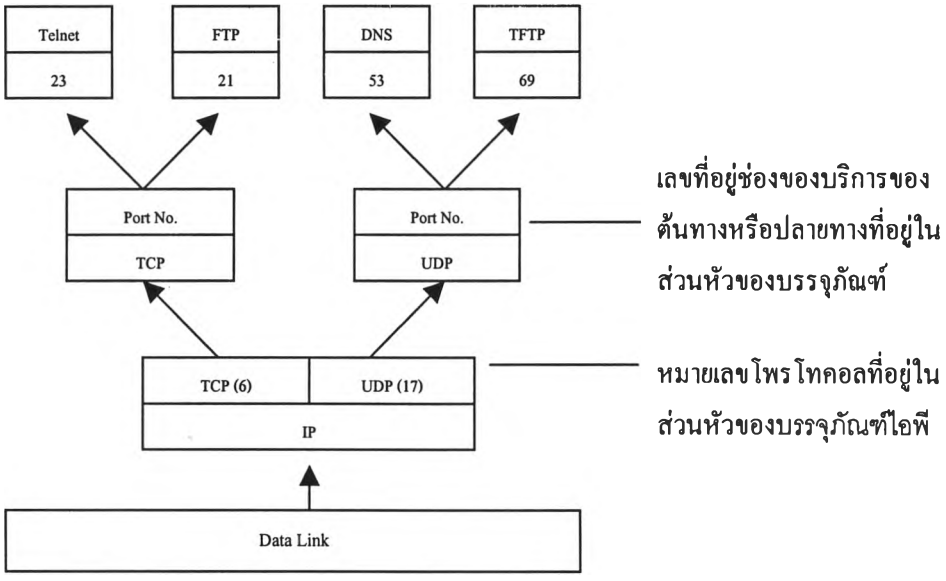
บทที่ 2

ลักษณะและวิธีการเก็บสถิติการใช้งานข้อมูลผ่านระบบเครือข่าย

ข้อมูลที่ถูกรับและส่งผ่านระบบเครือข่ายอินเทอร์เน็ตจะใช้โพรโทคอลแบบทีซีพี/ไอพี (TCP/IP) (J. Postel, 1981 : 2) ซึ่งจะมีการทำงานโดยมีชั้นของการสื่อสารที่จัดเป็นมาตราฐานของ ไอเอซโอ (ISO) 7 ชั้น โดยดังรูปที่ 2.1 บรรจุภัณฑ์ไอพีจะถูกส่งจากชั้นเส้นทางเชื่อมโยงข้อมูล (Datalink Layer) เข้าสู่ชั้นเครือข่าย (Network Layer) ซึ่งที่ชั้นนี้จะมีการดูที่ส่วนหัวของบรรจุภัณฑ์ไอพี โดยดูที่หมายเลขโพรโทคอล เพื่อใช้ในการจำแนกบรรจุภัณฑ์ไอพีว่าเป็นโพรโทคอลใด แล้วส่งไปยังชั้นขนส่งข้อมูล (Transport Layer) ซึ่งที่ชั้นนี้จะมีการดูที่ส่วนหัวของบรรจุภัณฑ์ไอพี โดยดูที่เลขช่องบริการต้นทางและเลขช่องบริการปลายทาง เพื่อดูชนิดของการให้บริการซึ่งจำแนกตามอาร์เอฟซี 1700 (J. Reynolds and J. Postel, 1994 : 7-228) ก่อนที่จะส่งไปยังชั้นต่อๆไป



รูปที่ 2.1 แสดงความสัมพันธ์ของการเชื่อมต่อโดยใช้ ทีซีพี/ไอพี

การจัดเก็บสถิติการใช้งานการไหลของการลำเลียงข้อมูล (Traffic Flow accounting) ถูกกำหนดเขียนขึ้นโดย N. Brownlee (1997 : 4-32) ในอาร์เอฟซี เลขที่ 2063 ชื่อหัวข้อ "Traffic Flow Measurement "

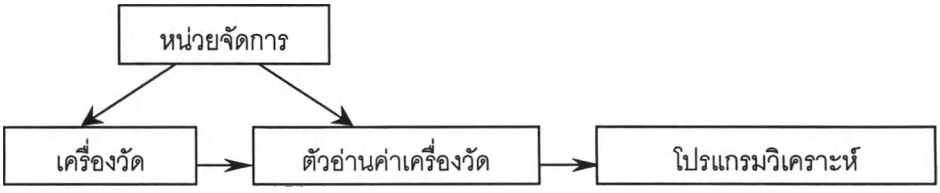
คำจำกัดความของ การไหลของการลำเลียงข้อมูล (Traffic flow) คือการติดต่อที่ถูกสมมติขึ้นเพื่อแทนการกระทำ (Activity) บางอย่างที่เกิดขึ้นบนเครือข่าย โดยมองว่าการไหล (flow) เป็นส่วนหนึ่งที่จะเกิดขึ้นในการลำเลียงของข้อมูลโดยมีเวลาเริ่มต้นของการไหลและเวลาสิ้นสุดของการไหล ซึ่งการไหลจะถูกสร้างขึ้นโดย Accountable Entities

Accountable entities จะประกอบด้วย 2 ส่วน คือ

ผู้ที่หรือสิ่งที่มีหน้าที่เกี่ยวกับ การกระทำบางอย่างบนเครือข่าย ซึ่งอาจจะเป็น ผู้ใช้ เครื่อง เครือข่าย กลุ่มของเครือข่าย ฯลฯ ซึ่งจะเป็นอะไรนั้นขึ้นอยู่กับคุณลักษณะของแต่ละโพรโทคอลที่กำหนดโดยเครื่องวัด เช่น เลขที่อยู่ของผู้ส่งและผู้รับ

สิ่งที่สะท้อนปริมาณที่เกิดการกระทำกิจกรรมที่เกิดขึ้น ตั้งแต่เวลาเริ่มต้นที่เกิดการไหล จนถึงระยะเวลาที่การไหล นั้นสิ้นสุดลง เช่น จำนวนบรรจุภัณฑ์ จำนวนไบต์ ฯลฯ

สำหรับการวัดการไหลของการลำเลียงซึ่งร่างจาก งานร่าง ของ OSI accounting model ซึ่งสามารถนำไปประยุกต์ใช้กับ โพรโทคอลและโปรแกรมประยุกต์ (Application Program) บนชั้นของเครือข่ายใดๆก็ได้ซึ่งประกอบไปด้วยส่วนต่างๆดังรูปที่ 2.2



รูปที่ 2.2 ส่วนประกอบของการวัดการไหลของการลำเลียง

2.1. ส่วนประกอบของการวัดการไหลของการลำเลียง

2.1.1. เครื่องวัด (Meter)

จะทำการนับคุณลักษณะ เช่น จำนวนบรรจุภัณฑ์ หรือ ไบต์ และทำการแบ่งจำพวกและจัดตามความสัมพันธ์ระหว่างคุณลักษณะ (Attribute) ที่เกิดขึ้น เช่น ที่อยู่ต้นทาง (Source Address) และที่อยู่ปลายทาง (Destination Address) ช่องสัญญาณต้นทาง (Source) และช่องสัญญาณปลายทาง (Destination) เพื่อให้ได้ Accountable Entities เครื่องวัดจะติดตั้งอยู่ ณ ตำแหน่งตรวจวัดที่กำหนดโดยผู้ปฏิบัติการเครือข่าย ซึ่งแต่ละเครื่องวัดจะทำการเลือก ระเบียนของการกระทำบนเครือข่าย ตามที่ได้รับการตั้งค่าการปรับแต่ง หลังจากการประมวลผล (Process) และสรุปข้อมูลแล้วจะได้ข้อมูลที่สามารถนำไปใช้งานได้ (Usage Data)

สำหรับเครือข่ายที่ใช้โพรโทคอล แบบ Connectionless เช่น โพรโทคอลไอพี ซึ่งไม่สามารถระบุได้ว่า บรรจุภัณฑ์แต่ละอันนั้นเป็นของกระแสข้อมูล (Stream) ใด เนื่องจากแต่ละ บรรจุภัณฑ์จะเป็นอิสระจากกันโดยสมบูรณ์ เครื่องวัดจะมีส่วนหนึ่งที่เป็นเซตของกฎ เพื่อกำหนดส่วนที่น่าสนใจของการไหล ซึ่งเป็นค่าของคุณลักษณะ ซึ่งได้มาจากบรรจุภัณฑ์ ที่สังเกตได้ และจะใช้ค่าที่ได้นี้ เพื่อดูว่ามันอยู่ในการไหลใด โดยจะทำการแยกบรรจุภัณฑ์เป็นหมวดหมู่ตามการไหล แบบนี้จะช่วยให้ประหยัดและสามารถนำไปใช้ได้จริงอย่างมีประสิทธิภาพในการวัดการลำเลียงของเครือข่าย และสามารถให้เหตุผลสรุปแก่ accountable entities

2.1.2. ตัวจัดการเครื่องวัดการไหลของการลำเลียง

ตัวจัดการเครื่องวัดการไหลของการลำเลียง เป็นโปรแกรมประยุกต์เพื่อทำการปรับแต่งค่า ของตัววัดการไหลของการลำเลียง และควบคุมตัววัดการไหลของการลำเลียง โดยการใช้ data requirement จากโปรแกรมวิเคราะห์ผล (analysis application) เพื่อกำหนด configuration ที่เหมาะสมแก่แต่ละตัววัด (Meter) และการปฏิบัติการ (Operation) ที่เหมาะสมแก่แต่ละตัวอ่านเครื่องวัด (meter reader) ทำให้เป็นการสะดวกที่จะให้ทั้งฟังก์ชัน (Function) ของตัวอ่านเครื่องวัดและ manager ใช้ network entity เดียวกัน

2.1.3. ตัวอ่านเครื่องวัด

จะทำการจัดส่งข้อมูลที่สามารถนำไปใช้งานได้จากเครื่องวัดเพื่อส่งให้แก่โปรแกรมวิเคราะห์ผล

2.1.4. โปรแกรมวิเคราะห์ผล

โปรแกรมวิเคราะห์ผล จะทำการประมวลผลจากข้อมูลที่จากตัวอ่านเครื่องวัดเพื่อให้ได้ข้อมูลสารสนเทศ (Information) ที่ต้องการ และทำการออกรายงาน (Report) ซึ่งจะเป็นประโยชน์ทางวิศวกรรมทางเครือข่าย และ การบำรุงรักษาเครือข่าย

2.2. การจัดเก็บข้อมูลการใช้งานสายสัญญาณโดยใช้โพรโทคอล เอสเอ็นเอ็มพี (SNMP)

ข้อมูลในอุปกรณ์เครือข่ายส่วนใหญ่แล้วจะมีการเก็บค่าเอ็มไอบี (Management Information Base) ซึ่งจะเก็บค่าสถานะเพื่อนำไปใช้ในการบริหารจัดการเครือข่ายโดยใช้โพรโทคอลเอสเอ็นเอ็มพี โดยในค่าเอ็มไอบี นี้จะมีค่าอยู่ชนิดหนึ่งเรียก ตัวนับการลำเลียงข้อมูล (Traffic counter) ซึ่งจะทำหน้าที่ในการตรวจนับปริมาณข้อมูลที่ถูกส่งเข้าและออกจากช่องสัญญาณต่างๆในอุปกรณ์สื่อสาร เราสามารถนำเอาค่านี้มาทำการเก็บสถิติการใช้งานอินเทอร์เน็ตโดย อ่านค่าตัวนับการลำเลียงข้อมูลนี้จากช่องสัญญาณที่เชื่อมต่อกับเกตเวย์ต่างประเทศเพื่อดูปริมาณการใช้งานช่องสัญญาณในช่วงเวลาต่างๆ

โปรแกรมเอ็มอาร์ทีจี (Multi router traffic grapher) เป็นโปรแกรมซึ่งจะอ่านค่า traffic couter นี้ โดยผ่านโพรโทคอลเอสเอ็นเอ็มพี โดยทุก ๆ ช่วงเวลาหนึ่ง เช่นทุก ๆ 5 นาที จะทำการอ่านค่าตัวนับการลำเลียงข้อมูล และมาเปรียบเทียบกับเมื่อ 5 นาที ที่ผ่านมาว่าใน 5 นาทีนี้มีปริมาณข้อมูลถูกรับและส่งผ่านสัญญาณนั้น ๆ เป็นเท่าไร และจะทำการคำนวณหาอัตราการใช้งานช่องสัญญาณ (Bandwidth) และทำการวาดกราฟ เพื่อแสดงผลได้ สามารถหาโปรแกรมเอ็มอาร์ทีจีได้จากที่

http://ee-staff.ethz.ch/~oetiker/webtools/mrtg/mrtg.html

2.2.1. ข้อดี

2.2.1.1. อุปกรณ์เครือข่ายส่วนใหญ่สนับสนุนการทำงานของโพรโทคอลเอสเอ็นเอ็มพี ในการจัดการเครือข่าย และมีตัวนับการลำเลียงข้อมูลอยู่ทำให้สามารถใช้อุปกรณ์เครือข่ายนั้นเป็นตัววัดปริมาณการใช้งานได้

2.2.1.2. เหมาะการบริหารจัดการเครือข่าย โดยสามารถตรวจหาช่องสัญญาณที่มีการทำงานผิดปกติหรือหยุดการทำงานได้

2.2.1.3. มีข้อมูลที่ประมวลผลน้อยทำให้ค่าใช้จ่ายในการดำเนินการต่ำ

2.2.2. ข้อเสีย

2.2.2.1. มีข้อมูลสารสนเทศน้อย คือมีเพียงแต่ปริมาณการใช้งานของแต่ละช่องสัญญาณในอุปกรณ์เครือข่ายเท่านั้น

2.3. การจัดเก็บข้อมูลการใช้งานสายสัญญาณโดยใช้เครื่องคอมพิวเตอร์เป็นตัวนับ

มีการจัดเก็บข้อมูลโดยนำเอาเครื่องคอมพิวเตอร์ติดตั้งบนสื่อสัญญาณ (Media) ระหว่างทางและจะคอยดักฟังการส่งและรับข้อมูลบนสื่อสัญญาณนั้นๆ

โปรแกรม เนทราเมท (NeTraMet) เป็นโปรแกรมในการตรวจนับข้อมูลที่มีการรับส่งผ่านเครือข่ายโดยทำงานบนเครื่องคอมพิวเตอร์ที่มีระบบปฏิบัติการ ดอส (DOS) และยูนิกซ์ โดยจะทำการดักจับข้อมูลที่วิ่งอยู่บนสื่อสัญญาณแบบอินเทอร์เน็ต สามารถหาโปรแกรมนี้ได้จาก http://www.auckland.ac.nz/net/Accounting/ntm.Release.not.html

2.3.1. ข้อดี

2.3.1.1. ง่ายต่อการเลือกว่าต้องการตรวจจับบริเวณใดๆ

2.3.1.2. ไม่ต้องการอุปกรณ์เครือข่ายที่มีความสามารถสูงในการตรวจจับข้อมูล

2.3.2. ข้อเสีย

2.3.2.1. อาจมีการสูญหายของข้อมูลที่ทำการดักจับหรือได้ข้อมูลเกินความเป็นจริง

2.3.2.2. เป็นการยากในการเข้าไปดักจับในสื่อสัญญาณบางชนิดได้

2.3.2.3. เครื่องที่นำไปดักจับจะต้องมีประสิทธิภาพมากเพียงพอที่จะจับข้อมูลที่ถูกรับส่งกันได้อย่างครบถ้วน

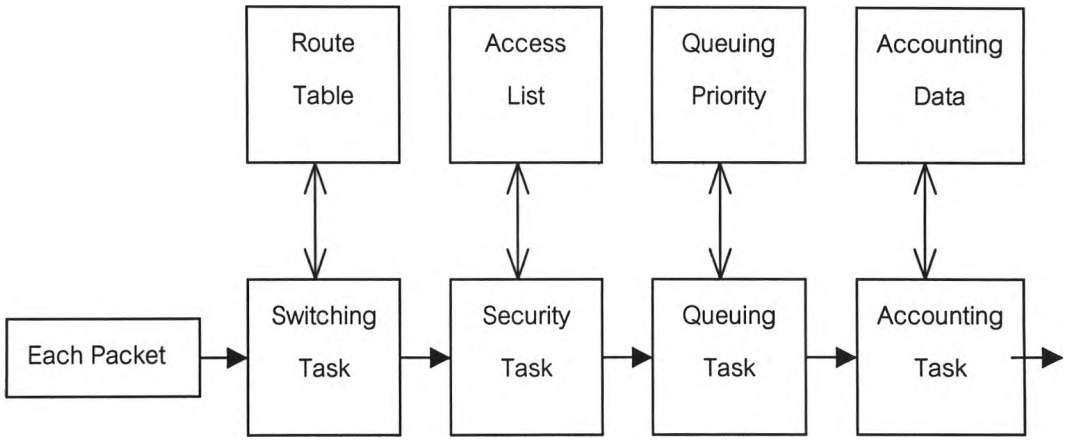
2.4. การจัดเก็บข้อมูลการใช้งานสายสัญญาณโดยใช้อุปกรณ์สื่อสารเร้าเตอร์ (Router) เป็นตัวนับ

เร้าเตอร์เป็นอุปกรณ์ซึ่งทำหน้าที่หาเส้นทางของการส่งข้อมูลจากเลขที่อยู่ไอพีต้นทางของผู้ส่ง กับ เลขที่อยู่ไอพีปลายทางของผู้รับ

2.4.1. ใช้ คุณสมบัติ IP Accounting

เร้าเตอร์ของซีสโก้ (Cisco) ที่มีไอโอเอส (IOS) ตั้งแต่รุ่น 9.0 ขึ้นไปจะมีส่วนการประมวลผลอยู่ส่วนหนึ่งเรียกว่า Accounting Task ทำหน้าที่เก็บข้อมูลของบรรจุภัณฑ์ที่ถูกส่งผ่านเร้าเตอร์ โดยจะทำการจะจัดเก็บข้อมูลจากการติดต่อจากไอพีต้นทางกับไอพีปลายทาง ในรูปแบบของจำนวนบรรจุภัณฑ์และจำนวนไบต์ที่มีการรับส่งกัน การเข้าไปอ่านค่านี้ในช่วงเวลาหนึ่ง ๆ จะทำให้เราทราบถึงประสิทธิภาพความเร็วในการใช้งานของ เครื่องต้นทางและเครื่องปลายทางได้ วิธีการทำ IP accounting บนเร้าเตอร์สามารถหาได้ที่

http://www.cisco.com/univercd/cc/td/doc/product/software/ssr91/csc_r/56645.htm#xtocid2550574



รูปที่ 2.4.1 ขั้นตอนการทำงานของเร้าเตอร์ในการส่งข้อมูล

2.4.1.1.เร้าเตอร์จะจัดเก็บข้อมูลซึ่งประกอบด้วยของข้อมูลดังต่อไปนี้

2.4.1.1.1. เลขที่อยู่ไอพีต้นทางของผู้ส่งข้อมูล

2.4.1.1.2. เลขที่อยู่ไอพีปลายทางของผู้รับข้อมูล

2.4.1.1.3. จำนวนของอักขระข้อมูลที่ถูกรับส่ง

2.4.1.1.4. จำนวนของบรรจุภัณฑ์ข้อมูลที่ถูกรับส่งกัน

เราสามารถนำข้อมูลข้างต้นนี้นำไปเก็บในช่วงเวลาหนึ่งๆเพื่อนำไปคำนวณหาปริมาณการใช้ช่องสัญญาณ ว่ามีการใช้งานมาจากที่ไหนในองค์กร โดยคำนวณจากการนำเอาปริมาณ ข้อมูลที่มีการรับส่งในช่วงเวลาหนึ่งๆมาหารกับช่วงเวลาที่มีการที่มีการตรวจนับเพื่อจะได้ อัตราการใช้งานช่องสัญญาณ

2.4.1.2.ข้อดี

2.4.1.2.1. ทำให้สามารถทราบถึงปริมาณการใช้งานในช่องสัญญาณนั้น โดยสามารถแจกแจงเป็นการใช้งานในแต่ละแห่งได้

2.4.1.2.2. สามารถนำข้อมูลที่ได้ไปคำนวนค่าใช้จ่ายในการใช้ช่องสัญญาณของผู้ส่งในแต่ละองค์กรภายในได้

2.4.1.2.3. สามารถนำไปประยุกต์ใช้ในการเรียกเก็บค่าใช้บริการสายได้ โดยดูจากอัตราการใช้งานช่องสัญญาณของแต่ละองค์กร

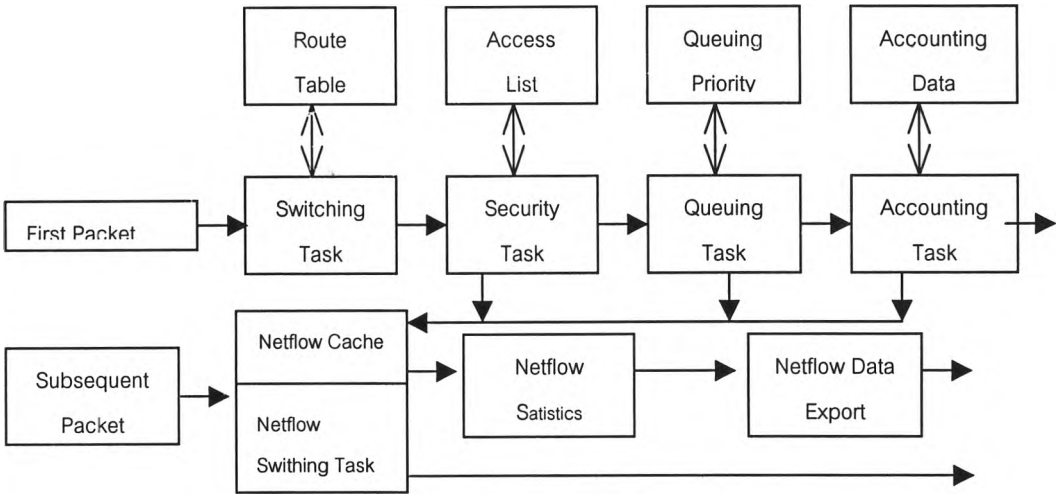
2.4.1.3.ข้อเสีย

2.4.1.3.1. ต้องใช้อุปกรณ์เร้าเตอร์ที่สามารถทำ Accounting Task เป็นตัววัดปริมาณการใช้งาน

2.4.1.3.2. ต้องทำ Post-processing ข้อมูลที่ได้จากเร้าเตอร์เพื่อให้ได้กลุ่มของผู้ใช้งานช่องสัญญาณ

2.4.2.ใช้ คุณสมบัติเน็ตโฟล์ว (Netflow)

เร้าเตอร์ของ ซีสโก้ ที่มี ไอโอเอส ตั้งแต่รุ่น 11.1 (10.05) ขึ้นไปมีความสามารถทำเน็ตโฟล์ว มีลักษณะการทำงานดังรูปที่ 2.3.2 ซึ่งจะมีการเก็บข้อมูลส่วนหัวของโพรโทคอลทีซีพี/ไอพีของตัวข้อมูลที่วิ่งผ่านเร้าเตอร์ ซึ่งข้อมูลนี้ใช้ในการทำสถิติเพื่อวิเคราะห์การใช้การอินเทอร์เน็ต ข้อมูลของเน็ตโฟล์วซึ่งถูกจัดเก็บบนเร้าเตอร์จะประกอบด้วยข้อมูลตามภาคผนวก ค



รูปที่ 2.3.2 ผังการทำงานของระบบเน็ตโฟล์วในเร้าเตอร์

บริษัทซีสโก้ได้ทำการพัฒนาโปรแกรมขึ้นมาใช้ร่วมกับระบบเน็ตโฟล์ว ซึ่งก็คือโปรแกรมเน็ตโฟล์วคอเล็คเตอร์ ซึ่งจะทำงานบนเครื่องแม่ข่าย (Server) โดยสามารถดึงข้อมูลจากเร้าเตอร์มาเก็บรวบรวมไว้ได้และสามารถกรองข้อมูลที่ไม่ต้องการ

ออกได้ และมีรูปแบบของการจัดเก็บเรียกว่า คอลเรคคอร์ด (Callrecord) ซึ่งเป็นรูปแบบที่เหมาะแก่การจัดเก็บสถิติข้อมูล ประกอบด้วยข้อมูลตามภาคผนวก ค

2.4.2.1.ข้อดี

2.4.2.1.1. สามารถเห็นกิจกรรมที่เกิดขึ้นบนเครือข่ายได้ละเอียด

2.4.2.1.2. มีความยืดหยุ่นในการจัดเก็บสถิติการใช้งาน เช่น สามารถปรับความละเอียดในการจัดเก็บสถิติได้

2.4.2.2.ข้อเสีย

2.4.2.2.1. เนื่องจากข้อมูลดิบที่ได้จากการไหลของการลำเลียงข้อมูลมีจำนวนมากจึงมีค่าใช้จ่ายในการดำเนินการสูง

2.4.2.2.2. ต้องทำ Post-processing ข้อมูลที่ได้เพื่อให้ได้สาระสำคัญของข่าวสารที่ต้องการเนื่องจากข้อมูลดิบที่ได้มีมาก