ระบบตรวจสอบช่องโหว่ของการคอนฟิกูเรชั่นบนอุปกรณ์เราเตอร์

Vulnerability Checking System for Router Configuration

H002404

โดย

ธนะพันธ์ เกตุอ่ำ

รหัสประจำตัว 45066089

อาจารย์ที่ปรึกษา

ผศ.ดร.โชติพัชร์ ภรณวลัย

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการพัฒนาระบบงาน

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 2 ปีการศึกษา 2548

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	ระบบตรวจสอบช่องโหว่ของการคอนฟีกูเรชั่นบนอุปกรณ์เราเตอร์
นักศึกษา	นายธนะพันธ์ เกตุอ่ำ
อาจารย์ที่ปรึกษา	ผศ.ดร.โชติพัชร์ ภรณวลัย
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	วิทยาการสารสนเทศ
ปีการศึกษา	2548

บทคัดย่อ

ในปัจจุบันนี้ภัยคุกคามที่มาพร้อมกับเครือข่ายคอมพิวเตอร์มีมากมายหลายประเภท ดังนั้นจึงต้องมีการจัดการเรื่องของการรักษาความปลอดภัยในเครือข่ายคอมพิวเตอร์ ซึ่งอุปกรณ์เราเตอร์เป็นอุปกรณ์หนึ่งที่สามารถจัดการเรื่องของการรักษาความปลอดภัยในเครือข่ายคอมพิวเตอร์ได้ แต่ลักษณะของการคอนฟีกูเรชั่นตัวอุปกรณ์เราเตอร์ มีหลายรูปแบบและหลายส่วนด้วยกัน ดังนั้นจึงจำเป็นต้องมีการตรวจสอบการคอนฟีกูเรชั่นตัวอุปกรณ์เราเตอร์ ก่อนที่จะมีการนำอุปกรณ์เราเตอร์มาใช้ในระบบเครือข่ายจริง เพื่อทำการค้นหาช่องโหว่ที่อาจจะเกิดขึ้นจากการเซ็ตอัพที่ไม่เหมาะสม เพื่อป้องกันปัญหาที่จะเกิดขึ้นซึ่งอาจจะทำให้ระบบเครือข่ายเกิดความเสียหายได้ โครงงานนี้จึงจัดทำเพื่อใช้สำหรับตรวจสอบช่องโหว่ของการคอนฟีกูเรชั่นบนอุปกรณ์เราเตอร์

Title	Vulnerability Checking System for Router Configuration
Student	Mr. Thanapan Ket-am
Advisor	Asst. Prof. Dr. Chotipat Pornavalai
Level of Study	Master of Science in Information Technology
Major	Information Science
Academic Year	2005

ABSTRACT

Routers provide services that are essential to the correct, secure operation of the networks. Compromise on a router can lead to various security problems on the network served by that router. In general, well-configured routers can greatly improve the overall security posture of a network. Security policy enforced at a router is difficult for negligent or malicious end-users to circumvent, thus avoiding a very serious potential source of security problems. So we must have tools for checking configuration on router before install on production system. This tool can reduce problem from hacker, virus etc. This project implements tool for checking configuration on router.

กิตติกรรมประกาศ

โครงงานพัฒนาระบบตรวจสอบช่องโหว่ของการคอนฟิกูเรชั่นบนอุปกรณ์เราเตอร์ที่ได้จัดทำขึ้นมานี้สำเร็จลุล่วงได้เนื่องจากได้รับการสนับสนุนร่วมมือ และการให้คำแนะนำปรึกษาในแนวทางต่างๆ จากหลายบุคคล ทำให้โครงงานนี้สำเร็จลุล่วงได้ตามเป้าหมายที่ได้วางไว้ ผู้จัดทำใคร่ขอขอบคุณบุคคลต่างๆ ดังนี้

- ผศ.ดร.โชติพัชร์ ภรณวลัย อาจารย์ที่ปรึกษาโครงงาน ผู้ซึ่งให้คำแนะนำปรึกษา แนะแนวทางในการแก้ไขปัญหาต่างๆ ในระหว่างทำการพัฒนาระบบ
- คุณผกาวรรณ ว่องวุฒิพรชัย ที่ช่วยให้ข้อมูลและให้คำปรึกษาด้านเทคนิคต่างๆ
- บิดามารดาและพี่สาว ที่คอยเป็นกำลังใจและให้ความช่วยเหลือในด้านต่างๆ จนโครงงานนี้สำเร็จลุล่วงได้ด้วยดี

จึงใคร่ขอขอบคุณบุคคลดังกล่าวข้างต้นมา ณ โอกาสนี้

นายธนะพันธ์ เกตุอ่ำ

ผู้จัดทำ

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญรูป

หน้า

รูปที่

สารบัญรูป (ต่อ)

หน้า

รูปที่

บทที่ 1
บทนำ

1.1 ความเป็นมาของปัญหา

ในยุคที่อินเตอร์เน็ตกลายเป็นสาธารณูปโภคเหมือนระบบโทรศัพท์ที่ทุกบ้านทุกองค์กรต้องมีไว้ใช้บริการในการติดต่อสื่อสารกับโลกภายนอก การติดต่อสื่อสารทั่วโลกกลายเป็นเครือข่ายขนาดมหึมาประกอบด้วยเครื่องคอมพิวเตอร์หลายพันล้านเครื่อง เครื่องคอมพิวเตอร์เหล่านี้มีการต่อเชื่อมโยงถึงกันเป็นระบบเครือข่ายซึ่งสามารถส่งข้อมูลข้ามโลกได้ภายในพริบตา ซึ่งภัยคุกคามที่อยู่บนอินเตอร์เน็ตจะสามารถโจมตีเครือข่ายของเราได้อย่างรวดเร็วเช่นกัน ดังนั้นการรักษาความปลอดภัยจึงเป็นเรื่องที่สำคัญ การป้องกันภัยคุกคามนั้นสามารถป้องกันได้จากหลายส่วนด้วยกันซึ่งการป้องกันภัยบนอุปกรณ์เครือข่านเป็นส่วนหนึ่งที่ควรกระทำ เนื่องจากบางครั้งผู้บุกรุกจะใช้ช่องโหว่ที่เกิดจากอุปกรณ์เครือข่ายมาเป็นเครื่องมือที่ช่วยในการโจมตี ซึ่งอุปกรณ์เราเตอร์เป็นอุปกรณ์เครือข่ายประเภทหนึ่งที่ผู้บุกรุกใช้เป็นช่องทางในการโจมตีได้ โครงงานนี้จึงจัดทำขึ้นเพื่อทำการตรวจสอบการคอนฟิกูเรชั่นตัวอุปกรณ์เราเตอร์ก่อนที่จะมีการนำอุปกรณ์เราเตอร์มาใช้ในระบบเครือข่ายจริง เพื่อทำการค้นหาช่องโหว่ที่อาจจะเกิดขึ้นจากการเซ็ตอัพที่ไม่เหมาะสมเพื่อป้องกันปัญหาที่จะเกิดขึ้นซึ่งอาจจะทำให้ระบบเครือข่ายเกิดความเสียหายได้

1.2 วัตถุประสงค์ของการพัฒนาระบบ

1. เพื่อพัฒนาระบบสารสนเทศไปสู่ความปลอดภัยเพื่อรอดพ้นการโจมตีจากผู้ไม่ประสงค์ดี
2. เพื่อสร้างความน่าเชื่อถือและความไว้ใจจากบุคคลภายนอก ในเชิงของทางธุรกิจ
3. เพื่อให้ระบบการทำงานขององค์กรสามารถก้าวไปข้างหน้าโดยที่ไม่มีอุปสรรค
4. เพื่อตรวจสอบหาสาเหตุของปัญหาของระบบเครือข่ายว่าเกิดขึ้นเพราะเหตุใด
5. เพื่อนำระบบที่พัฒนามาใช้ปรับปรุงระบบเครือข่ายต่อไปในอนาคตได้
6. เพื่อนำระบบที่พัฒนามาทำการวิเคราะห์ว่าองค์กรของเรานั้น ปัจจุบันมีความเสี่ยงมากหรือน้อยเพียงใดและนำไปรายงานผู้บริหารได้
7. สามารถออกแบบ ดูแลรักษาระบบเครือข่ายให้อยู่ในสภาวะที่มีความเสี่ยงน้อยที่สุดได้

1.3 ขั้นตอนการดำเนินงาน

1. ศึกษาความต้องการจากผู้ที่เกี่ยวข้องกับระบบงาน เพื่อนำมาวิเคราะห์ถึงปัญหา และหาแนวทางการแก้ไขปัญหาเหล่านั้น
2. ศึกษาการทำงานของอุปกรณ์เราเตอร์
3. ศึกษาการคอนฟิกูเรชั่นของอุปกรณ์เราเตอร์ในเรื่องของการรักษาความปลอดภัยบนเครือข่าย
4. ศึกษาการป้องกันและหาช่องโหว่ที่อาจจะเกิดขึ้นจากอุปกรณ์เราเตอร์เพื่อที่จะทำให้ระบบเครือข่ายมีความปลอดภัยมากยิ่งขึ้น
5. ออกแบบการทำงาน, จอภาพและฐานข้อมูลของระบบที่จะพัฒนา และคัดเลือกเครื่องมือที่จะใช้ในการพัฒนาระบบงาน
6. ทดสอบและให้ผู้ปฏิบัติหน้าที่ใช้งานจริง

1.4 ขอบเขตของระบบงาน

ศึกษาการป้องกันและหาช่องโหว่ที่อาจจะเกิดขึ้นจากอุปกรณ์เราเตอร์เพื่อที่จะทำให้ระบบเครือข่ายมีความปลอดภัยมากยิ่งขึ้น และทำให้การทำงานขององค์กรเป็นไปอย่างมีประสิทธิภาพ โดยการทำงานของระบบการตรวจสอบการคอนฟิกูเรชั่นตัวอุปกรณ์เราเตอร์ เพื่อการค้นหาช่องโหว่บนอุปกรณ์เราเตอร์ มีขอบเขตการทำงานดังนี้

1. ระบบสามารถทำ Router Security Scanner ซึ่งเป็นส่วนที่นำการคอนฟิกูเรชั่น ที่ได้จากอุปกรณ์เราเตอร์มาทำการตรวจสอบเพื่อหาช่องโหว่ก่อนที่จะนำไปติดตั้งในระบบจริงตามรูปแบบของช่องโหว่ (Pattern of Attack on Routers Management) ที่อาจเกิดขึ้นจากการคอนฟิกูเรชั่นที่ไม่เหมาะสมได้ โดยมีแยกเป็นหมวดหมู่ ดังนี้
    - Router Access Security
    - Router Service Security
    - Router Access List
    - Audit Management
    - Scan Routing
2. ระบบสามารถเก็บรูปแบบของการคอนฟิกูเรชั่น พร้อมทั้งเก็บปัญหาที่จะเกิดขึ้นเมื่อเราละเลยช่องโหว่เหล่านี้ได้

3. ระบบสามารถเพิ่มเติม ลบ หรือแก้ไขรูปแบบของการคอนฟีกูเรชั่นที่เหมาะสมได้ เพื่อความยืดหยุ่นที่จะเกิดขึ้นในอนาคตได้
4. ระบบสามารถเรียกดูรูปแบบของการคอนฟีกูเรชั่นที่เหมาะสมในแต่ละหัวข้อที่ใช้ในการตรวจสอบได้
5. ระบบสามารถแสดงรายละเอียดเกี่ยวกับความเสี่ยงที่อาจจะเกิดขึ้นการคอนฟีกูเรชั่น พร้อมทั้งบอกคำแนะนำว่าควรจะทำแบบใดถึงจะเหมาะสมกว่าและเกิดความเสี่ยงน้อยกว่าได้

1.5 เครื่องมือที่ใช้ในการพัฒนา

เครื่องมือที่ใช้ในการพัฒนาระบบการตรวจสอบการคอนฟีกูเรชั่นตัวอุปกรณ์เราเตอร์นี้ประกอบด้วย

1. Visual Studio .Net 2003 โดยใช้ภาษา Visual Basic .Net สำหรับการพัฒนาแอพพลิเคชั่น ที่จัดการในส่วนของการตรวจสอบการคอนฟีกูเรชั่นตัวอุปกรณ์เราเตอร์
2. Microsoft Access 2003 เพื่อใช้ในการจัดการกับฐานข้อมูลต่างๆ
3. เครื่องคอมพิวเตอร์ ที่ใช้ในการติดตั้งแอพพลิเคชั่น พร้อมทั้งได้ทำการติดตั้งระบบปฏิบัติการ Microsoft Windows XP ไว้แล้ว
4. อุปกรณ์เราเตอร์

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1. สามารถตรวจสอบการคอนฟีกูเรชั่นของอุปกรณ์เราเตอร์เพื่อหาช่องโหว่ของการเซ็ตอัพก่อนที่จะนำเราเตอร์มาใช้ในระบบจริง
2. ระบบเครือข่ายคอมพิวเตอร์ขององค์กรจะสามารถรอดพ้นการโจมตีจากผู้ไม่ประสงค์ดีได้ในระดับหนึ่ง
3. สามารถนำมาใช้ปรับปรุงระบบเครือข่ายต่อไปในอนาคตได้
4. สามารถวิเคราะห์ได้ว่าองค์กรของเรานั้นปัจจุบันมีความเสี่ยงมากหรือน้อยเพียงใดและนำไปรายงานผู้บริหารได้
5. สามารถออกแบบ ดูแลรักษาระบบเครือข่ายให้อยู่ในสภาวะที่มีความเสี่ยงน้อยที่สุดได้

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

ในการพัฒนาระบบตรวจสอบการคอนฟิกูเรชั่นบนอุปกรณ์เราเตอร์ ได้มีการนำหลักการและทฤษฎีต่างๆ ที่เกี่ยวข้องมาช่วยในการพัฒนา ซึ่งมีทฤษฎีที่เกี่ยวข้อง ดังนี้

2.1. แบบจำลอง OSI และ โปรโตคอล TCP/IP

โครงสร้างของเครือข่ายเป็นสิ่งที่ซับซ้อนมากและยากต่อการออกแบบและพัฒนาทั้งระบบ ดังนั้นจึงมีการแบ่งโครงสร้างออกเป็นชั้นหรือเลเยอร์ (Layer) ซึ่งจะช่วยให้ทั้งผู้ผลิตฮาร์ดแวร์และซอฟท์แวร์พัฒนาผลิตภัณฑ์ของตังเองได้โดยไม่ต้องกังวลกับส่วนอื่นๆ แต่ยังสามารถทำงานร่วมกันได้

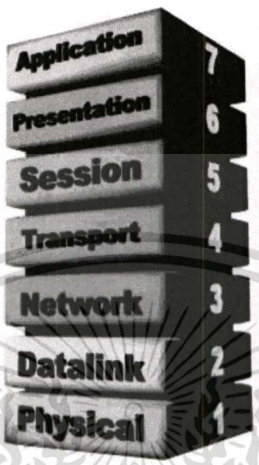
แบบจำลอง OSI (Open system Interconnection) ได้อธิบายสถาปัตยกรรมเครือข่ายโดยแบ่งฟังก์ชันการเคลื่อนย้ายข้อมูลจากคอมพิวเตอร์เครื่องหนึ่งไปยังคอมพิวเตอร์อีกเครื่องหนึ่ง ออกเป็น 7 เลเยอร์ ส่วนโปรโตคอล TCP/IP จะคล้ายๆ กับแบบจำลอง OSI คือจะมีการแบ่งออกเป็นเลเยอร์เช่นกัน แต่การออกแบบจะมุ่งเน้นไปที่การเชื่อมต่อระหว่างระบบที่ต่างกัน ดังนั้นแบบจำลอง OSI จะใช้ในการอธิบายการสื่อสารระหว่างคอมพิวเตอร์ในเครือข่าย ส่วนโปรโตคอล TCP/IP จะทำมาใช้ในการปฏิบัติจริง

แบบจำลอง OSI

องค์กรกำหนดมาตรฐานสากล (The International Organization for Standardization) หรือเรียกสั้นๆ ว่า ISO เป็นองค์กรที่กำหนดมาตรฐานสากลต่างๆ รวมถึงมาตรฐานในการสื่อสารด้วย นั่นคือแบบจำลอง OSI (Open System Interconnection)

แบบจำลอง OSI เป็นระบบเปิด (Open system) ที่ออกแบบขึ้นมาเพื่ออนุญาตให้ระบบที่มีความแตกต่างกันสามารถสื่อสารระหว่างกันได้ ด้วยการใช้มาตรฐานการสื่อสารที่เป็นสากล โดยไม่มีความจำเป็นที่จะต้องเปลี่ยนแปลงฮาร์ดแวร์หรือซอฟท์แวร์ใดๆ ซึ่งแบบจำลอง OSI ไม่ใช่โปรโตคอล แต่เป็นเพียงแบบจำลองแนวความคิด (Conceptual Model) ที่ออกแบบมาเพื่อสร้างความเข้าใจในสถาปัตยกรรมเครือข่ายเท่านั้น

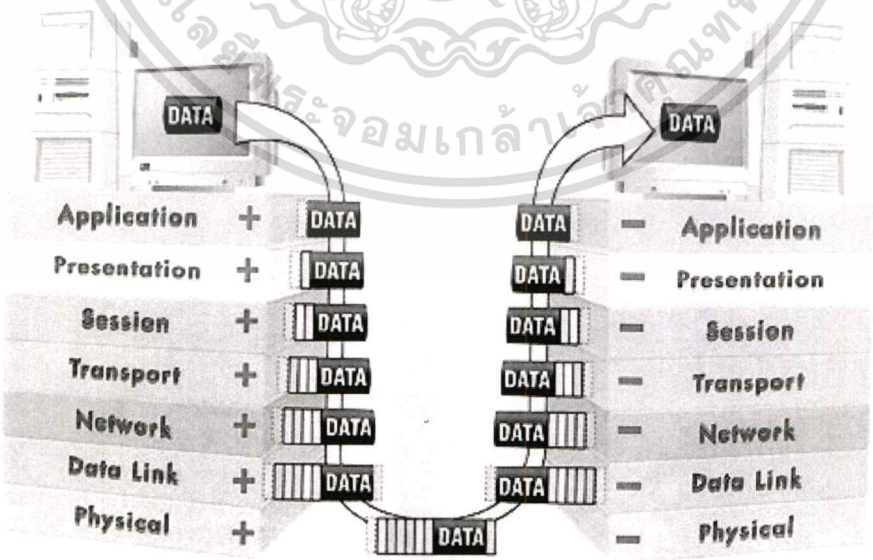
แบบจำลอง OSI มีการทำงานเป็นลำดับชั้น หรือเลเยอร์ (Layer) ซึ่งแต่ละลำดับชั้นจะมีชื่อเรียกและหน้าที่ที่แตกต่างกัน โดยแบบจำลอง OSI มีการแบ่งออกเป็น 7 ลำดับชั้น ดังรูป



รูปที่ 2.1 แบบจำลอง OSI

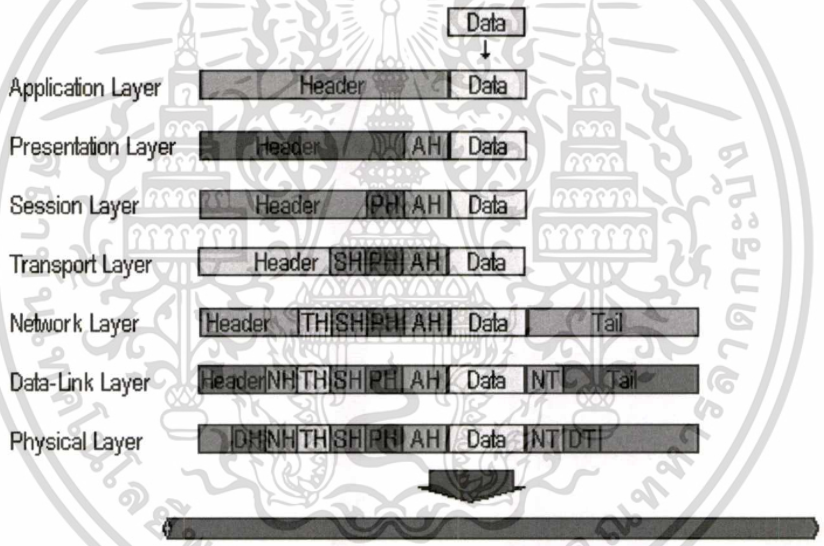
การสื่อสารบนแบบจำลอง OSI

การสื่อสารบนแบบจำลอง OSI จะมีรูปแบบการสื่อสารเป็นลำดับชั้นในลักษณะต่อ เนื่องกันไป ซึ่งสามารถอธิบายการทำงานได้ ตามรูป



รูปที่ 2.2 การสื่อสารบนแบบจำลอง OSI

จากรูป โฮสต์ A คือฝ่ายส่ง และโฮสต์ B คือฝ่ายรับ การส่งข้อมูลของโฮสต์ A จะเริ่มจากลำดับชั้นที่ 7 แอพพลิเคชั่นเลเยอร์ โดยข้อมูลจะถูกส่งจากลำดับชั้นหนึ่งไปอีกชั้นหนึ่งที่อยู่ติดกัน เรียงลำดับต่อเนื่องกันมา โดยในแต่ละลำดับชั้นจะมีการผนวกข่าวสารที่เรียกว่า "เฮดเดอร์" (Header) เข้ากับข้อมูลที่ส่งมาจากลำดับชั้นบน ซึ่งการผนวกเฮดเดอร์เข้าไปกับข้อมูลนี้ เราเรียกว่า "เอ็นแคปซูเลชั่น" (Encapsulation) เมื่อข้อมูลถูกส่งไปยังโฮสต์ B ที่เป็นปลายทาง สัญญาณจะเดินทางไปยังลำดับชั้นที่ 1 ของฝ่ายผู้รับ ข้อมูลจะถูกส่งขึ้นไปยังลำดับชั้นด้านบน ซึ่งในแต่ละลำดับชั้นก็จะทำการถอดเฮดเดอร์ประจำชั้นของตนออก การถอดเฮดเดอร์ เราจะเรียกว่า "ดีแคปซูเลชั่น" (Decapsulation) จะทำเช่นนี้ไปจนกระทั่งถึงชั้นบนสุด ซึ่งก็คือชั้นแอพพลิเคชั่น ก็จะเหลือเพียงข้อมูลเพียงอย่างเดียว



รูปที่ 2.3 กระบวนการทำงานของ OSI Layer

หน้าที่การทำงานของแต่ละลำดับชั้น

1. ลำดับชั้นกายภาพ (Physical Layer)

เลเยอร์นี้ทำหน้าที่เกี่ยวกับกำหนดวิธีควบคุมการรับและส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ในระดับบิต ชั้นนี้ทางฝั่งผู้ส่งจะรับข้อมูลจากเลเยอร์ที่ 2 หรือชั้นเชื่อมโยงข้อมูล ซึ่งข้อมูลชุดหนึ่งจะเรียกว่า เฟรม (Frame) และทำการส่งเฟรมของข้อมูลทีละบิตแบบเรียงตามลำดับ ส่วนทางฝั่งผู้รับจะทำการรับข้อมูลที่ถูกส่งมาเป็นบิต และจัดส่งผ่านข้อมูลนี้ต่อไปยังชั้นเชื่อมโยงข้อมูลเพื่อทำการประมวลผลต่อไป โดยกฎระเบียบในชั้นนี้จะเกี่ยวพันโดยตรงกับการ

ทำงานของอุปกรณ์สัญญาณไฟฟ้า (หรือสัญญาณใดๆ), ขั้นตอนในการใช้อุปกรณ์เหล่านั้น และความสัมพันธ์กับสื่อที่ใช้รับส่งข้อมูล

2. ลำดับชั้นเชื่อมต่อข้อมูล (Data Link Layer)

เลเยอร์นี้จะรับผิดชอบในการรับส่งข้อมูลและทำการตรวจสอบความถูกต้องของข้อมูลด้วย โดยทางฝั่งผู้ส่ง ข้อมูลจะถูกจัดให้อยู่ในรูปเฟรม ซึ่งในเฟรมจะมีข้อมูลที่ทำให้สามารถส่งข้อมูลไปยังปลายทางภายในเครือข่ายแลนได้อย่างถูกต้อง หรืออีกนัยหนึ่งคือ รับผิดชอบในการส่งข้อมูลในลักษณะ Node-to-Node นั่นเองในกรณีที่การรับส่งข้อมูล ทำให้เฟรมเกิดการเสียหาย ในเลเยอร์นี้จะทำการตรวจสอบและแก้ไขข้อผิดพลาดต่างๆ ให้

3. ลำดับชั้นเครือข่าย (Network Layer)

ในเลเยอร์นี้จะรับผิดชอบเกี่ยวกับ การส่งแพ็คเก็ตจากต้นทางไปยังปลายทางผ่านเครือข่ายหลายๆ เครือข่ายเข้าด้วยกัน โดยจะทำหน้าที่ในการเลือกเส้นทางการส่งข้อมูลที่ดีที่สุด หรือเหมาะสมที่สุดโดยในชั้นนี้ข้อมูลจะถูกแบ่งออกเป็นส่วนๆ ที่เรียกว่า “แพ็คเก็ต” (Packet)

4. ลำดับชั้นขนส่งข้อมูล (Transport Layer)

ในเลเยอร์นี้จะรับผิดชอบในการส่งข้อมูลในลักษณะ End-to-End ด้วยการสร้างความน่าเชื่อถือถึงการรับประกันการบริการรับส่งข้อมูลว่าการส่งข้อมูลจะไปถึงผู้รับแน่นอน หากเกิดข้อผิดพลาดระหว่างการส่งจะทำการส่งข้อมูลนั้นใหม่ โดยปกติจะมีอยู่ 2 โปรโตคอลที่ทำงานบนชั้นนี้ คือ โปรโตคอล TCP และ โปรโตคอล UDP และในชั้นนี้จะมีการแบ่งข้อมูลออกเป็นส่วนเรียกว่า เซกเมนต์ (Segment)

5. ลำดับชั้นเซสชั่น (Session Layer)

ในเลเยอร์นี้จะทำการควบคุมการเชื่อมต่อระหว่างต้นทางและปลายทางตั้งแต่เริ่มต้นการสื่อสารจนยุติการสื่อสาร โดยจะคอยทำการ จัดการการแลกเปลี่ยนข่าวสาร (Dialogue Control: Full Duplex, Half Duplex, Simplex) ซึ่งตั้งแต่ชั้นเซสชั่นจะทำหน้าที่บริการหรือคอยอำนวยความสะดวกให้แก่ผู้ใช้ โดยแต่ละเซสชั่นนั้นอาจเกิดจาการทำงานของคนเพียงคนเดียวหรือหลายๆ คนก็ได้

6. ลำดับชั้นนำเสนอข้อมูล (Presentation Layer)

ในเลเยอร์นี้จะจัดการเกี่ยวกับรูปแบบของการนำเสนอข้อมูลให้สามารถเข้าใจได้ทั้ง 2 ฝ่าย ถึงแม้ว่าระบบที่สื่อสารกันจะใช้เครื่องที่มีการเข้ารหัสแทนข้อมูลที่แตกต่างกัน, ทำการ

รักษาความปลอดภัยของข้อมูล โดยการเข้ารหัสข้อมูลก่อนที่จะมีการส่งออกไปได้ และสามารถทำการบีบอัดข้อมูลเพื่อให้ข้อมูลมีขนาดเล็กลง เพื่อความรวดเร็วในการสื่อสาร

7. ลำดับชั้นโปรแกรมประยุกต์ (Application Layer)

ในเลเยอร์นี้เป็นชั้นที่อำนวยความสะดวกแก่ผู้ใช้ให้สามารถใช้งานซอฟท์แวร์ต่างๆ ผ่านเครือข่ายได้ โดยบริการต่างๆ ในเลเยอร์นี้จะมุ่งเน้นการอำนวยความสะดวกแก่ผู้ใช้ด้วยโปรโตคอลต่างๆ ซึ่งจะมีโปรแกรมประยุกต์ต่างๆ ให้เลือกใช้งานเพื่อติดต่อกับเครือข่ายตามความเหมาะสม

2.2 โปรโตคอล TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) เป็นชุดของโปรโตคอลที่ถูกใช้ในการสื่อสารผ่านเครือข่ายอินเตอร์เน็ต โดยมีวัตถุประสงค์เพื่อให้สามารถใช้สื่อสารจากต้นทางข้ามเครือข่ายไปยังปลายทางได้ และสามารถหาเส้นทางที่จะส่งข้อมูลไปได้เองโดยอัตโนมัติ ถึงแม้ว่าในระหว่างทางอาจจะผ่านเครือข่ายที่มีปัญหา โปรโตคอลก็ยังคงหาเส้นทางอื่นในการส่งผ่านข้อมูลไปให้ถึงปลายทางได้

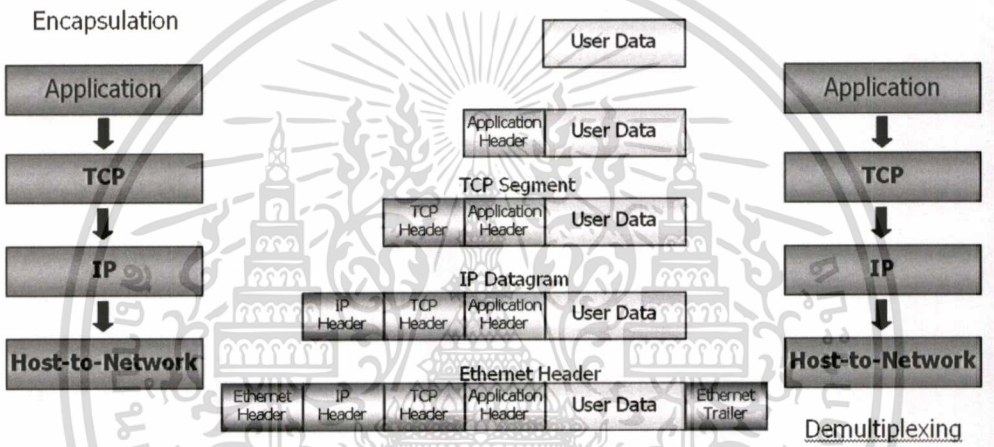
ชุดโปรโตคอลนี้ได้รับการพัฒนามาตั้งแต่ปี 1960 ซึ่งถูกใช้เป็นครั้งแรกในเครือข่าย ARPANET ซึ่งต่อมาได้ขยายการเชื่อมต่อไปทั่วโลกเป็นเครือข่ายอินเตอร์เน็ต ทำให้ TCP/IP เป็นที่ยอมรับอย่างกว้างขวางจนถึงปัจจุบัน

TCP/IP มีจุดประสงค์ของการสื่อสารตามมาตรฐาน 3 ประการคือ

1. เพื่อใช้ติดต่อสื่อสารระหว่างระบบที่มีความแตกต่างกัน
2. ความสามารถในการแก้ไขปัญหาที่เกิดขึ้นในระบบเครือข่าย เช่นในกรณีที่ผู้ส่งและผู้รับยังคงมีการติดต่อกันอยู่ แต่โหนดกลางที่ใช้เป็นผู้ช่วยรับ-ส่งเกิดเสียหายใช้การไม่ได้ หรือสายสื่อสารบางช่วงถูกตัดขาด กฎการสื่อสารนี้จะต้องสามารถจัดหาทางเลือกอื่นเพื่อทำให้การสื่อสารดำเนินต่อไปได้โดยอัตโนมัติ
3. มีความคล่องตัวต่อการสื่อสารข้อมูลได้หลายชนิดทั้งแบบที่ไม่มีความเร่งด่วน เช่น การจัดส่งแฟ้มข้อมูล และแบบที่ต้องการรับประกันความเร่งด่วนของข้อมูล เช่น การสื่อสารแบบ Real-time และทั้งการสื่อสารแบบเสียง (Voice) และข้อมูล (Data)

การสื่อสารบนโปรโตคอล TCP/IP

การส่งข้อมูลผ่านในแต่ละเลเยอร์ แต่ละเลเยอร์จะทำการประกอบข้อมูลที่ได้รับมา กับข้อมูลส่วนควบคุมซึ่งถูกนำมาไว้ในส่วนหัวของข้อมูลเรียกว่า "เฮดเดอร์" (Header) ภายในเฮดเดอร์จะบรรจุข้อมูลที่สำคัญของโปรโตคอลที่ทำการ Encapsulate เมื่อผู้รับได้รับข้อมูล ก็จะเกิดกระบวนการทำงานย้อนกลับคือโปรโตคอลเดียวกัน ทางฝั่งผู้รับก็จะได้รับข้อมูลส่วนที่เป็นเฮดเดอร์ก่อนและนำไปประมวลและทราบว่าข้อมูลที่ตามมามีลักษณะอย่างไร ซึ่งกระบวนการย้อนกลับนี้เรียกว่า Decapsulation



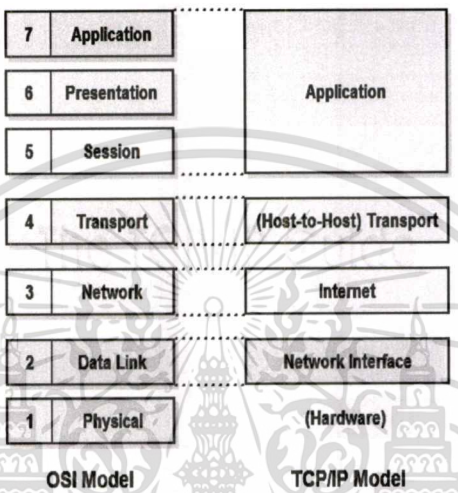
รูปที่2.4 ขั้นตอนการ Encapsulation และ Demultiplexing

ข้อมูลที่ผ่านการ Encapsulate ในแต่ละเลเยอร์มีชื่อเรียกแตกต่างกัน ดังนี้

- ข้อมูลที่มาจากผู้ใช้หรือก็คือข้อมูลที่ผู้ใช้เป็นผู้ป้อนให้กับ Application เรียกว่า User Data
- เมื่อแอพพลิเคชั่นได้รับข้อมูลจากผู้ใช้ก็จะนำมาประกอบกับส่วนหัวของแอพพลิเคชั่น เรียกว่า Application Data และส่งต่อไปยังโปรโตคอล TCP
- เมื่อโปรโตคอล TCP ได้รับ Application Data ก็จะนำมารวมกับเฮดเดอร์ของโปรโตคอล TCP เรียกว่า TCP Segment และส่งต่อไปยังโปรโตคอล IP
- เมื่อโปรโตคอล IP ได้รับ TCP Segment ก็จะนำมารวมกับเฮดเดอร์ของโปรโตคอล IP เรียกว่า IP Datagram และส่งต่อไปยังเลเยอร์ Host-to-Network Layer
- ในระดับ Host-to-Network จะนำ IP Datagram มาเพิ่มส่วน Error Correction และ Flag เรียกว่า Ethernet Frame ก่อนจะแปลงข้อมูลเป็นสัญญาณไฟฟ้า ส่งผ่านสายสัญญาณที่เชื่อมโยงอยู่ต่อไป

การแบ่งชั้นของ TCP/IP

โปรโตคอล TCP/IP ได้มีการพัฒนาขึ้นมาก่อนแบบจำลอง OSI ดังนั้น ลำดับชั้นต่างๆ ในโปรโตคอลจึงไม่ตรงกับแบบจำลอง OSI แต่มีหลักการทำงานที่คล้ายคลึงกันมาก โดย TCP/IP จะมีเพียง 4 ลำดับชั้น ส่วนแบบจำลอง OSI จะมี 7 ชั้น ดังรูป



รูปที่ 2.5 การแบ่งชั้นของโปรโตคอล TCP/IP

หน้าที่การทำงานของแต่ละลำดับชั้น

1. ชั้นโฮสต์-เครือข่าย (Host-to-Network Layer)

เลเยอร์นี้มีหน้าที่ควบคุมการรับส่งข้อมูลในระดับฮาร์ดแวร์ของเครือข่าย รับผิดชอบการรับส่งข้อมูลในระดับกายภาพ จนถึงการแปลความจากสัญญาณไฟฟ้า เป็นข้อมูลทางคอมพิวเตอร์

2. ชั้นสื่อสารอินเตอร์เน็ต (The Internet Layer)

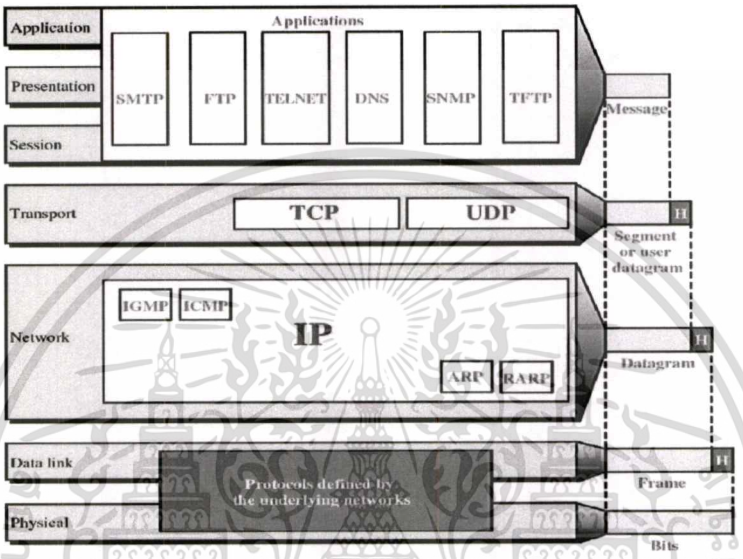
ทำหน้าที่รับข้อมูลจากชั้น Transport Layer และค้นหาและเลือกเส้นทางระหว่างผู้รับและผู้ส่ง เทียบได้กับชั้น Network Layer ของ OSI Model โปรโตคอลในเลเยอร์นี้ได้แก่ IP, ICMP, IGMP

3. ชั้นสื่อสารนำส่งข้อมูล (Transport Layer)

รับผิดชอบการรับส่งข้อมูลระหว่างปลายด้านส่งและด้านรับข้อมูล และส่งข้อมูลขึ้นไปให้ Application Layer นำไปใช้งานต่อ ซึ่งเทียบได้กับ Session Layer และ Transport Layer ของ OSI Model

4. ชั้นสื่อสารการประยุกต์ (Application Layer)

เป็นเลเยอร์ที่แอพพลิเคชั่นเรียกโปรโตคอลระดับล่างๆ ลงไป เพื่อให้บริการต่างๆ เช่น FTP, SMTP, Telnet, HTTP, POP



รูปที่ 2.6 โปรโตคอลต่างๆ ที่ทำงานบนโปรโตคอล TCP/IP

2.3 Internet Protocol

ด้วยเหตุที่ IP เป็นโปรโตคอลหลักในการสื่อสารข้อมูล และถือได้ว่าเป็นหัวใจสำคัญของโปรโตคอล TCP/IP ในหัวข้อนี้อธิบายเกี่ยวกับหน้าที่และลักษณะของโปรโตคอล IP, Internet Address, รูปร่างของ IP Header, การ Routing และ การจัดสรร IP ด้วย Subnet

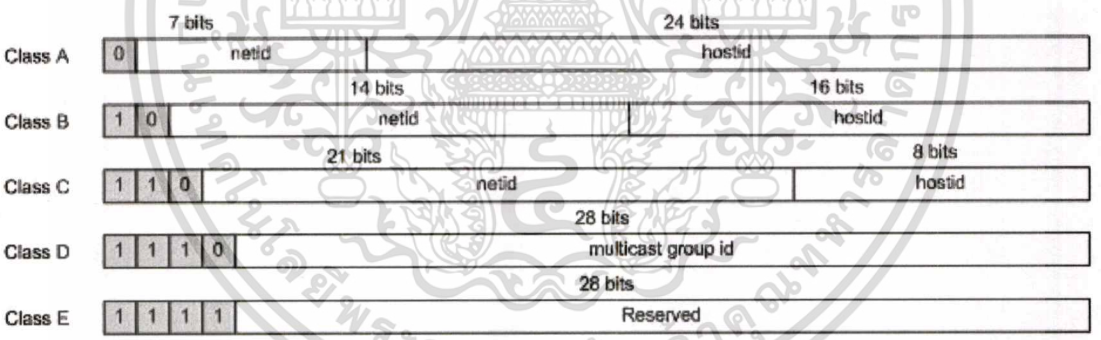
IP เป็นโปรโตคอลที่ทำหน้าที่รับภาระในการนำข้อมูลไปส่งยังผู้รับ ที่เชื่อมต่ออยู่ในระบบเครือข่ายซึ่งทั้งสองฝั่งอาจอยู่คนละเครือข่ายกันก็ได้ โปรโตคอลอื่นๆ ในระดับ Network Layer ขึ้นไปทั้ง TCP, UDP, ICMP ต่าง ต้องอาศัยโปรโตคอล IP ในการรับส่งข้อมูลทั้งสิ้น

โปรโตคอล IP มีความสามารถในการค้นหาเส้นทางจากผู้รับไปยังผู้ส่ง มีกลไกที่ชาญฉลาดในการค้นหาเส้นทาง สามารถค้นหาเส้นทางได้ไปถึงผู้รับได้เอง หากมีเส้นทางที่สามารถไปได้ แต่ไม่ได้ติดต่อระหว่างผู้รับกับผู้ส่งโดยตรง และไม่มีการยืนยันว่า ข้อมูลถึงผู้รับจริงหรือไม่ ทั้งนี้อาจเกิดจากหลายสาเหตุ เช่น ที่อยู่ของผู้รับไม่มีการเชื่อมต่ออยู่ในระบบอินเตอร์เน็ต กล่าวได้ว่า โปรโตคอล IP มีหน้าที่ในการค้นหาเส้นทางเท่านั้น ไม่มีการยืนยันผลสำเร็จในการส่งข้อมูล หากเกิดข้อผิดพลาดในการส่งข้อมูล แม้ว่าจะมีการส่ง icmp massage กลับมารายงานข้อผิดพลาด แต่ก็รับประกัน

ไม่ได้อยู่ดีว่า icmp message จะกลับมาถึงเรียบร้อยหรือไม่ ด้วยเหตุนี้ จึงถือว่า IP เป็นโปรโตคอลที่ไม่มีความน่าเชื่อถือ (Reliable)

IP Addressing

ทุกอินเตอร์เฟซที่ต่ออยู่บนอินเตอร์เน็ตจะต้องมีหมายเลขประจำตัวเพื่อใช้ในการสื่อสารข้อมูล เรียกว่า Internet Address หรือเรียกย่อๆ ว่า IP Address โดยค่า IP Address นี้จะเป็นหมายเลขจำนวน 32 บิต แต่แทนที่จะกำหนดให้เลขทั้ง 32 บิตนั้นถูกนับต่อเนื่องกันไป ก็จะใช้วิธีการแบ่งหมายเลขดังกล่าวออกเป็นกลุ่มของเลขขนาด 8 บิตจำนวน 4 ชุด และคั่นแต่ละชุดด้วยจุด ตัวอย่าง เช่น 172.17.3.12 นอกจากนี้ใน IP Address นั้นยังถูกแบ่งออกเป็น 2 ส่วนคือ ส่วนที่เป็นหมายเลขของเครือข่าย (Network ID) และส่วนที่เป็นหมายเลขของโฮสต์ (Host ID) ซึ่งข้อมูลในส่วนนี้จะถูกใช้สำหรับ ค้นหาเส้นทางของ IP ในการที่จะขนส่งข้อมูลจากต้นทางให้ถึงปลายทางอย่างถูกต้อง เพื่อเป็นการกำหนดขนาดของเน็ตเวิร์ก สำหรับ IP Address ต่างๆ ดังนั้นจึงมีการจัด IP Address ในแต่ละช่วงออกเป็นคลาส (class) ต่างๆ กันจาก A ถึง E เพื่อจะได้ทำการจัดสรร IP Address ได้อย่างเหมาะสมกับขนาดของเครือข่าย



รูปที่ 2.7 การกำหนด IP Address ในคลาสต่างๆ

IP Routing

IP Routing เป็นกระบวนการค้นหาเส้นทางในการส่งผ่านข้อมูลจากต้นทางไปยังปลายทาง โดยผ่านการส่งต่อข้อมูลไปจนกว่าจะถึงปลายทาง นับเป็นกลไกสำคัญที่ทำให้ IP เป็นโปรโตคอลที่สามารถส่งข้อมูลจากโฮสต์หนึ่งไปอีกโฮสต์หนึ่งได้แม้ว่าจะอยู่ไกลแสนไกล

ส่วนประกอบต่างๆ ของเครือข่ายในแง่ของ IP Routing มีดังนี้

1. **Host** โฮสต์เป็นอุปกรณ์ที่ทำหน้าที่ให้กำเนิดข้อมูลในกรณีเป็นผู้ส่ง หรือทำหน้าที่รับข้อมูลไปใช้งานในกรณีเป็นผู้รับ การสื่อสาร ข้อมูลใดๆ จะต้องเป็นการสื่อสารจากโฮสต์ไปยังโฮสต์เสมอ สำหรับ IP Packet แล้วข้อมูลในเฮดเดอร์ที่ปรากฏอยู่ในฟิลด์ Source Address

และ Destination Address ซึ่งเรียกว่า IP Address จะเป็นหมายเลขระบุตำแหน่งของโฮสต์ต้นทางและโฮสต์ปลายทางเท่านั้น

2. **Network** เน็ตเวิร์คเป็นเครือข่ายที่มีการเชื่อมต่อกันของโฮส 2 ตัวขึ้นไป โฮสต์แต่ละตัวในเครือข่ายเดียวกันสามารถเชื่อมต่อถึงกันได้โดยตรง
3. **Router** เราเตอร์ทำหน้าที่ในการ ส่งผ่านข้อมูลจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง ตำแหน่งของอุปกรณ์เราเตอร์จะอยู่ในจุดที่เชื่อมต่อระหว่างสองเครือข่ายเข้าด้วยกัน ด้วยข้อกำหนดของ IP ข้อมูลจะส่งไปถึงกันโดยตรงข้ามเครือข่ายไม่ได้ จะต้องอาศัยเราเตอร์เป็นผู้ทำหน้าที่ส่งผ่านข้อมูลไปให้ ในอุปกรณ์เราเตอร์จะมี Routing Table สำหรับเก็บข้อมูล เพื่อใช้ในการพิจารณาเลือกเส้นทางในการส่งดาต้าแกรม

2.4 อุปกรณ์เราเตอร์ (Router)

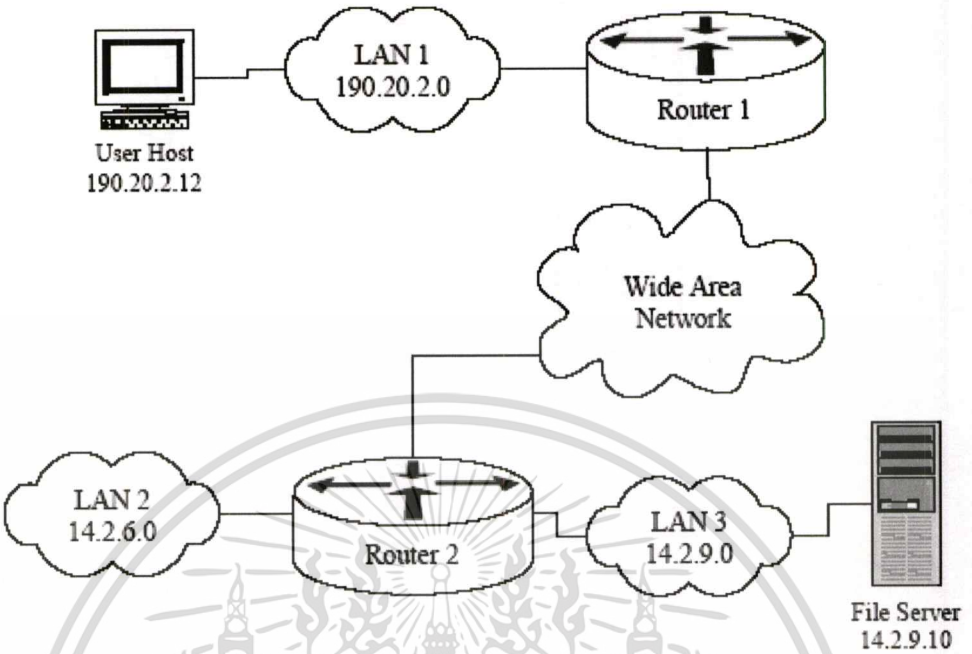
หลักการทำของอุปกรณ์เราเตอร์ (Router)

อุปกรณ์เราเตอร์ถือเป็นสิ่งจำเป็นสำหรับกรณีที่ต้องการเชื่อมต่อหลายๆ เครือข่ายเข้าด้วยกัน ไม่ว่าจะเป็นเครือข่ายระหว่างแลนด้วยกัน หรือเครือข่ายระหว่างแลนกับแวน โดยอุปกรณ์เราเตอร์จะทำงานอยู่ในระดับชั้นที่ 3 ชั้นเครือข่ายของแบบจำลอง OSI ซึ่งฟังก์ชั่นการทำงานที่สำคัญของอุปกรณ์เราเตอร์คือ การเลือกเส้นทางเพื่อส่งแพ็คเก็ตข้อมูลไปยังปลายทางได้อย่างถูกต้องและเหมาะสม รวมถึงความสามารถในการเปลี่ยนเส้นทางเดินของข้อมูลในกรณีที่เส้นทางเดิมที่ใช้งานอยู่เกิดขัดข้อง

อุปกรณ์เราเตอร์จะรับข้อมูลเป็นแพ็คเก็ตเข้ามาตรวจสอบแอดเดรสปลายทาง จากนั้นนำมาเปรียบเทียบกับตารางเส้นทางที่ได้รับการโปรแกรมไว้เพื่อหาเส้นทางที่ส่งต่อ หากเส้นทางที่ส่งมาจากอีเทอร์เน็ต (Ethernet) และส่งต่อออกช่องทางของ Port WAN เป็นแบบ Point-to-Point ก็จะมีการปรับปรุงรูปแบบสัญญาณให้เข้ากับมาตรฐานใหม่ เพื่อส่งไปยังเครือข่าย WAN ได้

ปัจจุบันอุปกรณ์เราเตอร์ได้รับการพัฒนาไปมากทำให้การใช้งานอุปกรณ์เราเตอร์มีประสิทธิภาพ โดยเฉพาะเมื่อเชื่อมอุปกรณ์เราเตอร์หลาย ๆ ตัวเข้าด้วยกันเป็นเครือข่ายขนาดใหญ่ อุปกรณ์เราเตอร์สามารถทำงานอย่างมีประสิทธิภาพ โดยการหาเส้นทางเดินที่สั้นที่สุดซึ่งเลือกตามความเหมาะสมและแก้ปัญหาที่เกิดขึ้นเองได้

เครือข่ายต่างๆ ที่เชื่อมต่อด้วยอุปกรณ์เราเตอร์อาจมีโปรโตคอลที่ใช้งานแตกต่างกันได้ และด้วยความสามารถของอุปกรณ์เราเตอร์ทำให้เหมาะอย่างยิ่งสำหรับเครือข่ายที่มีการเชื่อมต่อระหว่างกันหลายๆ เครือข่าย โดยเฉพาะเครือข่ายอินเตอร์เน็ต



รูปที่ 2.8 การเชื่อมต่อเครือข่ายด้วยอุปกรณ์เราเตอร์

Routing Protocol

หัวใจสำคัญในการทำงานของอุปกรณ์เราเตอร์ ได้แก่ การเลือกเส้นทาง และวิธีการเลือกเส้นทาง ก็อาศัยการคำนวณโดยใช้ค่าที่ได้มาจากการสำรวจ รวมทั้งตัวแปรมาตรฐานที่มีอยู่ นำมาใช้เพื่อการคำนวณ เส้นทาง ที่ดีที่สุดที่จะนำพาแพ็คเก็ตไปที่ปลายทาง สำหรับอุปกรณ์เราเตอร์ที่เชื่อมต่อกันแบบ Point To Point หรือแบบที่มีเพียงเส้นทางเดียวในการเชื่อมต่อระหว่างกัน ไม่ต้องใช้โปรโตคอลเลือกเส้นทาง เพราะจะทำให้เกิด Delay และปัญหาความล่าช้าอื่นๆ มากมาย ควรใช้การวิธีการที่เรียกว่า Static Route จะดีกว่า โดยกำหนดเส้นทางในการนำส่งแพ็คเก็ตที่ตายตัวให้กับอุปกรณ์เราเตอร์ซึ่งจะได้ประโยชน์ ไม่ว่าจะเป็นเรื่องความเร็ว ปัญหาเกี่ยวกับความปลอดภัยของข้อมูล และอื่นๆ

เมื่อหัวใจหลักของอุปกรณ์เราเตอร์คือ การเลือกเส้นทางที่ดีที่สุด ดังนั้นผู้ที่มอบประสิทธิภาพนี้ให้แก่เราเตอร์คือ โปรโตคอลเลือกเส้นทาง อันเป็นวิถีทางในการคำนวณและจัดหาเส้นทางที่ดีที่สุด ที่เร็วที่สุด ไปสู่ปลายทางในรูปแบบของซอฟท์แวร์ที่ฝังตัวอยู่ในอุปกรณ์เราเตอร์สำหรับอุปกรณ์เราเตอร์ของ Cisco ตัวโปรโตคอลนี้มาจากระบบปฏิบัติการ I/O ของ Cisco หรือ IOS ภายใต้ IOS Version ต่างๆ อุปกรณ์เราเตอร์จะมีความสามารถในการใช้โปรโตคอลเลือกเส้นทางที่แตกต่างกันออกไป โดยโปรโตคอลเลือกเส้นทางจะสั่งการให้อุปกรณ์เราเตอร์ทำกิจกรรมเบื้องต้น ใน

ทันทีที่อุปกรณ์เราเตอร์เริ่มทำงานและโปรโตคอลเลือกเส้นทางได้รับการจัดตั้งขึ้นเรียบร้อย กิจกรรมเบื้องต้นในที่นี้ได้แก่ การส่งข้อมูลข่าวสารชิ้นเล็กๆ ออกไปที่อุปกรณ์เราเตอร์เพื่อนบ้าน ในลักษณะทักทายกันเพื่อให้ได้ข้อมูลมา อย่างน้อย 3 ประการ ได้แก่

1. ความมีตัวตนในขณะนั้นของเราเตอร์เพื่อนบ้าน โดยจะได้รับการตอบรับหาก มีตัวตน
2. ระยะทางความห่าง ในรูปแบบของ Delay หรือ จำนวนครั้งที่จะโดดข้าม
3. Port ที่สามารถเข้าถึงเราเตอร์เพื่อนบ้าน เป็นพอร์ตใดบ้าง

หลังจากที่ได้ข้อมูลมาแล้วเราเตอร์จะทำการปรับแต่งหรือจัดสร้างตารางเลือกเส้นทางหรือ Routing Table ขึ้น จากนั้น จะนำข้อมูลนี้ส่งออกไปให้อุปกรณ์เราเตอร์เพื่อนบ้าน เพื่อให้ อุปกรณ์เราเตอร์เพื่อนบ้านนี้ นำไปปรับปรุงตารางเส้นทางของตนเองต่อไป กิจกรรมแบบนี้จะเกิดขึ้นซ้ำแล้วซ้ำอีก เป็นห้วงเวลาที่แน่นอน ซึ่งเราเตอร์ที่เชื่อมต่อกันโดยตรง จะใช้กิจกรรมในลักษณะนี้ต่อกัน ตามการชี้นำของโปรโตคอลเลือกเส้นทางโดยโปรโตคอลเลือกเส้นทาง สามารถแบ่งออกเป็นระดับขั้นได้ 2 แบบ ดังนี้

1. ระดับขั้น Interior Domain หรือ Intra-Domain Routing Protocol
2. ระดับขั้น Exterior หรือ Inter Domain Gateway Routing Protocol

Interior Domain Routing Protocol

สามารถแบ่งออกเป็น 2 ประเภท ดังนี้

1. Distance Vector Routing Protocol

เป็นโปรโตคอลเลือกเส้นทางที่อาศัย ระยะทางเป็นตัวกำหนด ข้อเสียของ Distance Vector ได้แก่ การที่อุปกรณ์เราเตอร์จะต้องมีการส่งข่าวสารเพื่อหยั่งดูความมีตัวตนของอุปกรณ์เราเตอร์เพื่อนบ้าน รวมทั้งการปรับปรุงตารางเส้นทางของตนเองให้แก่เพื่อนบ้านอย่างสม่ำเสมอตรงเวลา ทำให้อุปกรณ์เราเตอร์ที่ใช้โปรโตคอลเลือกเส้นทางต้องทำงานหนักกว่าอุปกรณ์เราเตอร์ที่ถูกกำหนดให้ทำงานแบบ Static Route อีกทั้งยังทำให้ Bandwidth ส่วนหนึ่งของช่องสัญญาณถูกแบ่งออกไปใช้งานที่ไม่ใช่เพื่อการส่งข้อมูลจริง

ตัวอย่างของ โปรโตคอลเลือกเส้นทางแบบ Distance Vector ได้แก่ RIP Version 1 และ 2 IGRP และ EIGRP ของ Cisco เป็นต้น

2. Link State Routing Protocol

โปรโตคอลเลือกเส้นทางแบบ Link State อาศัยสถานะการเชื่อมต่อระหว่างอุปกรณ์เราเตอร์เป็นหลักเกณฑ์ในการตัดสินใจเลือกเส้นทาง โดยจะมีการส่งข่าวสารใน

ลักษณะทักทายกันออกไป เพื่อตรวจสอบหรือหยั่งดูความมีตัวตนของอุปกรณ์เราเตอร์เพื่อนบ้าน เมื่อใดที่ไม่ปรากฏการตอบรับของอุปกรณ์เราเตอร์เพื่อนบ้าน อุปกรณ์เราเตอร์จะรีบปรับปรุงตารางเลือกเส้นทางของตนเอง จากนั้นจะรีบประกาศให้อุปกรณ์เราเตอร์ทุกตัวบนเครือข่าย หรือกลุ่มของอุปกรณ์เราเตอร์ตัวแทนที่เชื่อมต่อระหว่างกันทราบ ดังนั้น การเปลี่ยนแปลงใดๆ ที่เกิดขึ้นบนเครือข่ายอุปกรณ์เราเตอร์ทุกตัวจะได้รับข่าวสารที่ทันเหตุการณ์

โปรโตคอลแบบ Link State มีประสิทธิภาพในการทำงานที่ดีกว่า Distance Vector ตรงที่ การปรับปรุงตารางเส้นทางของอุปกรณ์เราเตอร์แต่ละตัวจะเกิดขึ้นก็ต่อเมื่อมีการเปลี่ยนแปลงเกิดขึ้นเท่านั้น และหากมีการเปลี่ยนแปลงเกิดขึ้นจริง การปรับปรุงตารางเส้นทางก็เป็นเพียงบางส่วนที่เปลี่ยนแปลงจริงเท่านั้น เปรียบเทียบกับ Distance Vector ที่มีการปรับปรุงเป็นห้วงเวลาที่แน่นอน อีกทั้งการปรับปรุงที่เกิดขึ้นเป็นการปรับปรุงใหม่หมดทั้งตาราง ในลักษณะทำสำเนาทับทั้งตาราง ซึ่งทำให้การปรับปรุงแต่ละครั้งมีการใช้ Bandwidth ของเส้นทางค่อนข้างมาก

Inter-Domain Gateway Routing Protocol

เป็นโปรโตคอลเลือกเส้นทางที่นำมาใช้เพื่อเชื่อมกลุ่มของอุปกรณ์เราเตอร์จำนวนมากหลายๆ กลุ่มเข้าด้วยกัน โดยมีอุปกรณ์เราเตอร์อยู่หนึ่งตัวหรือมากกว่านั้น ที่เป็นตัวแทนของอุปกรณ์เราเตอร์ทั้งกลุ่ม เพื่อเชื่อมต่อกับอุปกรณ์เราเตอร์อีกกลุ่มหรือหลายๆ กลุ่มเข้าด้วยกัน โดยอุปกรณ์เราเตอร์ตัวแทนจะใช้โปรโตคอลเลือกเส้นทาง ที่มีวิธีการเลือกเส้นทางที่แตกต่างออกไปจากที่ได้กล่าวมาแล้วทั้งหมด ตัวอย่างของโปรโตคอลเลือกเส้นทางแบบนี้ ได้แก่ BGP ซึ่งบรรดา ISP ทั้งหลาย ต่างก็นำมาใช้เพื่อเชื่อมเครือข่ายเข้ากับอินเตอร์เน็ต หรือระหว่างกัน

2.5 ความปลอดภัยบนอุปกรณ์เราเตอร์

หน้าที่หลักของอุปกรณ์เราเตอร์ คือ การรักษาความปลอดภัยของเครือข่าย ซึ่งในหัวข้อนี้จะอธิบายถึงการป้องกันความปลอดภัยบนอุปกรณ์เราเตอร์ การป้องกันเครือข่ายด้วยอุปกรณ์เราเตอร์ และ วิธีการจัดการความปลอดภัยบนอุปกรณ์เราเตอร์

การป้องกันความปลอดภัยบนอุปกรณ์เราเตอร์

การป้องกันความปลอดภัยบนอุปกรณ์เราเตอร์ สามารถจัดการได้ 3 ส่วนด้วยกัน คือ

1. Physical Security

การป้องกันความปลอดภัยบนอุปกรณ์เราเตอร์ทางด้านกายภาพ มีด้วยกันหลายวิธีดังนี้

- ห้องที่เก็บอุปกรณ์เราเตอร์จะต้องไม่มีสัญญาณรบกวนจากคลื่นแม่เหล็กไฟฟ้า หรือไฟฟ้าสถิตย์
- ห้องที่เก็บอุปกรณ์เราเตอร์จะต้องมีการควบคุมอุณหภูมิและความชื้น
- อุปกรณ์เราเตอร์จะต้องต่อเข้ากับอุปกรณ์สำรองไฟ (UPS) เสมอ
- อุปกรณ์เราเตอร์ควรมีจำนวนหน่วยความจำให้มากที่สุดเท่าที่จะทำได้
- ห้องที่เก็บอุปกรณ์เราเตอร์ควรอนุญาตให้เฉพาะผู้ที่มีส่วนเกี่ยวข้องเท่านั้นที่สามารถเข้าไปได้ และควรมีการล็อกกุญแจเสมอ

2. Operating System

ระบบปฏิบัติการที่ใช้บนอุปกรณ์เราเตอร์ ควรใช้ระบบปฏิบัติการที่เป็นเวอร์ชั่นใหม่ แต่ไม่ควรเป็นเวอร์ชั่นที่ใหม่ล่าสุด เนื่องจากระบบปฏิบัติการที่เป็นเวอร์ชั่นใหม่ล่าสุดนั้น ส่วนใหญ่ยังมีรูรั่วอยู่ ดังนั้นจึงควรใช้เป็นเวอร์ชั่นใหม่ที่มีการอัพเดตและแก้ไขรูรั่วเรียบร้อยแล้ว

3. Configuration Hardening

บนอุปกรณ์เราเตอร์สามารถทำการคอนฟิกูเรชั่นบริการต่างๆ ได้หลายบริการ ซึ่งเป็นจุดเด่นหนึ่งของอุปกรณ์เราเตอร์ แต่ถ้าเราเปิดบริการทุกอย่างบนตัวอุปกรณ์เราเตอร์อาจส่งผลเสียได้ เนื่องจากยิ่งเปิดบริการมากเท่าไร ก็จะเกิดช่องโหว่มากขึ้นเท่านั้น ดังนั้น ในการคอนฟิกูเรชั่นอุปกรณ์เราเตอร์ ควรทำการปิดบริการให้หมด แล้วทำการเปิดบริการเฉพาะบริการที่ต้องการใช้งานเท่านั้น ถ้าบริการใดที่ไม่จำเป็นต้องใช้ ก็ไม่ควรจะเปิดใช้

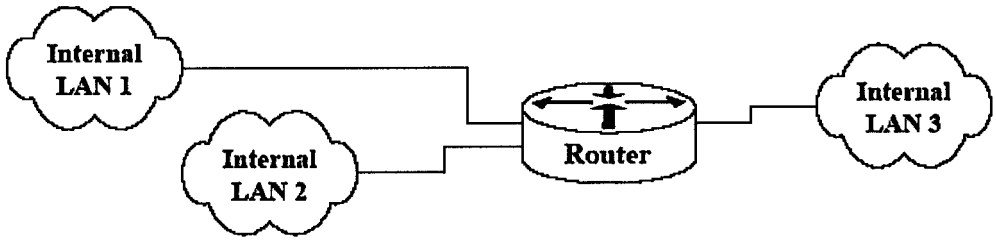
การป้องกันเครือข่ายด้วยอุปกรณ์เราเตอร์

1. หน้าที่ในการปฏิบัติงานด้านเครือข่ายของอุปกรณ์เราเตอร์และระดับความปลอดภัย

อุปกรณ์เราเตอร์ตัวหนึ่งๆ สามารถทำงานต่างๆ กันได้หลายหน้าที่ ขึ้นอยู่กับระดับการรักษาความปลอดภัยและการนำไปใช้งาน โดยทั่วไปแล้วมีอยู่ด้วยกัน 3 หน้าที่หลัก คือ

1. Interior Router

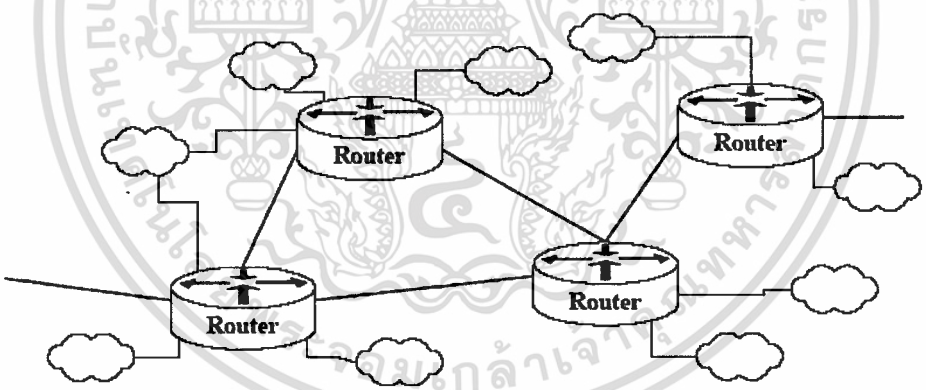
Interior Router คือ เราเตอร์ที่ใช้ในการขนส่งข้อมูลภายในเครือข่ายแลนหลายๆ เครือข่ายในองค์กรเข้าด้วยกัน ซึ่งระดับความน่าเชื่อถือของการเชื่อมต่อโดยใช้ Interior Router นี้จะสูง



รูปที่ 2.9 การเชื่อมต่อของ Interior Router กับเครือข่ายแลน

2. Backbone Router

Backbone Router หรือ Exterior Router คือ อุปกรณ์เราเตอร์ที่ใช้ในการขนส่งข้อมูลระหว่างเครือข่ายขององค์กรแต่ละองค์กร เข้าด้วยกันเป็นอินเตอร์เน็ต ซึ่งระดับความน่าเชื่อถือของการเชื่อมต่อโดยใช้ Backbone Router นี้จะต่ำ เนื่องจากถูกออกแบบมาให้สามารถส่งข้อมูลด้วยความเร็วสูง ดังนั้นจึงไม่มีการตรวจสอบในเรื่องของความปลอดภัย

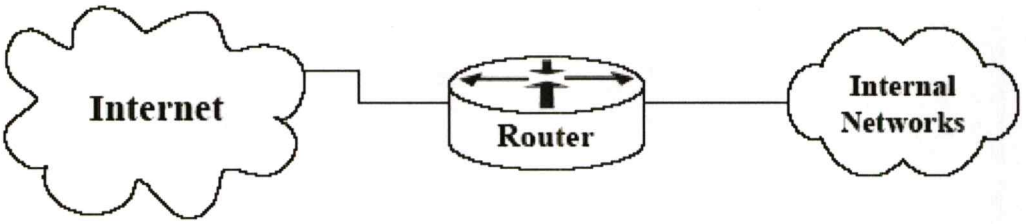


รูปที่ 2.10 การเชื่อมต่อของ Backbone Router กับเครือข่ายต่างๆ

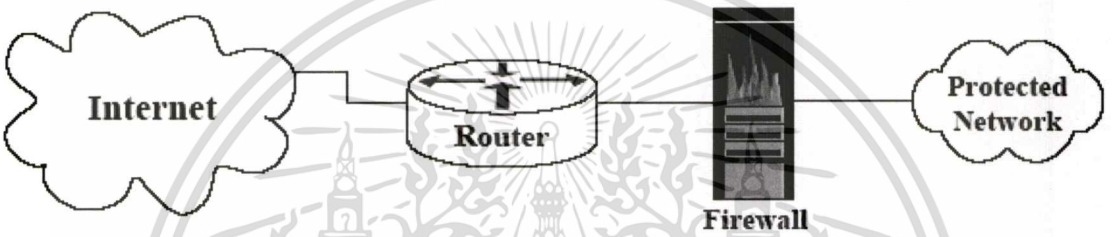
3. Border Router

Border Router คือ เราเตอร์ที่ใช้ในการขนส่งข้อมูลระหว่างเครือข่ายในองค์กรกับเครือข่ายภายนอก หรืออินเตอร์เน็ต ซึ่งระดับความน่าเชื่อถือของการเชื่อมต่อโดยใช้ Border Router นี้ในส่วนที่เป็นเครือข่ายภายในจะมีระดับความน่าเชื่อถือสูงแต่ในส่วนที่เป็นเครือข่ายภายนอกจะมีระดับความน่าเชื่อถือต่ำ

ในแบบ Border Router นี้เราสามารถป้องกันความปลอดภัยให้กับเครือข่ายภายในได้โดยการติดตั้ง Firewall ในฝั่งเครือข่ายภายในได้ ดังรูป



รูปที่ 2.11 การเชื่อมต่อและการติดตั้ง Firewall ในกรณีที่ใช้อุปกรณ์เราเตอร์ตัวเดียว



รูปที่ 2.12 การเชื่อมต่อและการติดตั้ง Firewall ในกรณีที่ใช้อุปกรณ์เราเตอร์สองตัว

2. การกรองแพ็คเก็ตสำหรับโปรโตคอล TCP/IP

อุปกรณ์เราเตอร์สามารถทำการกรองแพ็คเก็ต ทั้งขาเข้าและขาออกได้ โดยที่อุปกรณ์เราเตอร์ นั้นสามารถระบุเงื่อนไขในการกรองแพ็คเก็ตได้หลายรูปแบบ เช่น Source IP Address, Destination IP Address, Source Port, Destination Port, และชนิดของโปรโตคอล โดยที่อุปกรณ์เราเตอร์บางตัวนั้น สามารถทำการกรองแพ็คเก็ตได้จนถึงระดับบิตหรือสามารถเข้าไปดูเฮดเดอร์ของข้อมูลได้ด้วย

การกรองแพ็คเก็ตเป็นหน้าที่ที่สำคัญของอุปกรณ์เราเตอร์ ซึ่งจะทำหน้าที่เสมือนเป็นเกตเวย์ (Gateway) ระหว่างเครือข่ายที่น่าเชื่อถือ (Trusted Network) กับเครื่องข่ายที่ไม่น่าเชื่อถือ (Untrusted Network) โดยอุปกรณ์เราเตอร์จะสามารถบังคับการกำหนดนโยบายของการรักษาความปลอดภัยได้โดยการยกเลิกโปรโตคอลที่ไม่ต้องการและสามารถจำกัดพอร์ต (Port) ให้เป็นไปตามนโยบายของระบบเครือข่ายที่น่าเชื่อถือได้

เราสามารถกำหนดนโยบายได้ 2 รูปแบบ คือ

1. default ACCEPT : ผู้ดูแลอุปกรณ์เราเตอร์จะต้องสร้างกฎ (Rule) เพื่อกำหนดว่าจะปิดบริการและโฮสต์ใดบ้าง โดยบริการและโฮสต์อื่นๆ ที่ไม่ถูกกำหนดไว้ จะมีค่าเป็นเปิด

2. default DROP : ผู้ดูแลอุปกรณ์เราเตอร์จะต้องสร้างกฎ (Rule) เพื่อกำหนดว่าจะเปิดบริการและโฮสต์ใดบ้าง โดยบริการและโฮสต์อื่นๆ ที่ไม่ถูกกำหนดไว้ จะมีค่าเป็นปิด

อย่างไรก็ตาม ไม่ว่าจะกำหนดนโยบายในรูปแบบใด ผู้ดูแลอุปกรณ์เราเตอร์ ก็ควรทราบ TCP/IP service ที่เป็นจุดอ่อนต่างๆ ในระบบด้วย ดังนี้

ตารางที่ 2.1 TCP/UDP service ที่ควรปิดกั้นไม่ให้ใช้ทั้งจากภายใน - นอกเครือข่าย

Port(s) (Transport)	Server	Port(s) (Transport)	Server
1 (TCP & UDP)	tcpmux	1761 - 1764	sms-helpdesk
7 (TCP & UDP)	echo	(TCP & UDP)	
9 (TCP & UDP)	discard	1807 (TCP)	SpySender
11 (TCP & UDP)	systat	1981 (TCP)	Shockrave
13 (TCP & UDP)	daytime	1999 (TCP)	BackDoor
15 (TCP & UDP)	netstat	2001 (TCP)	Trojan Cow
17 (TCP & UDP)	qotd	2023 (TCP)	Ripper
19 (TCP & UDP)	chargen	2049 (TCP & UDP)	nfs
37 (TCP & UDP)	time	2115 (TCP)	Bugs
43 (TCP & UDP)	whois	2140 (TCP)	Deep Throat
67 (TCP & UDP)	bootps	2222 (TCP)	Subseven21
68 (TCP & UDP)	bootpc	2301 (TCP & UDP)	compaqdiag
69 (UDP)	tftp	2565 (TCP)	Striker
93 (TCP)	supdup	2583 (TCP)	WinCrash
111 (TCP & UDP)	sunrpc	2701 (TCP & UDP)	sms-rcinfo
135 (TCP & UDP)	loc-srv	2702 (TCP & UDP)	sms-remctrl
137 (TCP & UDP)	netbios-ns	2703 (TCP & UDP)	sms-chat
138 (TCP & UDP)	netbios-dgm	2704 (TCP & UDP)	sms-xfer
139 (TCP & UDP)	netbios-ssn	2801 (TCP)	Phineas P.
177 (TCP & UDP)	xdmcp	4045 (TCP)	lockd

ตารางที่ 2.1 TCP/UDP service ที่ควรปิดกั้นไม่ให้ใช้ทั้งจากภายใน - นอกเครือข่าย (ต่อ)

Port(s) (Transport)	Server	Port(s) (Transport)	Server
445 (TCP & UDP)	microsoft-ds	5800 - 5899 (TCP)	winvnc web server
512 (TCP)	rexec	5900 - 5999 (TCP)	winvnc
513 (TCP)	rlogin	6000 - 6063 (TCP)	X11 Window System
513 (UDP)	who	6665 - 6669 (TCP)	irc
514 (TCP)	rsh, rcp, rdist,	6711 - 6712 (TCP)	Subseven
	rdump, rrestore	6776 (TCP)	Subseven
515 (TCP)	lpr	7000 (TCP)	Subseven21
517 (UCP)	talk	12345 - 12346 (TCP)	NetBus
518 (UCP)	ntalk	16660 (TCP)	Stacheldraht
540 (TCP)	uucp	27444 (UCP)	Trinoo
1024 (TCP)	NetSpy	27666 (TCP)	Trinoo
1045 (TCP)	Rasmin	31335 (UCP)	Trinoo
1090 (TCP)	Xtreme	31337 -31338	Back Orifice
1170 (TCP)	Psyber S.S	(TCP & UDP)	RPC services
1234 (TCP)	Ultors Trojan	32700 – 32900	Trinity V3
1243 (TCP)	Backdoor-G	(TCP & UDP)	
1245 (TCP)	VooDoo Doll	32720 (TCP)	Trinity V3
1349 (UCP)	Back Orifice DLL	39168 (TCP)	
1492 (TCP)	FTP99CMP	65000 (TCP)	Stacheldraht
1600 (TCP)	Shivka-Burka		

ตารางที่ 2.2 แสดง TCP/UDP service ที่ควรปิดกั้นไม่ให้เข้ามาจากภายนอก

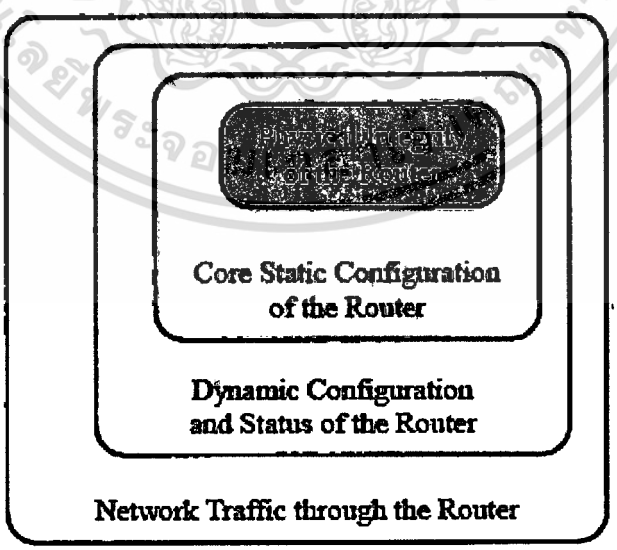
Port(s) (Transport)	Server
79 (TCP)	finger
161 (TCP & UDP)	snmp
162 (TCP & UDP)	snmp trap
514 (UDP)	syslog
550 (TCP & UDP)	new who

2.6 นโยบายการรักษาความปลอดภัยสำหรับเราเตอร์

อุปกรณ์เราเตอร์เป็นส่วนสำคัญส่วนหนึ่งของเครือข่ายคอมพิวเตอร์ ดังนั้นการรักษาความปลอดภัยบนอุปกรณ์เราเตอร์จึงเป็นสิ่งสำคัญอย่างมากที่จะช่วยรักษาความปลอดภัยบนเครือข่ายได้ ซึ่งเราควรทำการเรียนรู้เกี่ยวกับนโยบายการรักษาความปลอดภัยบนอุปกรณ์เราเตอร์ในเรื่องต่างๆ ดังนี้

1. แนวความคิดพื้นฐานของนโยบายการรักษาความปลอดภัยบนอุปกรณ์เราเตอร์

การรักษาความปลอดภัยของอุปกรณ์เราเตอร์ แบ่งออกเป็นลำดับชั้นได้ 4 ชั้นด้วยกัน ดังรูป



รูปที่ 2.13 ลำดับชั้นของความปลอดภัยบนอุปกรณ์เราเตอร์

โดยมีรายละเอียดในแต่ละลำดับชั้น ดังนี้

1. Physical Integrity

เป็นชั้นที่อยู่ในสุดของนโยบายการรักษาความปลอดภัยบนอุปกรณ์เราเตอร์ ซึ่งเป็นการรักษาความปลอดภัยทางด้านกายภาพของอุปกรณ์เราเตอร์ โดยที่อุปกรณ์เราเตอร์สามารถถูกโจมตีจากผู้ที่ไม่ประสงค์ดี ได้ด้วยวิธีการเข้าถึงอุปกรณ์เราเตอร์ทางกายภาพนี้ได้โดยตรง ดังนั้นในการเข้าถึงทางด้านกายภาพจึงจำเป็นต้องถูกควบคุมและจัดหาองค์ประกอบที่แข็งแรงมาปกป้องการเข้าถึงทางด้านกายภาพ โดยที่อุปกรณ์เราเตอร์ทั้งหมดสามารถเสนอทางเลือกขึ้นมาในการสร้างการเชื่อมต่อโดยตรงซึ่ง เราเรียกว่า Console Port โดยที่พอร์ตเหล่านี้เป็นพอร์ตพิเศษที่ใช้ในการควบคุมอุปกรณ์เราเตอร์ ซึ่งนโยบายการรักษาความปลอดภัยบนอุปกรณ์เราเตอร์ควรจะประกาศกฎว่าจะมีการเข้าถึงและใช้งานผ่านทางพอร์ตนี้ได้อย่างไร

2. Core Static Configuration

เป็นลำดับชั้นถัดมาของรูปภาพ ซึ่งเป็นส่วนที่เก็บซอฟท์แวร์และสถานะของการคอนฟิกูเรชั่นของอุปกรณ์เราเตอร์เอง ถ้าผู้ไม่ประสงค์ดีสามารถโจมตีเข้ามาได้ทั้งสองส่วนนี้ ผู้ไม่ประสงค์ดีจะสามารถเข้าควบคุมอุปกรณ์เราเตอร์ได้ทุกส่วน ตามปกติแล้วนโยบายการรักษาความปลอดภัยบนอุปกรณ์เราเตอร์ในส่วนนี้ควรจะมีกฎที่เข้มงวดเกี่ยวกับการเข้าถึงอุปกรณ์เราเตอร์ในลำดับนี้ให้มาก

3. Dynamic Configuration

ส่วนในลำดับชั้นที่ 3 เป็นส่วนของการคอนฟิกูเรชั่นที่ไม่ตายตัวของอุปกรณ์เราเตอร์ นั่นคือในส่วนของการคอนฟิกูเรชั่น Routing Protocol โดยข้อมูลที่ไม่ตายตัวนั้นจะประกอบไปด้วยสถานะของ Interface, ARP Table และ Log file ถ้าผู้ไม่ประสงค์ดีสามารถโจมตีในส่วนนี้ได้ จะสามารถเข้าควบคุมลำดับชั้นในส่วนสุดท้ายหรือส่วนนอกสุดได้

4. Network Traffic through the router

ในลำดับชั้นสุดท้ายหรือนอกสุดนี้ เป็นส่วนที่เกี่ยวข้องกับ Traffic ของระบบเครือข่ายภายในและระบบเครือข่ายภายนอกที่อุปกรณ์เราเตอร์ใช้ในการจัดการเกี่ยวกับนโยบายการรักษาความปลอดภัยของเครือข่ายทั้งหมด โดยจะรวมถึงกฎที่เกี่ยวข้องกับการอนุญาตในการเข้าถึงโปรโตคอลและบริการ

2. นโยบายการรักษาความปลอดภัยบนอุปกรณ์เราเตอร์และบนเครือข่ายทั้งหมด

นโยบายสำหรับการรักษาความปลอดภัยบนอุปกรณ์ราเตอร์ต้องปรับให้เหมาะสมกับโครงสร้างทั้งหมดของเครือข่าย ซึ่งหน้าที่ที่ถูกกำหนดในนโยบายการรักษาความปลอดภัยบนอุปกรณ์เราเตอร์ทั้งหมดนั้น โดยปกติแล้วจะเป็นเพียงส่วนหนึ่งของนโยบายรักษาความปลอดภัยของเครือข่ายเท่านั้น ซึ่งกฎต่างๆ ของการปฏิบัติงานสำหรับผู้ดูแลอุปกรณ์เราเตอร์จะต้องถูกกำหนดไว้อย่างชัดเจน โดยส่วนใหญ่นโยบายการรักษาความปลอดภัยของระบบเครือข่ายจะมีการประกาศหน้าที่ออกเป็น 3 ส่วนด้วยกัน คือ ส่วนของผู้ดูแลระบบ (Administrator), ส่วนของผู้ปฏิบัติงาน (Operator) และส่วนของผู้ใช้งาน (User) แต่สำหรับนโยบายการรักษาความปลอดภัยบนอุปกรณ์เราเตอร์จะมีการประกาศหน้าที่เพียง 2 ส่วนคือ ส่วนของผู้ดูแลระบบ (Administrator), ส่วนของผู้ปฏิบัติงาน (Operator) เท่านั้น ตัวอย่างเช่น หน้าที่ของผู้ปฏิบัติงานจะสามารถดูได้ในส่วนที่เป็น Audit Log เท่านั้น

3. การสร้างนโยบายด้านความปลอดภัยสำหรับอุปกรณ์เราเตอร์

มีหลายสิ่งที่จะต้องจดจำเมื่อมีการสร้างนโยบายด้านความปลอดภัยสำหรับอุปกรณ์เราเตอร์นั่นคือ

- วัตถุประสงค์หลักของการรักษาความปลอดภัย ไม่ใช่แค่คำสั่งหรือกระบวนการเท่านั้นแต่ควรพิจารณาถึงผลที่จะเกิดขึ้นจากนโยบายที่กำหนดด้วย
- นโยบายจะต้องครอบคลุมลำดับชั้นของการรักษาความปลอดภัยบนอุปกรณ์เราเตอร์ทั้ง 4 ชั้น ที่ได้กล่าวไว้ข้างต้นด้วย

□ บริการและโปรโตคอลใดที่ไม่มีการใช้งาน ก็ไม่ควรเปิดให้ใช้งาน

4. Checklist สำหรับบริหารจัดการอุปกรณ์เราเตอร์

ควรมีการออกแบบ Checklist ขึ้นมาเพื่อเป็นเครื่องช่วยในการตรวจสอบความปลอดภัยในการกำหนดค่าการทำงานให้กับอุปกรณ์เราเตอร์และช่วยทบทวนถึงรายละเอียดความปลอดภัยทั้งหมดที่เกี่ยวข้อง ซึ่งลักษณะของ Checklist สำหรับบริหารจัดการอุปกรณ์เราเตอร์ควรมีลักษณะ ดังนี้

- กำหนดให้การสร้างเส้นทางในระบบเครือข่ายต้องมีการพิสูจน์ตัวตนด้วย MD5 ให้กับอุปกรณ์เราเตอร์ทั้งหมดขององค์กรที่อยู่ภายใต้ Autonomous Systems (AS) เดียวกัน ซึ่งโปรโตคอลที่ใช้ในการสร้างเส้นทางและมีคุณสมบัติรองรับ MD5 ได้แก่ BGP, OSPF, IS-IS, EIGRP และ RIPv.2

- จำกัดให้เฉพาะอุปกรณ์เราเตอร์ภายนอกที่จะทำการเชื่อมต่อกับอุปกรณ์เราเตอร์ภายในองค์กรกับพอร์ต TCP 179 จะต้องเป็นอุปกรณ์เราเตอร์ที่มี AS ที่เชื่อถือได้เท่านั้น
- กำหนดให้มีการใช้งานเครื่องเซิร์ฟเวอร์ที่ทำหน้าที่พิสูจน์ตัวตนสำหรับบุคคลที่จะเข้าใช้งาน โดยจะต้องพิสูจน์ตัวตนทุกครั้งก่อนการใช้งาน
- กำหนดให้มีบัญชีผู้ใช้งานภายในอุปกรณ์เราเตอร์ให้น้อยที่สุด
- กำหนดสิทธิและขอบเขตการใช้งานให้แก่ผู้ใช้งานไว้ที่ระดับต่ำที่สุด เพื่อให้ผู้ใช้มีสิทธิเข้าปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมายเท่านั้น
- ปิดการใช้งานพอร์ต AUX
- สร้างแบนเนอร์ (Banner) เพื่อแจ้งให้กับผู้ที่ไม่ได้รับอนุญาตให้เข้าถึงการใช้งานอุปกรณ์เราเตอร์ทราบ
- กำหนดให้มีการใช้รหัสผ่านให้กับผู้ใช้ที่ผ่านทางคอนโซล และจากระยะไกลโดยเทอร์มินัล VTY
- กำหนดเวลาในการเชื่อมต่อกับอุปกรณ์เราเตอร์ ถ้าหากไม่มีการใช้งานนานเกินกว่า 15 นาที ให้ยุติการเชื่อมต่อทันที
- ปิดอินเตอร์เฟสบนอุปกรณ์เราเตอร์ที่ไม่มีความจำเป็นในการใช้งาน
- กำหนดให้การเชื่อมต่อในลักษณะ In-band เพื่อติดต่อกับอุปกรณ์เราเตอร์ต้องมีการใช้รหัสผ่านก่อนทุกครั้ง
- อนุญาตเฉพาะบาง IP Address ภายในระบบเครือข่ายเท่านั้น ที่มีสิทธิเชื่อมต่อกับอุปกรณ์เราเตอร์เพื่อบริหารจัดการโดยใช้ Access Control Lists (ACLs)
- กำหนดให้ใช้ SSH สำหรับการเชื่อมต่อ เพื่อบริหารจัดการอุปกรณ์เราเตอร์เพื่อความปลอดภัย
- กำหนดเวลาในการเชื่อมต่อกับอุปกรณ์เราเตอร์ให้จำกัดไม่เกิน 15 นาทีต่อการเชื่อมต่อ 1 ครั้ง
- กำหนดให้อุปกรณ์เราเตอร์มีการบันทึกการใช้งานทุกครั้งที่มีการเชื่อมต่อกับอุปกรณ์เราเตอร์จากระยะไกลโดยเทอร์มินัล VTY
- ปิดการบริหารจัดการอุปกรณ์เราเตอร์ผ่านทางโปรโตคอล HTTP, FTP หรือ BSD r เพื่อจำกัดการเชื่อมต่อที่ไม่จำเป็น

- กำหนดอินเตอร์เฟสที่เชื่อมต่อกับภายนอกไม่ให้ตอบสนองต่อแพ็คเก็ต ICMP ขาออกประเภท IP Unreachable, IP Redirects และ IP Mask-reply เพื่อลดโอกาสในการโจมตีจากภายนอก
- กำหนดรูปแบบของเหตุการณ์ที่ทำการบันทึกโดยให้ระบุวันเวลาของเหตุการณ์ที่เกิดขึ้นให้เป็นมาตรฐาน
- กำหนดอุปกรณ์เราเตอร์ให้ตั้งสัญญาณนาฬิกาตามเวลามาตรฐานโดยใช้งาน NTP Server อย่างน้อย 2 เครื่อง เพราะหากเครื่องแรกไม่สามารถให้บริการได้จะยังสามารถตั้งสัญญาณนาฬิกาจากอีกเครื่องได้
- หากมีความจำเป็นต้องใช้บริการแปลงชื่อโดเมนกับ IP Address ให้กำหนด DNS ไว้ในอุปกรณ์เราเตอร์เพื่อใช้งาน
- กำหนด ACL ที่ใช้ในอุปกรณ์เราเตอร์เพื่ออนุญาตให้ใช้งานตามที่จำเป็นเท่านั้น ที่เหลือให้ปฏิเสธทิ้งให้หมด
- ตรวจสอบ ACL ที่ใช้งานให้ตรงกับอินเตอร์เฟส เช่น ACL ที่สร้างเพื่อใช้งานแค่ภายในไม่ควรนำไปใช้กับอินเตอร์เฟสที่ติดต่อกับด้านนอก
- กำหนดให้อุปกรณ์เราเตอร์ทำการบันทึกทุกครั้งที่พบว่า อุปกรณ์เราเตอร์มีการปฏิเสธการใช้งาน ไม่ว่าจะเกิดจากการเชื่อมต่อมายังพอร์ต โปรโตคอลหรือผ่านทางบริการต่างๆ ที่อยู่ในอุปกรณ์เราเตอร์ด้วย
- กำหนดให้อุปกรณ์เราเตอร์ทำการบันทึกเหตุการณ์ตั้งแต่ระดับ 0 - 6 และส่งข้อมูลไปยังเครื่องเซิร์ฟเวอร์ SysLog
- จำกัดการติดต่อประเภท SNMP กับอุปกรณ์เราเตอร์โดยอนุญาตให้เฉพาะ IP Address ที่ได้รับอนุญาตไว้แล้วเท่านั้น
- กำหนดการใช้งาน SNMP ให้อยู่ในโหมดที่สามารถอ่านได้อย่างเดียว (Read-Only) เท่านั้น หรือกำหนดสิทธิอื่นที่สูงกว่าจะขึ้นอยู่กับความจำเป็นซึ่งได้พิจารณาจากผู้ดูแลระบบแล้ว
- ใช้ ACL ในการกำหนดให้อุปกรณ์เราเตอร์ยอมรับการเชื่อมต่อเฉพาะแพ็คเก็ตที่มาจาก IP Address ที่ใช้งานภายในระบบเครือข่ายเท่านั้น
- กำหนดให้มีการตรวจสอบ ACL อย่างน้อยปีละหนึ่งครั้ง หรือตามรอบระยะเวลาที่หน่วยงานกำหนดไว้

- อนุญาตให้แพ็คเก็ตขาออกบางประเภทเท่านั้นที่สามารถใช้งานได้ เช่น HTTP, Mail และต้องอนุญาตให้ทำการเชื่อมต่อกับ IP Address ที่มีอยู่จริงเท่านั้น โดยใช้คำสั่งประเภท ACL ร่วมกับ Unicast Reverse Path Forwarding เพื่อตรวจสอบแพ็คเก็ตของ IP Address ต้นทาง
- กำหนดให้อุปกรณ์เราเตอร์ใช้คำสั่งประเภท TCP Intercept command เพื่อป้องกันการโจมตีจากเครือข่ายภายนอก เช่น ป้องกันการทำ TCP SYN flood จากเครือข่ายภายนอก
- ปฏิเสธการติดต่อจากแพ็คเก็ต ICMP ขาเข้าประเภท Echo Reply (type 0), Time Exceeded (type 11) และ Destination Unreachable (type 3)
- ปฏิเสธการติดต่อของแพ็คเก็ต ICMP ขอออกประเภท Echo Request (type 8), Parameter Problem (type 12) และ Source Quench (type 4)
- กำหนดให้อุปกรณ์เราเตอร์ไม่อนุญาตให้แพ็คเก็ตจากโปรแกรม traceroute ที่เข้ามายังอุปกรณ์เราเตอร์ไม่ให้มีการใช้งาน
- ไม่ใช้โปรโตคอลประเภท TFTP ในการโอนถ่ายข้อมูลคอนฟิกูเรชั่น หรือเฟิร์มแวร์ของอุปกรณ์เราเตอร์เนื่องจากโปรโตคอล ดังกล่าวไม่มีการเข้ารหัส

บทที่ 3
การออกแบบโครงสร้างระบบ

เดิมการค้นหาช่องโหว่ของการคอนฟิกูเรชั่น ผู้ดูแลระบบรักษาความปลอดภัยจะต้องนำคอนฟิกูเรชั่นที่ได้จากอุปกรณ์เราเตอร์ มาทำการตรวจสอบด้วยสายตาเพื่อหาช่องโหว่ที่เกิดจากการคอนฟิกูเรชั่นได้ ซึ่งในบางครั้งอาจเกิดการผิดพลาด หลงลืมเกี่ยวกับคำสั่งของอุปกรณ์เราเตอร์ทำให้การคอนฟิกูเรชั่นมีข้อผิดพลาดได้ และเมื่อมีการนำอุปกรณ์เราเตอร์ที่มีการคอนฟิกูเรชั่นที่ไม่สมควรมาใช้งานในระบบจริง อาจทำให้ผู้ไม่ประสงค์ดีสามารถโจมตีเข้าสู่ระบบเครือข่ายของเราได้ หรือบางทีอาจจะใช้ตัวอุปกรณ์เราเตอร์ของเราเป็นสื่อในการโจมตีต่อระบบเครือข่ายของผู้อื่นได้อีกด้วย ดังนั้นจึงเห็นได้ว่าอุปกรณ์เราเตอร์มีความจำเป็นที่จะต้องปิดช่องโหว่เหล่านั้น เพื่อลดปัญหาภัยคุกคามที่เกิดจากผู้ไม่ประสงค์ดีหรือไวรัสได้

ในการพัฒนาระบบการตรวจสอบการคอนฟิกูเรชั่นตัวอุปกรณ์เราเตอร์นี้ จะจัดทำการตรวจสอบเฉพาะการคอนฟิกูเรชั่นอุปกรณ์เราเตอร์ของ CISCO เท่านั้น เนื่องจากการคอนฟิกูเรชั่นในอุปกรณ์เราเตอร์แต่ละผู้ผลิตจะมีลักษณะการคอนฟิกูเรชั่นและลักษณะของคำสั่งที่แตกต่างกันออกไป

3.1 การสำรวจความต้องการของระบบ

ในการสำรวจความต้องการของการพัฒนาระบบการตรวจสอบการคอนฟิกูเรชั่นของอุปกรณ์เราเตอร์ ได้มีการกระทำ 2 วิธี คือ

1. ทำการสัมภาษณ์ผู้ดูแลระบบเครือข่ายและเจ้าหน้าที่ด้านการรักษาความปลอดภัยของระบบเครือข่ายเพื่อศึกษาหาปัญหาที่เกิดขึ้นและความต้องการของใช้งานของระบบ
2. ทำการศึกษาและวิเคราะห์จากเอกสารต่างๆ ที่มีอยู่ และการเฝ้าสังเกตการณ์รวมถึงการลองทำงานด้วยตัวเอง

เมื่อได้ทำการสำรวจความต้องการของบุคคลต่างๆ ที่เกี่ยวข้องกับระบบแล้ว พบว่าการตรวจสอบคอนฟิกูเรชั่นด้วยตนเองนั้น มีความยุ่งยาก และเสียเวลามาก และผู้เกี่ยวข้องเห็นด้วยกับการที่จะมีระบบนี้ขึ้นมาเพื่อช่วยเสริมการทำงานให้มีประสิทธิภาพที่ดีขึ้น

3.2 แนวทางการพัฒนาระบบ

เมื่อได้ศึกษาวิธีการทำงานแบบเดิมและวิเคราะห์ปัญหาที่เกิดขึ้นแล้ว จึงได้มีการออกแบบระบบการตรวจสอบการคอนฟีกูเรชั่นตัวอุปกรณ์เราเตอร์ของ Cisco ขึ้น เพื่อช่วยในการหาช่องโหว่ของการคอนฟีกูเรชั่นที่เกิดขึ้นได้อย่างถูกต้อง แม่นยำ และรวดเร็วขึ้น

ซึ่งระบบจะมีการทำงาน ดังนี้

1. ระบบสามารถทำการตรวจสอบช่องโหว่ได้ โดยมีการแบ่งการตรวจสอบออกเป็นหมวดหมู่ ดังนี้
    - Router Access Security
    - Router Service Security
    - Router Access List
    - Audit Management
    - Scan Routing
2. ระบบสามารถเก็บรูปแบบของการคอนฟีกูเรชั่น พร้อมทั้งเก็บระดับความเสี่ยงและปัญหาที่จะเกิดขึ้นเมื่อเราละเลยช่องโหว่เหล่านี้ได้
3. ระบบสามารถเพิ่มเติม ลด หรือแก้ไขรูปแบบของการคอนฟีกูเรชั่นได้ เพื่อความยืดหยุ่นที่จะเกิดขึ้นในอนาคตได้
4. ระบบสามารถแสดงรูปแบบของการคอนฟีกูเรชั่นที่มีอยู่ได้
5. ระบบสามารถแสดงรายละเอียดเกี่ยวกับระดับของความเสี่ยงที่อาจจะเกิดขึ้นการคอนฟีกูเร ชั่น พร้อมทั้งบอกคำแนะนำว่าควรจะทำแบบใดถึงจะเหมาะสมกว่าและเกิดความเสี่ยงน้อยกว่าได้

ระบบการตรวจสอบ Router Access security

ในระบบนี้จะทำการตรวจสอบการคอนฟีกูเรชั่นในเรื่องต่างๆ ดังต่อไปนี้

1. การคอนฟีกูเรชั่นเกี่ยวกับการ Login

ในการตรวจสอบการ Login นั้น ระบบจะทำการตรวจสอบคอนฟีกูเรชั่นของอุปกรณ์เราเตอร์ในส่วนของการติดต่อกับ Console Line, Auxiliary Line และ Virtual Terminal Line ของอุปกรณ์เราเตอร์ซึ่งการคอนฟีกูเรชั่นที่ดีและมีความปลอดภัยนั้น ควรใช้คำสั่งดังที่จะกล่าวต่อไปนี้ กำหนดไว้ที่ Console Line และ Virtual Terminal Line ส่วน Auxiliary Line หากไม่มีการใช้งานควรถูกปิด โดยมีการกำหนดค่าตามตัวอย่างด้านล่าง

Console Line	-	line con 0
		exec-timeout 5 0
		login
		transport input telnet
Auxiliary Line	-	line aux 0
		no exec
		exec-timeout 0 10
		transport input telnet
VTY lines	-	line vty 0 4
		exec-timeout 5 0
		login
		transport input telnet

2. การคอนฟิกูเรชั่นเกี่ยวกับ Privilege

ในอุปกรณ์เราเตอร์ของ Cisco จะมีการแบ่งระดับของ Privilege ออกเป็น 16 ระดับด้วยกัน โดยที่แต่ละระดับนั้นจะมีความสามารถในการทำงานที่แตกต่างกัน ซึ่งเราสามารถกำหนดระดับการทำงานให้กับผู้ที่มีสิทธิเข้าถึงตัวอุปกรณ์เราเตอร์ได้ ซึ่งตัวอย่างของการคอนฟิกูเรชั่นระดับของ Privilege มีดังนี้

Central(config)# **privilege exec level 15 connect**

Central(config)# **privilege exec level 15 telnet**

Central(config)# **privilege exec level 15 rlogin**

Central(config)# privilege exec level 15 show ip access-lists

Central(config)# **privilege exec level 15 show access-lists**

Central(config)# privilege exec level 15 show logging

Central(config)# ! if SSH is supported..

Central(config)# privilege exec level 15 ssh

Central(config)# privilege exec level 1 show ip

3. การคอนฟิกูเรชั่นเกี่ยวกับ Password

มี Password อยู่ 2 ประเภทที่ถูกป้องกันโดยซอฟท์แวร์ของ Cisco (IOS) คือ

1. Type 7 : Cisco ได้ประกาศไว้เพื่อใช้ในการเข้ารหัสกับ Password แบบนี้
2. Type 5 : ใช้การเข้ารหัสแบบ MD5 ซึ่งมีความแข็งแรงมากกว่าแบบ Type 7

ซึ่งมีตัวอย่างการคอนฟิกูเรชั่น ดังนี้

South# **config t**

Enter configuration commands, one per line. End with CNTL/Z.

South(config)# **enable secret 2-mAny-rOUtEs**

South(config)# **no enable password**

South(config)# **end**

South#

4. การคอนฟิกูเรชั่นเกี่ยวกับ Account

ควรมีการกำหนด Username ที่ใช้ Login ให้กับผู้ดูแลระบบ ซึ่งมีตัวอย่างการคอนฟิกูเรชั่น ดังนี้

Central# **config t**

Enter configuration commands, one per line. End with CNTL/Z.

Central(config)# **service password-encryption**

Central(config)# **username rsmith password 3d-zirc0nia**

Central(config)# **username rsmith privilege 1**

Central(config)# **username bjones password 2B-or-3B**

Central(config)# **username bjones privilege 1**

Central(config)# **no username brian**

Central(config)# **end**

Central#

ระบบการตรวจสอบ Router Service Security

ระบบจะทำการตรวจสอบการปิดการให้บริการที่ไม่จำเป็นต้องใช้ของอุปกรณ์เราเตอร์ ซึ่งบริการเหล่านี้ใช้เพื่อการอนุญาตให้ส่งแพ็คเก็ตหลายชนิดผ่านอุปกรณ์เราเตอร์หรือส่งแพ็คเก็ตชนิดพิเศษบางชนิด หรือใช้เพื่อการปรับแต่งค่าการทำงานของอุปกรณ์เราเตอร์จากภายนอก โดยทั่วไปบริการของอุปกรณ์เราเตอร์ที่ควรถูกปิดไม่ให้ใช้งานแสดงได้ ดังตาราง

ตารางที่ 3.1 Service ที่ควรถูกปิดไม่ให้ใช้งาน

Feature	Description	Default	Recommendation
Cisco Discovery protocol (CDP)	Proprietary layer 2 Protocol between Cisco devices.	Enabled	CDP is almost never needed, disable it.
TCP small servers	Standard TCP network services: echo, chargen, etc.	11.3: disabled 11.2: enabled	This is a legacy feature, disable it explicitly.
UDP small servers	Standard UDP network services: echo, chargen, etc.	11.3: disabled 11.2: enabled	This is a legacy feature, disable it explicitly.
Finger	Unix user lookup service, allows remote listing of logged in users.	Enabled	Unauthorized persons don't need to know this, disable it.
HTTP server	Some Cisco IOS devices offer web-based configuration.	Varies by device	If not in use, explicitly disable, otherwise restrict access.
Configuration auto-loading	Router will attempt to load its configuration via TFTP.	disabled	This is rarely used, disable it if it is not in use.
Bootp server	Service to allow other routers to boot from this one.	Enabled	This is rarely needed and may open a security hole, disabled it.
NTP service	Router can act as a time server for other devices and hosts.	Enabled (if NTP is Configured)	If not in use, explicitly disable, otherwise restrict access.

ตารางที่ 3.1 Service ที่ควรถูกปิดไม่ให้ใช้งาน (ต่อ)

Feature	Description	Default	Recommendation
IP source routing	Feature that allows a packet to specify its own route.	Enabled	Can be helpful in attacks, disable it.
Proxy ARP	Router will act as a proxy for layer 2 address resolution	Enabled	Disable this service unless the router is serving as a LAN bridge.
IP unreachable notifications	Router will explicitly notify senders of incorrect IP Addresses	Enabled	Can aid network mapping, disable on interfaces to untrusted network
IP mask reply	Router will send an interface's IP address mask in response to an ICMP mask request.	Disabled	Can aid IP address mapping; explicitly disable on interfaces to untrusted networks.
IP redirects	Router will send an ICMP redirect message in response to certain routed IP packets.	Enabled	Can aid network mapping, disable on interfaces to untrusted networks.
Maintenance Operations Protocol (MOP)	Legacy management protocol, part of the DECNet protocol suite.	Enabled (on Ethernet interfaces)	Disable if not explicitly needed.
Domain Name Service	Routers can perform DNS name resolution.	Enabled (broadcast)	Set the DNS server addresses explicitly, or disable DNS lookup.
Simple Network Management Protocol	Routers can support SNMP remote query and configuration.	Enabled	If not in use, remove default community strings and explicitly disable, otherwise restrict access.

ตารางที่ 3.1 Service ที่ควรถูกปิดไม่ให้ใช้งาน (ต่อ)

Feature	Description	Default	Recommendation
PAD service	Router will support X.25 packet assembler service.	Enabled	Disable if not explicitly Need.
IP directed broadcast	Packets can identify a target LAN for broadcasts.	Enabled (11.3 & earlier)	Directed broadcast can be used for attacks, disable it.

ระบบการตรวจสอบ Router Access List

ในส่วนนี้ระบบจะทำการตรวจสอบการคอนฟิกูเรชั่นเกี่ยวกับ Router Access List ของอุปกรณ์เราเตอร์ ว่ามีการคอนฟิกูเรชั่นที่เหมาะสมหรือไม่ โดยระบบมีการตรวจสอบการคอนฟิกูเรชั่น ดังนี้

1. การสร้าง Access-List ขึ้นใหม่แต่ละครั้งควรจะเริ่มต้นด้วยคำสั่ง **no access-list nnn** ก่อนเสมอ เพื่อกำจัดค่าเดิมใดๆ ที่อาจมีการใช้งาน access-list ที่ *nnn* ให้หมด

   East (config) # **no access-list 51**

   East (config) # **access-list 51 permit host 14.2.9.6**

   East (config) # **access-list 51 deny any log**

2. กำหนดหมายเลขพอร์ตที่ต้องการควบคุมสำหรับแต่ละ Access List ซึ่งจะช่วยเพิ่มประสิทธิภาพการทำงานของ IOS ให้ไม่จำเป็นต้องตรวจสอบเฮดเดอร์ (header) ทั้งหมดของแพ็คเก็ตโดยไม่จำเป็น และเพื่อให้แน่ใจว่าข้อมูลการใช้งานที่เก็บอยู่ใน Log มีข้อมูลหมายเลขพอร์ตที่ถูกต้อง โดยการกำหนดหมายเลขพอร์ตในช่วงที่ต้องการเป็นอาร์กิวเมนต์หนึ่งของ Access List ที่สร้างขึ้น ดังตัวอย่าง

   no access-list 106

   access-list 106 deny udp any range 1 65535 any range 1 65535 log

   access-list 106 deny tcp any range 1 65535 any range 1 65535 log

   access-list 106 deny ip any any log

คำสั่งในบรรทัดสุดท้ายใส่เพื่อให้แน่ใจว่าอุปกรณ์เราเตอร์จะปฏิเสธแพ็คเก็ตที่ใช้งานโปรโตคอลอื่นๆ นอกเหนือจาก TCP และ UDP รวมทั้งเก็บค่าลงในล็อก (Log)

3. อนุญาตให้เฉพาะแอดเดรสของเครือข่ายภายในส่งข้อมูลเข้าสู่อุปกรณ์เราเตอร์ผ่านทางอินเตอร์เฟสภายใน โดยการบังคับที่ Access List รวมทั้งการปิดไม่ให้แอดเดรสที่ไม่ถูกต้องออกจากเครือข่ายที่อินเตอร์เฟสที่เชื่อมต่อกับเครือข่ายภายนอก เพื่อป้องกันผู้บุกรุกไม่ให้ใช้อุปกรณ์เราเตอร์เป็นเครื่องมือในการโจมตีที่อื่น วิธีการนี้อาจจะไม่สามารถนำไปใช้งานได้จริงกับเครือข่ายที่มีความซับซ้อน

```
East (config) # no access-list 101
East (config) # access-list 101 permit ip 10.1.1.0 0.0.0.255 any
East (config) # access-list 101 deny udp any range 1 65535 any log
East (config) # access-list 101 deny tcp any range 1 65535 any log
East (config) # access-list 101 deny ip any any log
East (config) # interface eth 1
East (config-if) # ip access-group 101 in
East (config-if) # exit
East (config) # interface eth 0
East (config-if) # ip access-group 101 out
```

4. ไม่ควรให้แพ็คเก็ตที่มาจากภายนอก (จากเครือข่ายที่ไม่น่าเชื่อถือ) ซึ่งอาจจะเป็นแพ็คเก็ตที่มีการปลอมแปลงหรือส่งมาเพื่อโจมตีเครือข่าย สามารถทำได้โดยการแบ่งส่วนของเครือข่ายทั้งหมดตามแต่ละอินเตอร์เฟสของอุปกรณ์เราเตอร์ และออกแบบว่าจะเลือกให้มีการส่งผ่านข้อมูลที่มาจากเครือข่ายภายนอกและเครือข่ายที่ไม่น่าเชื่อถือจากที่ใดได้บ้าง
5. แพ็คเก็ตที่ส่งมาจากภายนอกโดยมีแอดเดรสต้นทางเหมือนกับแอดเดรสของเครือข่ายภายในใดๆ (เครือข่ายที่เชื่อถือ) จัดว่าเป็นแพ็คเก็ตที่ส่งเข้ามาเพื่อโจมตีระบบโดยวิธีการ TCP sequence number guessing หรือวิธีอื่นๆ ในทำนองเดียวกัน จึงไม่ควรให้ผ่านเข้ามาในเครือข่าย ป้องกันได้โดยการสร้าง Access List ขึ้นมาใช้งานที่แต่ละอินเตอร์เฟสที่ต้องติดต่อกับเครือข่ายที่ไม่น่าเชื่อถือ
6. สกัดกั้นแพ็คเก็ตชนิด loopback (มาจากเครือข่าย 127.0.0.0) เนื่องจากแพ็คเก็ตเหล่านี้ไม่มีทางเกิดขึ้นได้จริง นอกจากนั้น ให้กั้นแพ็คเก็ตที่มาจาก IP address ที่ถูกสำรองไว้ (ได้แก่ 10.0.0.0, 172.16.0.0 - 172.31.0.0 และ 192.168.0.0) [ตาม RFC 1918]
7. หากเครือข่ายไม่จำเป็นต้องใช้ IP multicast ก็ควรจะกั้นแพ็คเก็ตชนิด multicast ด้วย

8. สกัดกั้นแพ็คเก็ตชนิด broadcast (ข้อควรคำนึงถึงคือ การปิดแพ็คเก็ตชนิด broadcast อาจจะทำให้บริการ DHCP และ BOOTP ไม่สามารถใช้งานได้ด้วย อย่างไรก็ตาม บริการทั้งสองอันนี้ไม่ควรนำมาใช้ที่อินเตอร์เฟสที่ต่อกับเครือข่ายภายนอกอยู่แล้ว)
9. การโจมตีเครือข่ายจากภายนอกจำนวนมากใช้วิธีการส่ง ICMP redirect จึงควรปิดบริการนี้ (วิธีการที่ดีกว่านี้แต่มีความยุ่งยากมากขึ้นคือการอนุญาตให้แพ็คเก็ตชนิด ICMP ที่จำเป็นเพียงบางชนิดผ่านเข้าออก)

   ตัวอย่างที่แสดงดังต่อไปนี้ เป็นวิธีการหนึ่งที่จะนำเอาคำแนะนำด้านบนไปใช้งานจริง

   North (config) # **no access-list 107**

   North (config) # **! block internal addresses**

   North (config) # **access-list 107 deny ip 14.2.0.0 0.0.255.255 any log**

   North (config) # **access-list 107 deny ip 14.1.0.0 0.0.255.255 any log**

   North (config) # **! block loopback/reserved addresses**

   North (config) # **access-list 107 deny ip 127.0.0.0 0.255.255.255 any log**

   North (config) # **access-list 107 deny ip 10.0.0.0 0.255.255.255 any log**

   North (config) # **access-list 107 deny ip 172.16.0.0 0.15.255.255 any log**

   North (config) # **access-list 107 deny ip 192.168.0.0 0.0.255.255 any log**

   North (config) # **! block multicast (if not used)**

   North (config) # **access-list 107 deny ip 224.0.0.0 0.0.255.255 any**

   North (config) # **! block broadcast**

   North (config) # **access-list 107 deny ip host 0.0.0.0 any log**

   North (config) # **! block ICMP redirects**

   North (config) # **access-list 107 deny icmp any any redirect log**

   North (config) # **interface eth 0/0**

   North (config-if) # **ip access-group 107 in**

10. สกัดกั้นแพ็คเก็ตที่มีแอดเดรสต้นทางและปลายทางเหมือนกันไม่ให้เข้ามาในเครือข่าย (เพราะอาจจะเป็นการบุกรุกโดยวิธีการที่เรียกว่า “Land” เข้ามาตัวที่อุปกรณ์เราเตอร์) ทำได้โดยการสร้าง Access List ขึ้นมาใช้จำกัดข้อมูลที่จะเข้ามาที่แต่ละอินเตอร์เฟส โดยวิธีการดังที่แสดงในตัวอย่างด้านล่าง

no access-list 102

access-list 102 deny ip host 10.2.6.250 host 10.2.6.250 log

access-list 102 permit ip any any

interface Eth 0/0

ip address 10.2.6.250 255.255.255.0

ip access-group 102 in

11. กำหนดค่า Access List สำหรับใช้งานที่ Virtual Terminal Line เพื่อควบคุมการเข้าถึงอุปกรณ์เราเตอร์ผ่านทางการ telnet ตามตัวอย่าง

South (config) # **line vty 0 4**

South (config-line) # **access-class 92 in**

South (config-line) # **exit**

South (config) # **no access-list 92**

South (config) # **access-list 92 permit 10.1.1.1**

South (config) # **access-list 92 permit 10.1.1.2**

ระบบการตรวจสอบ Audit Management

ในส่วนนี้ระบบจะทำการตรวจสอบการคอนฟิกูเรชั่นเกี่ยวกับการจัดการเรื่องของการเก็บบันทึกค่าการทำงานของอุปกรณ์เราเตอร์ ว่ามีการคอนฟิกูเรชั่นที่เหมาะสมหรือไม่ โดยระบบมีการตรวจสอบการคอนฟิกูเรชั่น ดังนี้

1. นำความสามารถของอุปกรณ์เราเตอร์ในการเก็บบันทึกค่าการทำงานมาใช้งาน เพื่อใช้เก็บบันทึกค่าความผิดพลาดที่เกิดขึ้นและส่งแพ็คเก็ตไปยังเครื่องที่ใช้ในการเก็บ syslog ภายในเครือข่าย (ต้องเป็นเครือข่ายที่มีการเชื่อถือ) โดยจะต้องแน่ใจถึงเส้นทางที่ส่งข้อมูลไม่ผ่าน เครือข่ายที่ไม่น่าเชื่อถือ มีวิธีการดังต่อไปนี้

Central (config) # **logging on**

Central (config) # **logging 10.1.1.200**

Central (config) # **logging buffered**

Central (config) # **logging console critical**

Central (config) # **logging trap debugging**

Central (config) # **logging facility local1**

2. กำหนดค่าการทำงานของอุปกรณ์เราเตอร์โดยให้เก็บค่าเวลาลงในบันทึกการทำงานลงใน Log ด้วย โดยการตั้งค่าเวลาจากเครื่องเซิร์ฟเวอร์ NTP ที่แตกต่างกันอย่างน้อย 2 เครื่อง เพื่อให้ค่าที่ได้มีความถูกต้อง ซึ่งจะช่วยให้ผู้ดูแลระบบติดตามเหตุการณ์การบุกรุกเครือข่ายได้สะดวกแม่นยำ มีวิธีการดังตัวอย่างด้านล่าง

```
service timestamps log datetime localtime show-timezone
clock timezone EST -5
clock summer-time EDT recurring
ntp source Ethernet 0/1
ntp server 192.5.41.40
ntp server 192.5.41.41
```

3. หากมีการใช้งาน SNMP ใช้เลือกใช้ SNMP community string ที่ยากต่อการเดา คำสั่งที่ได้แสดงไว้ดังตัวอย่างด้านล่างแสดงให้เห็นถึงวิธีการในการลบค่า community string ที่อุปกรณ์เราเตอร์กำหนดไว้ขณะเริ่มต้น และควรกำหนดให้ community string เป็นแบบอ่านอย่างเดียว

```
East (config) # no snmp community public
East (config) # no snmp community private
East (config) # snmp community BTR-18+never
```

การเก็บข้อมูล Log ของอุปกรณ์เราเตอร์เป็นเรื่องที่จำเป็นอย่างยิ่ง โดยเฉพาะในกรณีที่เครื่องโดนบุกรุกเข้าไปในระบบเครือข่ายไปแล้ว จะถือว่าเป็นหลักฐานที่แสดงให้เห็นถึงรูปแบบการโจมตีได้ มีคำแนะนำสำหรับการบันทึกข้อมูล Log ดังนี้

- ให้ส่งข้อมูล Log ที่มีความสำคัญไปยัง console ของอุปกรณ์เราเตอร์
- ส่งข้อมูล Log ไปยังเครื่องที่ทำหน้าที่เก็บ Log โดยเฉพาะ ซึ่งเครื่องนี้ได้รับการควบคุมการเข้าถึงอย่างเคร่งครัด และไม่ได้เปิดให้บริการอื่นใดยกเว้น syslog
- ตั้งเวลาอุปกรณ์เราเตอร์และเครื่องอื่นๆ ในเครือข่ายให้ใช้เวลาที่ตรงกันทั้งหมด โดยใช้ NTP (network time protocol) เพื่อรับข้อมูลเวลาจาก clock server เดียวกัน
- ป้องกันการโจมตีแบบ log flooding ซึ่งจะทำให้ฮาร์ดดิสก์เต็มอย่างรวดเร็ว
- ไม่ควรส่งข้อมูล Log ออกไปยังเครื่องพิมพ์โดยตรง เพราะอาจจะเสี่ยงต่อการสูญเสียข้อมูลในกรณีที่เครื่องพิมพ์มีปัญหา

ระบบการตรวจสอบ Scan Routing

ในส่วนนี้ระบบจะทำการตรวจสอบการคอนฟิกูเรชั่นเกี่ยวกับการจัดการเรื่องของการทำ Routing ของอุปกรณ์เราเตอร์ เพื่อป้องกันอุปกรณ์เราเตอร์จากการโจมตีในส่วนของการทำ Routing ว่ามีการคอนฟิกูเรชั่นที่เหมาะสมหรือไม่ โดยระบบมีการตรวจสอบการคอนฟิกูเรชั่น ดังนี้

1. Router Neighbor Authentication

จุดประสงค์หลักของการทำ Router Neighbor Authentication คือ การป้องกันความมั่นคงของ Routing Domain ซึ่งการทำการตรวจสอบตัวตนของผู้ใช้งาน (Authentication) จะเป็นการยืนยันการรับส่งข้อมูลเกี่ยวกับ Routing Table ภายใต้องค์กรเดียวกันเท่านั้น ทำให้สามารถลดปัญหาภัยคุกคามที่เกิดจาก Traffic ของการทำ Routing และการปฏิเสธการให้บริการ (DOS) อีกด้วย

2. OSPF Authentication

โปรโตคอล OSPF เป็นโปรโตคอลที่ใช้วิธีพิจารณาเส้นทางและปรับปรุงสถานะแบบ Link-state โดยมีการพัฒนาขึ้นในราวปี ค.ศ. 1989 มีคุณสมบัติเด่นคือจะมี overhead หรือใช้ทรัพยากรในเครื่องไม่มาก ทำให้บริษัท ISP และเครือข่ายต่างๆ ที่เชื่อมต่อในอินเตอร์เน็ตหันมาใช้โปรโตคอล OSPF เพื่อเชื่อมต่อภายในเครือข่ายตนเองกันมากขึ้น และสามารถรองรับกับเครือข่ายขนาดใหญ่ได้ดี นอกจากนี้โปรโตคอล OSPF ยังสามารถรองรับการกำหนดเครือข่ายย่อย Subset ได้อย่ามีประสิทธิภาพอีกด้วย ซึ่งช่วยให้ผู้จัดการเครือข่ายสามารถกำหนดแยกเครือข่ายออกเป็นเครือข่ายย่อยๆ ได้หลายรูปแบบ

ในการแลกเปลี่ยนข้อมูลและสถานะของเครือข่ายและ Routing table นั้นโปรโตคอล OSPF จะติดต่อแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์เราเตอร์ที่อยู่ในระบบ Autonomous System เดียวกัน คือมีอุปกรณ์เราเตอร์หลักและอุปกรณ์เราเตอร์บริวารติดต่อกัน นอกจากนี้ยังสามารถแลกเปลี่ยนข้อมูลกับอุปกรณ์เราเตอร์ที่ใช้โปรโตคอลอื่น เช่น โปรโตคอล RIP หรือโปรโตคอล EGP ได้อีกด้วย โดยอาศัยกลไกการอ้างอิงของ Autonomous System เช่นเดียวกัน

<u>OSPF MD 5</u>

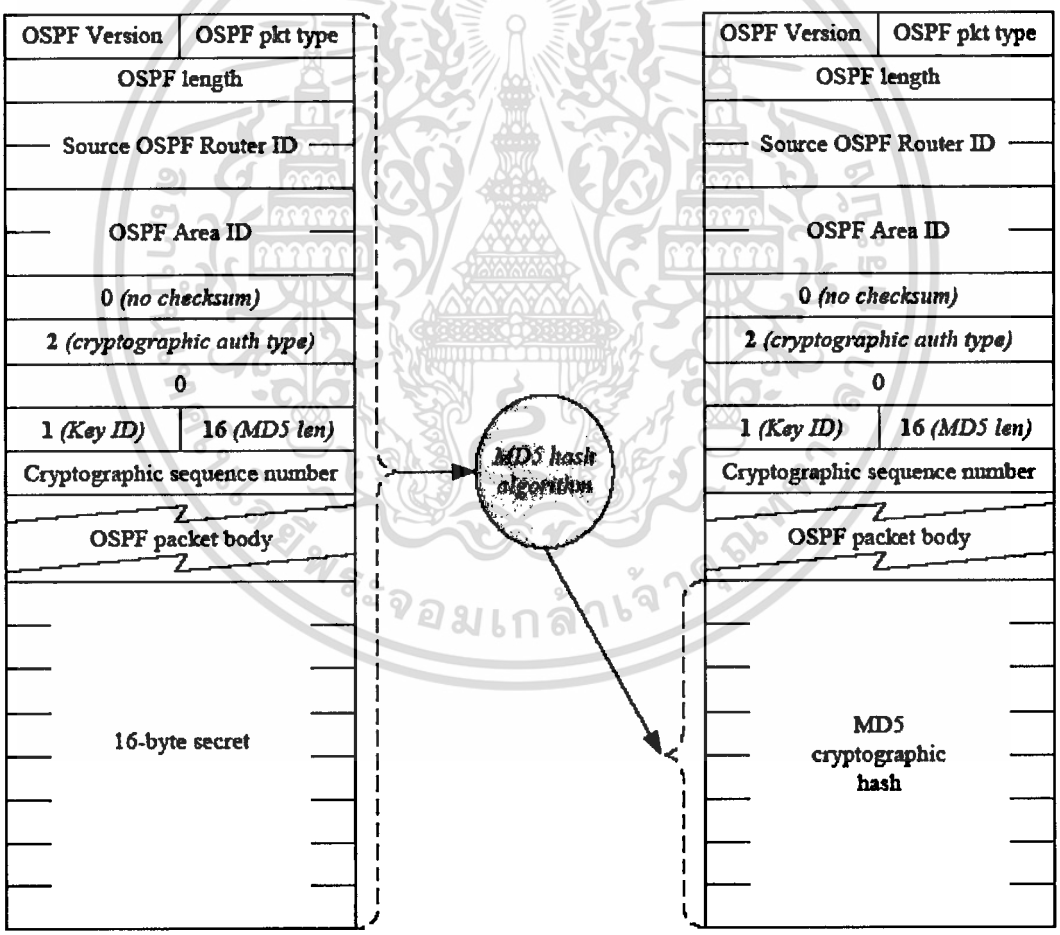
โปรโตคอล OSPF มีรูปแบบการตรวจสอบตัวตนของผู้ใช้งานอยู่ 2 รูปแบบ คือ

1. แบบ Plain Text
2. แบบ MD5 (Message Digest)

โดยการตรวจสอบตัวตนของผู้ใช้งานแบบ Plain Text นั้น จะมีการใช้ Secret Key ร่วมกันกับอุปกรณ์เราเตอร์ตัวอื่นๆ ในเน็ตเวิร์คเซกเมนต์ แต่การใช้ Plain Text เราสามารถใช้

โปรแกรม Sniffer ทำการจับแพ็คเก็ตมาทำการอ่านได้ ดังนั้น เราจึงใช้ MD5 เข้ามาช่วยในการเข้ารหัสข้อมูล

ส่วน MD 5 เป็นอัลกอลิทึมที่ใช้ในการเข้ารหัสข้อมูล โดยการเปลี่ยนข้อความที่เป็น Plain Text ไปเป็นข้อความที่ไม่สามารถอ่านได้ด้วยการดำเนินการทางคณิตศาสตร์ โดยไม่มีการใช้คีย์ ดังนั้น การทำ Hash ของข้อความใดๆ จึงไม่สามารถเปลี่ยนกลับมาเป็นข้อความเดิมได้ (one-way property) การเข้ารหัสแบบนี้ มีประโยชน์เพื่อใช้ยืนยันบุคคล (Authentication) มิได้ใช้เพื่อป้องกันข้อมูลจากผู้ไม่หวังดีมาลักลอบอ่านระหว่างการส่ง อย่างเช่นการทำ Digital signature ที่ใช้ยืนยันบุคคลใน E-commerce ว่าผู้ที่สั่งซื้อเป็นตัวจริง



รูปที่ 3.1 ลักษณะของ OSPF ที่มีการคำนวณด้วย MD5 Authentication

ซึ่งลักษณะการคอนฟิกูเรชั่นอุปกรณ์เราเตอร์เพื่อทำ OSPF MD5 มีดังนี้

North# **config t**

Enter configuration commands, one per line. End with CNTL/Z.

North(config)# **router ospf 1**

North(config-router)# **network 14.1.0.0 0.0.255.255 area 0**

North(config-router)# **area 0 authentication message-digest**

North(config-router)# **exit**

North(config)# **int eth0/1**

North(config-if)# **ip ospf message-digest-key 1 md5 r0utes-4-all**

North(config-if)# **end**

North#

East# **config t**

Enter configuration commands, one per line. End with CNTL/Z.

East(config)# **router ospf 1**

East(config-router)# **area 0 authentication message-digest**

East(config-router)# **network 14.1.0.0 0.0.255.255 area 0**

East(config-router)# **network 14.2.6.0 0.0.0.255 area 0**

East(config-router)# **exit**

East(config)# **int eth0**

East(config-if)# **ip ospf message-digest-key 1 md5 r0utes-4-all**

East(config-if)# **end**

East#

3. RIP Authentication

Routing Information Protocol หรือ RIP เป็นโปรโตคอลเลือกเส้นทางประเภท Distance Vector ที่ถูกออกแบบมาให้ใช้กับเครือข่ายขนาดเล็กไปจนถึงขนาดกลาง เป็นโปร

โตคอลเลือกเส้นทางมาตรฐานที่ไม่ขึ้นอยู่กับผู้ผลิตรายใด โดยมี RIP Version 1 ที่ได้รับมาตรฐาน RFC 1058

RIP MD5

โปรโตคอล RIP มีรูปแบบการตรวจสอบตัวตนของผู้ใช้งานอยู่ 2 รูปแบบ ซึ่งเหมือนกับของ OSPF ดังนั้น เพื่อความปลอดภัยในการตรวจสอบตัวตนจึงควรใช้เป็นแบบ RIP MD5

ซึ่งลักษณะการคอนฟิกูเรชั่นอุปกรณ์เราเตอร์เพื่อทำ RIP MD5 มีดังนี้

```
Central# config t
Enter configuration commands, one per line. End with CNTL/Z.
Central(config)# router rip
Central(config-router)# version 2
Central(config-router)# network 14.0.0.0
Central(config-router)# end
Central#

South# config t
Enter configuration commands, one per line. End with CNTL/Z.
South(config)# router rip
South(config-router)# version 2
South(config-router)# network 14.0.0.0
South(config-router)# end
South#
```

วิธีการคอนฟิกูเรชั่นเกี่ยวกับการ Authentication คือ

```
Central# config t
Enter configuration commands, one per line. End with CNTL/Z.
Central(config)# int ethernet0/1
Central(config-if)# ip rip authentication key-chain CENTRAL-KC
Central(config-if)# ip rip authentication mode md5
```

Central(config-if)# end

Central#

South# config t

Enter configuration commands, one per line. End with CNTL/Z.

South(config)# int ethernet0/0

South(config-if)# ip rip authentication key-chain SOUTH-KC

South(config-if)# ip rip authentication mode md5

South(config-if)# end

South#

4. EIGRP Authentication

เป็น Routing Protocol ชนิดหนึ่ง พัฒนาโดยบริษัท Cisco มีคุณลักษณะผสมระหว่างโปรโตคอลชนิด Distance Vector กับ Link State โดยเอาข้อดีของทั้ง 2 แบบมารวมกัน

การทำ EIGRP Authentication มีหลักการทำ ดังนี้

1. ทำการเลือกโหมดของการทำ Authentication เป็นแบบ MD5
2. ทำการ Enable การ Authentication สำหรับ EIGRP Message
3. ระบุ Key Chain, Key Number และ Key String ที่ไว้ใช้งาน
4. ทำ Configure key management (Optional)

วิธีการคอนฟิกูเรชั่นเกี่ยวกับการ EIGRP Authentication คือ

North# **config t**

Enter configuration commands, one per line.End with CNTL/Z.

North(config)# **router eigrp 100**

North(config-router)# **network 14.1.0.0 255.255.0.0**

North(config-router)# **exit**

North(config)# **interface eth 0/1**

North(config-if)# **ip authentication mode eigrp 100 md5**

North(config-if)# **ip authentication key-chain eigrp 100 NORTH-KC**

North(config-if)# **exit**

North(config)# **key chain NORTH-KC**

North(config-keychain)# **key 1**

North(config-keychain-key)# **key-string my-secret-key**

North(config-keychain-key)# **send-lifetime 00:00:00 Oct 1 2003 00:00:00 Jan 1 2004**

North(config-keychain-key)# **accept-lifetime 00:00:00 Oct 1 200300:00:00 Jan 7 2000**

North(config-keychain-key)# **end**

North#

East# **config t**

Enter configuration commands, one per line. End with CNTL/Z.

East(config)# **router eigrp 100**

East(config-router)# **network 14.1.0.0 255.255.0.0**

East(config-router)# **network 14.2.6.0 255.255.255.0**

East(config-router)# **passive-interface eth1**

East(config-router)# **exit**

East(config)# **interface eth 0**

East(config-if)# **ip authentication mode eigrp 100 md5**

East(config-if)# **ip authentication key-chain eigrp 100 EAST-KC**

East(config-if)# **exit**

East(config)# **key chain EAST-KC**

East(config-keychain)# **key 1**

East(config-keychain-key)# **key-string my-secret-key**

East(config-keychain-key)# **send-lifetime 00:00:00 Oct 1 2003 00:00:00 Jan 1 2004**

East(config-keychain-key)# **accept-lifetime 00:00:00 Oct 1 200300:00:00 Jan 7 2004**

East(config-keychain-key)# **end**

East#

5. IS-IS Authentication

IS-IS Authentication มีวิธีการจัดการอยู่ 3 แบบเพื่อป้องกันจากโจมตีการ Routing คือ

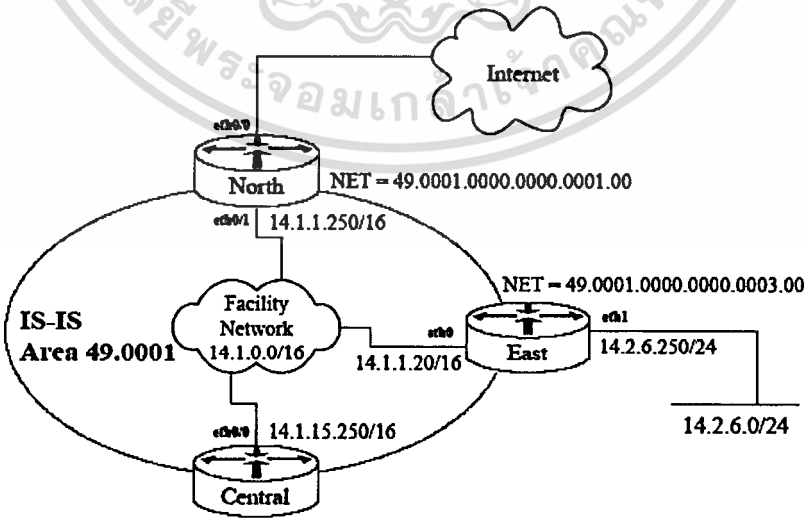
1. Plain Text (or clear text)
2. Enhanced Clear Text
3. Hashed Message Authentication Code Message Digest 5 (HMAC-MD5)

ซึ่ง Plain Text จะทำการตรวจสอบตัวตนของผู้ใช้งานโดยใช้ shared secret key ที่อุปกรณ์เราเตอร์ทุกตัวในเครือข่ายจะต้องรู้จักทั้งหมด ซึ่งวิธีนี้จะไม่ค่อยมาความปลอดภัยเนื่องจากคีย์จะถูกส่งไปอยู่ในรูปที่ไม่มีการเข้ารหัส ส่วน Enhanced Clear Text authentication จะเหมือนกับการตรวจสอบตัวตนแบบ Plain Text แต่ต่างที่ ตัวคีย์ที่ใช้จะมีการเข้ารหัสก่อนที่จะส่งออกไป ส่วนแบบสุดท้ายจะมีการทำงานโดยใช้ HMAC-MD5 เข้ามาร่วมด้วย

การ Authentication โดยใช้ Hashed Message Authentication Code Message Digest 5 (HMAC-MD5) จะต้องทำการคอนฟิกูเรชั่น 3 ส่วน ด้วยกัน คือ

1. A key chain
2. IS-IS routing protocol
3. HMAC-MD5 authentication

ซึ่งลักษณะของการคอนฟิกูเรชั่น จะมีลักษณะดังตัวอย่างด้านล่าง ซึ่งลักษณะของการคอนฟิกูเรชั่นจะทำการคอนฟิกูเรชั่นตามรูป



รูปที่ 3.2 ตัวอย่างของ Routing Architecture

```
North# config t
Enter configuration commands, one per line. End with CNTL/Z.
North(config)# router isis secure-network
North(config-router)# net 49.0001.0000.0000.0001.00
North(config-router)# is-type level-1
North(config-router)# authentication mode md5 level-1
North(config-router)# authentication key-chain ISIS-KC level-1
North(config-router)# exit
North(config)# interface ethernet 0/1
North(config-if)# ip address 14.1.1.250 255.255.0.0
North(config-if)# ip router isis secure-network
North(config-if)# isis authentication mode md5 level-1
North(config-if)# isis authentication key-chain ISIS-KC level-1
North(config-if)# end
North#

East# config t
Enter configuration commands, one per line. End with CNTL/Z.
East(config)# router isis secure-network
East(config-router)# net 49.0001.0000.0000.0003.00
East(config-router)# is-type level-1
East(config-router)# authentication mode md5 level-1
East(config-router)# authentication key-chain ISIS-KC level-1
East(config-router)# exit
East(config)# interface ethernet 0
East(config-if)# ip address 14.1.1.20 255.255.0.0
East(config-if)# ip router isis secure-network
```

East(config-if)# isis authentication mode md5 level-1

East(config-if)# isis authentication key-chain ISIS-KC level-1

East(config-if)# end

East#

6. Static Routes

เป็น Routing Table ที่ปลอดภัยที่สุดใน Routing Protocol ทั้งหมด ซึ่ง Routing Table ประเภทนี้ไม่มีช่องโหว่ในการโจมตี เนื่องมาจากการอัพเดต Routing Packet ของอุปกรณ์เราเตอร์ข้างเคียง

3.3 วิธีการทำงานของระบบ

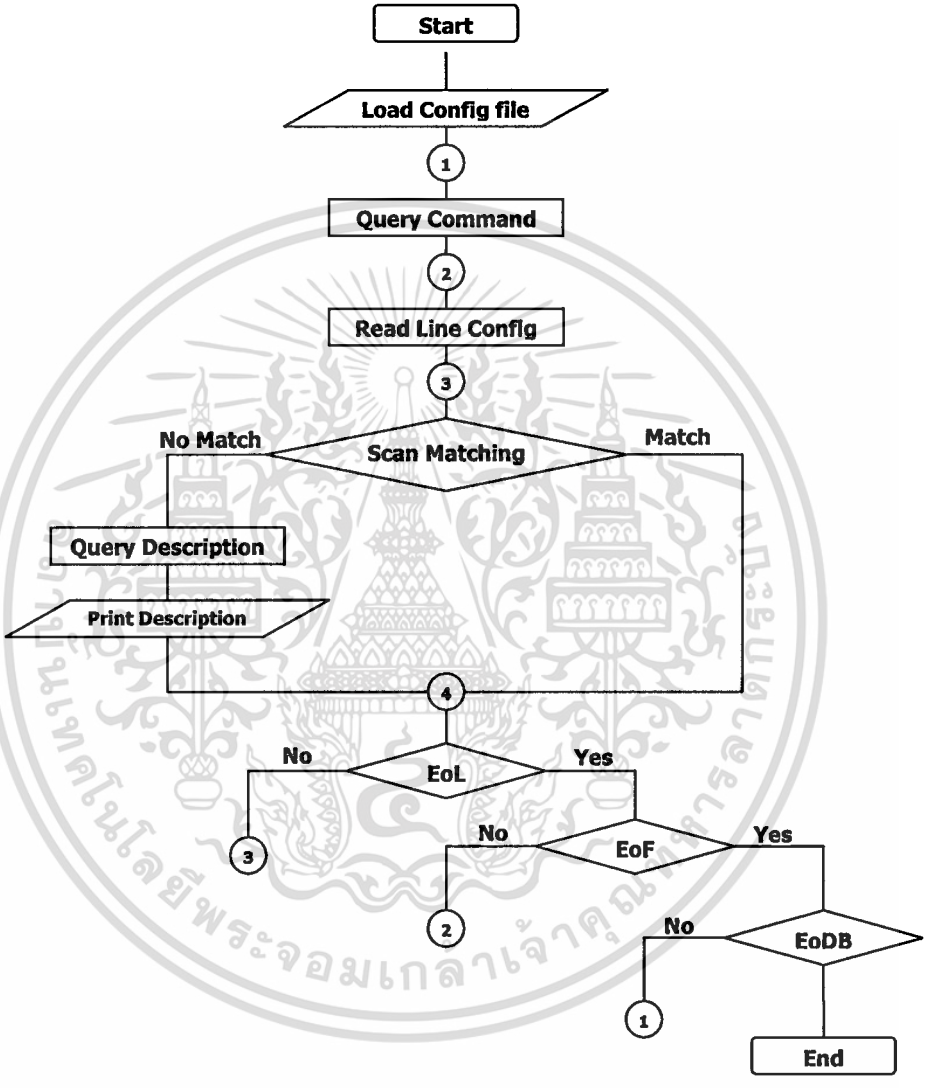
จากแนวทางการออกแบบระบบการตรวจสอบการคอนฟิกูเรชั่นตัวอุปกรณ์เราเตอร์ของ CISCO ที่ได้ทำการออกแบบไว้ในหัวข้อที่แล้ว ในหัวข้อนี้จะอธิบายถึงวิธีการที่ใช้ในการตรวจสอบการคอนฟิกูเรชั่น ว่ามีลักษณะและวิธีการในการตรวจสอบอย่างไร โดยจะทำการอธิบายถึงภาพรวมของกระบวนการทำงานของระบบในการตรวจสอบว่า มีการใช้หลักการอย่างไรในการตรวจสอบ ซึ่งแสดงได้ดังรูปที่ 3.3

จากรูป สามารถทำการอธิบายระบบการทำงานได้ เป็นขั้นตอนดังนี้

1. ระบบจะทำการอ่านข้อมูลการคอนฟิกูเรชั่น เข้ามาในระบบ โดยระบบสามารถอ่านไฟล์ที่อยู่ในรูปของไฟล์เอกสารได้ (ไฟล์ที่มีนามสกุลเป็น .txt, .doc)
2. เมื่ออ่านค่าคอนฟิกูเรชั่นแล้ว ระบบจะทำการ query คำสั่งที่ใช้ในการตรวจสอบขึ้นมาจากฐานข้อมูลโดยระบบจะ query ข้อมูลตามที่ผู้ใช้งานเลือกว่าจะตรวจสอบในเรื่องใด
3. เมื่อได้คำสั่งที่ต้องการตรวจสอบมาจากฐานข้อมูลแล้ว ระบบจะทำการอ่านค่าคอนฟิกูเรชั่นที่อ่านเข้ามาในตอนแรกขึ้นมาทีละบรรทัด
4. ระบบจะทำการตรวจสอบ (check) ค่าคอนฟิกูเรชั่น เทียบกับคำสั่งที่ query ขึ้นมา ถ้าไม่เจอระบบจะทำการ query คำแนะนำขึ้นมาจากฐานข้อมูลเพื่อนำมาแสดงบนหน้าจอ

หมายเหตุ : ในฐานข้อมูลของระบบนี้ จะทำการจัดเก็บคำสั่งที่ควรจะต้องมีการคอนฟิกูเรชั่นในแต่ละหัวข้อเอาไว้ แล้วทำการตรวจสอบกับคอนฟิกูเรชั่น ถ้าไม่เจอคำสั่งที่กำหนดไว้ ให้สรุปว่าการคอนฟิกูเรชั่นนั้นไม่เหมาะสม

5. ในกรณีที่เจอ แสดงว่าการคอนฟีกูเรชั่นนั้นเหมาะสมอยู่แล้ว ระบบจะทำการตรวจสอบเช่นนี้ไปจนกว่าจะหมดการคอนฟีกูเรชั่น และจนกว่าจะหมดข้อมูลในฐานข้อมูลทุกตัว

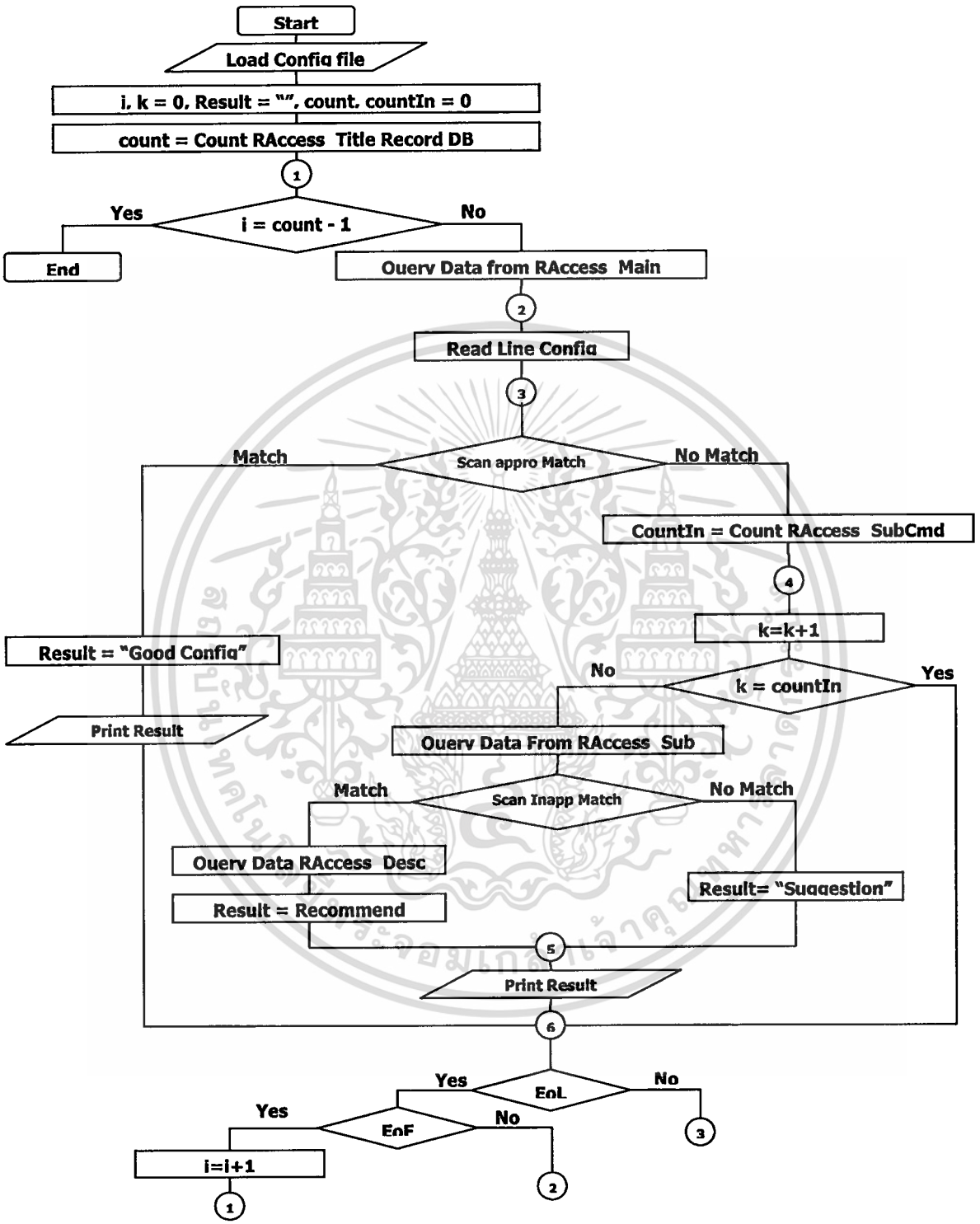


รูปที่ 3.3 ภาพรวมของกระบวนการทำงานของระบบ

จากรูป แสดงภาพรวมของกระบวนการตรวจสอบนี้ สามารถอธิบายวิธีการตรวจสอบคอนฟีกูเรชั่นแบบภาพรวมได้ทุกหัวข้อของการตรวจสอบ แต่ในการตรวจสอบในแต่ละหัวเรื่องนั้นจะมีรายละเอียดในการตรวจสอบที่แตกต่างกันไป ดังจะแสดงให้เห็นเป็นหัวข้อ ดังนี้

1. Router Access Security

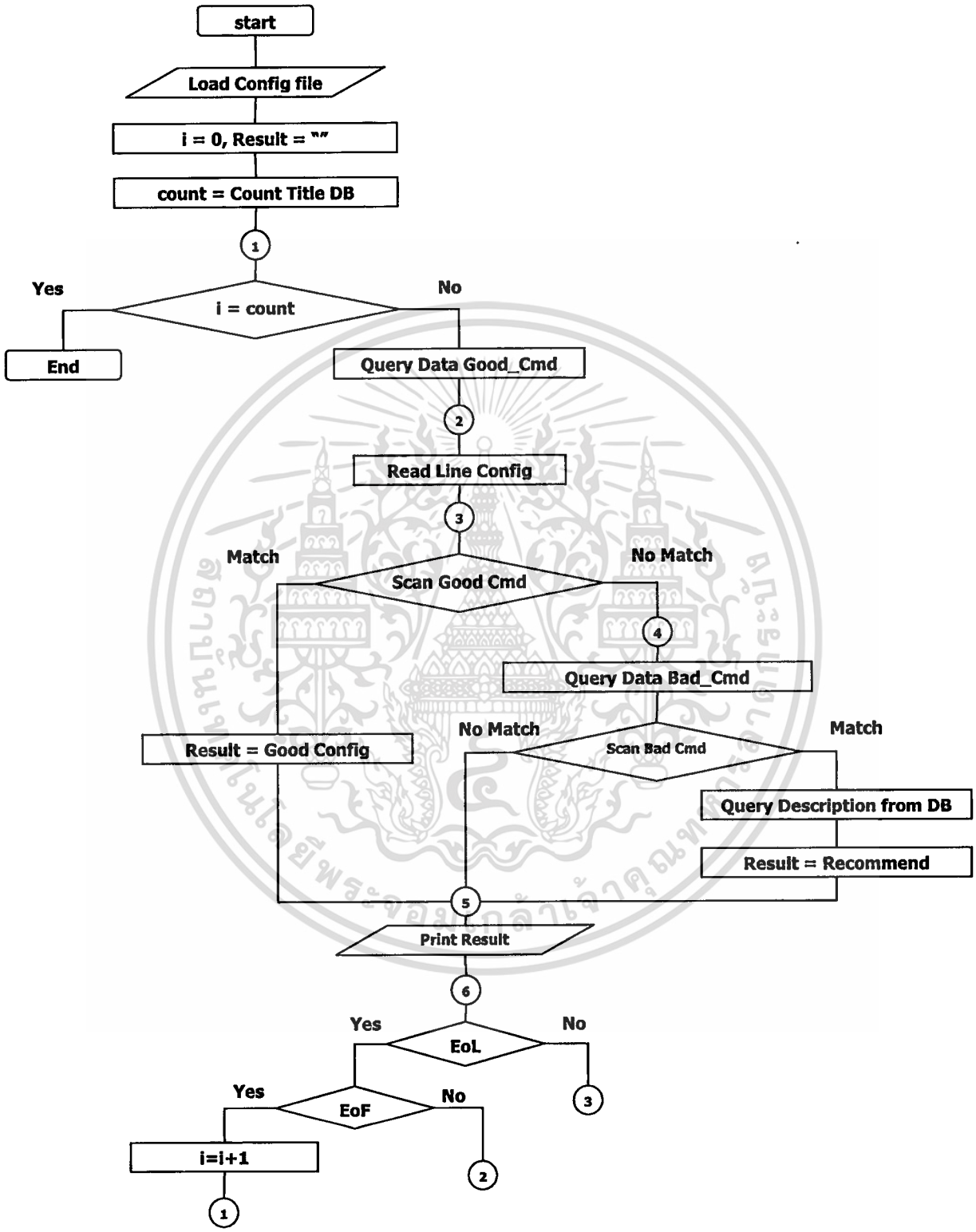
1. เมื่อระบบทำการอ่านค่าไฟล์ที่ต้องการตรวจสอบแล้ว ระบบจะทำการสร้างตัวแปร i และ k มีค่าเท่ากับ 0 และตัวแปร count และ countIn ขึ้นมาเพื่อทำการเช็คและนับจำนวนของ คำสั่งที่เหมาะสม และคำสั่งที่ไม่เหมาะสมที่จะใช้ในการตรวจสอบจากฐานข้อมูล
2. ถ้า count = i , countIn = k แล้วแสดงว่าไม่มีค่าหรือคำสั่งต่างๆ อยู่ในฐานข้อมูล หรือทำการตรวจสอบหมดแล้ว ระบบจะจบการทำงานทันที
3. แต่ถ้า count มีค่ามากกว่า 0 ระบบจะทำการ query ค่าจากฟิลด์ RAccess_MainCommand เพื่อทำการดึงค่า Appropriate Command หรือคำสั่งที่เหมาะสมขึ้นมาเพื่อทำการตรวจหา Appropriate Command ในแต่ละบรรทัดต่อ
4. ถ้าไม่พบ Appropriate Command ในแต่ละบรรทัด ระบบจะทำการ query ค่าจากฟิลด์ RAccess_SubCommand ขึ้นมาจากฐานข้อมูล เพื่อดึงค่า Inappropriate Command หรือ คำสั่งที่ไม่เหมาะสมขึ้นมา เพื่อทำการตรวจสอบต่อว่า มีการคอนฟิกูเรชั่นที่ไม่เหมาะสมในหัวข้อนั้นๆ หรือไม่
5. ถ้าพบการคอนฟิกูเรชั่นที่ไม่เหมาะสม ระบบจะทำการ query ค่าจากฟิลด์ RAccess_Desc ขึ้นมาเพื่อแสดงคำอธิบายเกี่ยวกับการคอนฟิกูเรชั่นนั้นๆ แต่ถ้าไม่พบการคอนฟิกูเรชั่นที่ไม่เหมาะสม ระบบจะทำการแสดงผลคำแนะนำทั่วไป
6. ในกรณีที่ตรวจหา Appropriate Command ในบรรทัด แล้วพบค่า Appropriate Command ระบบจะแสดงผลว่าการคอนฟิกูเรชั่นนั้นมีความเหมาะสมดีอยู่แล้ว
7. ระบบจะทำการตรวจสอบเช่นนี้ไปจนกว่าจะหมดไฟล์คอนฟิกูเรชั่น และจนกว่าจะหมดข้อมูลในฐานข้อมูลทุกตัว หรือ count = i



รูปที่ 3.4 กระบวนการทำงานของระบบในส่วนของ Router Access Security

2. Router Service Security

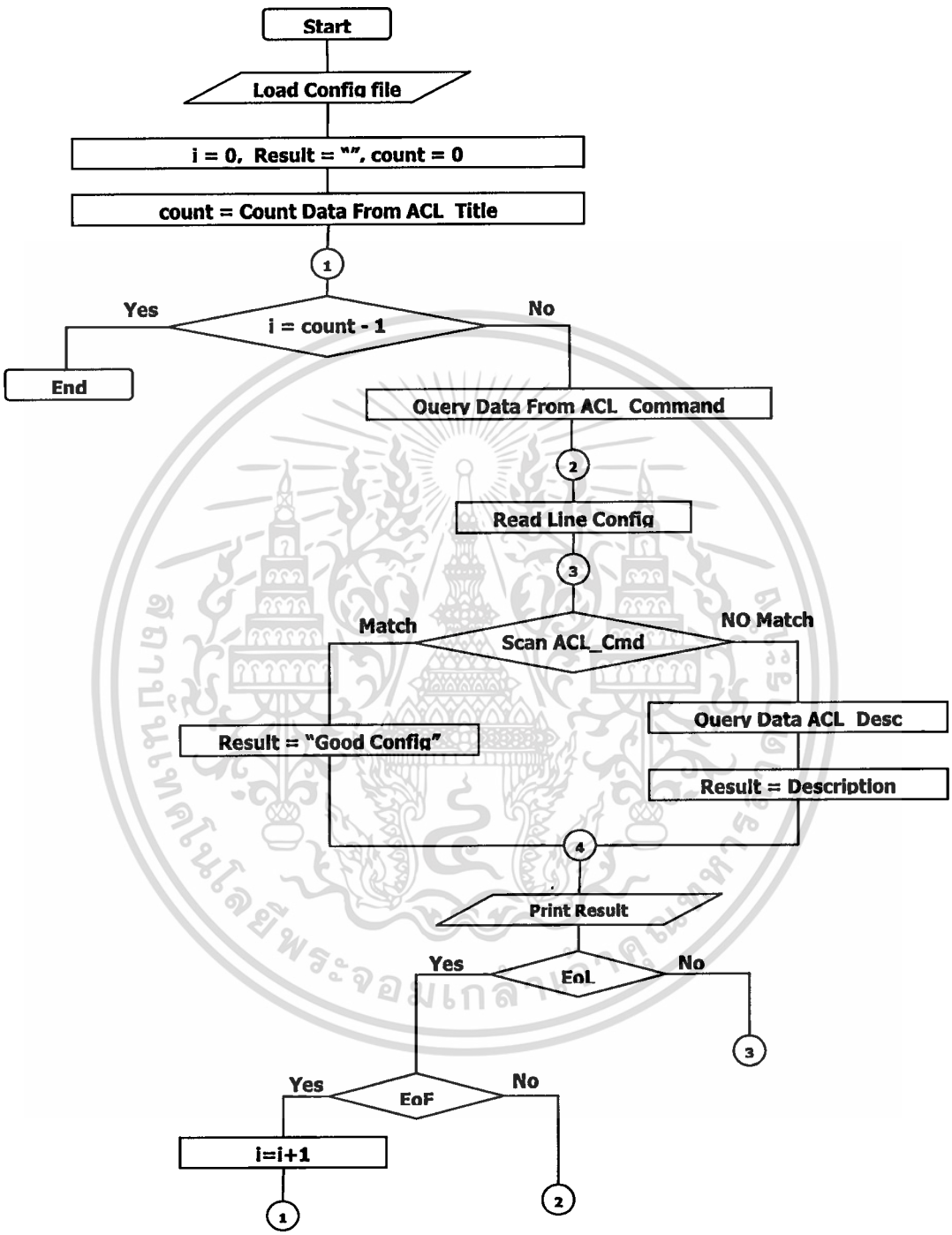
1. เมื่อระบบทำการอ่านค่าไฟล์ที่ต้องการตรวจสอบแล้ว ระบบจะทำการสร้างตัวแปร I มีค่าเท่ากับ 0 และตัวแปร Count ขึ้นมาเพื่อทำการเช็คและนับจำนวนของคำสั่งที่จะตรวจสอบจากฐานข้อมูล
2. ถ้า count = i แล้วแสดงว่าไม่มีค่าหรือคำสั่งอยู่ในฐานข้อมูล ระบบจะจบการทำงานทันที แต่ถ้า count มีค่ามากกว่า 0 ระบบจะทำการ query ค่าจากฟิลด์ Good_Command เพื่อทำการดึงค่าคำสั่งที่เหมาะสมสำหรับการคอนฟิกูเรชั่นขึ้นมาจากฐานข้อมูล เพื่อนำค่า Good_Command นี้มาทำการตรวจหาคำในไฟล์คอนฟิกูเรชั่นในแต่ละบรรทัด
3. ในการตรวจหา Good_Command ถ้าไม่พบค่าของ Good_Command ในไฟล์คอนฟิกูเรชั่นในแต่ละบรรทัด ระบบจะทำการ query ค่าจากฟิลด์ Bad_Command เพื่อทำการดึงค่าคำสั่งที่ไม่เหมาะสมสำหรับการคอนฟิกูเรชั่นขึ้นมาจากฐานข้อมูล เพื่อนำค่า Bad_Command นี้มาทำการตรวจหาคำในไฟล์คอนฟิกูเรชั่นในแต่ละบรรทัด
4. ถ้าไม่พบ Bad_Command ระบบจะทำการquery ค่าจากฟิลด์ Description ขึ้นมา จากฐานข้อมูล เพื่อนำค่า Description นี้มาทำการแสดงเป็นค่า Result เพื่อแสดงข้อแนะนำเกี่ยวกับการคอนฟิกูเรชั่น
5. ในการตรวจหา Good_Command ถ้าตรวจสอบพบ ระบบจะทำการแสดงผลว่าในหัวข้อที่ตรวจหานั้น มีการคอนฟิกูเรชั่นที่เหมาะสมแล้ว
6. ระบบจะทำการตรวจสอบเช่นนี้ไปจนกว่าจะหมดไฟล์คอนฟิกูเรชั่น และจนกว่าจะหมดข้อมูลในฐานข้อมูลทุกตัว หรือ count = i



รูปที่ 3.5 กระบวนการทำงานของระบบในส่วนของ Router Service Security

3. Router Access List

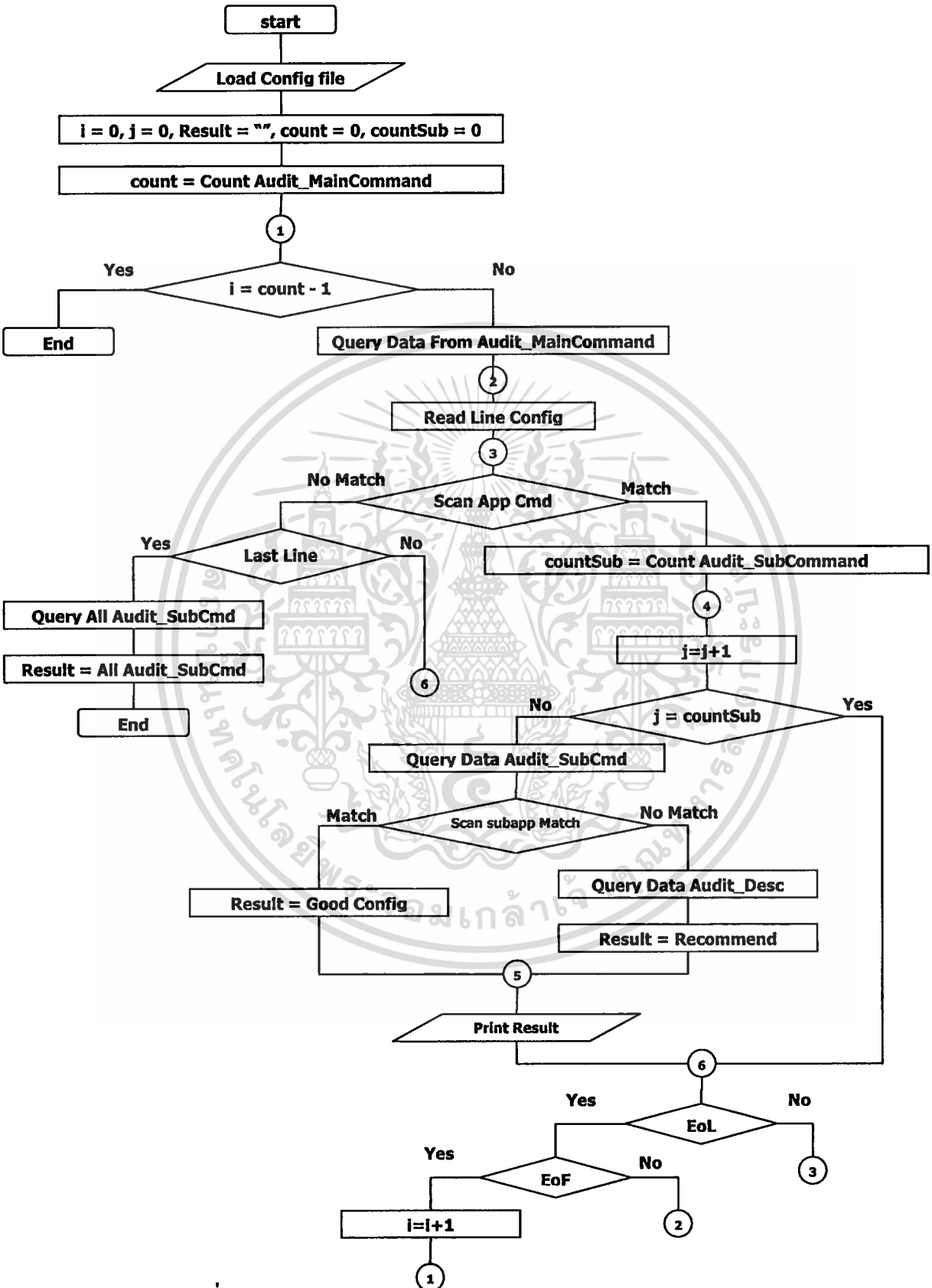
1. เมื่อระบบทำการอ่านค่าไฟล์ที่ต้องการตรวจสอบแล้ว ระบบจะทำการสร้างตัวแปร i มีค่าเท่ากับ 0 และตัวแปร count ขึ้นมาเพื่อทำการเช็คและนับจำนวนของหัวข้อหลักของคำสั่งและคำสั่งเหมาะสมที่จะใช้ในการตรวจสอบจากฐานข้อมูล
2. ถ้า count = i แล้วแสดงว่าไม่มีค่าหรือคำสั่งต่างๆ อยู่ในฐานข้อมูล หรือ ทำการตรวจเช็คหมดแล้ว ระบบจะจบการทำงานทันที แต่ถ้า count มีค่ามากกว่า 0 ระบบจะทำการ query ค่าจากฟิลด์ ACL_Command ขึ้นมาจากฐานข้อมูลเพื่อดึงค่า Appropriate Command หรือคำสั่งที่เหมาะสมในการคอนฟิกูเรชั่นขึ้นมาเพื่อทำการตรวจหา Appropriate Command ในแต่ละบรรทัด
3. ถ้าไม่พบ Appropriate Command ระบบจะทำการ query ค่าจากฟิลด์ ACL_Desc เพื่อดึงค่า Description ขึ้นมาเพื่อแสดงคำแนะนำเกี่ยวกับการคอนฟิกูเรชั่น Appropriate Command ที่เหมาะสม
4. แต่ถ้าพบ Appropriate Command ระบบจะทำการแสดงผลว่า การคอนฟิกูเรชั่นนั้นเหมาะสมดีแล้ว
5. ระบบจะทำการตรวจสอบเช่นนี้ไปจนกว่าจะหมดไฟล์คอนฟิกูเรชั่น และจนกว่าจะหมดข้อมูลในฐานข้อมูลทุกตัว หรือ count = i



รูปที่ 3.6 กระบวนการทำงานของระบบในส่วนของ Router Access List

4. Audit Management

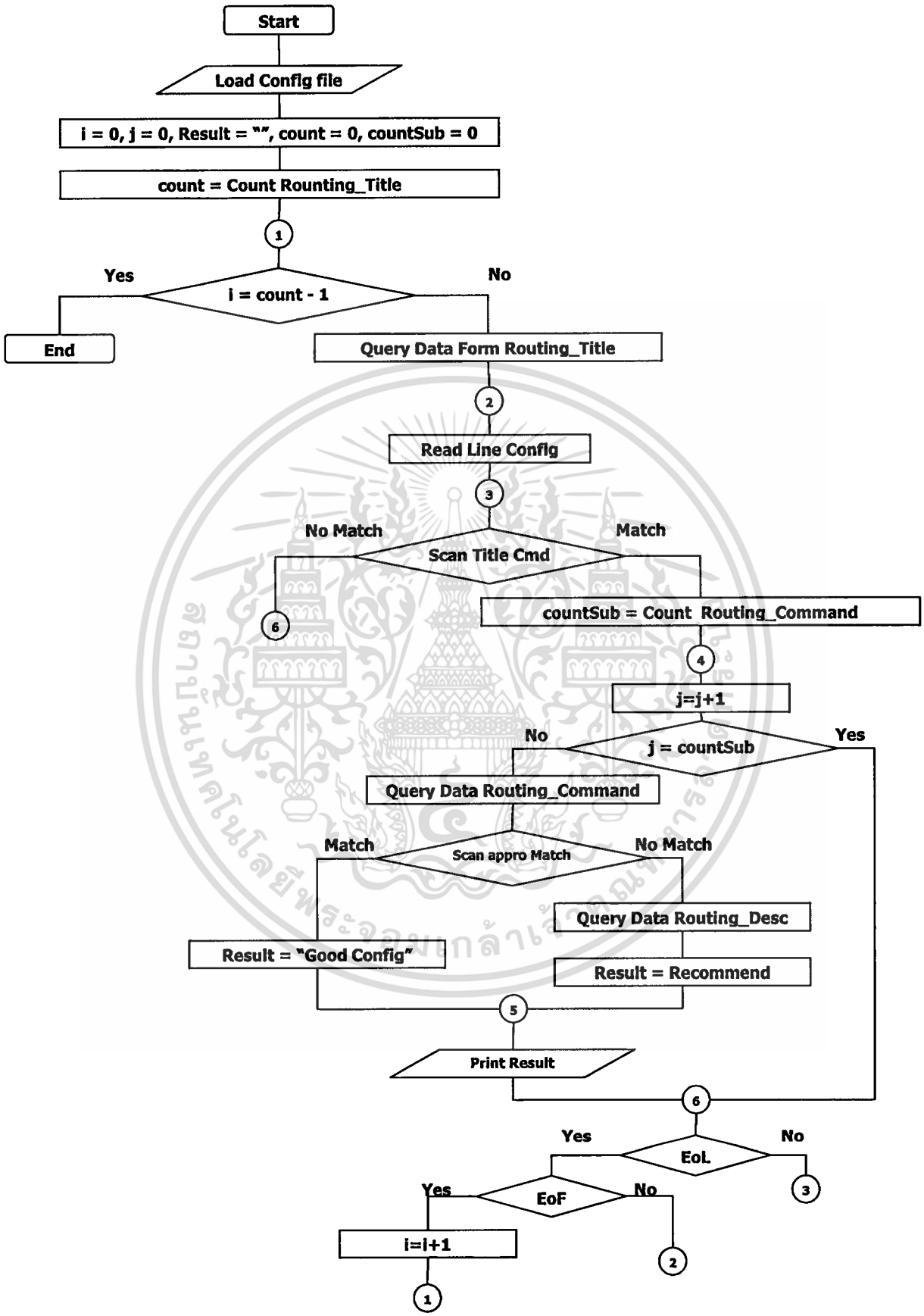
1. เมื่อระบบทำการอ่านค่าไฟล์ที่ต้องการตรวจสอบแล้ว ระบบจะทำการสร้างตัวแปร i และ j มีค่าเท่ากับ 0 และตัวแปร count และ countSub ขึ้นมาเพื่อทำการเช็คและนับจำนวนของคำสั่งที่เหมาะสม และคำสั่งย่อยที่เหมาะสมที่จะใช้ในการตรวจสอบจากฐานข้อมูล
2. ถ้า count = i และ countSub = j แล้วแสดงว่าไม่มีค่าหรือคำสั่งต่างๆ อยู่ในฐานข้อมูล หรือทำการตรวจเช็คหมดแล้ว ระบบจะจบการทำงานทันที
3. แต่ถ้า count มีค่ามากกว่า 0 ระบบจะทำการ query ค่าจากฟิลด์ Audit_MainCommand เพื่อทำการดึงค่า Appropriate Command หรือคำสั่งที่เหมาะสมขึ้นมาจากฐานข้อมูล เพื่อนำค่า Appropriate Command นี้มาทำการตรวจหาคำในไฟล์คอนฟิกูเรชั่นในแต่ละบรรทัด
4. ในการตรวจหาAppropriate Command ถ้าไม่พบค่าของ Appropriate Command ในไฟล์คอนฟิกูเรชั่นในทุกบรรทัด ระบบจะทำการ query ค่าจากฟิลด์ Audit_SubCommand เพื่อทำการดึงค่า Appropriate Subcommand หรือคำสั่งย่อยที่เหมาะสมขึ้นมา จากฐานข้อมูล ทั้งหมดเพื่อนำค่าที่ได้มาทำการแสดง เพื่อเป็นการแนะนำคำสั่งต่างๆ ที่สมควรมีการคอนฟิกูเรชั่น
5. ในการตรวจหา Appropriate Command ถ้าพบค่าของ Appropriate Command ในไฟล์คอนฟิกูเรชั่นในแต่ละบรรทัด ระบบจะทำการ query ค่าจากฟิลด์ Audit_SubCommand ขึ้นมาเช่นกัน เพื่อทำการตรวจหา Appropriate Subcommand ในแต่ละบรรทัด
6. ถ้าไม่พบ Appropriate Subcommand ระบบจะทำการ query ค่าจากฟิลด์ Audit_Desc ขึ้นมาจากฐานข้อมูล เพื่อแสดงคำแนะนำเกี่ยวกับการคอนฟิกูเรชั่น Appropriate Command ที่เหมาะสม ถ้าพบระบบจะทำการแสดงผลว่า การคอนฟิกูเรชั่นนั้นเหมาะสมดีแล้ว
7. ระบบจะทำการตรวจสอบเช่นนี้ไปจนกว่าจะหมดไฟล์คอนฟิกูเรชั่น และจนกว่าจะหมดข้อมูลในฐานข้อมูลทุกตัว หรือ count = i



รูปที่ 3.7 กระบวนการทำงานของระบบในส่วนของ Audit Management

5. Scan Routing

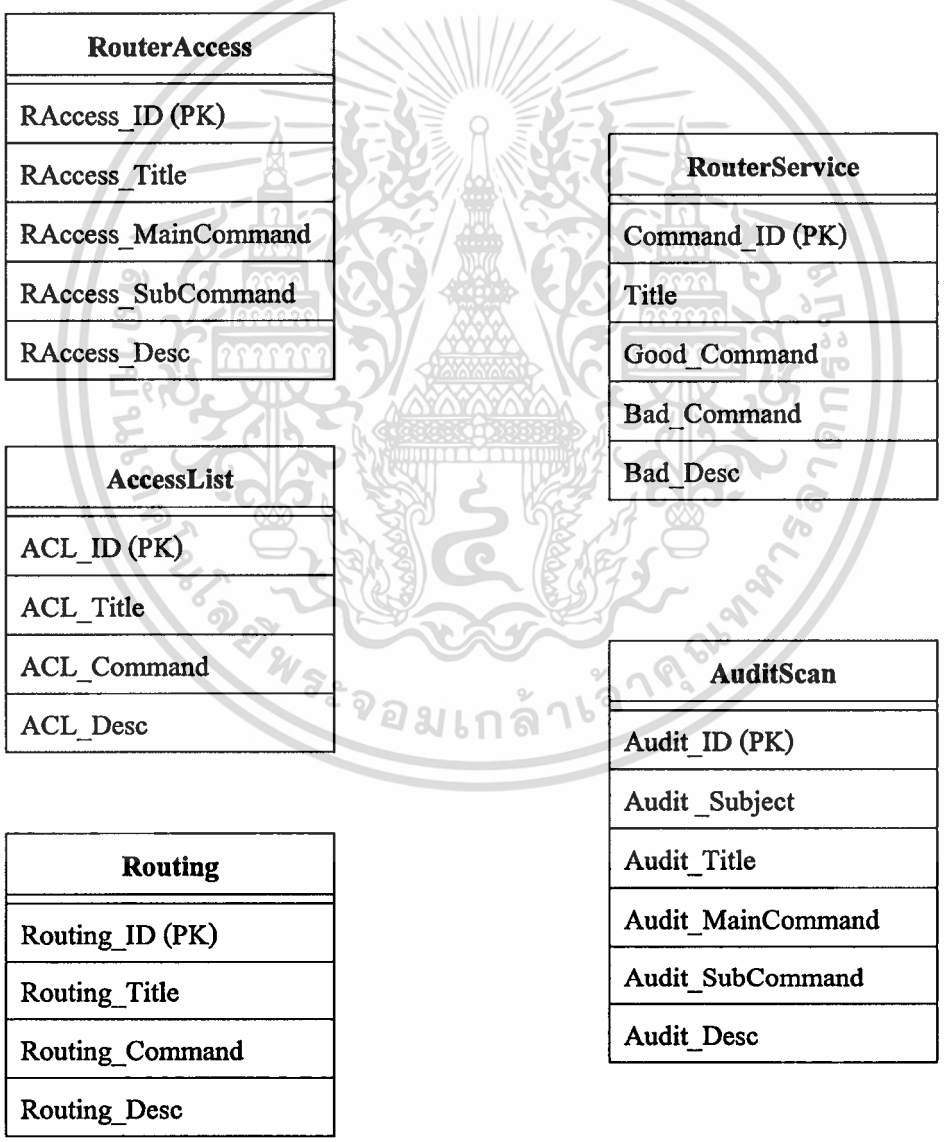
1. เมื่อระบบทำการอ่านค่าไฟล์ที่ต้องการตรวจสอบแล้ว ระบบจะทำการสร้างตัวแปร i และ j มีค่าเท่ากับ 0 และตัวแปร count และ countSub ขึ้นมาเพื่อทำการเช็คและนับจำนวนของหัวข้อหลักของคำสั่งและคำสั่งเหมาะสมที่จะใช้ในการตรวจสอบจากฐานข้อมูล
2. ถ้า count = i และ countSub = j แล้วแสดงว่าไม่มีค่าหรือคำสั่งต่างๆ อยู่ในฐานข้อมูล หรือทำการตรวจเช็คหมดแล้ว ระบบจะจบการทำงานทันที แต่ถ้า count มีค่ามากกว่า 0 ระบบจะทำการ query ค่าจากฟิลด์ Routing_Title ขึ้นมาจากฐานข้อมูล เพื่อนำค่า Title Command นี้มาทำการตรวจหาคำในไฟล์คอนฟิกูเรชั่นในแต่ละบรรทัด
3. ในการตรวจหา Title Command ถ้าไม่พบค่าของ Title Command ในไฟล์คอนฟิกูเรชั่นในทุกบรรทัด ระบบจะจบการทำงาน เนื่องจากมีการคอนฟิกูเรชั่นที่เหมาะสมอยู่แล้ว
4. แต่ถ้าในการตรวจหา Title Command ถ้าพบค่าของ Title Command ในไฟล์คอนฟิกูเรชั่นในแต่ละบรรทัด ระบบจะทำการ query ค่าจากฟิลด์ Routing_Command เพื่อทำการดึงค่า Appropriate Command หรือคำสั่งที่เหมาะสมขึ้นมาเพื่อทำการตรวจหา Appropriate Command ในแต่ละบรรทัด
5. ถ้าไม่พบ Appropriate Command ระบบจะทำการ query ค่าจากฟิลด์ Routing_Desc ขึ้นมาเพื่อทำการแสดง Recommend ขึ้นมาเพื่อแสดงคำแนะนำเกี่ยวกับการคอนฟิกูเรชั่น Appropriate Command ที่เหมาะสม แต่ถ้าพบระบบจะทำการแสดงผลว่า การคอนฟิกูเรชั่นนั้นเหมาะสมดีแล้ว
6. ระบบจะทำการตรวจสอบเช่นนี้ไปจนกว่าจะหมดไฟล์คอนฟิกูเรชั่น และจนกว่าจะหมดข้อมูลในฐานข้อมูลทุกตัว หรือ count = i



รูปที่ 3.8 กระบวนการทำงานของระบบในส่วนของ Scan Routing

3.4 การออกแบบระบบฐานข้อมูล

การออกแบบฐานข้อมูล เป็นขั้นตอนแรกของการสร้างแอพพลิเคชั่น ซึ่งการออกแบบฐานข้อมูลที่ดีจะทำให้ลดความซ้ำซ้อนของข้อมูล และสามารถตอบสนองต่อการเข้าถึงข้อมูลได้สะดวกและรวดเร็ว มีความเป็นอิสระระหว่างข้อมูลและแอพพลิเคชั่น โดยการออกแบบฐานข้อมูลของระบบนี้ จะพบว่าตารางแต่ละตารางในฐานข้อมูลจะไม่มีความสัมพันธ์กัน ซึ่งสามารถลักษณะของฐานข้อมูลของระบบการตรวจสอบการคอนฟิกูเรชั่นของอุปกรณ์เราเตอร์ ได้ดังรูป



รูปที่ 3.9 เอนทิตี้ต่างๆ ของระบบ

3.5 รายละเอียดของตารางต่างๆ

จากแผนภาพแสดงความสัมพันธ์ของข้อมูลที่เกี่ยวของในระบบการตรวจสอบการคอนฟิกูเรชั่นของอุปกรณ์เราเตอร์ นั้นเราสามารถแทนที่ความสัมพันธได้ด้วยตาราง ซึ่งมีทั้งหมด 5 ตาราง โดยจะแสดงพร้อมกับการทำพจนานุกรมข้อมูล จะได้ดังตารางต่อไปนี้

ตารางที่ 3.1 แสดงตาราง RouterService

Table : RouterService (ตารางรายการคำสั่งที่ใช้ในการตรวจสอบ Router Service Security)				
Attribute	**Data Type**	**Key**	**Description**	**ข้อกำหนด**
Command_ID	char(7)	PK	รหัสคำสั่งที่ใช้ในการตรวจสอบ	Not Null
Title	char(50)		หัวข้อการตรวจสอบ Router Service	Not Null
Good_Command	char(50)		คำสั่งที่ควรมีการคอนฟิกูเรชั่น	
Bad_Command	char(50)		คำสั่งที่ไม่ควรมีการคอนฟิกูเรชั่น	
Bad_Desc	Memo		คำอธิบายสาเหตุของคำสั่งที่ไม่ควรมี	

ตารางที่ 3.2 แสดงตาราง AuditScan

Table : AuditScan (ตารางรายการคำสั่งที่ใช้ในการตรวจสอบ Audit Scan)				
Attribute	**Data Type**	**Key**	**Description**	**ข้อกำหนด**
Audit_ID	char(7)	PK	รหัสคำสั่งที่ใช้ในการตรวจสอบ	Not Null
Audit _Subject	char(50)		หัวเรื่องคำสั่งที่ใช้ในการตรวจสอบ	Not Null
Audit_Title	char(50)		หัวข้อการตรวจสอบ Audit	
Audit_ MainCommand	char(50)		คำสั่งหลักที่ควรมีการคอนฟิกูเรชั่น เกี่ยวกับหัวข้อที่ใช้ในการตรวจสอบ	
Audit_ SubCommand	char(50)		คำสั่งย่อยที่ควรมีการคอนฟิกูเรชั่น เกี่ยวกับหัวข้อที่ใช้ในการตรวจสอบ	
Audit_Desc	Memo		คำอธิบายหัวข้อการตรวจสอบ Audit	

ตารางที่ 3.3 แสดงตาราง RouterAccess

Table : RouterAccess (ตารางรายการคำสั่งที่ใช้ในการตรวจสอบ Router Access Security)				
Attribute	**Data Type**	**Key**	**Description**	**ข้อกำหนด**
RAccess_ID	char(7)	PK	รหัสคำสั่งที่ใช้ในการตรวจสอบ	Not Null
RAccess_Title	char(50)		หัวข้อการตรวจสอบ Router Access	Not Null
RAccess_ MainCommand	char(50)		คำสั่งหลักที่ควรมีการคอนฟิกูเรชั่นเกี่ยวกับหัวข้อที่ใช้ในการตรวจสอบ	
RAccess_ SubCommand	char(50)		คำสั่งย่อยที่ควรมีการคอนฟิกูเรชั่นเกี่ยวกับหัวข้อที่ใช้ในการตรวจสอบ	
RAccess_Desc	Memo		คำอธิบายการตรวจสอบ Router Access	

ตารางที่ 3.4 แสดงตาราง AccessList

Table : AccessList (ตารางรายการคำสั่งที่ใช้ในการตรวจสอบ Access Control List)				
Attribute	**Data Type**	**Key**	**Description**	**ข้อกำหนด**
ACL_ID	char(7)	PK	รหัสคำสั่งที่ใช้ในการตรวจสอบ	Not Null
ACL_Title	char(50)		หัวข้อการตรวจสอบ Access Control	Not Null
ACL_Command	char(50)		คำสั่งที่เหมาะสมในการคอนฟิกูเรชั่น	
ACL_Desc	Memo		คำอธิบายของคำสั่งที่เกี่ยวกับ ACL	

ตารางที่ 3.5 แสดงตาราง Routing

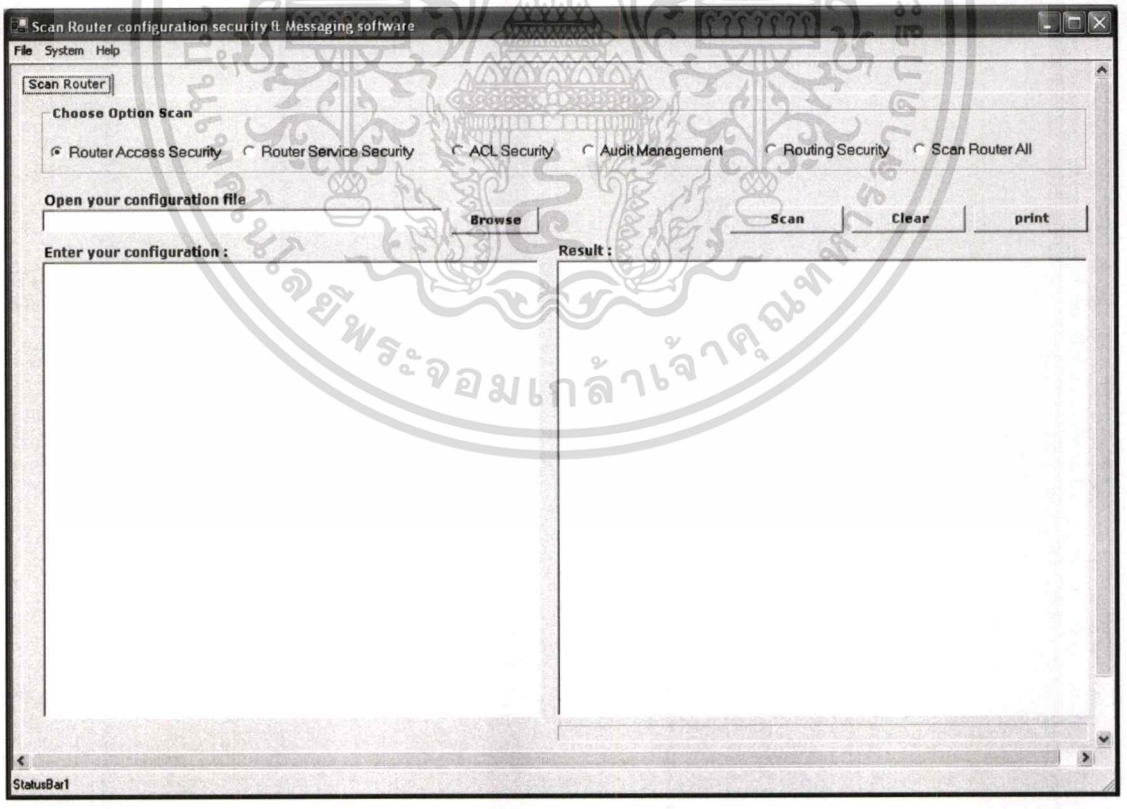
Table : Routing (ตารางรายการคำสั่งที่ใช้ในการตรวจสอบ Routing)				
Attribute	**Data Type**	**Key**	**Description**	**ข้อกำหนด**
Routing_ID	char(7)	PK	รหัสคำสั่งที่ใช้ในการตรวจสอบ	Not Null
Routing_Title	char(50)		หัวข้อการตรวจสอบ Routing	Not Null
Routing_Command	char(50)		คำสั่งที่เหมาะสมในการคอนฟิก	
Routing_Desc	Memo		คำอธิบายคำสั่งที่เกี่ยวกับ Routing	

บทที่ 4

การพัฒนาระบบ

จากการวิเคราะห์และออกแบบระบบงานที่ได้กล่าวมาแล้วนั้น ทำให้เราสามารถทำการพัฒนาระบบงาน โดยแยกตามลักษณะของการทำงานได้ 2 ส่วนด้วยกัน คือ ส่วนที่จัดการเกี่ยวกับการตรวจสอบคอนฟิกูเรชั่น และส่วนที่จัดจัดเก็บคำสั่งพื้นฐานที่ควรมีการคอนฟิกูเรชั่น ซึ่งในโปรแกรมยังมีส่วนประกอบต่างๆ ที่นำมาใช้ในการจัดการเกี่ยวกับการใช้งานแอพพลิเคชั่น เช่น การพิมพ์เอกสารคำแนะนำเกี่ยวกับการคอนฟิกูเรชั่น ด้วย

โดยในบทนี้ จะกล่าวถึงการพัฒนาโปรแกรมและผลที่ได้จากการพัฒนาโปรแกรมโดยแสดงออกมาเป็นลักษณะจอภาพส่วนต่างๆ ของโปรแกรมได้ ดังนี้



รูปที่ 4.1 หน้าจอหลักของระบบการตรวจสอบการคอนฟิกูเรชั่นบนอุปกรณ์เราเตอร์

จากรูปที่ 4.1 จะแสดงหน้าจอหลักของระบบการตรวจสอบการคอนฟิกูเรชั่นบนอุปกรณ์เราเตอร์ โดยเมื่อผู้เข้าเข้าใช้โปรแกรมจะปรากฏหน้าจอนี้เป็นหน้าแรก

ผู้ใช้สามารถเลือกเข้าใช้งานตามเมนูต่างๆ ที่อยู่ในส่วนของเมนูบาร์ได้ ซึ่งจะมี 3 ส่วนหลัก คือ เมนู File, เมนู System และ เมนู Help

รูปที่ 4.2 เมนูย่อยที่มีอยู่ในเมนู File

จากรูป 4.2 จะเห็นว่า ส่วนของเมนู File นั้นประกอบด้วยเมนูย่อยหลายเมนู ซึ่งสามารถอธิบายวัตถุประสงค์ของเมนูย่อยต่างๆ ได้ดังนี้

Load Config คือ เมนูที่ใช้สำหรับทำการ Load ไฟล์คอนฟิกูเรชั่นของอุปกรณ์เราเตอร์ขึ้นมาใช้ในระบบ

Scan คือ เมนูที่ใช้สำหรับเรียกหน้าจอ Scan Routing ขึ้นมา เพื่อทำการ Scan หรือตรวจสอบไฟล์คอนฟิกูเรชั่นของอุปกรณ์เราเตอร์

Export to File คือ เมนูที่ใช้สำหรับทำการ Export ผลลัพธ์ที่ได้จากการตรวจสอบคอนฟิกูเรชั่นของอุปกรณ์เราเตอร์

Print Preview แสดงภาพก่อนพิมพ์

Print Setting ทำการเซ็ตหน้าจอของการพิมพ์และเครื่องพิมพ์

Print พิมพ์ผลลัพธ์ที่ได้จากการตรวจสอบคอนฟิกูเรชั่นออกสู่เครื่องพิมพ์

Exit ออกจากโปรแกรม

รูปที่ 4.3 เมนูย่อยที่มีอยู่ในเมนู System

จากรูป 4.3 จะเห็นว่า ส่วนของเมนู System นั้นประกอบด้วยเมนูย่อยหลายเมนู ซึ่งแต่ละเมนูย่อยนี้ จะเกี่ยวข้องกับการจัดเก็บคำสั่งต่างๆ ที่ควรมีการคอนฟิกูเรชั่น เพื่อนำคำสั่งเหล่านี้มาใช้ในการตรวจสอบคอนฟิกูเรชั่นในหัวข้อต่างๆ ซึ่งมีทั้งหมด 5 เมนูย่อย ด้วยกัน

รูปที่ 4.4 เมนูย่อยที่มีอยู่ในเมนู Help

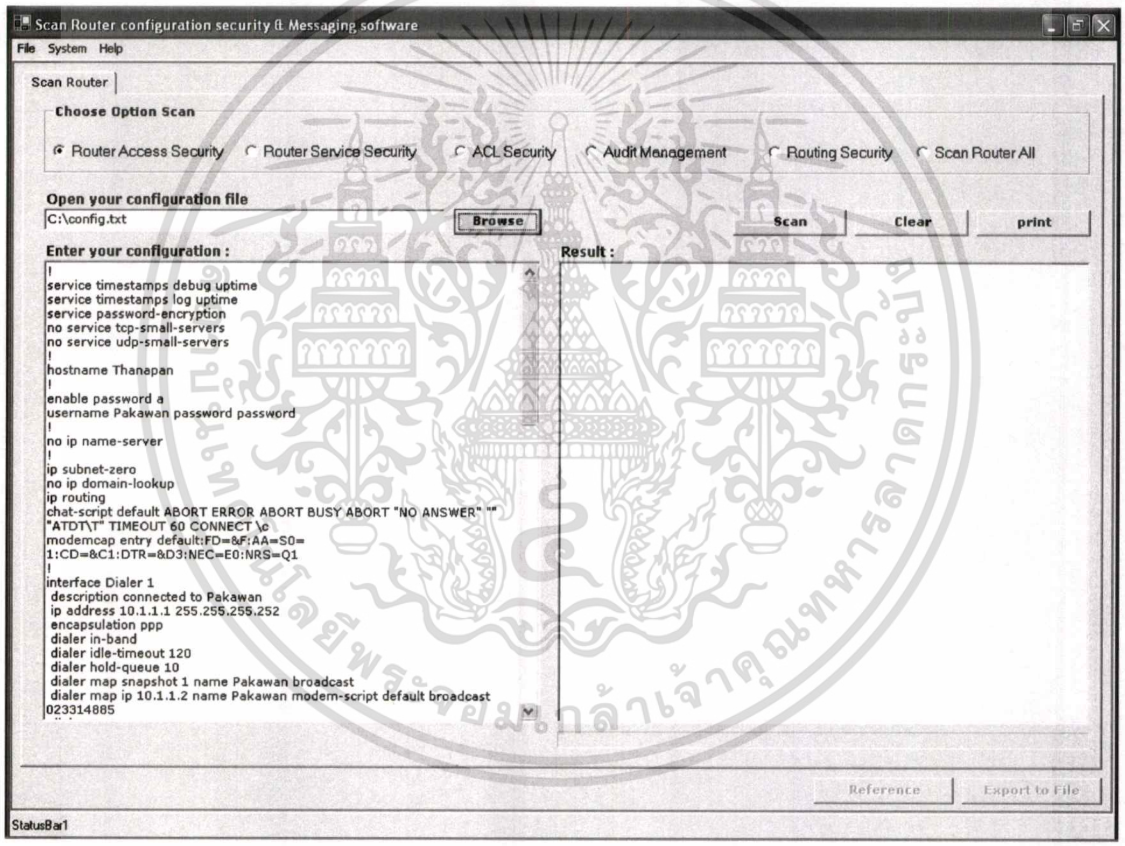
จากรูป 4.4 จะเห็นว่า ส่วนของเมนู Help นั้นประกอบด้วยเมนูย่อย 3 เมนู ซึ่งเมนูย่อย Reference จะแสดงคำแนะนำในการคอนฟิกูเรชั่นในหัวข้อที่เลือกไว้ในหน้าจอหลักที่ทำการตรวจสอบอยู่ ส่วนเมนูย่อย Help on Help จะแสดงคำแนะนำในการคอนฟิกูเรชั่นทั้งหมด ส่วนเมนูย่อยสุดท้ายคือ เมนูย่อย About จะเป็นการแสดงเวอร์ชั่นของโปรแกรม

4.1 การพัฒนาโปรแกรมส่วนที่จัดการเกี่ยวกับการตรวจสอบคอนฟิกูเรชั่น

ในการพัฒนาโปรแกรมในส่วนนี้ จะเป็นส่วนของการจัดการเกี่ยวกับการตรวจสอบวิธีการคอนฟิกูเรชั่นของอุปกรณ์เราเตอร์ และเป็นหน้าหลักของโปรแกรม ดังนั้น เมื่อผู้ใช้เปิดโปรแกรมนี้ขึ้นมาจะพบหน้านี้เป็นหน้าแรก

โปรแกรมนี้ไม่มีส่วนของหน้าจอที่ใช้สำหรับการ Login และไม่มีส่วนของ Administrator เนื่องจากโปรแกรมนี้เป็นโปรแกรมที่ใช้สำหรับตรวจสอบวิธีการคอนฟิกูเรชั่น เท่านั้น ซึ่งไม่จำเป็นที่จะต้องจัดการในเรื่องของการรักษาความปลอดภัย

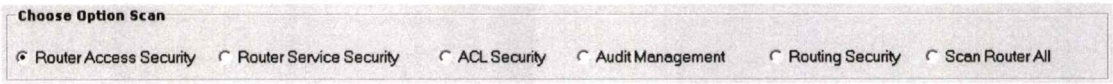
ผู้ที่ต้องการใช้งานในระบบนี้ จะต้องทำการจัดเตรียมไฟล์ที่เป็นวิธีการคอนฟิกูเรชั่นของอุปกรณ์เราเตอร์ที่ต้องการทำการตรวจสอบให้อยู่ในรูปของไฟล์เอกสาร ซึ่งโปรแกรมสามารถรองรับไฟล์นามสกุล .txt, .doc และ .rtf ได้ และเมื่อผู้ใช้งานเข้ามาในโปรแกรมแล้ว ผู้ใช้งานสามารถโหลดไฟล์คอนฟิกูเรชั่นที่เตรียมไว้ เข้าไปในโปรแกรมได้โดยการกดปุ่ม Browse หรือกดปุ่ม Load Config ในส่วนของเมนูไฟล์ เพื่อทำการเลือกไฟล์ที่ต้องการทำการตรวจสอบขึ้นมา ไฟล์คอนฟิกูเรชั่นที่ทำการโหลดเข้ามานั้นจะปรากฏอยู่ในส่วนของ Enter your configuration: ที่อยู่ทางด้านซ้ายมือของโปรแกรม ดังรูป 4.5



รูปที่ 4.5 หน้าจอเมื่อมีการโหลดไฟล์คอนฟิกูเรชั่นเข้ามาในโปรแกรม

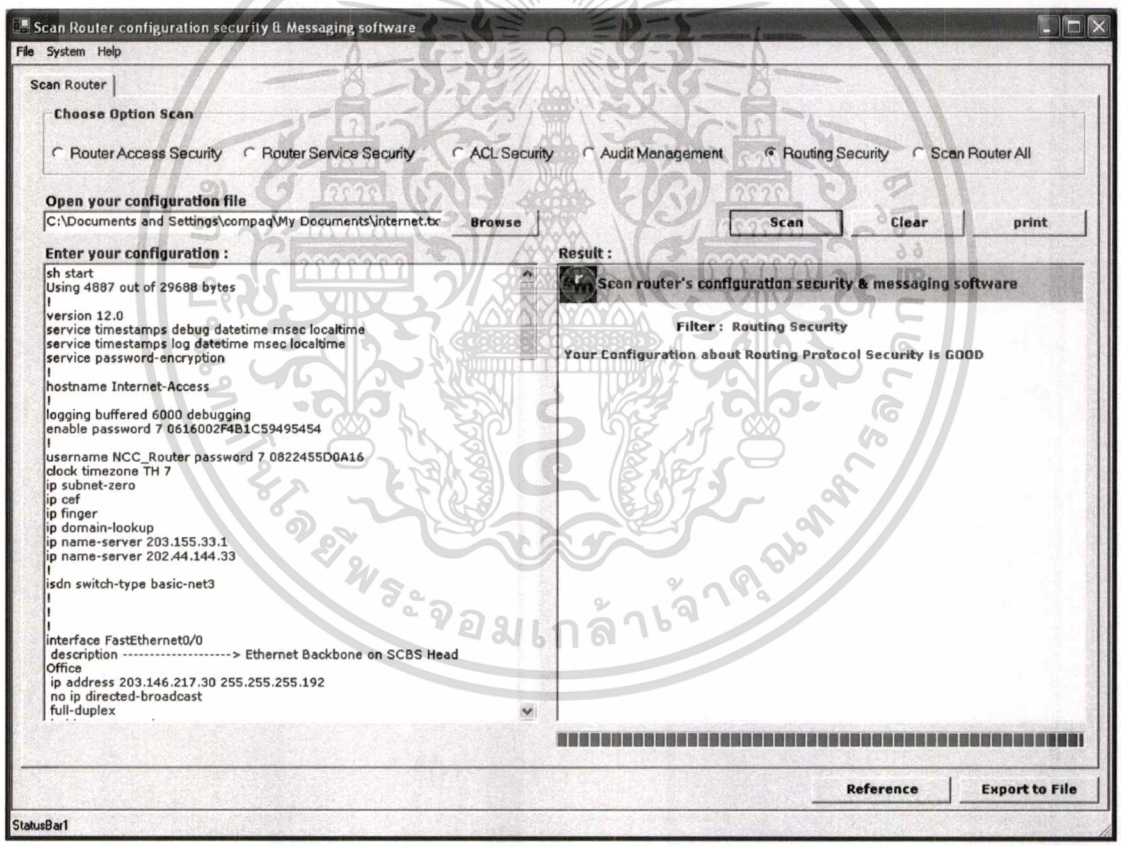
ในส่วนของ Enter your configuration: ผู้ใช้สามารถทำการพิมพ์วิธีการคอนฟิกูเรชั่นที่ต้องการตรวจสอบเข้าไปในส่วนของ Enter your configuration: เพื่อทำการตรวจสอบได้โดยตรง

ในส่วนของ Choose Option Scan จะเป็นการเลือกหัวข้อที่ต้องการทำการตรวจสอบซึ่งจะมีหัวข้อที่สามารถตรวจสอบได้ 6 ประเภทด้วยกัน โดยโปรแกรมจะเลือกหัวข้อที่จะตรวจสอบไว้ที่ Router Access Security ไว้เป็นค่าเริ่มต้น ดังรูป



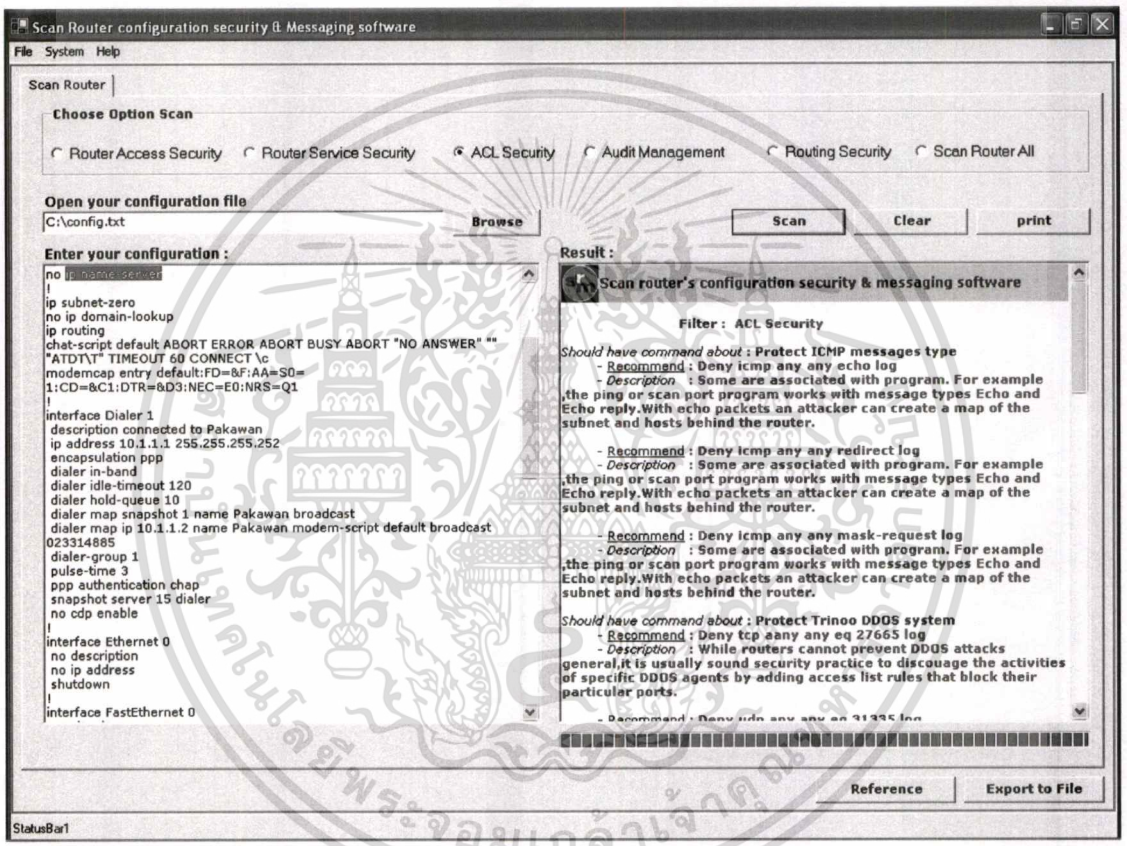
รูปที่ 4.6 หน้าจอในส่วนของ Choose Option Scan

เมื่อผู้ใช้ทำการเลือก Choose Option Scan แล้ว สามารถทำการตรวจสอบไฟล์คอนฟิกูเรชั่นได้โดยกดปุ่ม Scan หรือกดปุ่ม Scan ในส่วนของเมนูไฟล์ โปรแกรมจะทำการตรวจสอบว่าไฟล์คอนฟิกูเรชั่นนั้น มีการคอนฟิกูเรชั่นที่เหมาะสมหรือไม่ ถ้ามีการคอนฟิกูเรชั่นที่เหมาะสมแล้ว ระบบจะแสดงผลการตรวจสอบทางด้านขวามือของหน้าจอ ในส่วนของ Result: ดังรูป



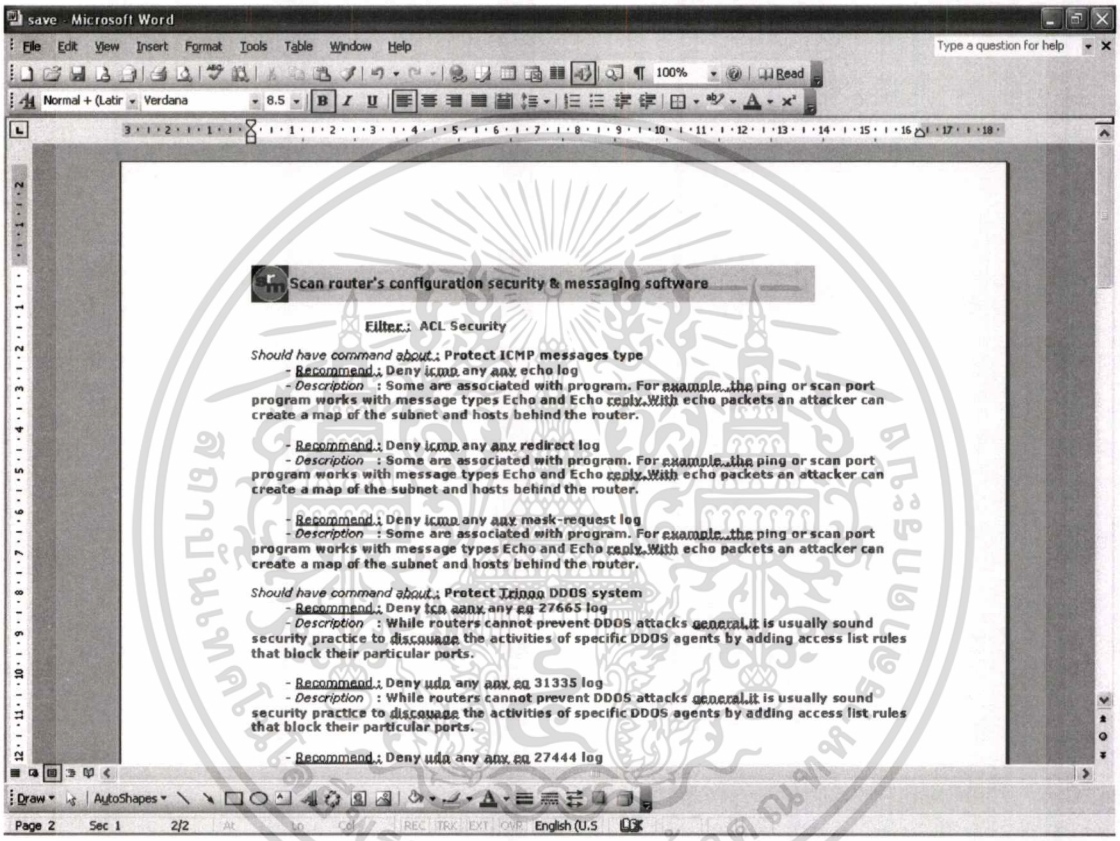
รูปที่ 4.7 หน้าจอเมื่อตรวจสอบคอนฟิกูเรชั่นแล้วพบว่ามีการคอนฟิกูเรชั่นที่เหมาะสม

ในกรณีที่มีการคอนฟิกูเรชั่นที่ไม่เหมาะสม ระบบจะแสดงผลการตรวจสอบทางด้านขวามือของหน้าจอในส่วนของ Result: โดยแสดงถึงคำแนะนำที่เหมาสมที่ควรจะต้องมีการคอนฟิกูเรชั่นลงไปเพื่อเพิ่มความปลอดภัยให้กับอุปกรณ์เราเตอร์ โดยจะแสดงถึงหัวข้อหลักที่ควรมีการคอนฟิกูเรชั่น ซึ่งโปรแกรมจะแนะนำคำสั่งที่ควรจะต้องมี และเหตุผลของการคอนฟิกูเรชั่น คำสั่งนั้นๆ ดังรูป



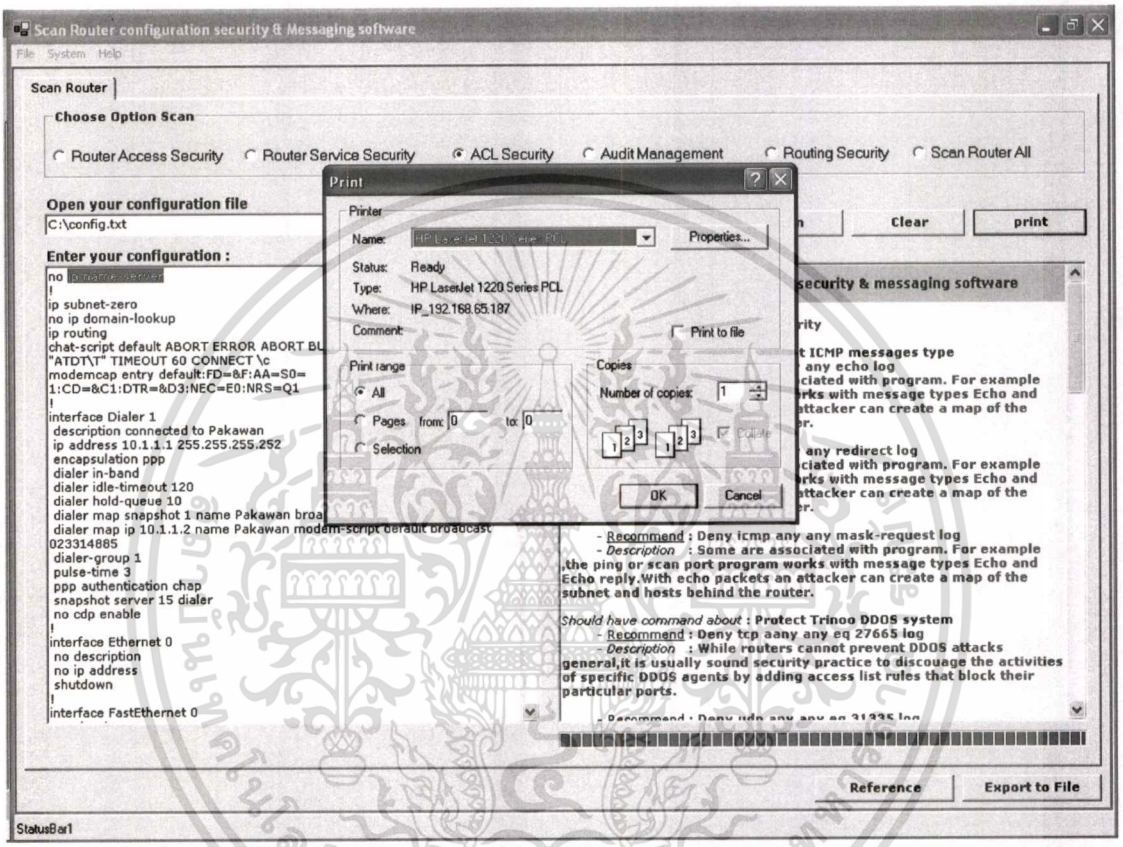
รูปที่ 4.8 หน้าจอเมื่อตรวจสอบคอนฟิกูเรชั่นแล้วพบว่ามีการคอนฟิกูเรชั่นที่ไม่เหมาะสม

เมื่อทำการตรวจสอบเรียบร้อยแล้ว ถ้าผู้ใช้ต้องการที่จะ Export ผลลัพธ์ที่ได้จากการตรวจสอบออกมาอยู่ในรูปของไฟล์เอกสาร (นามสกุล .doc) สามารถทำได้โดยการกดปุ่ม **Export to File** หรือกดปุ่ม Export to File ในส่วนของเมนูไฟล์ โปรแกรมจะทำการเปิดไฟล์ Microsoft Word ขึ้นมาและแสดงผลลัพธ์ที่ได้จากการตรวจสอบ ดังรูป



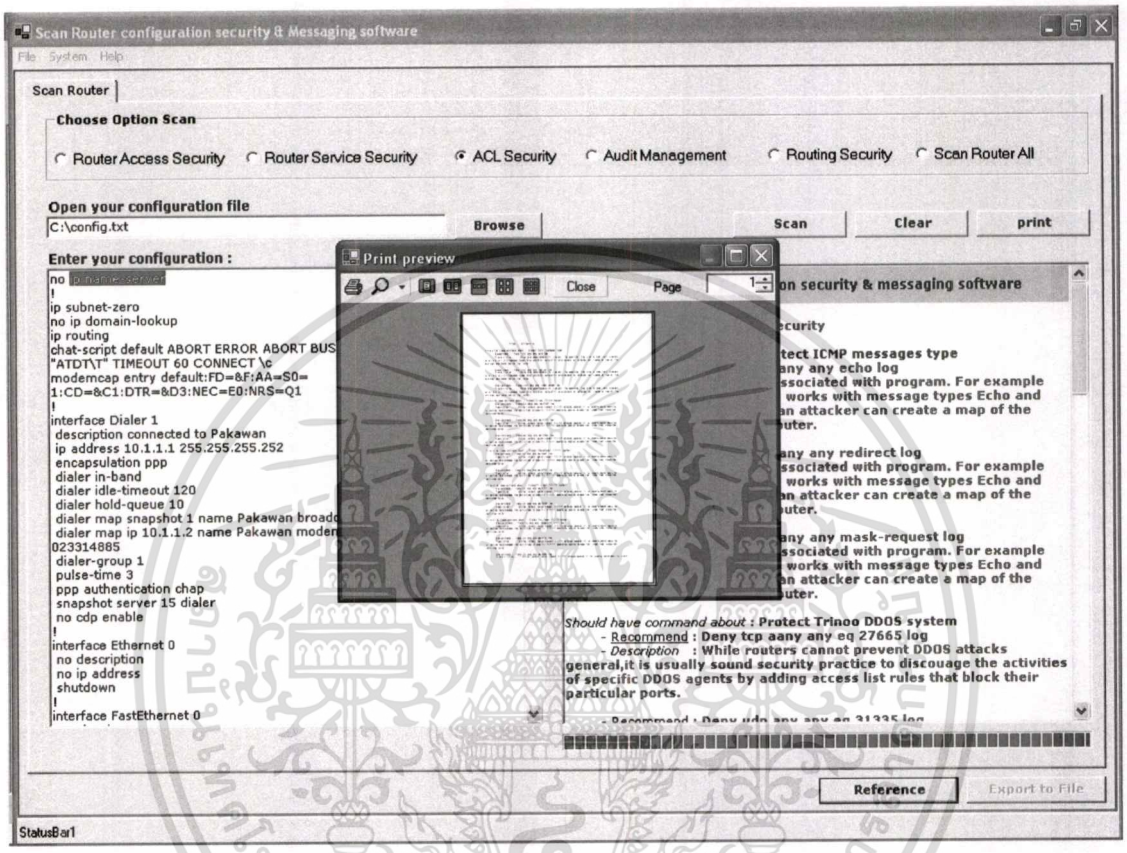
รูปที่ 4.9 หน้าจอเมื่อทำการ Export ผลลัพธ์ที่ได้จากการตรวจสอบ

โปรแกรมสามารถทำการพิมพ์ผลลัพธ์ที่ได้จากการตรวจสอบออกทางเครื่องพิมพ์ได้ โดยการกดปุ่ม print หรือกดปุ่ม Print ในส่วนของเมนูไฟล์ได้ เมื่อกดปุ่ม Print จะปรากฏหน้าจอ ดังรูป



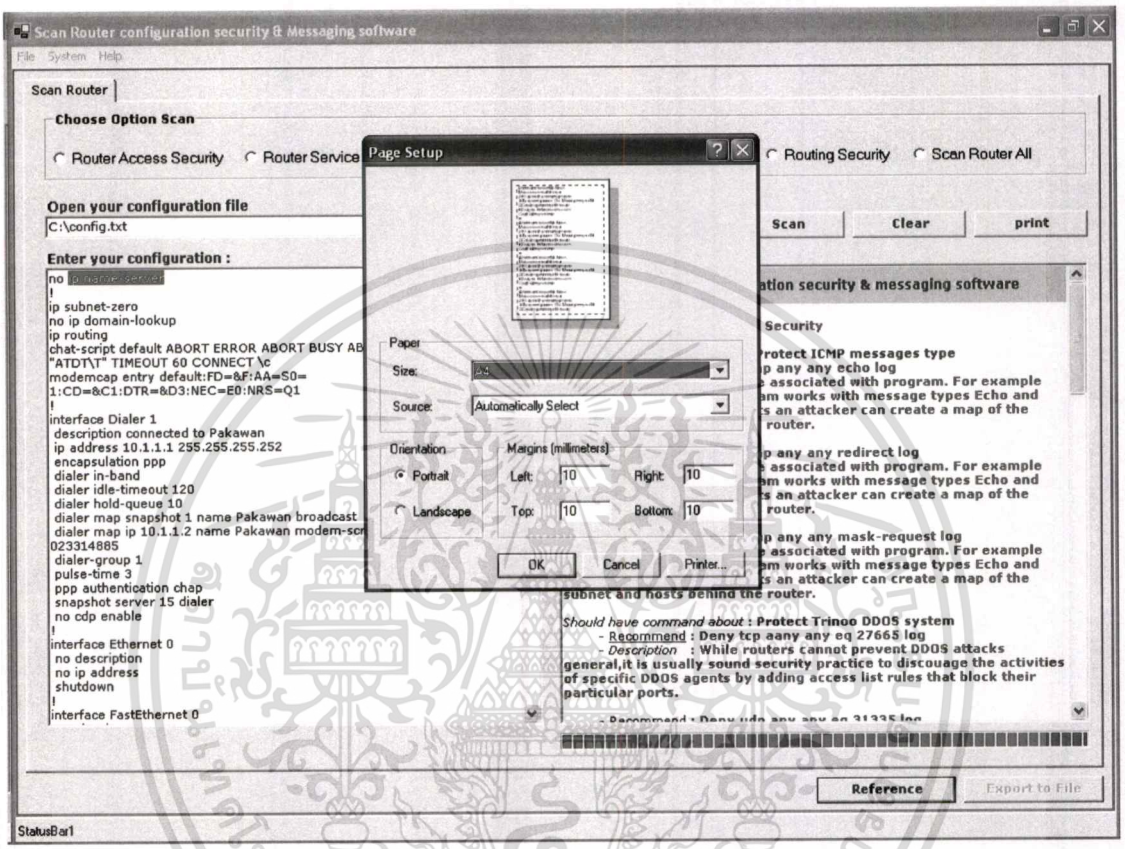
รูปที่ 4.10 หน้าจอเมื่อทำการสั่งพิมพ์ผลลัพธ์ออกทางเครื่องพิมพ์

โปรแกรมสามารถทำการดูภาพก่อนพิมพ์ก่อนการสั่งพิมพ์ไปยังเครื่องพิมพ์ได้ โดยการกดปุ่ม Print Preview ในส่วนของเมนูไฟล์ได้ เมื่อกดปุ่ม Print Preview จะปรากฏหน้าจอ ดังรูป



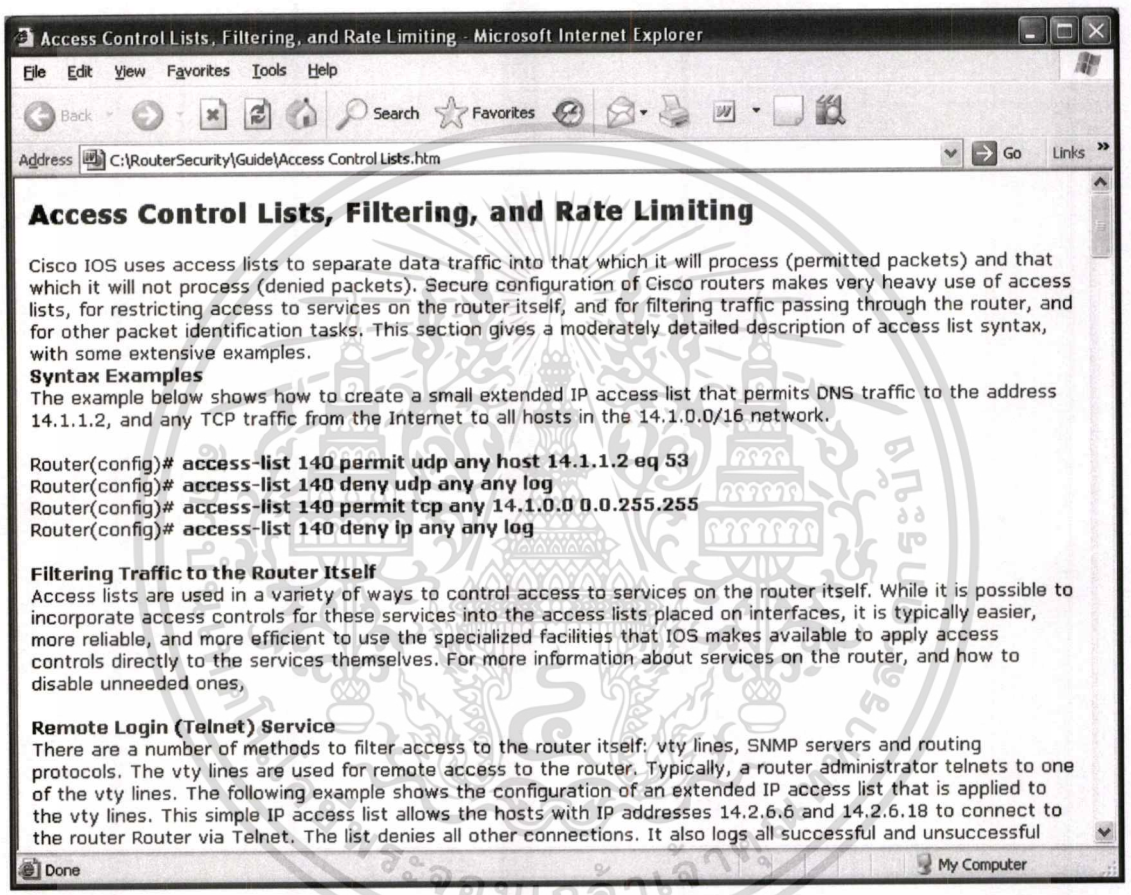
รูปที่ 4.11 หน้าจอเมื่อทำการดูภาพก่อนพิมพ์ผลลัพธ์ออกทางเครื่องพิมพ์

โปรแกรมสามารถทำการเซ็ตค่ากระดาษก่อนส่งพิมพ์ทางเครื่องพิมพ์ได้ โดยการกดปุ่ม Print setting ในส่วนของเมนูไฟล์ได้ เมื่อกดปุ่ม Print setting จะปรากฏหน้าจอ ดังรูป



รูปที่ 4.12 หน้าจอเมื่อทำการเซ็ตค่ากระดาษก่อนส่งพิมพ์ทางเครื่องพิมพ์

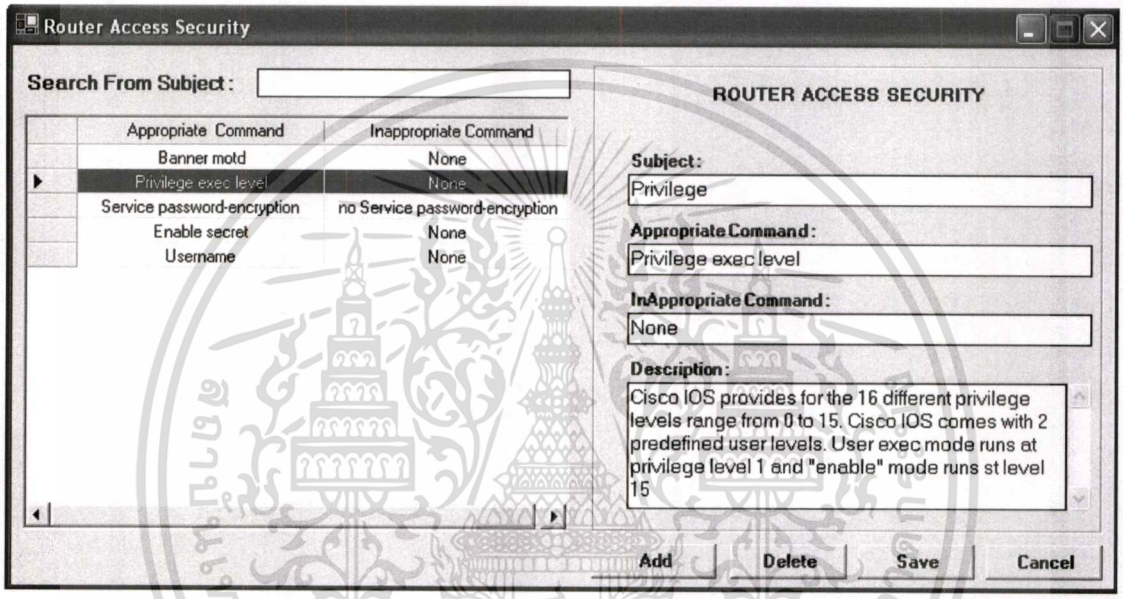
ผู้ใช้สามารถดูคำแนะนำวิธีการคอนฟิกูเรชั่นอุปกรณ์เราเตอร์ในหัวข้อต่างๆ ที่ใช้ในการตรวจสอบได้โดยการกดปุ่ม **Reference** หรือกดปุ่ม Reference บนเมนู Help หรือผู้ใช้สามารถดูคำแนะนำวิธีการคอนฟิกูเรชั่นอุปกรณ์เราเตอร์ในทุกหัวข้อ ที่ใช้ในการตรวจสอบได้โดยการกดปุ่ม Help on Help บนเมนู Help ดังรูป



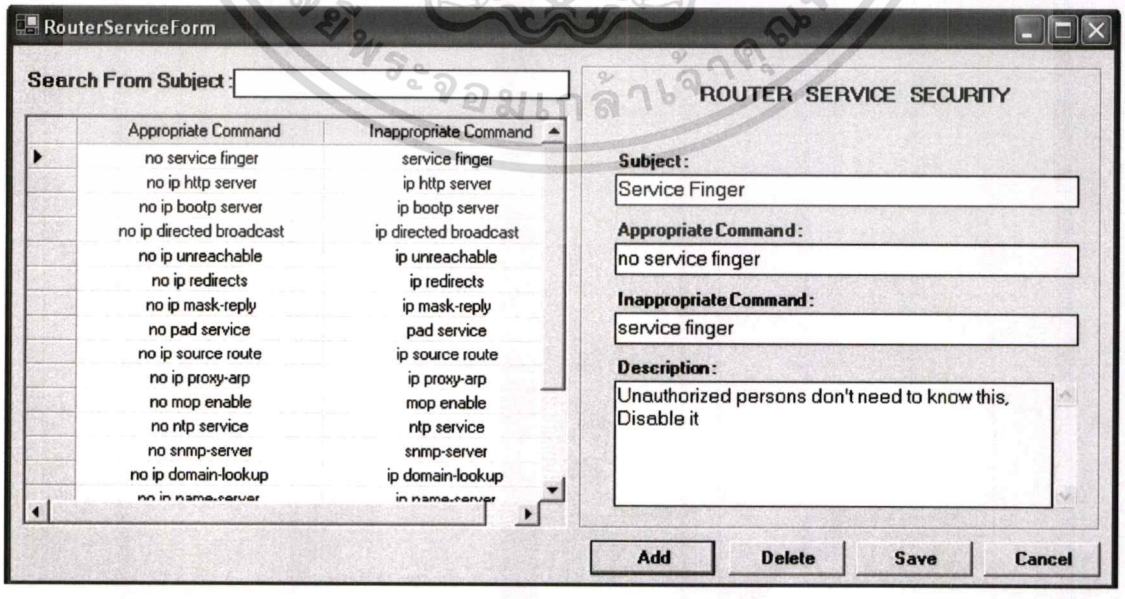
รูปที่ 4.13 หน้าจอเมื่อทำการกดปุ่ม Reference

4.2 การพัฒนาโปรแกรมส่วนที่จัดเก็บคำสั่งพื้นฐานที่ควรมีการคอนฟิกูเรชั่น

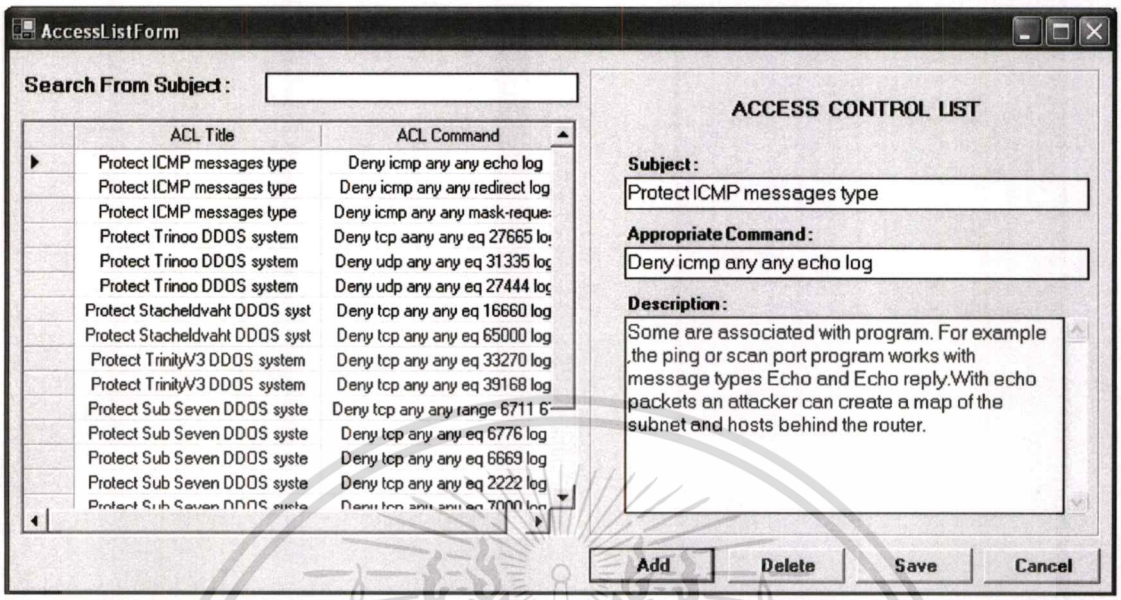
ในการพัฒนาโปรแกรมในส่วนนี้ จะเป็นส่วนของการจัดการเกี่ยวกับการจัดเก็บ แก้ไข และลบข้อมูลคำสั่งที่เหมาะสมเพื่อใช้สำหรับการตรวจสอบวิธีการคอนฟิกูเรชั่นของอุปกรณ์เราเตอร์ว่ามีการคอนฟิกูเรชั่นที่เหมาะสมหรือไม่ ซึ่งในส่วนนี้จะประกอบไปด้วยหน้าจอที่เกี่ยวข้องทั้งหมด 5 ส่วน ซึ่งสามารถแสดงหน้าจอการเพิ่ม, แก้ไข และลบข้อมูลของส่วนต่างๆ ได้ดังรูปที่ 4.14 – 4.18



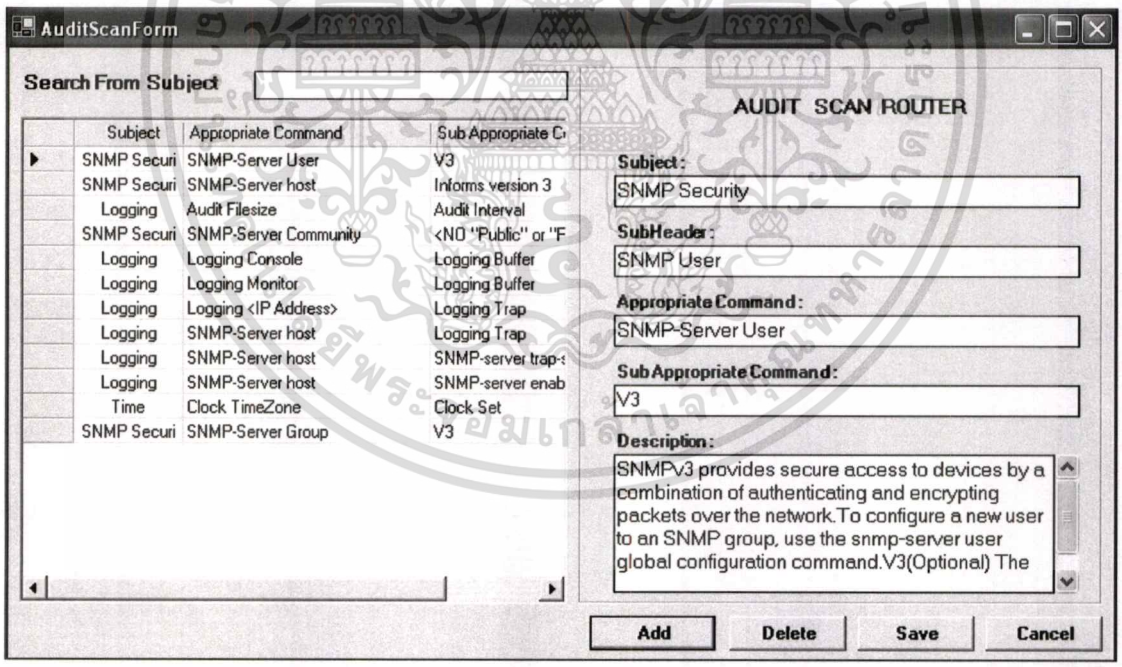
รูปที่ 4.14 หน้าจอการเพิ่ม – ลบ – แก้ไข ข้อมูล Router Access Security



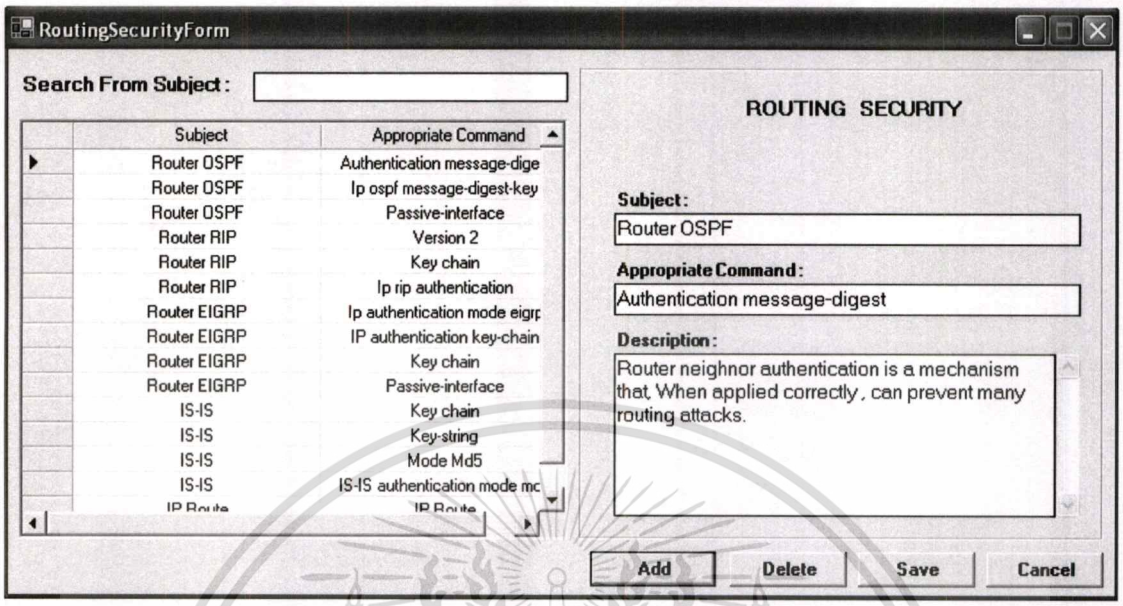
รูปที่ 4.15 หน้าจอการเพิ่ม – ลบ – แก้ไข ข้อมูล Router Service Security



รูปที่ 4.16 หน้าจอการเพิ่ม – ลบ – แก้ไข ข้อมูล Access Control List



รูปที่ 4.17 หน้าจอการเพิ่ม – ลบ – แก้ไข ข้อมูล Audit Scan Router



รูปที่ 4.18 หน้าจอการเพิ่ม – ลบ – แก้ไข ข้อมูล Routing Security

ซึ่งลักษณะการทำงานของหน้าจอในส่วนนี้จะมีลักษณะการทำงานที่เหมือนกัน แต่ลักษณะของการเก็บข้อมูลจะต่างกันออกไปในแต่ละหัวข้อ

บทที่ 5

บทสรุปและข้อเสนอแนะ

5.1 บทสรุป

ระบบการตรวจสอบช่องโหว่ของการคอนฟิกูเรชั่นบนอุปกรณ์เราเตอร์ ช่วยทำให้อุปกรณ์เราเตอร์และระบบเครือข่ายโดยรวมเกิดความปลอดภัยเพิ่มขึ้น โดยระบบนี้สามารถแยกลำดับของสิ่งที่ก่อให้เกิดช่องโหว่ออกเป็น 5 ลำดับได้ดังนี้

1. การเข้าถึงอุปกรณ์ Router
2. การให้บริการบนอุปกรณ์ Router จำพวก TCP และ UDP Port ต่างๆ
3. การกำหนดสิทธิในการใช้งานผ่าน ตัวอุปกรณ์ Router จำพวก Access Control List, DDOS, Virus, Worm, Trojan
4. การตรวจสอบสิ่งที่เกิดขึ้นบนอุปกรณ์ Router จาก Log
5. การตรวจสอบ Routing Protocol

ในการพัฒนาระบบนั้นได้ใช้ Visual Studio.NET 2003 เป็น Tools ที่ใช้ในการเขียนโปรแกรม และโปรแกรมที่ช่วยทางด้านจัดการฐานข้อมูลคือ Microsoft Access 2003 เนื่องจากว่าข้อมูลของระบบมีขนาดเล็ก ส่วน Visual Studio.NET 2003 เป็น Tools ที่ใช้กันอย่างแพร่หลาย ทำให้การศึกษาและการพัฒนาระบบสามารถทำความเข้าใจได้ง่ายและสะดวก

5.2 ข้อเสนอแนะ

1. ระบบที่พัฒนาขึ้นนั้นยังไม่สามารถใช้กับอุปกรณ์เราเตอร์ของผู้ผลิตอื่นได้นอกจาก Router Cisco
2. ระบบที่พัฒนาขึ้นนั้นยังไม่สามารถใช้งานร่วมกับ Protocol SNMP ในการ Load Configuration ได้ ซึ่งต้องอ่านไฟล์คอนฟิกูเรชั่นจากไฟล์เอกสาร (.txt, .doc, rtf) เท่านั้น
3. ระบบไม่สามารถทำการตรวจสอบคอนฟิกูเรชั่นว่าถูกหรือผิด แต่จะทำการตรวจสอบเฉพาะคอนฟิกูเรชั่นที่จะก่อให้เกิดช่องโหว่เท่านั้น
4. ระบบที่พัฒนาขึ้นนั้นยังไม่สามารถใช้กับ IOS Cisco ครบทุกเวอร์ชั่น

บรรณานุกรม

มนัชยา ชมธวัช. 2544. **คำแนะนำในการปรับแต่งค่าความปลอดภัยของ Router.** [Online] Available:http://www.thaicert.nectec.or.th/paper/RouterSec_Config.htm.

ศุภามน วาณิชย์ก่อกุล และคณะ. 2548. **ความรู้พื้นฐานเกี่ยวกับ Port scanning และวิธีการป้องกัน.** [Online] Available:http://www.thaicert.nectec.or.th/paper/portscanning.htm.

สมันต์ภูมิ ปฐมภัททพันธุ์ และ พุธ นาฑีสุวรรณ. 2548. **Checklist สำหรับบริหารจัดการเราเตอร์.** [Online] Available:http://www.thaicert.nectec.or.th/paper/checklist.htm.

ITWizard. 2548. **การคอนฟิกเราเตอร์ขั้นพื้นฐาน.** [Online] Available:http://www.itwizard.info/technology/router/basic_cisco_router_conf.htm.

System and Network Attack Center. 2003. **Router Security Configuration Guide.** United States of America: National Security Agency.

ประวัติผู้เขียน

ชื่อผู้เขียน นายธนะพันธ์ เกตุอ่ำ

วันเดือนปีเกิด 2 มิถุนายน 2520

ประวัติการศึกษา ปริญญาตรี วทบ. วิทยาการคอมพิวเตอร์
สถาบันเทคโนโลยีพระจอมเกล้าพระนครเหนือ
ปีที่สำเร็จการศึกษา 2541

ประวัติการทำงาน ปี 2541 - 2546
บริษัทซิสเท็มแอดไวเซอร์กรุ๊ป จำกัด
ตำแหน่ง Network System Engineer
ปี 2547 - ปัจจุบัน
บริษัทหลักทรัพย์ไทยพาณิชย์ จำกัด
ตำแหน่ง Network Security