การแสดงผล Netflow โดยใช้ Nfsen บน VMware

Netflow processing and traffic monitoring by Nfsen on VMware

นายชูเดช สุรบูรณ์กุล

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรบัณฑิต สาขาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย-ญี่ปุ่น
พ.ศ. 2558

การแสดงผล Netflow โดยใช้ Nfsen บน VMware

Netflow processing and traffic monitoring by Nfsen on VMware

นายชูเดช สุรบูรณ์กุล

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรบัณฑิต สาขาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย-ญี่ปุ่น
พ.ศ. 2558

คณะกรรมการสอบ

..... ประธานกรรมการสอบ
(อาจารย์ ดร.ประจักษ์ เฉิดโฉม)

..... กรรมการสอบ
(อาจารย์ ดร.สรมย์พร เจริญทิพย์)

..... อาจารย์ที่ปรึกษา
(อาจารย์อมรพันธ์ ชมกลิ่น)

..... ประธานสหกิจศึกษาสาขาวิชา
(อาจารย์อมรพันธ์ ชมกลิ่น)

ชื่อโครงงาน	การแสดงผล Netflow โดยใช้ Nfsen บน VMware
	Netflow processing and traffic monitoring by Nfsen on VMware
ผู้เขียน	นายชูเดช สุรบูรณ์กุล
คณะวิชา	เทคโนโลยีสารสนเทศ สาขาวิชา เทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา	อาจารย์อมรพันธ์ ชมกลิ่น
พนักงานที่ปรึกษา	นายจักรพันธ์ คุ้มญาติ
ชื่อบริษัท	บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)
ประเภทธุรกิจ/สินค้า	ผู้ให้บริการอินเทอร์เน็ตแก่บุคคลทั่วไปและองค์กร

บทสรุป

ในการสหกิจศึกษา ณ บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน) ได้มอบหมายให้ศึกษาถึงระบบเครือข่ายเทคโนโลยี Netflow ซึ่งเป็นข้อมูล Traffic ที่ไหลผ่านในระบบเน็ตเวิร์คหรือเกตเวย์ เราสามารถนำข้อมูลที่มีใน Netflow มาใช้ประโยชน์ในการวิเคราะห์หาสาเหตุ หรือนำไปประยุกต์ใช้อะไรได้บ้าง หรือตรวจสอบสถานะต่างๆในการใช้งาน ซึ่ง Netflow คือข้อมูลเชื่อมต่อกันระหว่างผู้รับ-ผู้ส่ง ถ้าเราดึงข้อมูลจาก Netflow ที่ไหลมาตลอดเวลาหรือเก็บไว้ มาวิเคราะห์ข้อมูล โดยในโครงการนี้ได้นำเครื่องมือในการแสดงผลที่ชื่อว่า Nfsen มาช่วยในการตรวจจับและเป็นเครื่องมือหลักในโครงการนี้

การตรวจสอบในโครงการนี้สามารถดูผ่านเว็บอินเตอร์เฟส สามารถเก็บรวบรวมข้อมูลการใช้งานเอาไว้เพื่อใช้วิเคราะห์สถิติการใช้งานได้ในภายหลังอีกทั้งยังช่วยตรวจสอบถึงพฤติกรรมการใช้งานเพื่อวางแผนการให้บริการให้ดียิ่งขึ้นได้อีกด้วยจึงเป็นที่มาของการจัดทำโครงการนี้

กิตติกรรมประกาศ

การสหกิจศึกษาของข้าพเจ้า ณ บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน) ในครั้งนี้จะไม่สามารถลุล่วงได้เลยหากไม่ได้รับการอนุเคราะห์จากแผนก Internet Servive บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน) ที่มอบโอกาสให้ข้าพเจ้า เข้าร่วมฝึกปฏิบัติงานเป็นส่วนหนึ่งของทีมเจ้าหน้าที่ฝ่าย Network และมอบประสบการณ์ต่างๆในการทำงานให้ข้าพเจ้า

ข้าพเจ้าขอขอบพระคุณ คุณจักรพันธ์ อุ้มญาติ ผู้ให้คำปรึกษาในการทำงานสหกิจครั้งนี้และเจ้าหน้าที่บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน) ทุกท่านที่ให้คำแนะนำ การสนับสนุน และคอยให้ความช่วยเหลือตลอดการทำงาน ตั้งแต่วันที่ 2 มิถุนายน 2558 จนถึงวันที่ 30 กันยายน 2558 เป็นระยะเวลาทั้งสิ้นประมาณ 4 เดือน ในระยะเวลานี้ทำให้ข้าพเจ้าได้เรียนรู้ประสบการณ์จากการทำงานจริงซึ่งไม่สามารถเรียนรู้ได้จากในห้องเรียนละยังเป็นประสบการณ์ที่มีค่าอย่างยิ่งซึ่งข้าพเจ้าสามารถนำไปใช้พัฒนาทักษะของตนเองในอนาคต นอกจากนี้ข้าพเจ้าขอขอบคุณผู้ที่เกี่ยวข้องทุกท่านที่มีส่วนช่วยเหลือให้รายงานฉบับนี้เสร็จสมบูรณ์ไปได้อย่างราบรื่นโดยเฉพาะอย่างยิ่งท่าน อาจารย์ อมรพันธ์ ชมกลิ่น ผู้เป็นอาจารย์ที่ปรึกษาในการจัดทำรายงานฉบับนี้ที่คอยชี้แนะและให้ความช่วยเหลือแก่ข้าพเจ้า

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพประกอบ

สารบัญภาพประกอบ

ภาพที่ **หน้า**

สารบัญภาพประกอบ

สารบัญภาพประกอบ

ภาพที่ **หน้า**

บทที่ 1
บทนำ

1.1 ชื่อและที่ตั้งของสถานประกอบการณ์

ชื่อของสถานประกอบการ:บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)

ที่ตั้งของสถานประกอบการ: 200 หมู่4 ถนนแจ้งวัฒนะ ตำบลปากเกร็ด อำเภอปากเกร็ด จังหวัด นนทบุรี 11120

โทรศัพท์: 66-2-100-2100

โทรสาร : 66-2-100-2121

ภาพที่ 1.1 แผนที่ บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)

1.2 ลักษณะธุรกิจของสถานประกอบการ หรือการให้บริการหลักขององค์กร

บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน)เป็นบริษัทที่ให้บริการอินเตอร์เน็ตแบบครบวงจรที่พร้อมให้บริการสำหรับบุคคลทั่วไปและในส่วนของภาคธุรกิจ โดยแบ่งการบริการหลายประเภท เช่น 3BB ADSL , 3BB Corporate และ 3BB VAS

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร

องค์กรไม่อนุญาติให้เปิดเผยข้อมูล

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับมอบหมาย

ตำแหน่งงานที่ได้รับมอบหมายในการสหกิจศึกษาครั้งนี้คือ การศึกษาถึงการทำงานของโพรโทคอล Netflow การศึกษาระบบเครือข่าย traffic ของเร้าเตอร์ โดยมีขอบเขตงานคือการแสดงผล traffic ของเร้าเตอร์บน web page

1.5 พนักงานที่ปรึกษา และ ตำแหน่งของพนักงานที่ปรึกษา

พนักงานที่ปรึกษา : จักรพันธุ์ อุ้มญาติ

ตำแหน่ง : Engineer

1.6 ระยะเวลาที่ปฏิบัติงาน

ระยะเวลาที่ปฏิบัติงานสหกิจศึกษาประมาณ 4 เดือน นับตั้งแต่วันที่ 2 มิถุนายน 2558 ถึงวันที่ 30 กันยายน 2558

1.7 ที่มาและความสำคัญของปัญหา

ปัจจุบันระบบเครือข่ายถือได้ว่ามีความสำคัญสำหรับการใช้งานในชีวิตประจำวันเป็นอย่างมาก ไม่ว่าจะเป็นการใช้งานระบบเครือข่ายภายในองค์กรขนาดเล็กไปจนถึงองค์กรขนาดใหญ่ในแต่ละองค์กรได้มีการนำระบบเครือข่ายเข้ามาในการขับเคลื่อนธุรกิจในองค์กร การมีระบบเครือข่ายที่ดีสามารถช่วยให้องค์กรสามารถดำเนินงานได้อย่างมีประสิทธิภาพ สามารถตอบสนองต่อความต้องการขององค์กรได้ส่งผลให้องค์กรมีการพัฒนาได้อย่างรวดเร็ว แม้ระบบเครือข่ายดีอย่างไร แต่ ปัญหาของผู้ดูแลระบบเครือข่ายส่วนใหญ่ที่ได้รับการร้องเรียนคือ เรื่องการใช้งานระบบ มีอาการไม่ตอบสนองตามปกติเป็นหน้าที่ของผู้ดูแลที่จะต้องแก้ไข บางครั้งการตรวจสอบอาจจะไม่สะดวกและไม่เห็นถึงปัญหาที่แท้จริงหรือต้องใช้เวลาในการวิเคราะห์

จึงได้มีแนวคิดการวิเคราะห์ปริมาณการใช้งานบนเครือข่าย โดยใช้ข้อมูลจาก Netflow ซึ่งเป็นโพรโทคอลชนิดหนึ่งที่พัฒนาโดย Cisco โดยฟังก์ชั่นนี้ถูกบรรจุอยู่ภายในเร้าเตอร์อยู่แล้ว สามารถเปิดการทำงานเพื่อให้ผู้ดูและระบบสามารถนำข้อมูลการจราจร (Traffic) ที่วิ่งผ่านเข้า – ออก นำไปวิเคราะห์หาสาเหตุได้ และไม่ส่งผลกระทบต่อการใช้งาน

1.8 วัตถุประสงค์หรือจุดมุ่งหมายของโครงงาน

1.8.1 เพื่อศึกษาว่าโพรโทคอล Netflow คืออะไร

1.8.2 เพื่อจัดทำระบบดูแลและบริหารจัดการเครือข่าย

1.8.3 เพื่อตรวจสอบพฤติกรรมการใช้งานของผู้ใช้งานในระบบ

1.8.4 เพื่อเก็บข้อมูลทางสถิติของการจราจรในเครือข่ายมาแสดงเป็นกราฟ

1.8.5 เพื่อระวัง ป้องกันปัญหาที่อาจะเกิดได้ล่วงหน้าก่อนปัญหาเกิดขึ้นจริง เพื่อลดผลกระทบต่อการใช้งาน

1.8.6 เพื่อศึกษาทฤษฎีการทำงานของ Nfsen

1.9 ผลที่คาดว่าจะได้รับจากการปฏิบัติงานหรือโครงงานที่ได้รับมอบหมาย

1.9.1 รู้พื้นฐานที่เกี่ยวข้องถึงวิธีการให้ได้มาซึ่งข้อมูล Netflow เพื่อใช้ในการวิเคราะห์

1.9.2 ดูปริมาณข้อมูลที่วิ่งผ่านอุปกรณ์ต่างๆเพื่อนำมาวิเคราะห์ปัญหา

1.9.3 สามารถนำผลลัพธ์ที่ได้จากการวิเคราะห์มาประเมินการใช้งานได้

1.9.4 ใช้ข้อมูลจาก Netflow แสดงผลเป็นกราฟผ่าน web Interface

1.9.5 ตรวจสอบสถานะข้อมูลจราจรที่วิ่งผ่านอุปกรณ์ในเครือข่าย

1.9.6 เข้าใจหลักการทำงาน Nfsen

1.10 คำจำกัดความ

ในรายงานจะใช้ระบบปฏิบัติการ linux CentOS 6.5 อาจจะมีบางคำสั่งที่ไม่เข้าใจว่าเอาไว้ใช้งานอะไร เพื่อเป็นการสื่อความหมายให้เป็นที่เข้าใจตรงกัน

yum : เป็นคำสั่งสำหรับติดตั้งโปรแกรมบน Linux

vi : เป็นคำสั่งสำหรับแก้ไขไฟล์ (ทุกการแก้ไขไฟล์ จะต้องกด i เพื่อแก้ไข ไฟล์ หลังจากแก้ไขไฟล์ตามที่ต้องการให้กด esc เพื่อ ใช้คำสั่งต่อ ไป)

“:wชื่อไฟล์” เพื่อเป็นการเซฟไฟล์ตามชื่อที่กำหนด

“:wq” เพื่อออกจากไฟล์โดยที่เซฟทับไฟล์เก่า

“:q!” เพื่อออกจากไฟล์โดยทีไม่บันทึก

“:set”

- set nu = แสดงหมายเลขบรรทัด
- set ic = สั่งให้ Search ไม่สนตัวเล็กตัวใหญ่ Ignore Case
- set nu ic ทำทั้งสองแบบ

tar : เป็นคำสั่งสำหรับการแตกไฟล์ทีต้องการ

บทที่ 2
พื้นฐานและทฤษฎีที่เกี่ยวข้อง

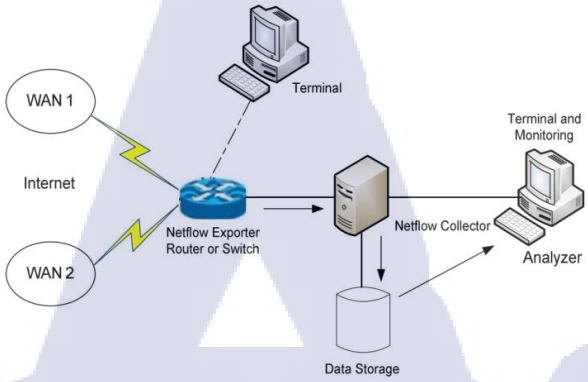
ในองค์กรหลากหลายองค์กรใช้ระบบเครือข่ายเพื่อใช้ในการติดต่อสื่อสารกันทั้งภายในและภายนอกองค์กร รวมทั้งใช้ระบบเครือข่ายในการทำงานเกือบทุกส่วน ดังนั้น ปัญหาการใช้งานระบบเครือข่ายที่ไม่เหมาะสมกับการใช้งาน การไม่มีการบริหารจัดการ การตรวจสอบและการออกแบบระบบเครือข่ายที่ถูกต้องจึงส่งผลให้การใช้งานระบบเครือข่ายนั้น ไม่มีประสิทธิภาพเพียงพอ แต่ยังมีเทคโนโลยีที่สามารถนำมาเพิ่มในระบบหรือช่วยในการบริหารเครือข่ายได้อีกอย่าง เช่น Netflow ที่สามารถนำมาตรวจสอบการใช้งานได้

2.1 ทฤษฎีที่ใช้ในการปฏิบัติงาน

2.1.1 ทฤษฎี Netflow

Netflow คือเทคโนโลยีการเฝ้าดูรูปแบบของ Traffic ที่ได้รับการพัฒนาโดย Darren Keer และ Barry Bruins ของบริษัท Cisco System ในปี 1996 ได้อธิบายวิธีการสำหรับเร้าเตอร์ (Router) ในการส่งสถิติเกี่ยวกับ ความสัมพันธ์เป็นคู่ของ Router Socket ออกมา และ ปัจจุบันคุณสมบัติพิเศษนี้ ได้ถูกบรรจุเข้าไปยังเร้าเตอร์ของ Cisco ทั้งหมด และผู้ผลิตหลายรายก็ได้บรรจุส่วนนี้เข้าไปยังเร้าเตอร์ และสวิตช์ (Switch)เรียบร้อยแล้ว

เมื่อผู้ดูแลระบบเครือข่ายได้เปิดการใช้งาน Netflow ให้ส่งออกมาจาก Router interface สถิติ Traffic ของ Packet ต่างๆที่ได้รับเข้ามาบน Interface นั้นจะถูกเก็บเป็น Flow และถูกเก็บไว้ในตัวสำรองข้อมูล Flow ชั่วคราวที่แปรผันอยู่ตลอด



ภาพที่ 2.1 สถาปัตยกรรม Netflow

จากภาพที่2.1 แสดงให้เห็นถึงสถาปัตยกรรมการเชื่อมต่อและการไหลของข้อมูลโฟล์วที่ได้จากอุปกรณ์ต่างๆมายัง Netflow Collector เพื่อ Dump ข้อมูล เข้าสู่ฐานข้อมูลเพื่อรอให้ Netflow analyzer ดึงข้อมูลในส่วนนี้ไปตรวจสอบการใช้งาน

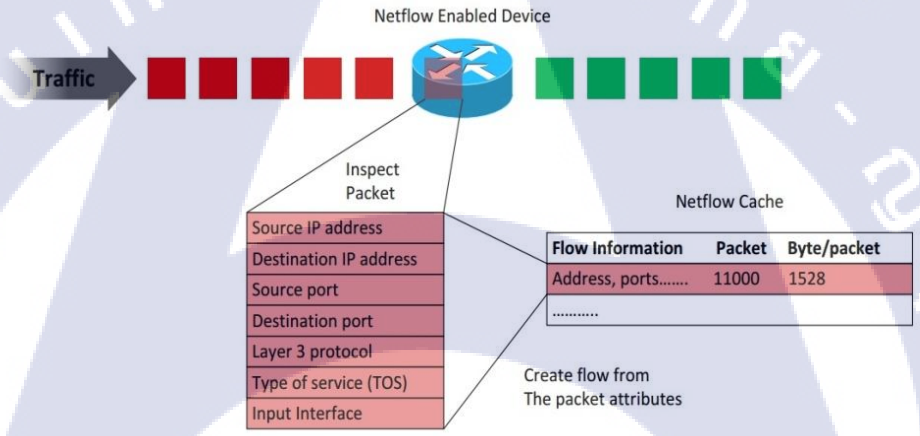
2.1.1.1 การนำเทคโนโลยี Netflow เข้ามาประยุกต์ใช้งานกับระบบเครือข่าย

1. การเฝ้าระวังการใช้งานโปรแกรมประยุกต์และการใช้งานของผู้ใช้ระบบเครือข่าย โพรโทคอล Netflow เข้ามาช่วยให้ผู้ใช้งานระบบเครือข่ายสามารถตรวจสอบรายละเอียดการ ใช้งานโปรแกรมประยุกต์ต่าง ๆ และการใช้งานระบบเครือข่าย ซึ่งข้อมูลเหล่านี้สามารถช่วยให้ ผู้ดูแลระบบเครือข่ายจัดสรรทรัพยากรเครือข่ายให้สอดคล้องกับการใช้งาน รวมไปถึงความสามารถ ในการตรวจสอบในรูปแบบที่ใกล้เคียงการใช้งานจริงของระบบเครือข่าย ทำให้การตรวจสอบปัญหา ที่เกิดขึ้นเป็นไปได้ด้วยความแม่นยำ และรวดเร็ว ส่งผลให้ผู้ดูแลระบบสามารถแก้ไขปัญหาระบบ เครือข่ายที่เกิดขึ้นได้อย่างทันเหตุการณ์

2. การวางแผนการออกแบบระบบเครือข่าย เทคโนโลยีโพรโทคอล Netflow สามารถใช้ในการตรวจสอบเฝ้าระวังระบบเครือข่ายและ จัดเก็บข้อมูลในรูปแบบระยะยาว เพื่อนำข้อมูลมาใช้ในการติดตามผล วิเคราะห์ผลการใช้งานระบบ เครือข่าย ส่งผลให้สามารถคาดการณ์สถานการณ์ที่จะเกิดขึ้นในอนาคตได้ รวมไปถึงการเพิ่ม หรือลด จำนวนของอุปกรณ์ที่ให้บริการ และใช้งานบนระบบเครือข่าย ข้อมูลดังกล่าวยังบ่งบอกถึงสถานการณ์ และจำนวนของทรัพยากรระบบเครือข่ายในปัจจุบันที่

สามารถใช้งานได้ ช่วยให้การออกแบบ 4 การวางแผน การกำหนดนโยบายการใช้งานระบบเครือข่ายเป็นไปอย่างเหมาะสม ลดต้นทุนรวมของ การดำเนินการ ทำให้ระบบเครือข่ายใช้งานได้มีประสิทธิภาพและมีเสถียรภาพ

3. การสร้างโฟล์วใน Netflow cache การสร้าง Netflow Cache มีรูปแบบการสร้างโดยที่ทุก ๆ Packet ที่มีหมายเลขไอพีแอดเดรส หมายเลยพอร์ต ทั้งต้นทางและปลายทาง Packet อินเตอร์เฟส และกลุ่มของการบริการที่เหมือนกัน จะถูกรวมเข้าสู่โฟล์ (Flow) โดยการเพิ่มจำนวนขนาดของข้อมูล ไบต์ (Byte) ณ ตำแหน่งท้ายของ Packet ซึ่งข้อมูลดังกล่าวจะถูกบันทึกลงในฐานข้อมูลของ Netflow เรียกว่า Netflow Cache ดังตัวอย่างภาพที่ 2.2



ภาพที่ 2.2 การตรวจสอบโฟล์วข้อมูล และการสร้าง Netflow Cache

2.1.1.2 เกี่ยวกับ Flow

Packet ที่ผ่านเข้าอุปกรณ์ ไม่ว่าจะเป็นเราเตอร์ หรือสวิตช์จะถูกตรวจสอบด้วยค่าของ IP Packet ซึ่งค่าต่าง ๆ เหล่านั้นจะเป็นสิ่งที่สามารถบ่งบอกตัวตนของ Packet ว่า Packet นั้นมีความแตกต่าง หรือเหมือนกับ Packet อื่น ๆ ที่เคยส่งผ่านในระบบเครือข่ายหรือไม่โดยพิจารณาจาก ค่าเหล่านี้หรือที่เรียกว่า ค่าลักษณะเฉพาะทั้ง7

1. หมายเลขไอแอดเดรสต้นทาง
2. หมายเลขไอพีแอดเดรสปลายทาง

3. หมายเลขพอร์ตต้นทาง

4. หมายเลขพอร์ตปลายทาง

5. ชนิดของโพรโทคอลในระดับของ Physical Layer Data Link Layer Network Layer และ Transport Layer เช่น TCP UDP และ ICMP เป็นต้น

6. ชนิดของการบริการ (Types of Service)

7. อินเตอร์เฟสของการนำเข้า และส่งออกข้อมูลจากอุปกรณ์

หลังจากรับ Packet เข้ามาตัวเร้าเตอร์จะตรวจสอบจาก 7 ส่วนนี้จากนั้นจะตั้งเงื่อนไขว่า ถ้า Packet เป็นสมาชิกของโฟล์วที่มีอยู่ในขณะนั้น สถิติรวมทราฟฟิกของโฟล์วที่สอดคล้องกันจะมีการเพิ่มขึ้น ถ้ามิเช่นนั้นแล้วโฟล์วใหม่จะถูกสร้างขึ้นแทน

โดยแนวความคิดของเทคโนโลยีของ Cisco, โฟล์วใหม่ๆ จะถูกสร้างขึ้นอย่างต่อเนื่องเมื่อ โฟล์วที่บันทึกไว้หมดอายุลงมันจะถูกส่งออกมาเป็น UPD Packet ไปยังสถานีเป้าดูหรือตัวเลือกรับ ข้อมูลที่ผู้ใช้งานกำหนดไว้ ถ้าเงื่อนไขดังต่อไปนี้ได้เกิดขึ้น เงื่อนไขการหมดอายุของโฟล์วนี้คือ

- Transport Protocal ได้ระบุว่าการเชื่อมต่อนั้นได้เสร็จสมบูรณ์แล้ว (TCP FIN) และมีความล่าช้าเล็กน้อยที่ยอมรับได้สำหรับความสำเร็จของการประสานงานกันเพื่อรับรู้และยอมรับกระบวนการ FIN

- ทราฟฟิกไม่มีการเคลื่อนไหวเกิน 15 นาที

- สำหรับโฟล์วที่มีการเคลื่อนไหวอย่างต่อเนื่อง การบันทึกโฟล์วของหน่วยความจำสำรองจะหมดอายุลงทุกๆ 30 นาทีเพื่อความแน่นอนของการรายงานผลแต่ละคาบเวลาของโฟล์วที่มีการเคลื่อนไหว

ผู้ผลิตอุปกรณ์เครือข่ายมีการนำ NetFlow มาใช้งานแต่ละรุ่นอย่างหลากหลาย แต่รุ่นที่ได้รับความนิยมส่วนใหญ่คือ รุ่นที่ 5 สำหรับ Datagram ของรุ่นที่ 5 นี้ทุกๆ UDP Datagram บรรจุไปด้วย Flow Header และ 30 Flow records ทุกๆ Flow records จะสร้างไว้หลายๆส่วน ซึ่ง ประกอบด้วย

1. หมายเลขตำแหน่งของ IP ต้นทางและปลายทาง
2. หมายเลขตำแหน่งของ Next Hop
3. หมายเลข Interface ขาเข้าและขาออก
4. จำนวนของ Packet ในโฟล์วนั้น
5. จำนวน Bytes สุทธิของโฟล์วนั้น

6. Source Port and Destination Port

7. Protocal

8. Type of Service

9. หมายเลข AS ต้นทางและปลายทาง และ TCP flags (ตัวเดียวหรือหลายตัวรวมกันของ TCP flags)

บนเครื่องรับข้อมูล (Colletor) การวิเคราะห์โฟล์วที่ได้รับมาจำเป็นต้องดำเนินการตามเวลาจริงคือกระทำทันที ตัวนี้สามารถจะซื้อ Software หรือ Hardware ที่มีจำหน่ายอยู่แล้วหรือสร้างขึ้นเองจากโปรแกรมที่ทำออกมาแจกจ่ายก็ได้

รูปแบบของ Netflow Export Datagram ประกอบด้วยส่วนหัวและลำดับของการบันทึกข้อมูลไฟล์ โดยในส่วนหัวของโฟล์วจะประกอบด้วยข้อมูล Sequence number Record Count และ System uptime เป็นต้น ส่วนลำดับการบันทึกค่าของโฟล์วจะประกอบด้วยข้อมูล เช่น IP Address, Port และ Routing information ดังต่อไปนี้แสดงถึงรุ่นของ Netflow Export Format (Netflow Introduction)

รุ่นที่ 1 เป็นรุ่นแรกของโพรโทคอล Netflow มีความสามารถในการรองรับรูปแบบ โพรโทคอล Netflow เท่านั้น ออกแบบรองรับเฉพาะ IPv4 ไม่รวมข้อมูลไอพีมาส (IP Mask) และ หมายเลยเอเอส (AS Number)

รุ่นที่ 2 รุ่นที่ 3 และ รุ่นที่ 4 เป็นรุ่นที่สร้างขึ้นเฉพาะการใช้งานภายใน Cisco เอง และสร้างขึ้นมาเพื่อพัฒนาเท่านั้น ไม่มี การประกาศให้น าไปใช้งานจริง

รุ่นที่ 5 พัฒนาจากรุ่นก่อนหน้าโดยได้มีการเพิ่มส่วนของ Border Gateway Protocol (BGP) ข้อมูลของ Autonomous System (AS Information) และข้อมูลลำดับของโฟล์ว

รุ่นที่ 7 รูปแบบการทำงานเหมือนกับรุ่นที่ 5 แต่ข้อแตกต่างในรุ่นนี้ คือ สามารถใช้งานได้เฉพาะในอุปกรณ์ Cisco Catalyst 5000 เท่านั้น

รุ่นที่ 8 มีรูปแบบที่ออกมาใช้เมื่อเราใช้งานจำเพาะบน เราเตอร์ ที่มีการร่วมกันทำงาน กับ Cisco IOS เราเตอร์ด้วยกันเอง

รุ่นที่ 9 มีรูปแบบเป็น Templates ส่วนมากใช้รายงาน IPv6, MPLS หรือแม้กระทั่ง IPv4 กับ Nexthop BGP

โดยโครงงานนี้จะใช้รุ่นที่ 5 ในการทำงานซึ่งเป็นรุ่นที่นิยมใช้งานในอุปกรณ์ส่งและรับข้อมูลการไหลเวียนที่ทำในเชิงพานิชย์ในปัจจุบันนี้ และเป็นรุ่นที่ไม่สิ้นเปลืองทรัพยากรรับข้อมูล และข้อมูล

ที่ถูกส่งออกมาจากอุปกรณ์ เร้าเตอร์และสวิทซ์ (switch) ก็มีปริมาณไม่มากนัก ซึ่งไม่ทำให้เป็นการรบกวนกระบวนการการทำงานปกติของเร้าเตอร์และสวิทซ์มากนัก

2.1.1.3 Netflow Packet Version 5

ตารางที่ 2.1 ตารางแสดงการอธิบาย Flow Header Format

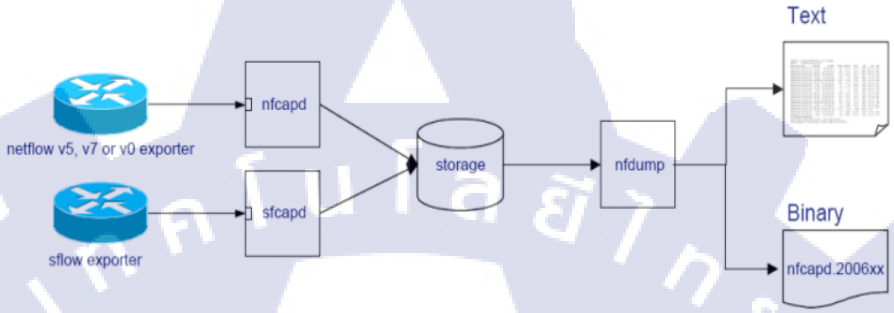
Bytes	Content	Description
0-1	Version	หมายเลขรุ่นของรูปแบบการส่งข้อมูล Netflow
2-3	Count	หมายเลขลำดับของflows ที่ถูกส่งออกของpacketsนี้(1-30)
4-7	Sys_uptime	เวลาปัจจุบัน เป็น missliseconds นับตั้งแต่อุปกรณ์ทีทำหน้าที่ส่งออกข้อมูลได้เปิดเครื่องให้เริ่มทำงาน
8-11	Unix_secs	เวลาปัจจุบันเป็น secounds เริ่มตั้งแต่ 0000 UTC 1970
12-15	Unix_nsecs	เวลาปัจจุบันอยู่เป็น Nanosecounds เริ่มตั้งแต่ 0000 UTC 1970
16-19	Flow_sequence	ตัวนับจำนวนต่อเนื่องของ flow ทั้งหมดที่ได้รับรู้แล้ว
20	Engine_type	ชนิดของเครื่องมือจัดการที่ทำการ flow-switching
21	Engine_id	หมายเลข Slot ของเครื่องมือจัดการ flow-swinching
22-23	Sampling_inverval	2bits แรกที่อยู่ใน sampling mode ยังคงเหลืออีก 14 bits หลังที่เป็นค่าของ sampling interval

ตารางที่ 2.2 ตารางแสดง Flow Record Format

Bytes	Content	Description
0-3	Srcaddr	หมายเลข IP Address ต้นทาง
4-7	Dstaddr	หมายเลข IP Address ปลายทาง
8-11	Nexthop	หมายเลข IP Address ของ router ตัวถัดไปของ flow
12-13	Input	ตัวบ่งชี้ SNMP ของ interface ที่รับข้อมูล
14-15	Output	ตัวบ่งชี้ SNMP ของ interface ที่ส่งข้อมูล
16-19	dPkts	ปริมาณ Packets ในการส่งข้อมูล
20-23	dOctets	จำนวนสูงสุดของ Layer 3 นับเป็น bytes ในปริมาณ Packets ในการส่งข้อมูล
24-27	First	เวลาเริ่มต้นตั้งแต่ส่งข้อมูล
28-31	Last	เวลานับตั้งแต่ได้รับ packet ล่าสุดเข้ามาของข้อมูลที่ได้รับแล้ว
32-33	Srcport	หมายเลข Port ต้นทางของ TCP/UDP หรือที่มีความหมายเหมือนกัน
34-35	Dstport	หมายเลข Port ปลายทางของ TCP/UDP หรือที่มีความหมายเหมือนกัน
36	Pad1	ไม่ถูกใช้งาน (มีค่าเป็น 0)
37	Tcp_flags	Cumulative OR ของ TCP flags
38	Prot	หมายเลขชนิดของ protocol (ตัวอย่างเช่น TCP = 6, UDP =17)
39	Tos	IP Type of service (TOS)
40-41	Src_as	หมายเลข AS ของต้นทาง จะเป็น origin หรือ peer อย่างใดอย่างหนึ่ง
42-43	Dst_as	หมายเลข AS ของปลายทาง จะเป็น origin หรือ peer อย่างใดอย่างหนึ่ง
44	Src_mask	Prefix bits ของ address ต้นทาง
45	Dst_mask	Prefix bits ของ address ปลายทาง

2.1.2 ทฤษฎี Nfdump

Nfdump เป็นเครื่องมือที่ทำหน้าที่ Collect and store flows และคอยส่งไปที่ Nfsen โดย Nfdump จะ Process Flow ผ่าน Command Line ซึ่งมีโครสร้างการทำงานดังภาพที่2.3



ภาพที่ 2.3 แสดงการทำงานของ Nfdump

2.1.2.1 NFDUMP Tools overview

1. Nfcapd – Netflow capture daemon มีหน้าที่อ่าน Netflow ที่มาจากระบบเครือข่าย และทำการเขียนข้อมูลลงไฟล์โดย ทำแบบอัตโนมัต หรือทำงานทุกๆ นาที (ปกติจะตั้งไว้ที่ 5 นาที)

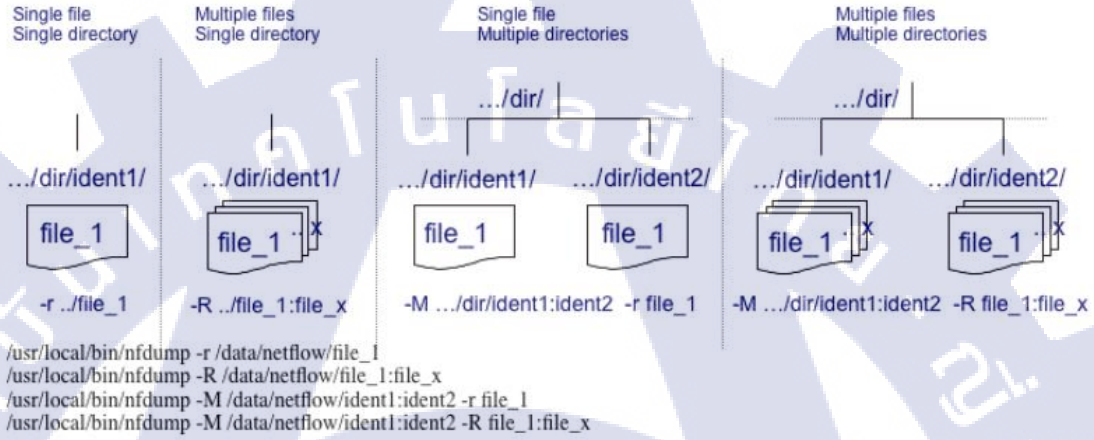
2. Nfdump – Netflow dump มีหน้าที่อ่าน Netflow Data จากไฟล์ที่เก็บโดย nfcapd มีหลักการทำงานคล้ายๆ tcp dump โดยเครื่องมือนี้มีหน้าที่แสดงผลข้อมูลและแสดงในรูปแบบ Top N statistics ซึ่งสามารถแสดงได้หลายรูปแบบตามที่เรา Query มันขึ้นมา

3. Nfprofile – Netflow profiler มีหน้าที่อ่านข้อมูลโฟล์วจากไฟล์ ที่เก็บโดย nfcapd โดยเครื่องมือตัวนี้สามารถคัดกรองข้อมูลโฟล์วได้ตามที่เราได้กำหนด

4. Nfreplay – Netflow replay มีหน้าที่อ่านข้อมูลโฟล์วจากไฟล์ที่เก็บโดย nfcapd และส่งมันผ่านเน็ตเวิร์คไปที่โฮสต์อื่นๆ

2.1.2.2 Netflow Processing

การอ่าน Netflow จากไฟล์มี 2 ลักษณะ 1. ดูจาก Single file 2. จาก Sequence of file ซึ่งจะมี 4 แบบจากภาพ 2.4



ภาพที่ 2.4 โครงสร้างไฟล์ ที่ nfdump ใช้อ่านข้อมูล

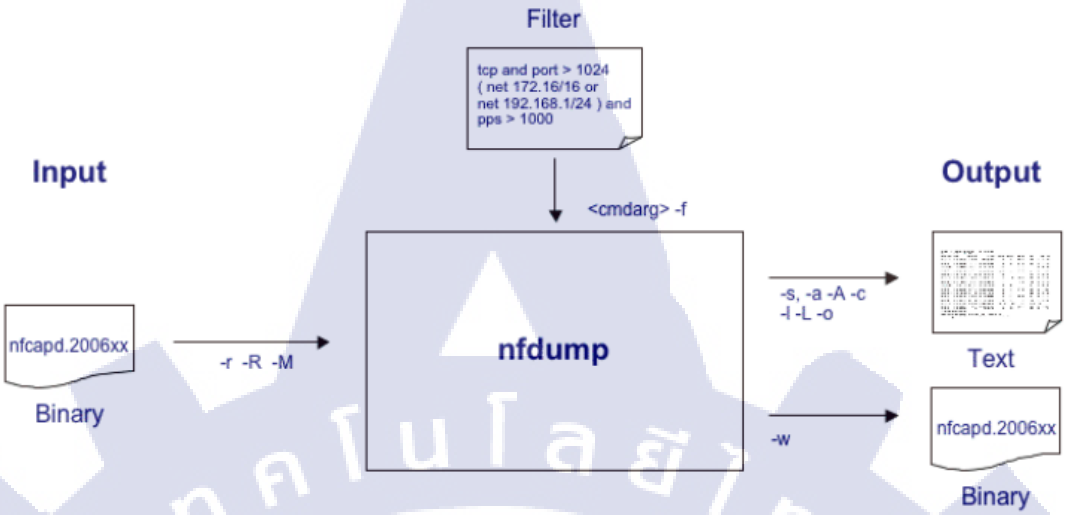
จะเห็นว่าการอ่านไฟล์มี 4 รูปแบบ

1) –r (การอ่านในรูปแบบ single file single directory)

2) –R > (การอ่านในรูปแบบ Multiple file single directory)

3) –M /path/to/first-dir:next-dir:last-dir –r (การอ่านในรูปแบบ single file Multiple directory)

4) –M /path/to/first-dir:next-dir:last-dir –R (การอ่านในรูปแบบ Multiple file Multiple directory)



ภาพที่ 2.5 กระบวนการแระมวลผลข้อมูลของ Nfdump

จากภาพที่2.5 คือกระบวนการที่ใช้ดำเนินการ แปลง Nfcapd ไปเป็นข้อมูลที่ต้องการ

2.1.3) ทฤษฎี Nfsen

Nfsen คือ Web Base Front End ทำหน้าที่ควบคู่กับ Nfdump ซึ่งเป็นเครื่องมือของ Netflow โดย Nfsen สามารถ

- แสดงข้อมูล Netflow , Packet ,Bytes ด้วย RRD (Round Robin Database).
- นำข้อมูล Netflow มาแสดงผลได้ง่าย
- ประมวลผลข้อมูล Netflowภายในเวลาที่กำหนด
- สร้างประวัติการใช้งานได้ต่อเนื่อง
- สร้างการแจ้งเตือนตามเงื่อนไขต่างๆได้
- บันทึก Plugin เพื่อประมวลผล ในช่วงเวลาปกติ

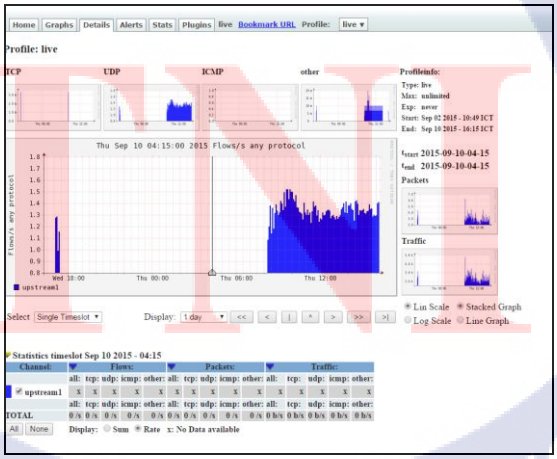
ลักษณะและหน้าที่ของ Nfsen

1. เป็นส่วนที่ทำหน้าที่ นำ Nfdump มาใช้เป็น Backend Tool ได้อย่างมีประสิทธิภาพโดยนำข้อมูลที่ได้จาก Nfdump ทำมาเป็นรูปภาพที่ผู้ใช้งานเข้าใจง่าย

2. มีส่วนที่สามารถที่จะเจาะลึกดูรายละเอียดข้อมูลต่างๆของโฟล์วในช่วงเวลาต่างๆ เช่น โปรโตคอล , ปริมาณทราฟฟิก , โฟล์ว ดังแสดงในภาพที่ 2.6

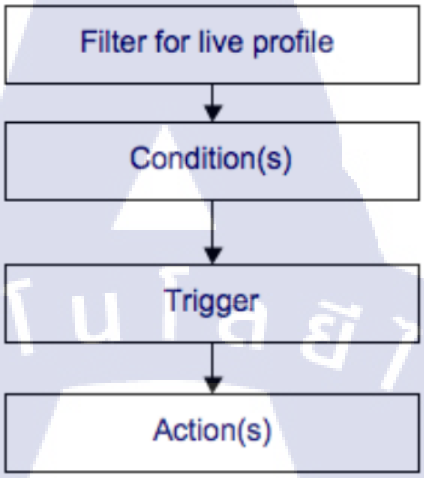
ภาพที่ 2.6 หน้าแสดงรายละเอียดต่างๆของ Nfsen

3. มีกราฟที่แสดงข้อมูลของเน็ตเวิร์คโดยมีระบบ Profile ที่สามารถเลือกดูข้อมูลในรูปแบบต่างๆได้

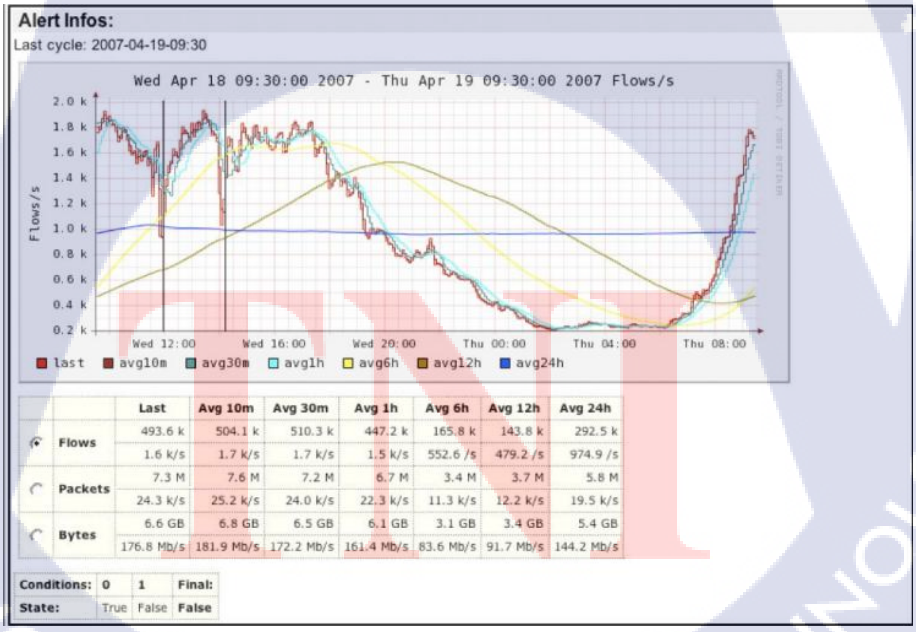


ภาพที่ 2.7 หน้าแสดงกราฟต่างๆของ Nfsen

4. ส่วนของการแสดงข้อมูลสำหรับ Report , Alert จะทำโดย Automatic ตามแต่ที่เราจะ Setup



ภาพที่ 2.8 แสดงขั้นตอนการทำงานของการแจ้งเตือน



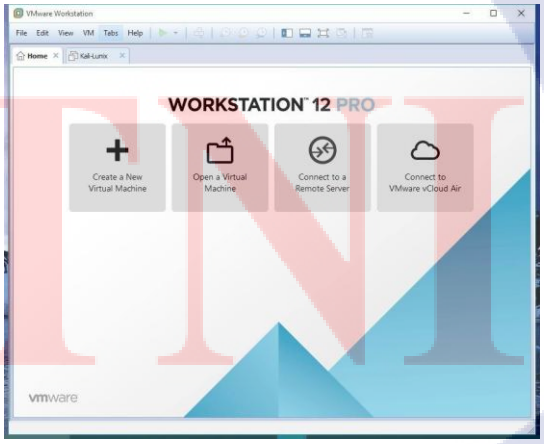
ภาพที่ 2.9 หน้าแสดงรายละเอียดการแจ้งเตือน

2.2 เทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.2.1 โปรแกรม VMWare Workstation

VMware Workstation คือ โปรแกรมจำลองเครื่องคอมพิวเตอร์ หลายๆเครื่อง ในคอมพิวเตอร์เพียง 1 เครื่อง ในการใช้งานสามารถประยุกต์ใช้งานได้หลากหลาย อาทิ ใช้เป็น Multi server os ในกรณีมีเครื่อง server เพียง 1 เครื่อง แต่ต้องการใช้งาน server ทั้ง windows base และ linux base หรือ บางท่านอาจจะใช้เป็น os testing ในการทดสอบการทำงานต่างๆของ os ก็ได้ เพราะเราสามารถลง os ใหม่ได้ง่าย ไม่กระทบกับ os จริง และ ยังสามารถ snapshot ไว้ เพื่อย้อนสภานะให้กลับมาในกรณี os มีปัญหาก็ได้

ภาพที่ 2.10 ภาพไอคอนโปรแกรม vmware workstation 12



ภาพที่ 2.11 โปรแกรม vmware workstation 12

บทที่ 3
แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

3.1 แผนงานปฏิบัติงาน

ตารางที่ 3.1 ตารางแสดงแผนปฏิบัติงานโครงงาน

หัวข้องาน	มิ.ย. 58				ก.ค. 58				ส.ค. 58				ก.ย. 58			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
ศึกษาข้อมูลของสถานประกอบการและลักษณะงานที่จะต้องทำ																
ศึกษาบทความการเขียน broad arduino เริ่มต้น																
ทดสอบโปรแกรมที่ทดลองเขียนลง broad arduino																
ศึกษาบทความเกี่ยวกับ IOT(Internet of thing)																
ทำเรื่องย้ายแผนกจาก IDC ไป Network																
ศึกษาทำความเข้าใจกับ Netflow																
ศึกษาtool แสดงผลบน Web Interface (Nfsen)																
ดำเนินการทดสอบในอุปกรณ์																
แก้ไขปัญหาบางครั้งที่เกิดขึ้น																
เก็บรายละเอียดโครงงาน																

3.2 รายละเอียดโครงงาน

การตรวจสอบระบบเป็นเรื่องยากสำหรับผู้ดูแลถ้าไม่มีเครื่องมืออำนวยความสะดวกที่ช่วยในการตัดสินใจ จึงได้มีโพรโทคอล Netflow ที่พัฒนาโดย Cisco ที่มาพร้อมใช้งานในอุปกรณ์อยู่แล้วโดยการทำโครงงานมีจุดมุ่งหมายคือ

- แสดงบันทึกข้อมูลการจราจรที่ผ่านอุปกรณ์ภายในเครือข่ายผ่านโพรโทคอล Netflow
- แสดงข้อมูล Netflow ในรูปแบบกราฟ ผ่าน web page เพื่อทำให้ข้อมูลดูง่ายยิ่งขึ้น

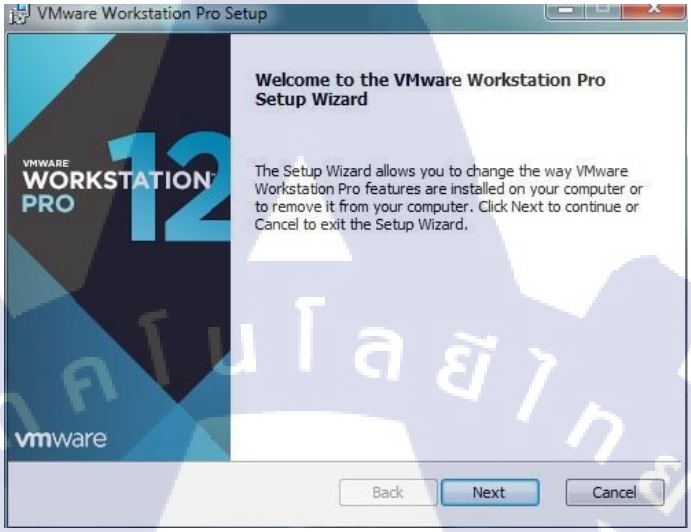
3.2.1 การสร้างเครื่องมือที่ใช้ในโครงงาน

3.2.1.1 วิธีการติดตั้งโปรแกรม VMware Workstation 12

1. ดาวน์โหลด VMware workstation ที่ http://www.vmware.com/products/workstation เมื่อดาวน์โหลดสำเร็จให้เปิดไฟล์ที่ดาวน์โหลดมา

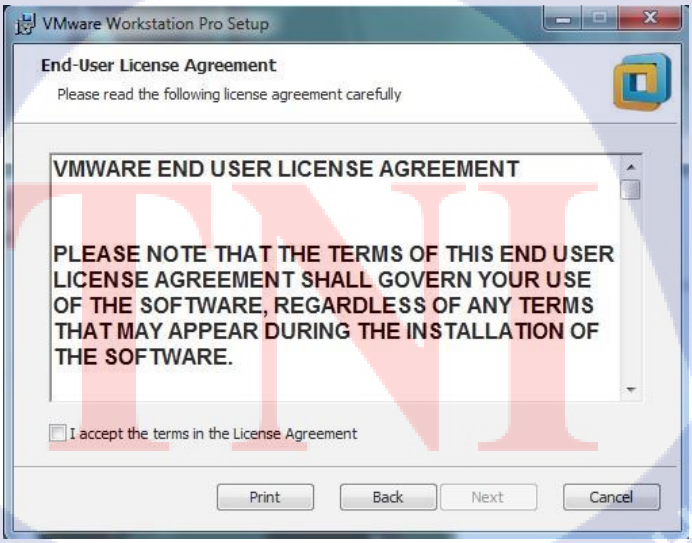
ภาพที่ 3.1 ขั้นตอนการลงโปรแกรม VMware workstation 12

2. กด next เพื่อติดตั้ง



ภาพที่ 3.2 ขั้นตอนการลงโปรแกรม VMware workstation 12

3. กด accept เพื่อยอมรับเงื่อนไข



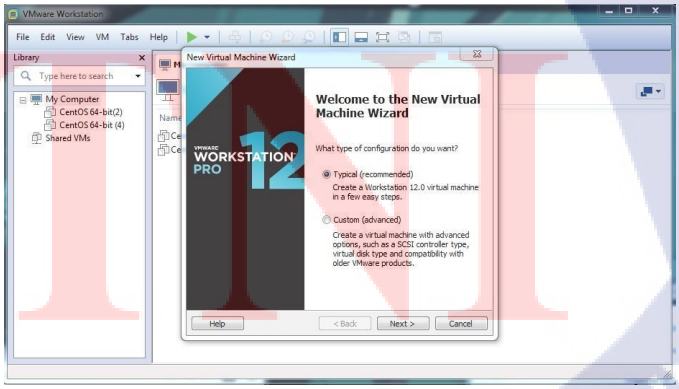
ภาพที่ 3.3 ขั้นตอนการลงโปรแกรม VMware workstation 12

4. กด Finish เพื่อ ออกจากการติดตั้ง

ภาพที่ 3.4 ขั้นตอนการลงโปรแกรม VMware workstation 12

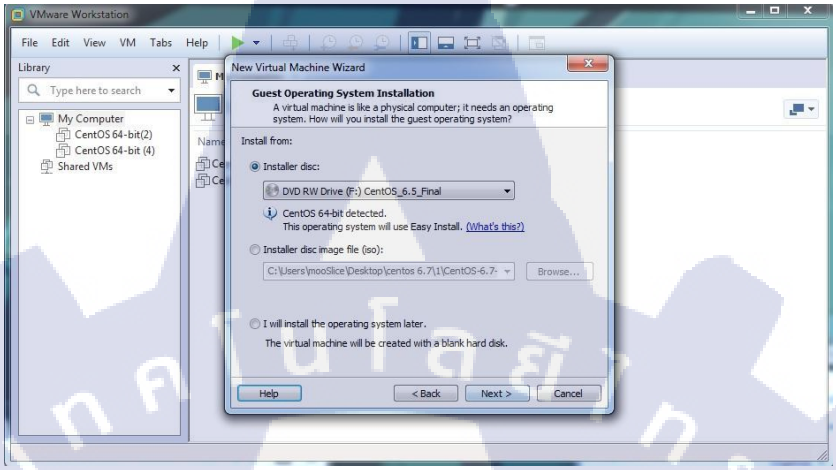
3.2.2.2 วิธีการติดตั้ง Operating System CentOS Linux 6.5 บน VMware Workstation 12

1. กด File > New Virtual Machine เลือก typical



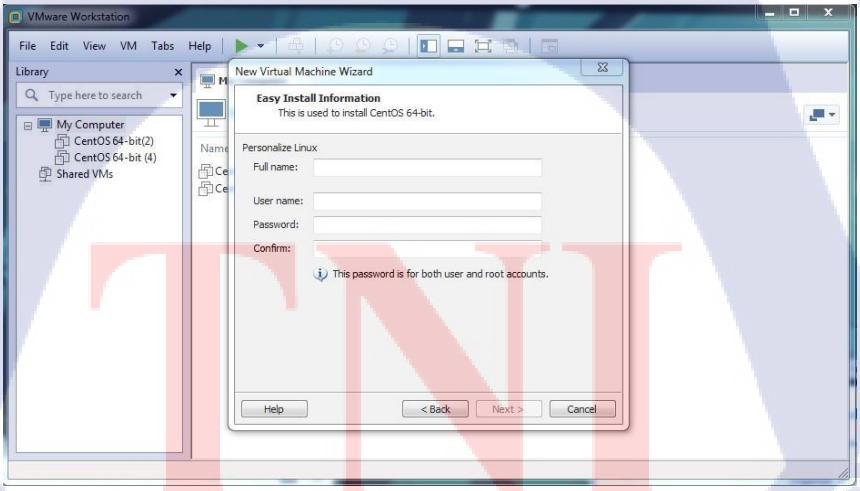
ภาพที่ 3.5 ขั้นตอนการลง Operating System CentOS Linux 6.5

2. เลือกวิธีการลง OS



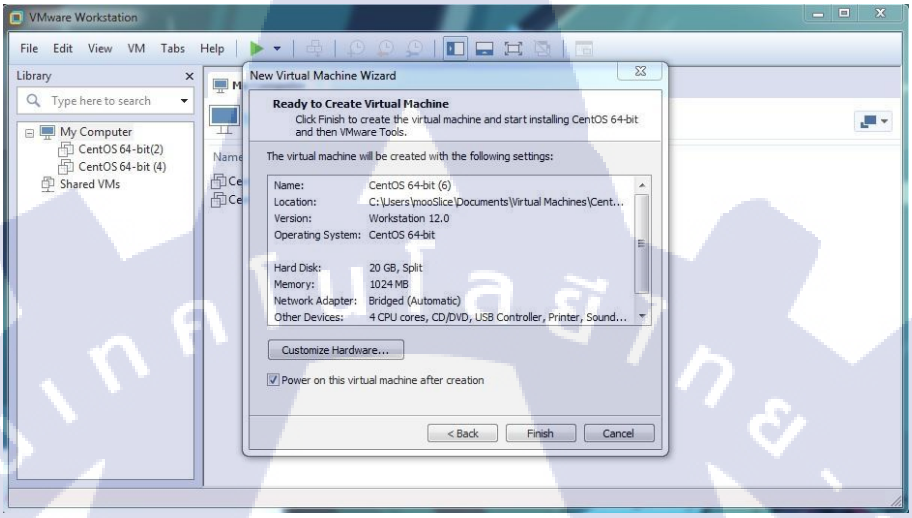
ภาพที่ 3.6 ขั้นตอนการลง Operating System CentOS Linux 6.5

3. ตั้งค่าข้อมูลผู้ใช้งาน

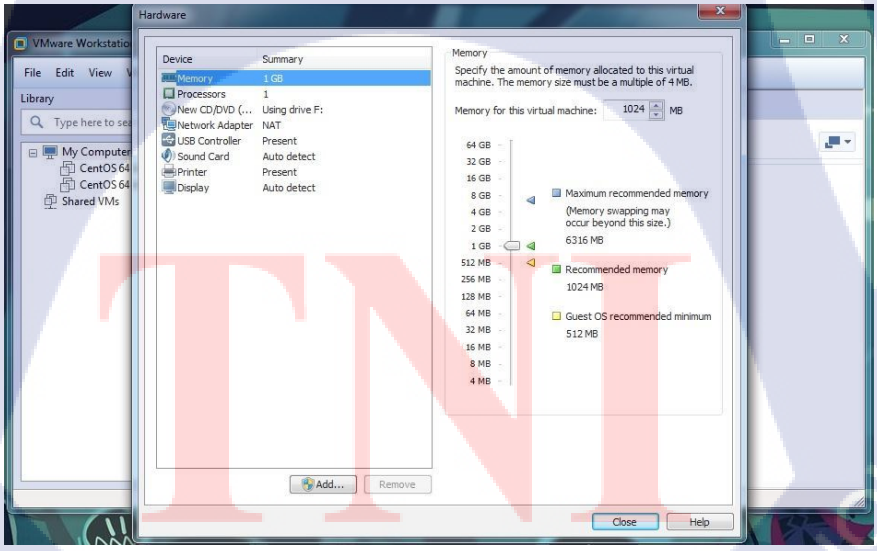


ภาพที่ 3.7 ขั้นตอนการลง Operating System CentOS Linux 6.5

4. รายละเอียดของ Virtual machine ที่ตั้งค่าไว้ ให้ตั้งค่า Network Adapter ให้อยู่ใน Bridged Mode

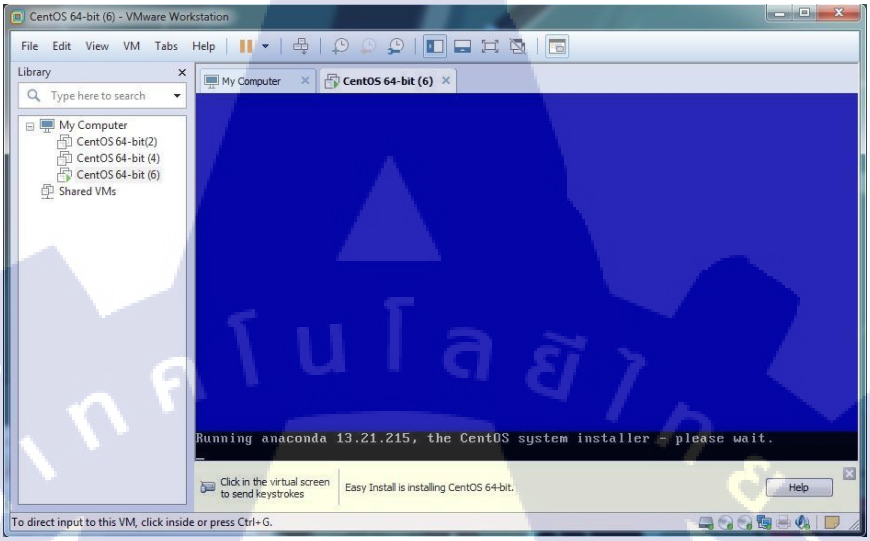


ภาพที่ 3.8 ขั้นตอนการลง Operating System CentOS Linux 6.5

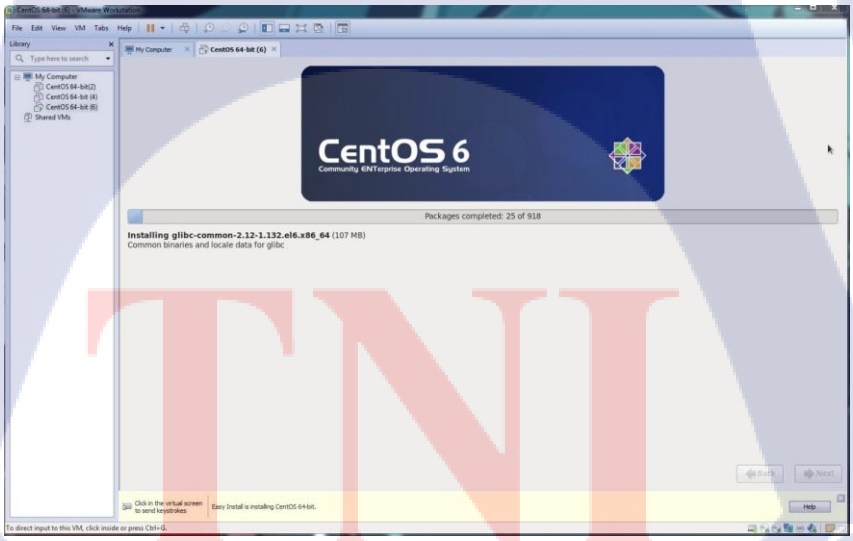


ภาพที่ 3.9 ขั้นตอนการลง Operating System CentOS Linux 6.5)

5. ขั้นตอนระหว่างการติดตั้ง

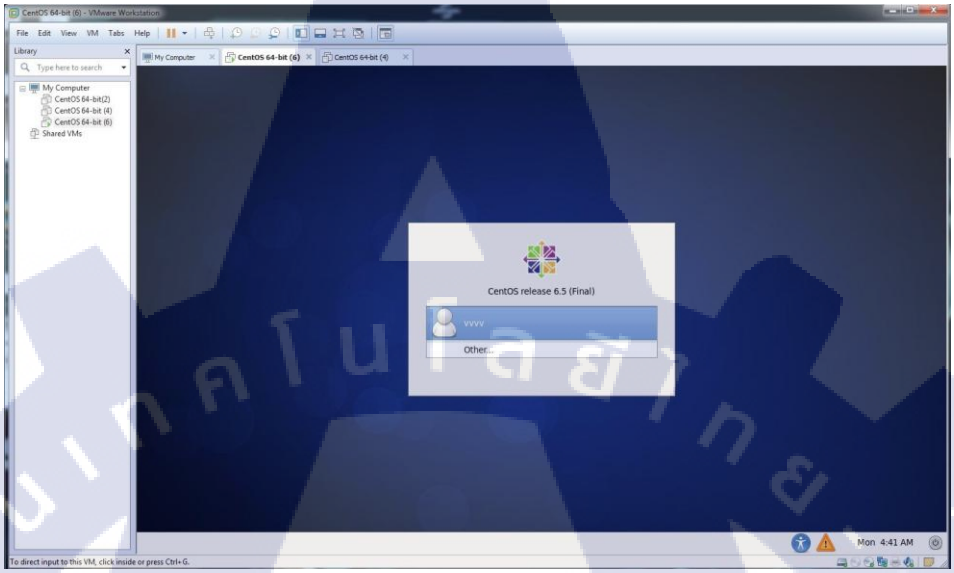


ภาพที่ 3.10 ขั้นตอนการลง Operating System CentOS Linux 6.5

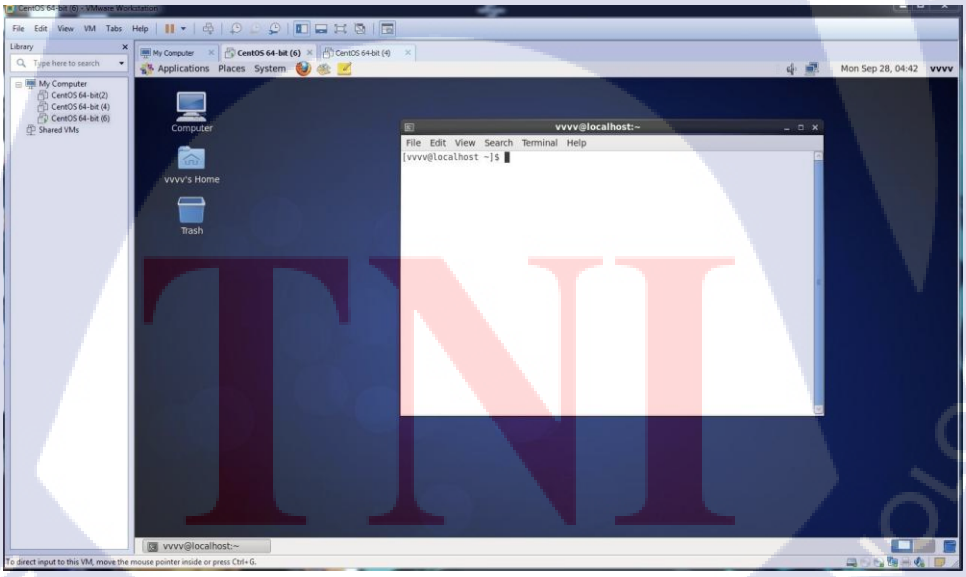


ภาพที่ 3.11 ขั้นตอนการลง Operating System CentOS Linux 6.5

6. ขั้นตอนการติดตั้งสำเร็จพร้อมใช้งาน



ภาพที่ 3.12 ขั้นตอนการลง Operating System CentOS Linux 6.5



ภาพที่ 3.13 ขั้นตอนการลง Operating System CentOS Linux 6.5

3.3 การเก็บรวบรวมข้อมูล

ในการจัดทำโครงงานในส่วนของการแสดงผลที่เป็นรายละเอียดต่างๆในโครงการจำเป็นต้องมีความแม่นยำและมีความถูกต้องจึงจำเป็นต้องทำการศึกษาด้วยตัวเองอย่างละเอียดก่อนที่จะเริ่มทำเพื่อให้ผลที่ออกมานั้น มีความถูกต้อง และมีความคลาดเคลื่อนน้อยที่สุด

3.3.1 โครงการ การแสดงผล Netflow

1. ศึกษารายละเอียดเกี่ยวกับ Netflow ต้องเข้าใจถึงหลักการทำงานเกี่ยวกับNetflow ว่าเกี่ยวข้องกับสิ่งใดและสามารถนำสิ่งนี้มาทำอะไรได้บ้าง พร้อมทั้งศึกษาอุปกรณ์ที่ช่วยในการแสดงผล Netflow ด้วย โดยการค้นคว้าหาความรู้เองยังช่วยเสริมสร้างทักษะการเรียนรู้ด้วยตนเองอีกด้วย

2. ศึกษาเกี่ยวกับ Nfdump เป็นเครื่องมือตัวหนึ่งที่ทำงานร่วมกับ Nfsen และยังมีหน้าที่ Process ข้อมูลอีกด้วย

3. ศึกษาเกี่ยวกับ Nfsen เป็นเครื่องมือหนึ่งที่ทำงานบน Web Base Front End โดยทำงานร่วมกับ Nfdump ซึ่งเป็น Tool ของ Netflow

4. คิดและวางแผนอุปกรณ์ที่จะใช้ทำการทดลอง โดยขั้นตอนนี้ต่อจากการศึกษาเครื่องมือที่จะต้องใช้ในการแสดงผล โดยต้องประสานงานไปยังผู้ที่เกี่ยวข้องกับโครงงาน เช่น พนักงานที่ปรึกษาเพื่อทำการตกลงถึงอุปกรณ์ที่จะต้องใช้และระยะเวลาที่จะใช้

3.4 ขั้นตอนการดำเนินงานที่นักศึกษาปฏิบัติงานหรือโครงงาน

ภายในระยะเวลาปฏิบัติงานสหกิจศึกษาตลอดระยะเวลา 4 เดือน ได้รับมอบหมายให้ทำงาน 2 อย่าง คือ การศึกษาเกี่ยวกับ board Arduino และ Netflow

1. Arduinoการศึกษาเกี่ยวกับ board Arduino นั้นใช้ภาษาพื้นฐานคือภาษา c โดยเป็นการใช้คำสั่งที่ไม่ยาก โดย board arduino สามารถสร้างผลงานได้หลากหลายมาก ไม่ว่าจะเป็น การสร้างหุ่นยนต์ หรือสร้างระบบเปิดปิดไฟเป็นต้น

2. Netflow การศึกษา Netflow ที่มีอยู่ใน internet เพื่อให้ทราบถึงกระบวนการทำงานของระบบค้นหาวิธีการที่ทำให้สามารถแสดงผลข้อมูล netflow บน web page ได้ โดยจะมีส่วนการตั้งค่าของ router และ collector(Netflow data)

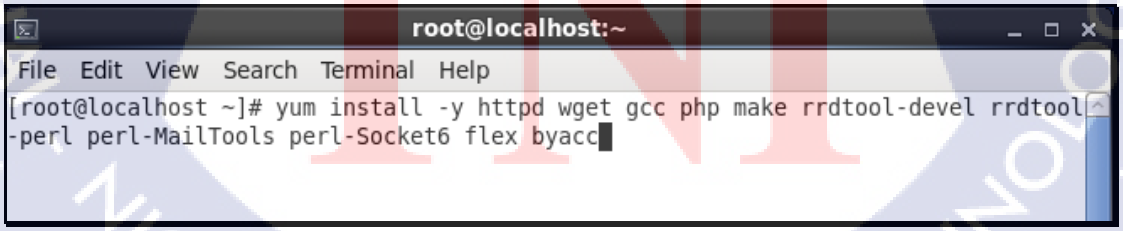
1) ค้นหาการตั้งค่าของ router การ export flow ข้อมูลต้องมีการตั้งค่าอะไรบ้าง เนื่องจากมีการไหลเข้าออกของ flow ข้อมูล (traffic) จึงจำเป็นต้องมีการ export ข้อมูลออกมายัง collector เพื่อนำไปประมวลผล และนำมาแสดงผลในภายหลัง
2) ค้นหาการตั้งค่าของ collector การแสดงผล จะต้องใช้ Tools อะไรบ้าง ในการแสดงผลบน web page
3) ลงมือปฏิบัติการตั้งค่าที่ได้สืบค้นข้อมูลมา

โดยการทดลอง การแสดงผลของโพรโทคอล Netflow จะใช้เครื่องมือในการแสดงผลที่ชื่อว่า Nfsen ซึ่งเป็นTool ที่ใช้แสดงผลบน Web Interface โดยการสร้างการแสดงผลจะทำดังนี้

1. ติดตั้ง Package ที่จำเป็นต้องใช้ ได้แก่

httpd	service web ,web server
php	เอาไว้รันภาษา php
wget	เอาไว้สำหรับdownload file จาก website
gcc	มีไว้เพื่อcompileภาษา c
rrdtool	คือฐานข้อมูล
perl-MailTools	เป็น moduleของ perl
perl-Socket6	เป็น moduleของ perl
flex	เป็น tool ที่ใช้ scanner เปลี่ยน input เป็น ตัวอักษร
byacc	เป็น compiler ชนิดหนึ่ง

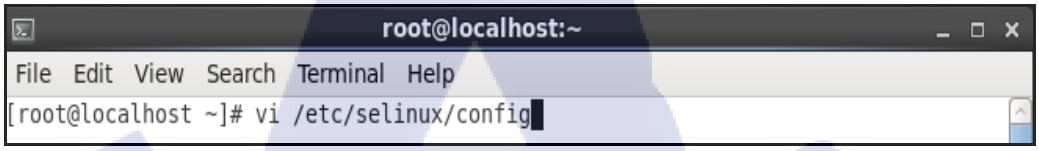
โดยใช้ command :yum install -y httpd php wget gcc make rrdtool-devel rrdtool-perl perl-MailTools perl-Socket6 flex byacc ตามภาพที่ 3.14



ภาพที่ 3.14 การใช้คำสั่ง yum ในการติดตั้ง

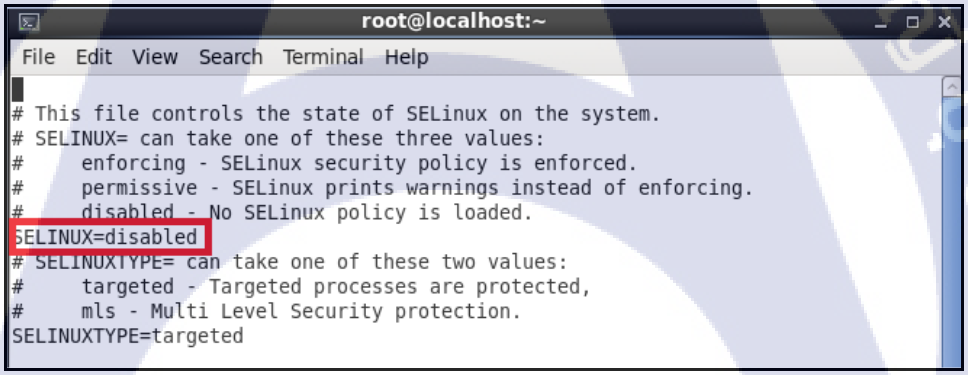
2. เปลี่ยนการตั้งค่า SELINUX จาก enforcing เป็น disabled

ทำการเข้าไปแก้ไขไฟล์ SELINUX โดยใช้ command : vi /etc/selinux/config ตามภาพที่ 3.15



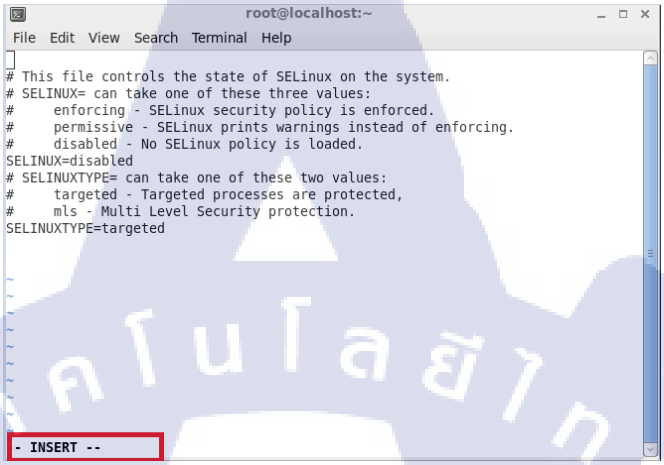
ภาพที่ 3.15 การใช้คำสั่ง vi เพื่อใช้แก้ไขไฟล์ SELINUX/config

เปลี่ยนค่าจาก enforcing เป็น disabled ตามภาพที่ 3.16



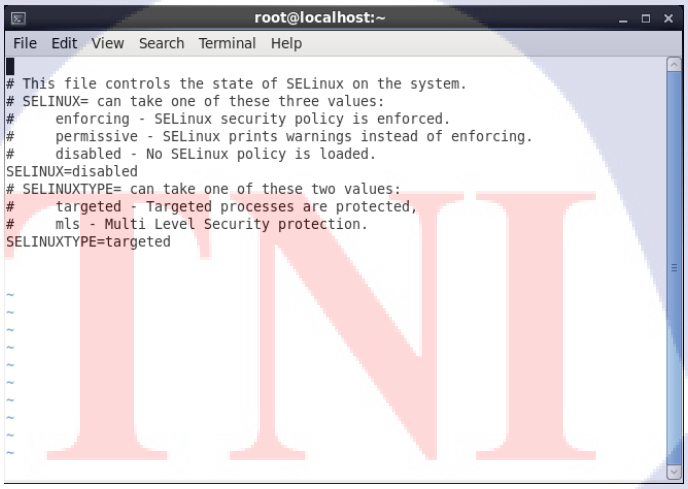
ภาพที่ 3.16 การแก้ไขไฟล์ SELINUX/config

กด Escape เพื่อออกจากโหมด insert ตามภาพที่ 3.17

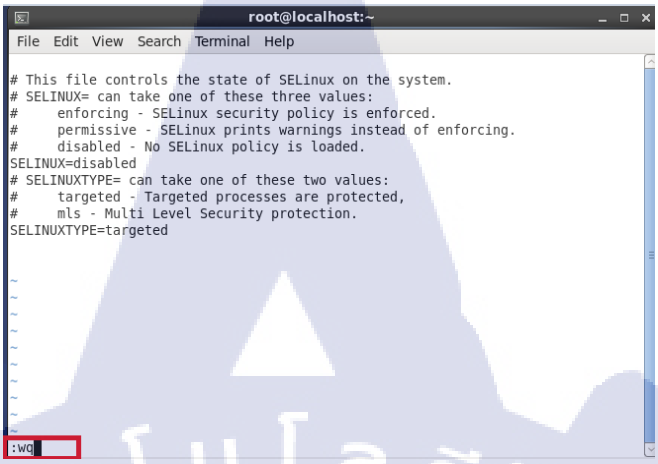


ภาพที่ 3.17 การแก้ไขไฟล์ SELINUX/config

หลังจากนั้นใช้ command " :wq " เพื่อเป็นการเซฟไฟล์และออกจากไฟล์ ตามภาพที่ 3.18 - 3.19



ภาพที่ 3.18 การแก้ไขไฟล์ SELINUX/config



ภาพที่ 3.19 การแก้ไขไฟล์ SELINUX/config

ทำการ reboot

3. เปิด service iptable rule

- เปิด service udp iptables,ip6tables port 9995iptables -I INPUT -p udp -m state --state NEW -m udp --dport 9995 -j ACCEPT
- ip6tables -I INPUT -p udp -m state --state NEW -m udp --dport 9995 -j ACCEPT
- เปิด service tcp iptables,ip6tables port 443,80
- iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
- ip6tables -I INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
- iptables -I INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
- ip6tables -I INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT

```
[root@localhost ~]# service iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
[root@localhost ~]#
```

ภาพที่ 3.20 service iptables save

```
[root@localhost ~]# service ip6tables save
ip6tables: Saving firewall rules to /etc/sysconfig/ip6table[  OK  ]
[root@localhost ~]#
```

ภาพที่ 3.21 service ip6tables save

4 .เปิด service httpd

- service httpd start
- chkconfig httpd on ตามภาพที่ 3.22

```
[root@localhost ~]# service httpd start
Starting httpd: httpd: Could not reliably determine the server's fully qualified
 domain name, using localhost.localdomain for ServerName
                                                           [  OK  ]
[root@localhost ~]# chkconfig httpd on
[root@localhost ~]#
```

ภาพที่ 3.22 เปิด service httpd

5. Install Nfdump & Nfsen

การ Install NfdumpDownload Nfdump มาก่อน โดยใช้ Command wget :wget http://downloads.sourceforge.net/project/nfdump/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz ตามภาพที่ 3.23

```
[root@localhost ~]# wget http://downloads.sourceforge.net/project/nfdump/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz
--2015-09-17 20:49:45--  http://downloads.sourceforge.net/project/nfdump/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz
Resolving downloads.sourceforge.net... 216.34.181.59
Connecting to downloads.sourceforge.net|216.34.181.59|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://jaist.dl.sourceforge.net/project/nfdump/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz [following]
--2015-09-17 20:49:45--  http://jaist.dl.sourceforge.net/project/nfdump/stable/nfdump-1.6.13/nfdump-1.6.13.tar.gz
Resolving jaist.dl.sourceforge.net... 150.65.7.130, 2001:df0:2ed:feed::feed
Connecting to jaist.dl.sourceforge.net|150.65.7.130|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 662006 (646K) [application/x-gzip]
Saving to: "nfdump-1.6.13.tar.gz"

100%[=======================================================================================>] 662,006     359K/s   in 1.8s

2015-09-17 20:49:48 (359 KB/s) - "nfdump-1.6.13.tar.gz" saved [662006/662006]

[root@localhost ~]#
```

ภาพที่ 3.23 การแสดงผล การ Download Nfdump

การแตกไฟล์ nfdump-1.6.13.tar.gz โดยใช้ command :

- tar -zxvf nfdump-1.6.13.tar.gz
- ย้ายไปยังไฟล์ที่แตกเมื่อสักครู่ ด้วย command cd :
- cd nfdump-1.6.13 ตามภาพที่ 3.24

```
[root@localhost ~]# cd nfdump-1.6.13
[root@localhost nfdump-1.6.13]#
```

ภาพที่ 3.24 การใช้ command cd เพื่อเข้า directory ที่กำหนด

- ./configure --enable-nfprofile --enable-nftrack
- make
- make install

การ install nfsen Download Nfdump มาก่อน โดยใช้ Command wget :wget http://downloads.sourceforge.net/project/nfsen/stable/nfsen-1.3.6p1/nfsen-1.3.6p1.tar.gz ตามภาพที่ 3.25

```
[root@localhost ~]# wget http://downloads.sourceforge.net/project/nfsen/stable/n
fsen-1.3.6p1/nfsen-1.3.6p1.tar.gz
--2015-09-21 01:12:13--  http://downloads.sourceforge.net/project/nfsen/stable/n
fsen-1.3.6p1/nfsen-1.3.6p1.tar.gz
Resolving downloads.sourceforge.net... 216.34.181.59
Connecting to downloads.sourceforge.net|216.34.181.59|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://jaist.dl.sourceforge.net/project/nfsen/stable/nfsen-1.3.6p1/nfs
en-1.3.6p1.tar.gz [following]
--2015-09-21 01:12:13--  http://jaist.dl.sourceforge.net/project/nfsen/stable/nf
sen-1.3.6p1/nfsen-1.3.6p1.tar.gz
Resolving jaist.dl.sourceforge.net... 150.65.7.130, 2001:df0:2ed:feed::feed
Connecting to jaist.dl.sourceforge.net|150.65.7.130|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 220620 (215K) [application/x-gzip]
Saving to: “nfsen-1.3.6p1.tar.gz”

100%[======================================>] 220,620     181K/s   in 1.2s

2015-09-21 01:12:15 (181 KB/s) - “nfsen-1.3.6p1.tar.gz” saved [220620/220620]
```

ภาพที่ 3.25 ภาพแสดงผล การ Download Nfsen

- การแตกไฟล์ nfsen-1.3.6p1.tar.gz โดยใช้ command :
- tar -zxvf nfsen-1.3.6p1.tar.gz
- ย้ายไปยังไฟล์ที่แตกเมื่อสักครู่ ด้วย command cd :
- cd nfsen-1.3.6p1
- ทำการ copy file nfsen-dist.conf แล้วเซฟเป็นอีกชื่อคือ nfsen.conf
- โดยใช้ command : cp etc/nfsen-dist.conf etc/nfsen.conf ตามภาพที่ 3.26

```
[root@localhost ~]# cd nfsen-1.3.6p1
[root@localhost nfsen-1.3.6p1]# cp etc/nfsen-dist.conf etc/nfsen.conf
[root@localhost nfsen-1.3.6p1]#
```

ภาพที่ 3.26 การใช้ Command cp ในการCopy file

6 .สร้าง Directory เพื่อเรียกใช้,สำรองไฟล์ที่จะติดตั้งไฟล์

- โดยการสร้างไฟล์หรือ Directory จะใช้ Command : mkdir –p /data/nfsen ตามภาพที่ 3.27

```
[root@localhost ~]# mkdir -p /data/nfsen
[root@localhost ~]#
```

ภาพที่ 3.27 การใช้ Command mkdir เพื่อสร้าง Directory

7. แก้ไขไฟล์ nfsen.conf ที่ path nfsen-1.3.6p1

โดยแก้ไขไฟล์ nfsen.conf โดยเข้าไปที่ ไดเรกทอรี่ nfsen-1.3.6p1 ก่อนด้วย command :

cd nfsen-1.3.6p1 หลังจากนั้นเข้า ไปแก้ไขไฟล์ยัง path ที่มีไฟล์ nfsen.conf โดย command : vi etc/nfsen.conf แก้ไขในจุดที่กำหนด ดังต่อไปนี้

- $HTMLDIR = "/var/www/nfsen/"; to /var/www/html/nfsen ตามภาพที่ 3.28 - 3.29

```
#
# NfSen html pages directory:
# All php scripts will be installed here.
# URL: Entry point for nfsen: http://<webserver>/nfsen/nfsen.php
$HTMLDIR    = "/var/www/nfsen/";
```

ภาพที่ 3.28 ภาพแสดงผลก่อนการแก้ไขตัวแปร $HTMLDIR

```
#
# NfSen html pages directory:
# All php scripts will be installed here.
# URL: Entry point for nfsen: http://<webserver>/nfsen/nfsen.php
$HTMLDIR    = "/var/www/html/nfsen/";
```

ภาพที่ 3.29 ภาพแสดงผลหลังการแก้ไขตัวแปร $HTMLDIR

- $WWWUSER to apache , $WWWGROUP to apache ตามภาพที่ 3.30 - 3.31

```
# Note: This user must be in group $WWWGROUP, otherwise nfcapd
#       is not able to write data files!
$USER    = "netflow";

# user and group of the web server process
# All netflow processing will be done with this user
$WWWUSER  = "www";
$WWWGROUP = "www";
```

ภาพที่ 3.30 ภาพแสดงผลก่อนการแก้ไขตัวแปร $USER , $WWWUSER , $WWWGROUP

```
# Note: This user must be in group $WWWGROUP, otherwise nfcapd
#       is not able to write data files!
$USER    = "apache";

# user and group of the web server process
# All netflow processing will be done with this user
$WWWUSER  = "apache";
$WWWGROUP = "apache";
```

ภาพที่ 3.31 ภาพแสดงผลหลังการแก้ไขตัวแปร $USER , $WWWUSER , $WWWGROUP

- uncomment $EXTENSIONS = 'all'; or add $EXTENSIONS = 'nsel'; ตามภาพที่ 3.32 -3.33

```
# list of extensions for each collector. See argument -T
# for nfcapd(1) for more detailes.
# defaults to empty -> compatible to nfdump-1.5.8
# $EXTENSIONS = '';
# Example:
# $EXTENSIONS = 'all';
# $EXTENSIONS = '+3,+4';
```

ภาพที่ 3.32 ภาพแสดงผลก่อนการ Uncommand $EXTENSION = 'all' และเพิ่มตัวแปร $EXTENSIONS = 'nsel'

```
# list of extensions for each collector. See argument -T
# for nfcapd(1) for more detailes.
# defaults to empty -> compatible to nfdump-1.5.8
# $EXTENSIONS = '';
# Example:
$EXTENSIONS = 'all';
$EXTENSIONS = 'nsel';
# $EXTENSIONS = '+3,+4';
#
```

ภาพที่ 3.33 ภาพแสดงผลหลังการ Uncommand $EXTENSION = 'all' และเพิ่มตัวแปร $EXTENSIONS = 'nsel'

- comment peer1 ,peer2 ตามภาพที่ 3.34 - 3.35

```
%sources = (
    'upstream1'    => { 'port' => '9995', 'col' => '#0000ff', 'type' => 'netflow' },
    'peer1'        => { 'port' => '9996', 'IP' => '172.16.17.18' },
    'peer2'        => { 'port' => '9996', 'IP' => '172.16.17.19' },
);
```

ภาพที่ 3.34 ภาพแสดงผลก่อนการ Comment peer1 ,peer2

```
%sources = (
    'upstream1'    => { 'port' => '9995', 'col' => '#0000ff', 'type' => 'netflow' },
  #  'peer1'        => { 'port' => '9996', 'IP' => '172.16.17.18' },
  #  'peer2'        => { 'port' => '9996', 'IP' => '172.16.17.19' },
);
```

ภาพที่ 3.35 แสดงผลหลังการ Comment peer1 ,peer2

- :wq เพื่อ เซฟ และ ออกจากไฟล์ nfsen.conf

8. ติดตั้งไฟล์ที่แก้ไขเมื่อสักครู่นี้ด้วยcommand ที่อยู่ใน path nfsen-1.3.6p1 : ./install.pl etc/nfsen.conf ตามภาพที่ 3.36

```
[root@localhost nfsen-1.3.6p1]# vi etc/nfsen.conf
[root@localhost nfsen-1.3.6p1]# ./install.pl etc/nfsen.conf
Check for required Perl modules: All modules found.
Upgrade from version '1.3.6p1' installed at Tue Aug 18 21:18:38 2015
Setup NfSen:
Version: 1.3.6p1: $Id: install.pl 53 2012-01-23 16:36:02Z peter $

Perl to use: [/usr/bin/perl]
```

ภาพที่ 3.36 แสดงการใช้ command ./install เพื่อติดตั้งไฟล์ nfsen.conf

9. เปิด Service Nfsen

- ใช้ Command : cd เพื่อเข้าไปยัง Pathที่ได้ติดตั้งจากไฟล์ nfsen.conf

```
#
# Required for default layout
$BASEDIR = "/data/nfsen";
```

ภาพที่ 3.37 แสดง Directory ที่ถูกตั้งค่าไว้ในไฟล์ nfsen.conf

- เข้าไปที่ Path bin โดยใช้ Command : cd /data/nfsen/bin
- เปิด Service Nfsen โดยใช้ Command : ./nfsen start ตามภาพที่ 3.38

```
[root@localhost ~]# cd /data/nfsen/bin
[root@localhost bin]# ./nfsen start
Starting nfcapd:(upstream1)[2820]
Starting nfsend.
[root@localhost bin]#
```

ภาพที่ 3.38 แสดงสถานะ ของ Nfsen

10. Restart Service Network

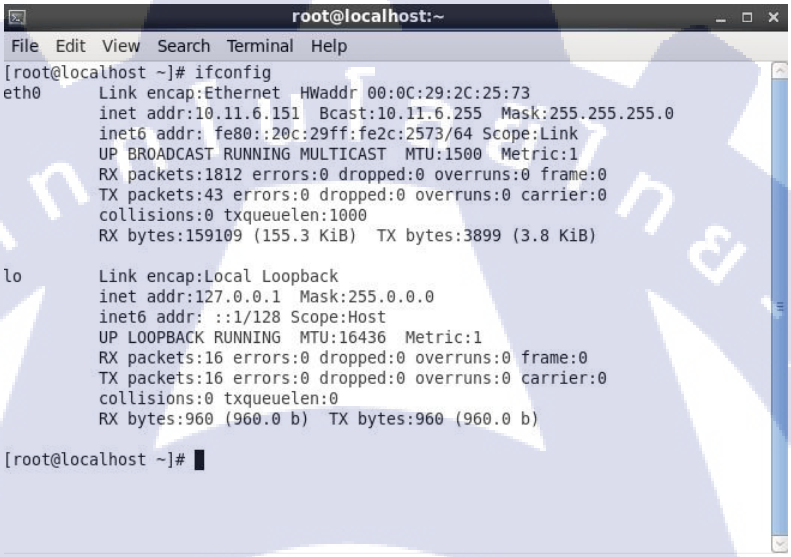
ทำการ Restart Service Network โดยใช้ Command : service network restart ตามภาพที่ 3.39

```
[root@localhost ~]# service network restart
Shutting down interface eth0:  Device state: 3 (disconnected)
                                                           [  OK  ]
Shutting down loopback interface:                          [  OK  ]
Bringing up loopback interface:                            [  OK  ]
Bringing up interface eth0:  Active connection state: activating
Active connection path: /org/freedesktop/NetworkManager/ActiveConnection/1
state: activated
Connection activated
                                                           [  OK  ]
[root@localhost ~]#
```

ภาพที่ 3.39แสดงสถานะ Service Network

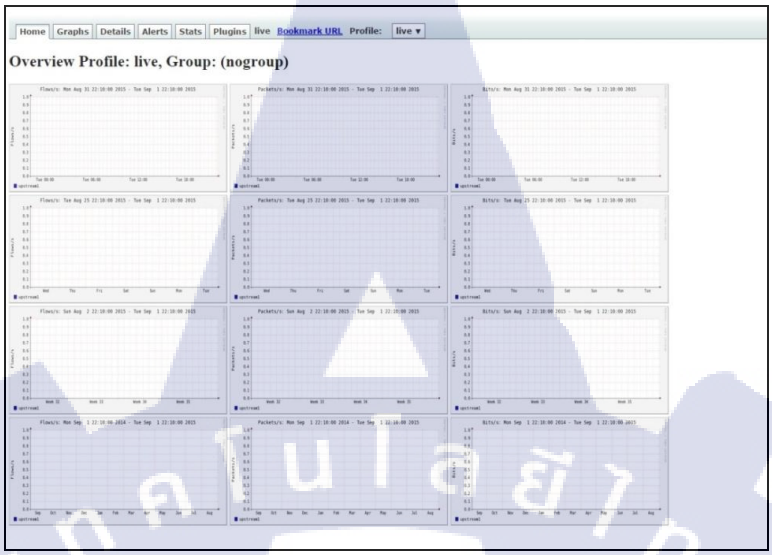
11.ตรวจสอบ IP Server

หลังจากการตั้งค่าทั้งหมด ให้ทดสอบโดยการเข้าไปยัง Browser โดยกำหนดให้ URL เป็นดังนี้ :http://<eth0 IP>/nfsen/nfsen.phpโดยการเช็คหมายเลขของ Collector คือ : ifconfig ตามภาพที่ 3.40



ภาพที่ 3.40 ภาพแสดงผลการใช้ command ifconfig

ทั้งนี้หมายเลย IP Server คือ 10.11.6.151 จะได้ URL ดังนี้ http://10.11.6.151/nfsen/nfsen.php เราจะได้กราฟเปล่าๆมา ดังภาพที่ 3.41



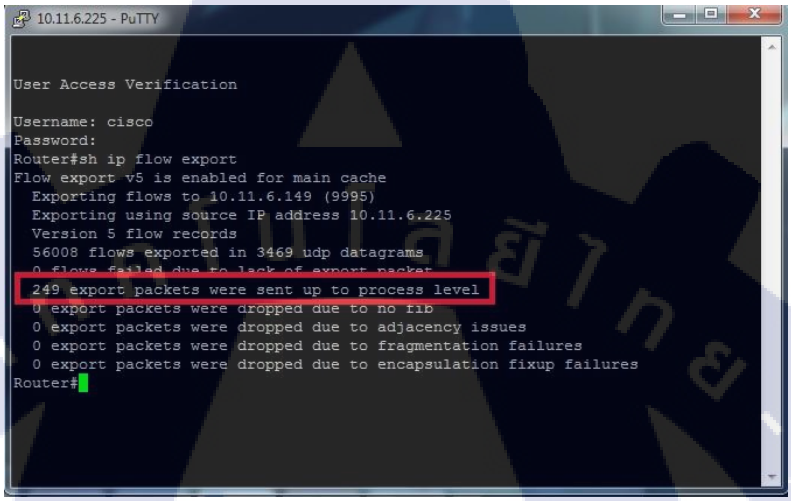
ภาพที่ 3.41 ภาพรวม nfsen

หลังจากการตั้งค่า Collector (Netflow Data) สำเร็จแล้ว จำเป็นต้องมีการตั้งค่าของ Router เพื่อให้ได้มาซึ่งข้อมูลที่จะนำมาแสดงผล

วิธีการ Config Router

- router#configure terminal
- router(config)#interface FastEthernet 0/0
- router(config-if)#ip route-cache flow
- router(config-if)#exit
- router(config)#ip flow-export destination 10.199.15.103 2055
- router(config)#ip flow-export version 5
- router(config)#ip flow-cache timeout active 1
- router(config)#ip flow-cache timeout inactive 15
- router(config)#snmp-server ifindex persist
- router(config)#end
- router#write

หลังจากการตั้งค่าแล้วให้ลองเช็คว่าโฟล์วถูกส่งออกมาหรือไม่ด้วย command :sh ip flow export ตามภาพที่ 3.42



ภาพที่ 3.42 แสดงค่า flow ที่ถูกส่งออก

สังเกตในภาพที่มีกรอบสีแดง มีการรายงานว่าโฟลถูกส่งออกมาเรียบร้อยแล้ว

บทที่ 4

ผลการดำเนินงานการวิเคราะห์และสรุปผลต่างๆ

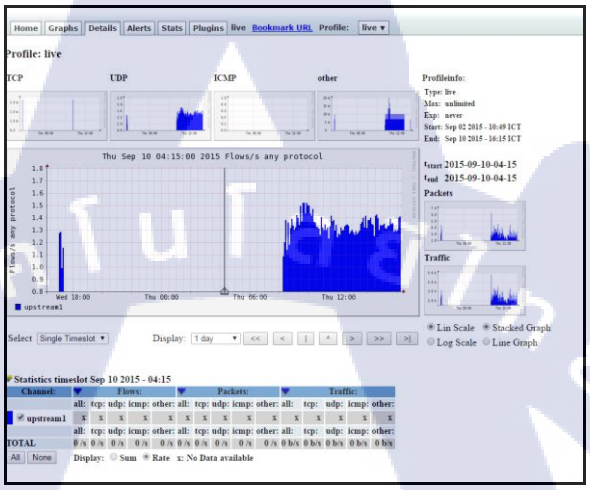
4.1 ผลการดำเนินงาน

ระบบเครือข่ายเทคโนโลยี Netflow ซึ่งเป็นข้อมูล Traffic ที่ไหลผ่านในระบบเน็ตเวิร์คหรือเกตเวย์ เราสามารถนำข้อมูลที่มีใน Netflow มาใช้ประโยชน์ในการวิเคราะห์หาสาเหตุ หรือนำไปประยุกต์ใช้อะไรได้บ้าง หรือตรวจสอบสถานะต่างๆในการใช้งาน ซึ่ง Netflow คือข้อมูลเชื่อมต่อกันระหว่างผู้รับ-ผู้ส่ง ถ้าเราดึงข้อมูลจาก Netflow ที่ไหลมาตลอดเวลาหรือเก็บไว้ มาวิเคราะห์ข้อมูล โดยในโครงการนี้ได้นำเครื่องมือในการแสดงผลที่ชื่อว่า Nfsen มาช่วยในการตรวจจับและเป็นเครื่องมือหลักในโครงการ ดังภาพที่ 4.1

ภาพที่ 4.1 ภาพรวมของ Nfsen

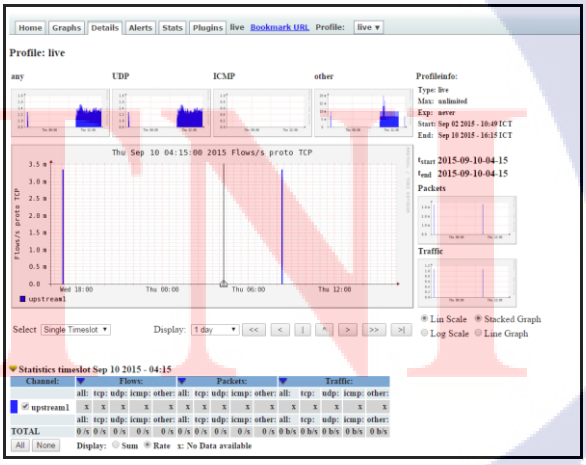
- โดยกราฟฝั่งซ้ายจะเป็นการแสดงผลของflows
- กราฟตรงกลางจะเป็นการแสดงผลของpacket
- กราฟฝั่งขวาจะเป็นการแสดงผลของtraffic

- ด้านบนสุดจะเป็นการรายงานแบบวันไล่ลงมาจะเป็นรายสัปดาห์ ถัดไปก็จะเป็นเดือ
- Any Protocol เป็นการแสดงรายละเอียดภาพรวมของโพรโทคอล ออกมาในรูปแบบกราฟ ดังภาพที่ 4.2



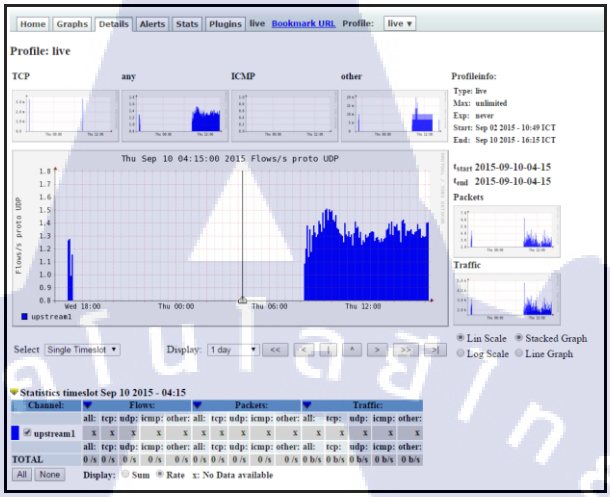
ภาพที่ 4.2 ภาพกราฟของ Any Protocol

- TCP Protocol การแสดงผลของ Packet TCP ในช่วงเวลานั้น ดังภาพที่ 4.3



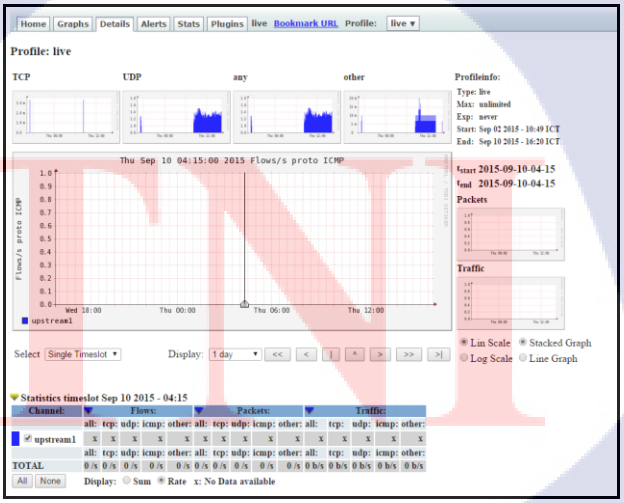
ภาพที่ 4.3 ภาพกราฟของ TCP Protocol

- UDP Protocol แสดงผล Packet ที่ผ่านเข้ามาในระบบ ในช่วงเวลานั้น ดังภาพที่ 4.4



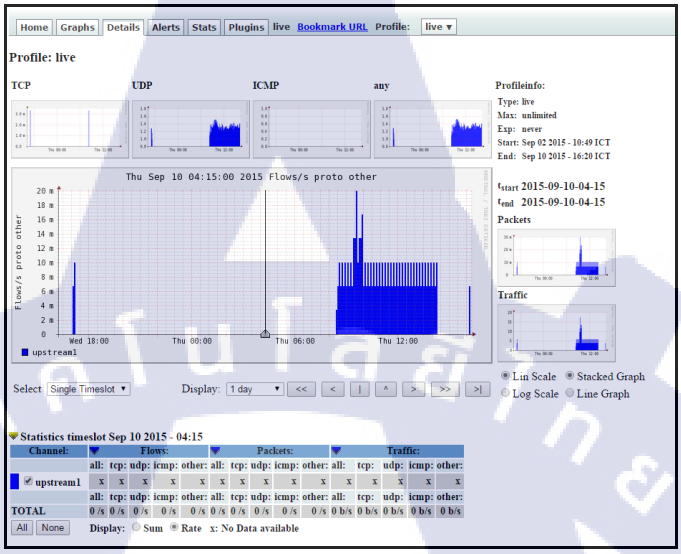
ภาพที่ 4.4 ภาพกราฟของ UDP Protocol

- ICMP Protocol แสดงผล Packet ICMP ที่ผ่านเข้ามาในระบบ ในช่วงเวลานั้น ดังภาพที่ 4.5



ภาพที่ 4.5 ภาพกราฟของ ICMP Protocol

- Other Protocol การแสดงผลของโพรโทคอลอื่นๆ ดังภาพที่ 4.6



ภาพที่4.6 ภาพกราฟของ Other Protocol

4.2 ผลการวิเคราะห์ข้อมูล

จากการวิเคราะห์ข้อมูลเกี่ยวกับการแสดงผล Traffic ของโพรโทคอล Netflow ในบทที่ 3 ซึ่งได้กล่าวถึงจุดมุ่งหมายว่าสามารถสร้างประโยชน์ให้แก่ผู้ดูและระบบได้มากเพียงไหน โดยการสร้างกราฟจะเป็นการที่ทำให้ผู้ดูแลระบบเข้าใจได้ง่ายทำให้มีความรวดเร็วในการตัดสินใจมากยิ่งขึ้น

4.3 วิจารณ์ข้อมูลโดยเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์และจุดมุ่งหมายการปฏิบัติงานและการจัดทำโครงการ

หลังจากการทดสอบการแสดงผลของโพรโทคอล Netflow แล้ววิเคราะห์และเปรียบเทียบผลที่ได้รับกับวัตถุประสงค์ที่ตั้งไว้ ซึ่งถือว่าผลลัพธ์ออกมาเป็นที่น่าพึงพอใจในระดับหนึ่ง เนื่องจากสามารถแสดงผลผ่าน web Interface ได้ แต่ก็ยังพบจุดบกพร่องที่ยังควรปรับปรุงอยู่บ้างเนื่องจากใช้เวลาในการศึกษาโพรโทคอล Netflow เป็นเวลานาน ประจวบเหมาะไม่มีพื้นฐานทางด้านการใช้งาน Linux จึงทำให้ใช้เวลานานเกินไปผลงานจึงออกมาไม่ดีเท่าที่ควร

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

จากการปฏิบัติงานสหกิจศึกษาที่บริษัท ทริปเปิลที บรอดแบนด์ จำกัด (มหาชน) เป็นระยะเวลารวมทั้งสิ้น 4 เดือน งานหลักที่ได้รับมอบหมายคือการแสดงผลข้อมูลทราฟิกโพรโทคอล Netflow โดยการแสดงผลนี้ได้ใช้ tool ที่ชื่อว่า nfsen ซึ่งเป็น tool ที่แสดงผลผ่าน web page มาช่วยในการแสดงผล

การตรวจสอบในโครงการนี้สามารถดูผ่านเว็บอินเตอร์เฟส สามารถเก็บรวบรวมข้อมูลการใช้งานเอาไว้เพื่อใช้วิเคราะห์สถิติการใช้งานได้ในภายหลังอีกทั้งยังช่วยตรวจสอบถึงพฤติกรรมการใช้งานเพื่อวางแผนการให้บริการให้ดียิ่งขึ้นได้อีกด้วย

ในส่วนของการสร้างระบบการรับข้อมูลโฟล์วจาก เร้าเตอร์มายัง server (collector) มีปัญหาในส่วนของการแสดงผลข้อมูลยังไม่ถูกต้อง เนื่องจากการเชื่อมต่อระบบเป็นเพียงระบบจำลอง ทำให้การส่งข้อมูลผิดพลาดและประมวลผลออกมาไม่ถูกต้อง 100%

5.2 แนวทางการแก้ไขปัญหา

การทดลองผลการทำงานของระบบแสดงผล Netflow โดยใช้ Nfsen ควรจะมีการปฏิบัติโดยใช้อุปกรณ์จริงเพื่อให้ได้การแสดงผลข้อมูลออกไม่อย่างถูกต้องและครบถ้วน

5.3 ข้อเสนอแนะจากการดำเนินงาน

การทำงานที่เกี่ยวข้องกับระบบเครือข่ายโพรโทคอล Netflow จะต้องมีพื้นฐานทางด้าน Network ในระดับหนึ่งและ ความเข้าใจพื้นฐาน Linux ความเข้าใจเกี่ยวกับกับโพรโทคอล Netflow อีกด้วยในระดับนึง รวมทั้งหลักการทำงานของเร้าเตอร์อีกด้วย

เอกสารอ้างอิง

บดินทร์ สืบสุดิน, 2556, **การเปรียบเทียบลักษณะของโพรโทคอล Netflow และ Flexible Netflow โดยใช้ซอฟต์แวร์ Scrutinizer** [Online], Available http://www.sit.kmutt.ac.th/tqf/is_report/pdf56/55440325.pdf [1 สิงหาคม 2558]

ภวัต ทรัพย์มงคล,2554, **ระบบวิเคราะห์เพื่อตรวจจับความผิดปกติและบริหารจัดการเครือข่ายโดยใช้ข้อมูลจาก Netflow**, วิทยาศาสตรมหาบัณฑิต, เทคโนโลยีสารสนเทศ, บัณฑิตวิทยาลัย, มหาวิทยาลัยเทคโนโลยีมหานคร

Cisco Systems, Inc., 2012, **ConfiguringNetflow and Netflow Data Export** [Online], Available :http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/12-4t/nf-12-4t-book/cfg-nflow-data-expt.html [2015,Aug 5]

Cisco Systems, Inc., 2012, **Introduction to Cisco IOS NetFlow -A Technical Overview** [Online], Available http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-netflow/prod_white_paper0900aecd80406232.html [2015,July 1]

Nick Buraglio, 2014, **Installnfsen and nfdump on CentOS 6.5 for netflow and or sflow collection** [Online], Available :https://www.forwardingplane.net/2014/01/install-nfsen-and-nfdump-on-centos-6-5-for-netflow-and-or-sflow-collection [2015,July 1]

ประวัติผู้จัดทำโครงงาน

ชื่อ - สกุล นายชูเดช สุรบูรณ์กุล

วัน เดือน ปีเกิด 5 พฤศจิกายน 2536

ประวัติการศึกษา

ระดับประถมศึกษา ประถมศึกษาตอนปลาย พ.ศ. 2548
โรงเรียนพระยามนธาตุราชศรีพิจิตร์

ระดับมัธยมศึกษา มัธยมศึกษาตอนปลาย พ.ศ. 2551
โรงเรียนมัธยมวัดสิงห์

ระดับอุดมศึกษา คณะเทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ พ.ศ. 2555
สถาบันเทคโนโลยีไทย-ญี่ปุ่น

ทุนการศึกษา - ไม่มี -

ประวัติฝึกอบรม - ไม่มี -

ผลงานที่ได้รับการตีพิมพ์ - ไม่มี -