอดเรสภายในภาควิชาวิทยาการคอมพิวเตอร์

จากรูปที่ 3 จะเห็นได้ว่าไอพีแอดเรสในภาควิชาวิทยาการคอมพิวเตอร์จะมี Volatility อยู่ในช่วง 0.004 – 0.02 คิดเป็น 33.33% Volatility มากกว่า 0.02 บอกได้ว่าไอพีแอดเรสกลุ่มดังกล่าวมีการใช้งานน้อย หรือไม่ได้ถูกใช้งาน คิดเป็น 34.15% และมีไอพีแอดเรสจำนวนหนึ่งที่มีค่า Volatility เป็น 0.004 หมายความว่าไอพีแอดเรสกลุ่มนี้มีการใช้งานสูงมาก คิดเป็น 32.52% ซึ่งเป็นกลุ่มของเครื่องแม่ข่าย



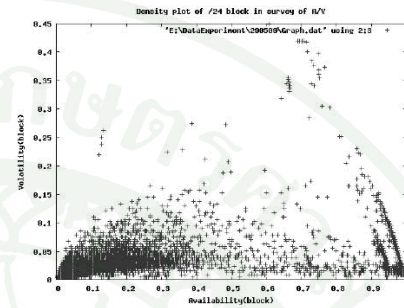
รูปที่ 4: แผนภาพค่า Uptime ของแต่ละไอพีแอดเดรสภายในภาควิชาวิทยาการคอมพิวเตอร์

จากรูปที่ 4 จะเห็นว่าไอพีแอดเดรสในภาควิชาวิทยาการคอมพิวเตอร์จะมี Uptime อยู่ในช่วง 0.026 – 0.95 คิดเป็น 27.64% บอกได้ว่าไอพีแอดเดรสกลุ่มดังกล่าวไม่ได้ทำงานตลอดเวลา ไอพีแอดเดรสที่มีค่าใกล้ถึง 0 คิดเป็น 41.46% และมีไอพีแอดเดรสจำนวนหนึ่งที่มีค่า Uptime มากกว่า 0.95 คิดเป็น 30.89% หมายความว่าไอพีแอดเดรสมีการใช้งานอยู่ตลอดเวลา ซึ่งตรงกับกลุ่มของเครื่องแม่ข่าย

ตารางที่ 2 จำนวนไอพีแอดเดรสในภาควิชาวิทยาการคอมพิวเตอร์แต่ละลักษณะการใช้งาน

ประเภท	จำนวนไอพีแอดเดรส
Always – stable	20
Sometimes – stable	29
Intermittent	14
Underutilized	59
Unclassifiable	134

จากตารางที่ 2 พบว่าไอพีแอดเดรสบล็อก 158.108.21.0/24 ของภาควิชาวิทยาการคอมพิวเตอร์มีลักษณะการใช้งานอยู่ในกลุ่ม Unclassifiable เป็นไอพีแอดเดรสที่ยังไม่มีการใช้งาน แสดงให้เห็นว่าไอพีแอดเดรสภายในภาควิชาวิทยาการคอมพิวเตอร์สามารถนำมาใช้งานได้ก็จะเป็นจำนวนมาก เพราะลักษณะการใช้งานจะเป็นการใช้งานแบบไม่ต่อเนื่อง ซึ่งทำให้ไอพีแอดเดรสยังถูกใช้งานไม่เต็มประสิทธิภาพ นอกจากนี้ได้ทำการประเมินภาพรวมลักษณะการใช้งานของไอพีแอดเดรสทั้งหมดที่ได้จากการสำรวจโดยพล็อต (A, V) เป็นแผนภาพการกระจายตัวของไอพีแอดเดรสภายในมหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตบางเขน



รูปที่ 5: การกระจายตัวของไอพีแอดเดรส

จากรูปที่ 5 การกระจายตัวของไอพีแอดเดรสโดยการพล็อต (A, V) เพื่อแสดงความเกี่ยวข้องของค่า Availability และ ค่า Volatility ในการจัดกลุ่มลักษณะการใช้งานของไอพีแอดเดรสโดยที่ (A,V) = (0.95,0.005) แสดงว่ามี Availability สูงและมีการใช้งานอย่างสม่ำเสมอ จัดอยู่ในกลุ่ม Always – stable คิดเป็น 0.7% โดยเครื่องคอมพิวเตอร์กลุ่มนี้จะเป็นเครื่องแม่ข่าย (server) (A,V) = (0.05,0.005) แสดงว่ามีการใช้งานในกลุ่ม Underutilized คิดเป็น 14.32% รวมทั้งการกระจายตัวของ (A, V) = (0.1-0.4,0.045 – 0.01) แสดงว่ามีการใช้งานอยู่ในกลุ่มของ Sometimes – stable คิดเป็น 8.86% Intermittent คิดเป็น 4.04% และ Unclassifiable คิดเป็น 72.85%

ในการทดลองสำรวจไอพีแอดเดรสที่มีการใช้งานในครั้งนี้เป็น การทดลองในมหาวิทยาลัยเกษตรศาสตร์จึงไม่ได้รับผลกระทบจากการถูกกรองด้วยไฟร์วอลล์ ทำให้ผลการทดลองมีความถูกต้องเชื่อถือได้ แต่ในการทดลองสำรวจพอร์ตยังไม่สามารถครอบคลุมการใช้งานทุกประเภท และระบบปฏิบัติการ จึงต้องมีการทำการสำรวจพอร์ตเพิ่มเติม เช่น พอร์ต 1433 (ms – sql – s) พอร์ต 1434 (ms – sql – m)

4. สรุป

งานวิจัยนี้เป็นการศึกษาการใช้งานจริงของไอพีแอดเดรสที่มีการจัดสรรภายในมหาวิทยาลัยเกษตรศาสตร์ได้ทำการสำรวจไอพีแอดเดรสของ /24 บล็อก จำนวน 207 บล็อก โดยการสำรวจได้เลือกสำรวจเฉพาะบล็อกที่มีการจัดสรรให้กับหน่วยงานหรือองค์กรภายในมหาวิทยาลัย ซึ่งใช้ ICMP และ TCP ที่พอร์ต 21 (ftp) 22 (ssh) 80 (http) 443 (https) 3306 (MySQL) 445 (microsoft-ds) และ 139 (netbios) ผลการทดลองที่ได้จากการสำรวจพบว่าไอพีแอดเดรสที่สำรวจพบว่ามีการใช้งานประมาณ 27.42% โดยการสำรวจด้วย ICMP สำรวจพบจำนวนไอพีแอดเดรสที่มีการใช้งานมากกว่าการสำรวจด้วย TCP และไอพีแอดเดรสส่วนใหญ่จะอยู่ในกลุ่ม Underutilized และ Unclassifiable เป็นไอพีแอดเดรสที่ยังไม่มีการใช้งาน และลักษณะการใช้งานแบบไม่ต่อเนื่อง ซึ่งเป็นการใช้งานไอ

ที่แอตแตรสไม่เต็มประสิทธิภาพแสดงให้เห็นว่าไอพีแอตแตรสภายในมหาวิทยาลัยเกษตรศาสตร์สามารถนำมาใช้งานได้อีกเป็นจำนวนมาก เพราะลักษณะการใช้งานจะเป็นการใช้งานแบบไม่ต่อเนื่อง ซึ่งทำให้ไอพีแอตแตรสยังถูกใช้งานไม่เต็มประสิทธิภาพ ในการทดลองครั้งต่อไปจะสำรวจบล็อกที่ขนาดแตกต่างกัน และสำรวจพอร์ตที่มีความหลากหลายมากขึ้น รวมทั้งต้องมีการทดลองซ้ำ เพื่อได้ข้อมูลที่ถูกต้อง สามารถนำมาแยกประเภทการใช้งาน เช่น การใช้งานเว็บไซต์ การใช้งานเป็นเครื่องแม่ข่าย เป็นต้น

5. กิตติกรรมประกาศ

ขอขอบพระคุณโครงการทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย หรือทุน TGIST ที่ให้ทุนการศึกษานับสนุนการเรียนในระดับบัณฑิตศึกษา

เอกสารอ้างอิง

- [1] B. Huffaker, D. Plummer, D. Moore, and K. C. Claffy. Topology Discovery by Active Probing. In *Proc. Of the Symposium on Applications and the Internet*, Jan. 2002.
- [2] X. Meng, Z. Xu, S. Lu, and L. Zhang. IPv4 Address Allocation and the BGP Routing Table Evolution. Technical Report 030046, CS Department, UCLA, 2002.
- [3] W. Mühlbauer, O. Maennel, S. Uhlig, A. Feldmann, and M. Roughan. Building an AS-topology model that captures route diversity. In *Proc. of the ACM SIGCOMM Conference*, pages 195–204, Sept. 2006.
- [4] X. Dimitropoulos, D. Krioukov, M. Fomenkov, B. Huffaker, Y. Hyun, K. C. Claffy, and G. Riley. AS relationships: Inference and validation. *ACM Computer Communication Review*, 37(1):29–40, Jan. 2007.
- [5] Genevieve Bartlett, John Heidemann and Christos Papadopoulos. Understanding Passive and Active Service Discovery (Extended). USC/ISI Technical Report ISI-TR-642, USC/Information Sciences Institute, May 2007.
- [6] John Heidemann, Yuri Pradkin, Ramesh Govindan, Christos Papadopoulos, Genevieve Bartlett and Joseph Bannister. Census and Survey of the Visible Internet. In *Proceeding of LMC'08, October 20 – 22, 2008, Vouliagmeni, Greece*. 2008.
- [7] Xue Cai and John Heidemann. Understanding Address Usage in the Visible Internet. USC/ISI Technical Report ISI-TR-656, USC/Information Sciences Institute, February 2009.
- [8] ANT Censuses of the Internet Address Space project. Web page <http://www.isi.edu/ant/address/>, June 2009.
- [9] Nmap. Web page <http://nmap.org/>, June 2009.

ประวัติผู้เขียนบทความ



มหาวิทยาลัยเกษตรศาสตร์

นางสาวแสงดาว พรทวีโชคสกุล
สำเร็จการศึกษาระดับปริญญาตรีจากสำนักวิชา
เทคโนโลยีสารสนเทศ สาขาวิชาวิทยาการ
คอมพิวเตอร์ มหาวิทยาลัยแม่ฟ้าหลวง
ขณะนี้กำลังศึกษาคณะระดับปริญญาโทที่ภาควิชา
วิทยาการคอมพิวเตอร์



งานวิจัยที่สนใจ ได้แก่

ผศ. ดร. ศุภมาล กิตติน
การศึกษา Ph.D. (Computer Science), University
of Southern California
ปัจจุบัน ผู้ช่วยศาสตราจารย์ / อาจารย์ประจำ
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์
มหาวิทยาลัยเกษตรศาสตร์



งานวิจัยที่สนใจ ได้แก่ Survivable and fault-tolerant networks, network
measurement, traffic classification, IPv6, mobile IP, intelligent transport
system

Distributed Systems, E-commerce, Computer
Networks, Recommender Systems

ดร.พินิตา พงษ์ไพบูลย์
การศึกษา Ph.D. in Electrical and Computer
Engineering, Carnegie Mellon University
ปัจจุบัน นักวิจัย หน่วยงานปฏิบัติการวิจัยเทคโนโลยี

A Study of IP Address Usage with Active and Passive Probing within Kasetsart University

Sangdao Prontaweechoksakul, Sukumal Kitisin and Panita Pongpaibool
Computer Science Department, Faculty of Science, Kasetsart University
Bangkok, 10903, Thailand

Email: g5064183@ku.ac.th, sukumal.I@ku.ac.th

National Electronics and Computer Technology Center (NECTEC)

112 Phahonyothin Road, Klong Neung, Klong Luang District, Pathumthani, 12120, Thailand

E-mail: panita@nectec.or.th

Abstract

This paper is a study on IP address allocation utilization at Kasetsart University. Referenced the previous study of Visible Internet by Heidemann, et al., we did a few experiments in order to understand IP addresses usage characteristics within the university. Kasetsart University was assigned a class B block address -- 158.108.0.0/16 for its domain. The university consists of five campuses throughout Thailand. Many campus computers are using private address behind firewalls. We have studied /24 blocks which are allocated to departments or organizations of the university. We used both active and passive probing where active probing can find all service currently on the network, except service temporarily unavailable or hidden by firewalls. Passive monitoring though can find transient service but miss services that are idle at the probing moment. We used Internet Control Message Protocol (ICMP) and Transmission Control Protocol (TCP) on various ports. The experimental results show that only 49.80% of allocated IP addresses are used and to find IP addresses, using TCP is more visible than using ICMP. We also analyzed the address characteristics, such as, availability, volatility, and uptime. The evaluations show that, IP addresses as the following characteristics: 3.95 % is always stable; 11.70 % is sometimes stable; 16.49 % is intermittent; 19.32% is underutilized; and finally 48.54 % is unclassifiable.

Keywords: Internet addresses allocation, IPv4, Survey, Measurement.

1. Introduction

Previous survey of visible IP addresses had studied on topological data structure and round trip time (RTT) measurements[1]. The result showed that the measured round trip time and structure were

correlated. There were a few topological studies focused on Autonomous System (AS) and router topology[2,3,4]. While these work explored population of edge host and the usage of IPv4 address space. Today, survey visible IP address studied the usage of IP addresses by using ICMP and TCP probing method [5,6,8] which the present two principles as census and survey that is a difference traditional survey in order to decrease the deviation of measured data. But the problem of the census survey is that it uses longer time to explore all IP addresses and the survey gathered more variant data because the approach uses the more frequent probes. The research is to study the IP addresses allocation utilization within Kasetsart University.

Our experiment use ICMP and TCP for probing /24 block IP addresses on the following ports: port 21 (ftp) 22 (ssh) 25(smtp) 53 (domain) 80 (http) 110 (pop3) 135 (epmap) 137 (netbios) 139 (netbios) 225 (smtp) 443 (https) 445 (microsoft-ds) 458 (appleqtcp) 587 (submission) 1433(ms-sql-s) 1434(ms-sql-m) 1863 (msnp) 1214 (kazaa) 3306 (mysql) 5000 (complex-main) 5001 (complex-link) 5010 (telepathstart) 5190 (aol) 6346(gnutella) 6881 (bittorrent) 6699 (napster) 6969 (acmsoda) 8007 8009 11999 27015 and 30010 within University. Then we analyze explored data and the IP address usage characteristics within the university to understand the utilization of the allocation by the office of computer service.

2. Overview of discovery techniques

In this section, we describe how the active and passive probing are used to discover services.

Active probing can find services by sending packets to each host and see the response from the running host. The result may be effected by the firewall or the host counter-measure setting. Hosts, which are on, are scanned by probing all target

ports on local area network. Host discovery probe can check status of host and skip the unused addresses.

Passive probing find host services by observing traffic passes at an observation point. TCP traffic can be monitored and detected with passive probing. It needs to capture TCP connection to send the messages, which have been set SYN bit. If the positive response, it has been set SYN-ACK bit for TCP service.

3. Methodology

This section introduces methodology in order to survey IP address usage. We collected raw data to analyze usage characteristics and classification.

3.1 Methodology for Active Probing

Our active probing is to scan all hosts within Kasetsart University which we have select protocol for probing as ICMP and TCP because ICMP can monitor the status of the host quickly and accurately and TCP is used for the port scan. TCP probe is used for repetitively explore services on hosts for accuracy check because some hosts block Ping command of ICMP but it required longer probing time than ICMP probe. Next, we selected a tool -- Nmap (Network Mapper) [9] for probing. Nmap is a program which can check for host status by scanning IP address for specified ports, which means the application or services running on the hosts, the operating system or firewall report. It can check host status in many format. The Nmap options used in our experiment for quickly scanned all allocated IP address blocks are--sP -n [target] where it sends ICMP ping to a target host for checking host status. It is send ICMP echo request to each address and waits for ICMP response. The Nmap -PA [portlist] -n [target] option is for sending TCP-ACK to find host that open an interested port. The operation will send an ACK packet and port numbers from source to destination. If destination host has the ports opened, it will return the RST packets to source. And nmap -PS [portlist] -n [target] option is to send TCP-SYN as same as TCP - ACK. The SYN packet will be sen to destination at the specified port. If the destination host has the port opened that it will send a SYN/ACK response and source will response with a RST packet.

Our experiment selects to following ports for the study: 21 (ftp), 22 (ssh), 25(smtp), 53 (domain), 80 (http), 110 (pop3), 135 (epmap), 137 (netbios), 139 (netbios), 225 (smtp), 443 (https), 445 (microsoft-ds), 458 (appleqt), 587 (submission), 1433 (ms-sql-s), 1434 (ms-sql-m), 1863 (msnp), 1214 (kazaa), 3306

(mysql), 5000 (complex-main), 5001 (complex-link), 5010 (telepathstart), 5190 (aol/icq), 6346(gnutella), 6881 (bittorrent), 6699 (napster), 6969 (acmsoda), 8007, 8009, 11999(sctp), 27015, and 30010 because those ports are popular in our university environment.

3.2 Methodology for Passive Probing

Our passive probing is to collect the data from all hosts within Kasetsart University. We used sniffer tool (Wireshark) to sniff the traffic and collect all TCP SYN and SYN-ACK packets in the network. To discover a service, any host sends SYN-ACK packet on specified ports thus runs the service.

3.3 Data Collection

We collect survey data by writing a script and setting it up as a crontab job on Linux machine for checking the host status. For setting the crontab job, we run the script every 20 minute for 3 – 5 hours to do the same probing on all address. When we found online host the script then write visible IP address to the log file for further analysis. Analyzing survey data, we count the number of responding addresses and evaluate the usage characteristics such as Availability (A) Volatility (V) and Uptime (U) of each address.

Table 1. Summary of survey

Name	Start Date	Active Duration (Days)	Prefix length probe	Active Seans
KU24 ₁	2009-02-03	3	/24	20 minute
KU24 ₂	2009-02-05	5	/24	20 minute
KU24 ₃	2009-04-29	7	/24	20 minute
KU24 ₄	2009-06-16	7	/24	3 hour
KU24 ₅	2009-08-11	7	/24	5 hour

Table 1 shows the survey done in our experiment. We used all data from the surveys for further analysis and evaluate usage characteristic of IP addresses. The active probing is explored by ICMP and TCP.

3.4 Metrics

In analysis survey data, we will analyze pattern of responses which is divided into 3 types as the Positive, Negative and No-reply response. Positive response means the presence of a host at that address. Negative response means that the host is either down or the address is unused and No reply is because the

address may not be occupied or filtered by a firewall.

We analyzed each address in order to evaluate character of visible IP addresses by applying a few statistic metrics that characterize address usage. The three metrics are Availability (A) which is the fraction of time a host is reachable. Volatility (V) is a normalized representation of how many consecutive periods the address is responsive. And the Uptime (U) is the mean interval time that host have continuous positive response. In addition, there are notions of Availability or A(block), Volatility or V(block) and Uptime or U (block) where block is the block address or the subnet and Median (A(address), V(address) and U (address)) of all positive response addresses within the address block

$$A(\text{address}) = \frac{1}{N_p} \left(\sum_{i=1}^{N_p} r_i \right) \quad (1)$$

Let, N_p is the number of all probes

r_i is positive or negative response of each probe

$$r_i(\text{address}) = 1 \text{ or } 0, \forall i \in [1, N_p] \quad (2)$$

$$V(\text{address}) = \frac{N_u}{N_p/2} \quad (3)$$

Let N_u is the number of hosts responding to probe

$$U(\text{address}) = \frac{A(\text{address})}{N_u} \quad (4)$$

Each metrics has a purpose as Availability shows how effectively address is used. High volatility indicates address that is only intermittently used and often dynamically allocated. Uptime suggests how long an address is used.

3.5 Classification

The Availability (A), Volatility (V), and Uptime (U) of each address can be classified into categories. Four thresholds are used as $A_H = 0.95$ indicates high availability, $A_L = 0.10$ indicates low availability, $V = 0.004$ is for low volatility, and $U = 0.048$ is for low uptime. Hence, the five categories can be classified as follow.

Always - stable: high available and stable

$$(A \geq 0.95 \text{ or } U \geq 0.95) \text{ and } (V < 0.004)$$

Sometimes – stable: changing more often than always-stable, but frequently up continuously for long time

$$(U \geq 0.048) \text{ and } (A \geq 0.1) \text{ and}$$

$$(A < 0.95 \text{ or } V > 0.004)$$

Intermittent: individual addresses are up for shot time

$$(U < 0.048) \text{ and } (A > 0.1) \text{ and}$$

$$(A < 0.95 \text{ or } V > 0.004)$$

Underutilized: addresses are sometime used

$$(A < 0.10) \text{ and } (A > 0.00)$$

Unclassifiable: addresses are few response and not response

$$(A=0.00) \text{ and } (V=0.00) \text{ and } (U=0.00)$$

4. Evaluation

The survey visible IP addresses within Kasetsart University by exploring all IP addresses. We compared the results obtained by Active and passive probing within seven days. Active probing experiments used Internet Control Message Protocol (ICMP) and Transmission Control Protocol (TCP) on various ports.

Table 2. Number of IP Addresses

Category	Number of IP Address	%
Address probed	65,536	100.00 %
non-response	32,896	50.20%
response either	32,640	49.80%

Table 2 is the number of IP Address that using in university by exploration all addresses. We can divide into two groups as response address and non response address. The number of response address is 49.80% and non response address is 50.20%.

4.1 Survey IP address

We were survey by active probing within seven days of all 65,536 addresses. A form of Active probing by Nmap is 2 forms (ICMP and TCP probing).

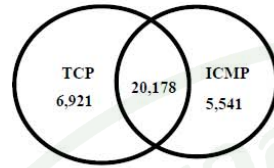


Figure 1. Number of IP addresses of Active probing

From our experiment results, TCP probing can explore visible IP address more than ICMP probing because the experiment got an affect from system block ICMP probing. Thus TCP probing is efficiency more than ICMP probing for our survey.

Table 3. ICMP – TCP comparison of quantifies IP addresses

Category	Number of IP Address	%
response either	32,640	100.00
ICMP	25,719	78.79
TCP	27,099	83.02
both ICMP and TCP	20,178	61.82
ICMP only	5,541	16.98
TCP only	6,921	21.20
both TCP-SYN and TCP - ACK	18,004	
TCP-SYN only	7,929	
TCP – ACK only	1,166	

Table 3 is number of IP addresses which shows the number of online hosts found in both type of probing (ICMP and TCP probing). Among all 65,536 addresses, 32,640 addresses responded to the active probing. In figure 1 show the number of IP addresses with ICMP and TCP probing by both ICMP and TCP probing found 20,178 online host addresses but only ICMP probing found 5,541 online host addresses and using only TCP probing found 6,921 online host addresses. Moreover, with two forms of TCP probing as TCP-SYN and TCP-ACK, probing using both TCP-SYN and TCP-ACK, 18,004 online host addresses were found, using only TCP-SYN 7,929 online host addresses were found, and using only TCP-ACK 1,166

online host addresses were found as seen in Figure 2.

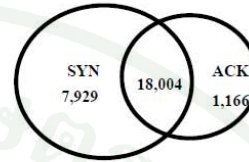


Figure 2. Number of IP addresses of TCP probing

We compare active probing and passive monitoring on seven days of all IP addresses allocated to the Computer Department which are 158.108.21.0/24 and 158.108.21.0/24. With both active and passive monitoring to observe all network traffic between our target network and its sources, the result can be seen in figure 3.

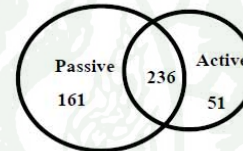


Figure 3. Number of IP addresses of Active and Passive

The number of IP Address that using in Computer Department by any method (union of active and passive methods) and any form of active probing. The experiment results as all 512 addresses have IP address those response 448 addresses. By Active probing (ICMP and TCP probing) found online host about 64.04% and passive probing found online host about 88.62%. And the observation of the IP address usage can be seen in table 5.

Table 5. Categorization from observations of IP address

Passive	Active	Categorization	Address count
Yes	Yes	Active server address	236
no	yes	idel server address	51
yes	no	firewalled address or birth	161
no	no	non - server address	64

4.2 Discovery of all service

We consider 32 service: 21 (ftp) 22 (ssh) 25(smtp) 53 (domain) 80 (http) 110 (pop3) 135 (epmap) 137 (netbios) 139 (netbios) 225 (smtp)

443 (https) 445 (microsoft-ds) 458 (appleqt) 587 (submission) 1433 (ms-sql-s) 1434 (ms-sql-m) 1863 (msnp) 1214 (kazaa) 3306 (mysql) 5000 (complex-main) 5001 (complex-link) 5010 (telepathstart) 5190 (aol) 6346(gnutella) 6881 (bittorrent) 6699 (napster) 6969 (acmsoda) 8007 8009 11999 27015 and 30010 of active probing. The result shows in figure 4.

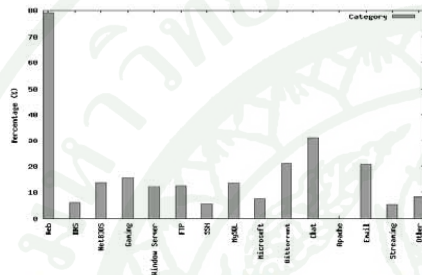


Figure 4. Number of service by Active Probing

4.3 Address characteristics

We take survey result of /24 blocks for classifying 5 categories by using Availability (A), Volatility (V), and Uptime (U) of each address.

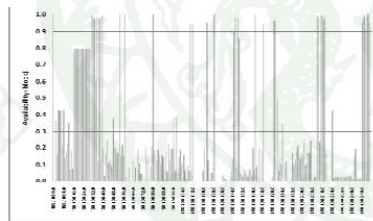


Figure 5. Availability of each address

Figure 5 shows Availability of each addresses in Kasetsart University. 19.14% of all addresses is availability as 0.75 – 1.00 that IP addresses are high available and stable because most IP address allocated to computer department. 0.78 % of all address have availability as 0.501 – 0.75, 4.69 % of all address availability as 0.261 – 0.50, 56.25% of all addresses have availability as 0.001 – 0.25 and 19.14 % availability as 0.00 that IP addresses not used.

Figure 6 shows Volatility of each addresses within Kasetsart University which 1.95 % of all addresses have volatility as 0.053 – 0.070 that IP

addresses are sometimes online host. 3.13 % of all address have volatility as 0.036 – 0.052, that IP addresses are online host in shot time and often offline. 32.42 % of all address volatility as 0.018 – 0.035 that IP addresses are online host in long time. 43.36 % of all addresses have volatility as 0.001 – 0.017 and 19.14 % volatility as 0.00 that IP addresses not used.

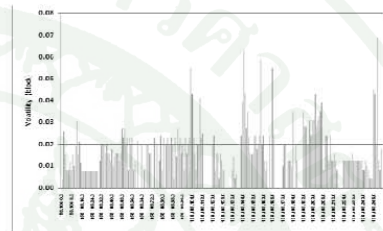


Figure 6. Volatility of each address

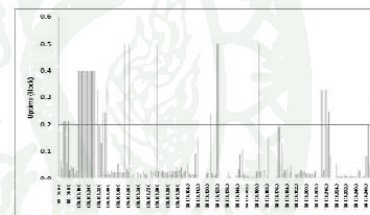


Figure 7. Uptime of each address

Figure 7 shows Uptime of each addresses in Kasetsart University. 8.20 % of all addresses is uptime as 0.371 – 0.50 that IP addresses are always uptime and 3.91 % of all address have uptime as 0.241 – 0.36 that IP addresses are uptime in long time but not always uptime. 6.25 % of all address uptime as 0.121 – 0.24 that IP addresses are uptime in shot time but often used. 62.50% of all addresses have uptime as 0.001 – 0.120 that IP addresses are not stabled uptime and 19.14 % uptime as 0.00 that IP addresses not used.

Table 6. /24 addresses in categories

Category	Number of IP address
Always – stable	5.86 %
Sometimes – stable	41.41%
Intermittent	5.86 %
Underutilized	27.73 %
Unclassifiable	19.14 %

Table 6 show /24 blocks addresses of Kasetsart University that we can classify categories of most IP addresses as Sometimes-stable which it's frequently up continuously for long time. In addition, we plotted density of /24 blocks in A/V plane of all address in Kasetsart University.

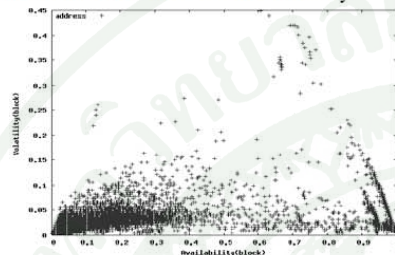


Figure 8. Density plot of /24 block in survey of A/V

Figure 8 is density of IP address in (A, V) plot to present related between Availability and Volatility. (A, V) = (0.95, 0.005) means high availability and stable as Always-stable about 0.7 % of all addresses which this computer group is server. (A, V) = (0.05, 0.05) as Underutilized about 14.32%. Moreover, density of (A, V) = (0.1 – 0.4, 0.045 – 0.01) as Sometimes – stable about 8.86%, Intermittent about 4.04 % and Unclassifiable about 72.85%.

5. Conclusion and Future Work

We did a study on IPv4 address allocation utilization at Kasetsart University on /24 blocks which are allocated to departments or organizations within the university. Our experiments use Active and Passive Probing on various port. The experimental results show that 49.80% of allocated IP addresses are used. TCP method can find more visible IP address than the ICMP method. And most characteristics of IP addresses are intermittent and underutilized. The survey number of IP address are used active probing (ICMP and TCP). The repeated active probing with ICMP provides information about how addresses are used. But a single ICMP response provides only limited information repeated probing can tell much more. The result showed that the survey IP address can be found all following 22.29% of ICMP missing and 20.46% of TCP missing. The result of this survey can show

active probe response to finds IP address usage. Comparison the accuracy of ICMP and TCP which show the survey ICMP and TCP can be shown to be effective in the survey. The results showed that the number of IP address with TCP protocol can find IP address more than ICMP about 2%. Compare the accuracy active probe with ground truth. The ground truth data from the computer center, Kasetsart University can use compare result with active probe. Which show the verify accuracy of the survey. The result showed that the survey have 0.3% false positive and 0.78% false negative.

6. Acknowledgments

The authors would like to thank the Thailand Graduate Institute of Science and Technology (TGIST) support in scholarship.

7. References

- [1] B. Huffaker, D. Plummer, D. Moore, and K. C. Claffy. Topology Discovery by Active Probing. In *Proc. Of the Symposium on Applications and the Internet*, Jan. 2002.
- [2] X. Meng, Z. Xu, S. Lu, and L. Zhang. IPv4 Address Allocation and the BGP Routing Table Evolution. Technical Report 030046, CS Department, UCLA, 2002.
- [3] X. S. Lu, and L. Zhang. IPv4 Address Allocation and the BGP Routing Table Evolution. Technical Report 030046, CS Department, UCLA, 2002.
- [4] W. M'uhlbauer, O. Maennel, S. Uhlig, A. Feldmann, and M. Roughan. Building an AS-topology model that captures route diversity. In *Proc. of the ACM SIGCOMM Conference*, pages 195–204, Sept. 2006.
- [5] X. Dimitropoulos, D. Krioukov, M. Fomenkov, B. Huffaker, Y. Hyun, K. C. Claffy, and G. Riley. AS relationships: Inference and validation. *ACM Computer Communication Review*, 37(1):29–40, Jan. 2007.
- [6] Genevieve Bartlett, John Heidemann and Christos Papadopoulos. Understanding Passive and Active Service Discovery (Extended). USC/ISI Technical Report ISI-TR-642, USC/Information Sciences Institute, May 2007.
- [7] John Heidemann, Yuri Pradkin, Ramesh Govindan, Christos Papadopoulos, Genevieve Bartlett and Joseph Bannister. Census and Survey of the Visible Internet. In *Proceeding of IMC'08, October 20 – 22, 2008, Vouliagmeni, Greece*. 2008.
- [8] Xue Cai and John Heidemann. Understanding Address Usage in the Visible Internet. USC/ISI Technical Report ISI-TR-656, USC/Information Sciences Institute, February 2009.
- [9] ANT Censuses of the Internet Address Space project. Web page <http://www.isi.edu/ant/address/>, June 2009.
- [10] Nmap. Web page <http://nmap.org/>, June

ประวัติการศึกษา และการทำงาน

ชื่อ –นามสกุล	แสงดาว พรทวีโชคสกุล
วัน เดือน ปี ที่เกิด	9 มีนาคม 2528
สถานที่เกิด	ราชบุรี
ประวัติการศึกษา	ระดับปริญญาตรี สาขาวิทยาการคอมพิวเตอร์ (เกียรตินิยม อันดับสอง) สำนักวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่ฟ้าหลวง
ตำแหน่งหน้าที่การงานปัจจุบัน	วิศวกรระบบ
สถานที่ทำงานปัจจุบัน	บริษัท ไทยเนม เซฟเวอร์ จำกัด
ผลงานดีเด่นและรางวัลทางวิชาการ	
ทุนการศึกษาที่ได้รับ	ทุนสถาบันบัณฑิตวิทยาศาสตร์และเทคโนโลยีไทย หรือ ทุน TGIST