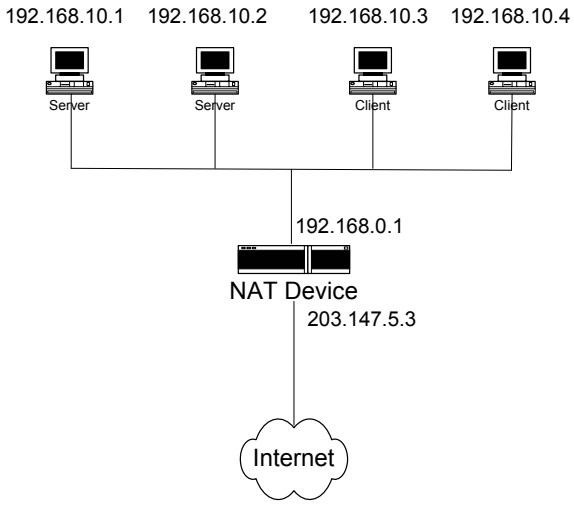
ทำความรู้จักกับแน็ท (NAT)

การเชื่อมต่ออินเตอร์เน็ตอย่างปลอดภัยและประหยัด

น.อ.ภาณุฤทธิ์ ยุกตะทัต
รองผู้อำนวยการ กองวิชาวิศวกรรมเครื่องกลเรือ ฝ่ายศึกษา โรงเรียนนายเรือ

ในอดีตการเชื่อมต่อกับอินเตอร์เนตเป็นเรื่องที่ยุ่งยาก ผู้ใช้จะต้องจ่ายค่าเช่าใช้ไอพีแอดเดรส (IP address) ให้กับผู้ให้บริการอินเตอร์เนต หรือ ไอเอสพี (Internet Service Provider) ด้วยค่าใช้จ่ายที่ยังมองไม่เห็นความคุ้มค่า อีกทั้งยังต้องเสี่ยงต่อภัยคุกคามจากผู้ไม่หวังดี ยุ่งยากต่อการรักษาความปลอดภัยข้อมูล แต่ในปัจจุบันเทคโนโลยีอินเตอร์เนตได้ล้ำหน้ากว่าที่คิด จากเดิมที่มีการนำเครื่องคอมพิวเตอร์เพียงเครื่องเดียวต่อโมเด็มเข้ากับอินเตอร์เนต กลายมาเป็นการนำเอาระบบเครือข่ายทั้งระบบไปเชื่อมต่อกับอินเตอร์เนตแทน มีการพัฒนาวิธีการซ่อนไอพีแอดเดรสของคอมพิวเตอร์ที่อยู่ภายในเครือข่าย (inside IP address) ทำให้คอมพิวเตอร์ ในอินเตอร์เนตไม่สามารถมองเห็นได้ เมื่อมองไม่เห็นก็ไม่สามารถทำอะไรคอมพิวเตอร์ที่อยู่ในเครือข่ายภายใน ได้ วิธีการเช่นนี้ได้รับความนิยมมากในช่วง ๒-๓ ปีที่ผ่านมา วิธีการนี้บนระบบปฏิบัติการลีนุกซ์ เรียกว่า IP Masquerading ซึ่งโดยทั่วไปจะเรียกว่า “แน็ท” Network Address Translation (NAT) ดังแสดงตามรูปที่ ๑



รูปที่ ๑ แสดงการวางตำแหน่งของ NAT Device ระหว่างเครือข่ายภายในกับภายนอก

NAT คืออะไร ?

Network Address Translation (NAT) เป็นมาตรฐานหนึ่งของ RFC ถูกเขียนขึ้นในปี ค.ศ.๑๙๙๔ เป็นวิธีการหนึ่งในการแปลงและแปลไอพีแอดเดรส (IP address) ของเครื่องคอมพิวเตอร์ในระบบเครือข่ายภายใน ซึ่งในที่นี้จะเรียกว่า ไอพีส่วนตัว (private IP address หรือ inside IP address) ให้เป็นไอพีแอดเดรสซึ่งเป็นที่ยอมรับและสื่อสารบนอินเตอร์เนต ซึ่งเรียกว่า ไอพีสาธารณะ (public IP address หรือ outside IP address) โดยมี NAT device ทำหน้าที่ในการแปลงไอพี จึงทำให้สามารถใช้ไอพีแอดเดรสที่ตั้งขึ้นมาเองได้ (เป็นไอพีแอดเดรสที่ไม่ต้องจดทะเบียนบนอินเตอร์เนตจึงไม่มีค่าใช้จ่าย) เพียงแต่ใช้ไอพีแอดเดรสที่ผู้ให้บริการอินเตอร์เนตให้มาก็เพียงพอสำหรับการเชื่อมต่ออินเตอร์เน็ตของคอมพิวเตอร์หลาย ๆ เครื่องในระบบเครือข่าย อีกทั้งยังสามารถซ่อนไอพีแอดเดรสของคอมพิวเตอร์ที่อยู่ภายในเครือข่าย (ไอพีแอดเดรสที่กำหนดขึ้นมาเอง) ได้ ทำให้มีความปลอดภัย รวมทั้งไม่จำเป็นต้องอ้างแอดเดรสเลขหมายซ้ำ ๆ อีก เมื่อต้องการติดต่อกับอินเตอร์เนต หรือเครือข่ายขององค์กรอื่น

NAT มีขั้นตอนการทำงานอย่างไร ?

เมื่อ NAT เริ่มทำงาน มันจะสร้างตารางภายในซึ่งมีไว้สำหรับบรรจุข้อมูลไอพีแอดเดรสของเครื่องคอมพิวเตอร์ในเครือข่ายภายในที่ส่ง packet ข้อมูล ผ่าน NAT device และจากนั้นมันก็จะสร้างตารางไว้สำหรับเก็บข้อมูลหมายเลขพอร์ต (port number) ที่ถูกใช้ไปโดย outside IP address (ในที่นี้สมมุติว่า คือ ๒๐๓.๑๔๗.๕.๓) และเมื่อมีการส่ง packet จากเครือข่ายภายในไปยังเครือข่ายภายนอก NAT device จะมีกระบวนการทำงานดังต่อไปนี้:

๑. NAT จะบันทึกข้อมูล source IP address และ source port number ไว้ในตารางที่เกี่ยวข้อง
๒. NAT จะแทนที่ IP ของ packet ด้วย IP ขาออกของ NAT device เอง (ในที่นี้คือ ๒๐๓.๑๔๗.๕.๓)
๓. NAT จะ assign หมายเลขพอร์ตใหม่ให้กับ packet และบันทึกค่าพอร์ตนี้ไว้ในตาราง และกำหนดค่านี้ลงไปใน source port number ของ packet นั้น
๔. จากนั้นจะคำนวณหา IP, TCP checksum อีกครั้งเพื่อตรวจสอบความถูกต้อง
๕. และเมื่อ NAT device ได้รับ packet ย้อนกลับมาจาก external network มันจะตรวจสอบ destination port number ของ packet นั้นๆ แล้วนำมาเปรียบเทียบกับข้อมูล source port number ในตารางที่บรรจุข้อมูลไว้ ถ้าเจอข้อมูลที่ตรงกันมันก็จะเขียนทับ destination port

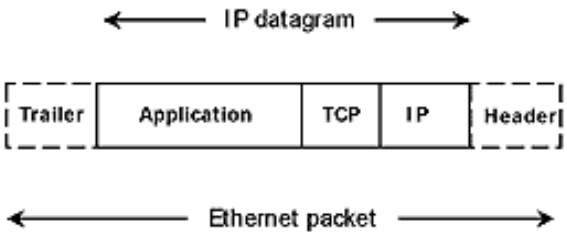
number, destination IP address ของ packet นั้นๆ แล้วจึงส่ง packet นั้นไปยังเครื่องซึ่งอยู่ภายในเครือข่ายภายในที่เป็นผู้สร้าง packet นี้ขึ้นมาในครั้งแรก

จากที่กล่าวมาแล้วจะเห็นได้ว่า NAT ทำหน้าที่แปลไอพีแอดเดรสของเครื่องต้นทางและเครื่องปลายทางขึ้นอยู่กับทิศทางของ Traffic ในการที่จะแปลงไอพีแอดเดรสนั้น NAT จะต้องตรวจสอบที่ช่องไอพีแอดเดรสของ packet ซึ่ง Packet ในที่นี้ เราเรียกว่า IP Datagram โดยที่ IP Datagram เป็นรูปแบบของข่าวสาร ที่ใช้ห่อหุ้มข้อมูลและ Protocol ในระดับสูงที่ใช้จัดการกับขนถ่ายข้อมูล อย่างเช่น TCP โดยให้บริการขนถ่ายข้อมูลจาก User File จาก Web Page หรือข่าวสาร E-mail เป็นต้น

IP Header

เมื่อคอมพิวเตอร์ได้สร้าง TCP/IP หรือ UDP Traffic ขึ้น เครื่องที่จะส่งข้อมูลจะต้องอาศัย Protocol เพื่อการสร้าง IP Header ขึ้น โดย IP Header จะหุ้มห่อ TCP Header รวมทั้ง Protocol อื่น ๆ รวมทั้งข้อมูลจากระดับชั้น Application ใน OSI Model (เช่น HTTP หรือ FTP เป็นต้น) เพื่อประกอบขึ้นมาเป็น packet ชิ้นหนึ่ง

หน้าที่หลักของ IP Header ในตัว packet ได้แก่ การแสดงแอดเดรสของผู้รับและผู้ส่งของ packet รวมทั้ง ข่าวสารที่แสดงขนาดของ Header และค่าที่ใช้แสดงสถานะของ IP Packet ซึ่งเปรียบได้กับ พัสดุไปรษณีย์ ที่จะต้องจ่าหน้าซองถึงผู้รับและส่ง ขนาดน้ำหนัก ชนิดของบริการขนส่ง (เปรียบได้กับชนิดของ Protocol ที่ใช้) และอื่นๆ ข้อมูลข่าวสารที่อยู่ภายใน IP Header นี้ NAT จำเป็นต้องนำมาใช้เพื่อการแปลไอพีแอดเดรส

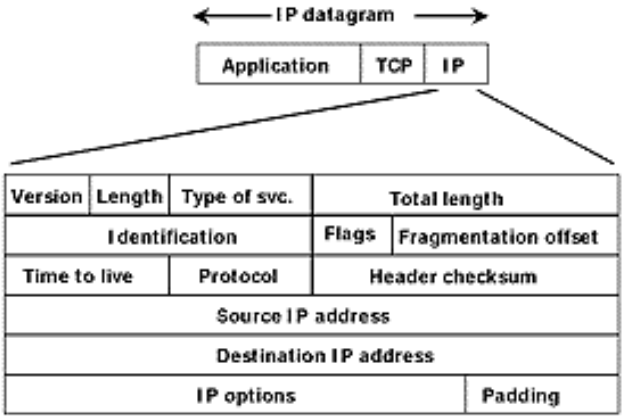


รูปที่ ๒ แสดงลักษณะของ IP Packet

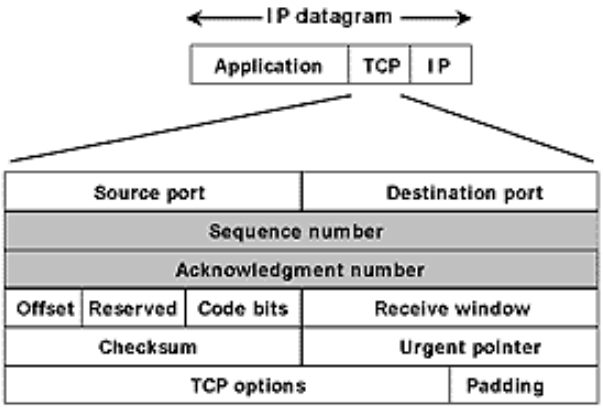
TCP Header

TCP Header ก็เป็นอีกจุดหนึ่งที่ NAT อาศัยข้อมูลภายในของมันเพื่อการจัดส่ง Packet เข้า ๆ ออกผ่าน NAT หน้าที่หลักของ TCP Header ได้แก่ การจัดการเพื่อให้แน่ใจว่าข้อมูลข่าวสารมีการรับส่งที่น่าเชื่อถือได้ นอกจากนี้ยังใช้เพื่อการควบคุมการไหลของข้อมูลข่าวสารระหว่างผู้รับและผู้ส่ง รวมทั้งมีระบบตรวจสอบความถูกต้องของ Header

จากภาพที่ ๔ จะเห็น ช่อง TCP Source Port และ TCP Destination Port ซึ่งมีไว้เพื่อเชื่อมต่อ Application Protocol กับข้อมูลเข้ากับไอพีแอดเดรสบนคอมพิวเตอร์ผู้รับและผู้ส่ง ซึ่งช่องต่าง ๆ เหล่านี้อาจต้องถูกปรับแต่งแก้ไขโดย NAT



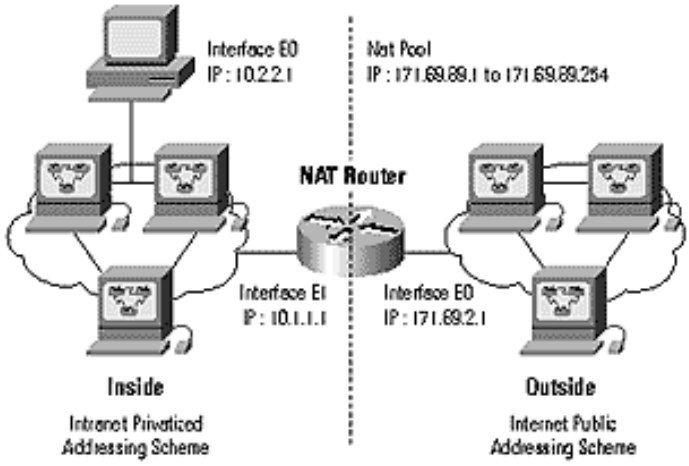
รูปที่ ๓ แสดงลักษณะของ IP Header



รูปที่ ๔ แสดงลักษณะของ TCP Header

การทำงานของ NAT

NAT เป็นระบบการอินเตอร์เฟซกับอินเตอร์เนต ที่ไม่ขึ้นอยู่กับ Protocol และ Application รวมทั้งอุปกรณ์ Hardware ใดๆ ซึ่งหมายความว่า NAT สามารถถูกนำมาประยุกต์ใช้งานกับ Router หรือคอมพิวเตอร์ที่ทำหน้าที่เป็น Router ใดๆ ที่มีลักษณะการเชื่อมต่อ โดยมีด้านหนึ่งสำหรับเครือข่ายภายในและอีกด้านหนึ่งกับเครือข่ายภายนอก ดังเช่น อินเตอร์เนต ตัวอย่างการเชื่อมต่อ เช่น การติดตั้ง NAT ที่ Border Router ซึ่งเป็น Router ที่เชื่อมต่อเครือข่ายย่อย ๆ ต่าง ๆ ภายในองค์กรกับเครือข่ายภายนอก ดูรูปที่ ๕



รูปที่ ๕ แสดงลักษณะการเชื่อมต่อของ NAT Router

NAT สามารถทำงานได้ในรูปแบบ ๒ ทาง หรือการเชื่อมต่อสื่อสารทั้งในแบบ Inbound และ outbound หมายความว่า สามารถจัดการกับไอพีแอดเดรสที่วิ่งเข้ามา หรือ ไอพีแอดเดรสที่วิ่งออกไป โดยสามารถจัดการกับไอพีแอดเดรสต้นทางและปลายทางได้เป็นอย่างดี NAT สามารถทำงานในสถานการณ์ ๓ ประการ ดังนี้

- ทำหน้าที่แปลงและแปล ไอพีแอดเดรส ต้นทางที่มาจากเครือข่ายภายใน
- ทำหน้าที่แปลงและแปล ไอพีแอดเดรส ต้นทางที่มาจากเครือข่ายภายนอก เช่น อินเตอร์เนต เป็นต้น
- ทำหน้าที่แปลงและแปล ไอพีแอดเดรส ปลายทางภายในเครือข่าย

แม้ว่า NAT สามารถใช้กับไอพีแอดเดรสภายนอกก็ตาม แต่โดยทั่วไป NAT มีไว้เพื่อการแปลไอพีแอดเดรสภายในเครือข่าย โดยมีจุดประสงค์ก็เพื่อที่จะซ่อนไอพีแอดเดรสภายในเครือข่าย และ/หรือ การแปลไอพีแอดเดรสที่ไม่ได้จดทะเบียนถูกต้อง (หรือไอพีแอดเดรสส่วนตัว) ไปใช้เป็นไอพีแอดเดรสที่จดทะเบียนถูกต้อง (หรือไอพีแอดเดรสสาธารณะ) สามารถวิ่งไปตามเส้นทางบนอินเตอร์เนตได้

การทำงานของ Port Address Translation หรือ PAT

Port แอดเดรส Translation (PAT) เป็น Option เพิ่มเติมที่เกี่ยวกับการทำงานของ NAT ซึ่งจัดเป็นชุดการทำงานรองของ NAT หน้าที่ของ PAT ได้แก่ การแปลไอพีแอดเดรสให้เป็น PAT ไอพีแอดเดรสเพียงชุดเดียว ซึ่ง PAT ให้การสนับสนุนการทำงานบนโปรโตคอล UDP และ TCP เท่านั้น

ภายใน PAT ประกอบด้วยตารางไอพีแอดเดรส ซึ่งภายในจะมีไอพีแอดเดรสที่ผ่านการจดทะเบียนถูกต้องแล้วอยู่ ๑ แอดเดรส โดย ไอพีแอดเดรสต้นทางที่อยู่ในเครือข่ายภายในจะถูกจัด Map เข้าไปไว้ภายใน PAT ไอพีแอดเดรสแห่งนี้ การทำงานในส่วนนี้ของ PAT จะคล้ายกันกับการทำงานของ NAT จะต่างกันก็ตรงที่ PAT จะใช้เพียงแค่ ๑ ไอพีแอดเดรส เท่านั้น การที่เรียกว่า PAT ก็เนื่องจากมีการทำงานในลักษณะแลกเปลี่ยน (Swapped) ไอพีแอดเดรสไปมาของ PAT โดยหมายเลข Port ที่เกี่ยวข้องกับการเชื่อมต่อในแต่ละครั้ง จะถูกแปลไปเป็นเลขหมาย Port ที่ต่างกัน ค่าจากการเปลี่ยนแปลงนี้จะถูกเก็บรักษาไว้ที่ตาราง PAT เพื่อใช้พิสูจน์ว่าข้อมูลที่ได้จากเครือข่ายภายในจะส่งออกไปให้ใครบ้างที่เคยขอจากเครือข่ายภายนอก โดยไม่เกิดการสับสนและผิดพลาด

ข้อดีของ Outbound Mode NAT เมื่อเปรียบเทียบกับ Firewall

อันตรายของอินเทอร์เน็ตในปัจจุบันนี้ก็คือ เมื่อเราเชื่อมต่อเข้ากับอินเทอร์เน็ตโอกาสที่เครื่องของเราจะถูก scan หรือ probe มีโอกาสสูงมาก เพราะ hackers, crackers หรือ script kiddies ต่างก็จ้องที่จะฉกฉวยข้อมูลไปจากเครื่องของเราตลอดเวลา

บริษัทต่าง ๆ มักจะใช้ไฟร์วอลล์เป็นตัวป้องกันอันตรายจากอินเทอร์เน็ต ไฟร์วอลล์เป็นอุปกรณ์ที่พิจารณา network traffic โดยจะดูในส่วนของ destination IP, source IP, destination port number, source port number หรือข้อมูล header อื่น ๆ ว่าจะให้ผ่านหรือไม่ให้ผ่านตัวไฟร์วอลล์ไป ข้อเสียของไฟร์วอลล์ก็คือความยากในการเขียนสคริปต์ rule และการบำรุงรักษา เพราะต้องใช้ความรู้เรื่องเครือข่ายเยอะพอสมควร และการบำรุงรักษานั้นถือเป็นเรื่องที่มีความสำคัญเพราะไฟร์วอลล์ที่มี rule set ที่ซับซ้อนและ

ยุ่งยากมากอาจจะมีช่องโหว่ที่ไม่รู้ตัวก็เป็นได้ ซึ่งอันนี้ก็จำเป็นต้องอาศัยผู้ที่มีประสบการณ์ด้านบำรุงรักษาระบบเครือข่ายในการดูแล

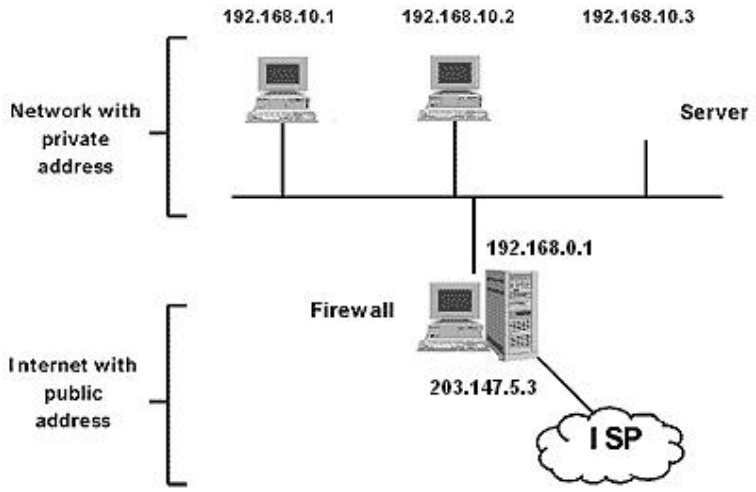
NAT สามารถทำงานได้ในระดับเดียวกันกับไฟร์วอลล์แต่จะช่วยลดค่าใช้จ่ายและไม่ต้องการความรู้ด้านเทคนิคมากมายนัก ทั้งนี้เนื่องจาก NAT สามารถซ่อน internal network IP address จากเครือข่ายภายนอกไว้ได้ ซึ่งผู้ที่อยู่ภายนอกจะมองเห็นแค่เพียง outside IP address ของ NAT device เท่านั้น ดังนั้นโอกาสในการ broadcast หรือ hack หรือ spoof จึงแทบไม่มีโอกาสเป็นไปได้

ข้อดีอีกอย่างหนึ่งของ NAT คือทำให้ลดภาระของผู้ดูแลระบบลง จากเดิมที่ต้องดูแลทั้ง NAT device และเครื่องต่างๆ ในเครือข่ายภายใน การใช้ NAT ทำให้ผู้ดูแลระบบให้ความสนใจเพียง NAT device เพียงเท่านั้น ซึ่งทำให้ผู้ที่อยู่ภายนอกไม่สามารถส่ง packet เข้ามาได้ ถ้าไม่มีการเริ่มส่งจากเครือข่ายภายในก่อน และทุก packet จะต้องส่งผ่าน NAT device เสมอ

ชนิดของ NAT

๑. Static NAT

Static NAT เป็นการแปลไอพีแอดเดรสชนิดกำหนดค่าแอดเดรสตายตัว จากเครือข่ายภายในไปยังเครือข่ายภายนอก ส่วนแอดเดรสภายนอกจะไม่มีการเปลี่ยนแปลง ดังนั้นความสัมพันธ์ระหว่างไอพีแอดเดรสของเครือข่ายภายนอกและภายในจะเป็นแบบแน่นอนตายตัว

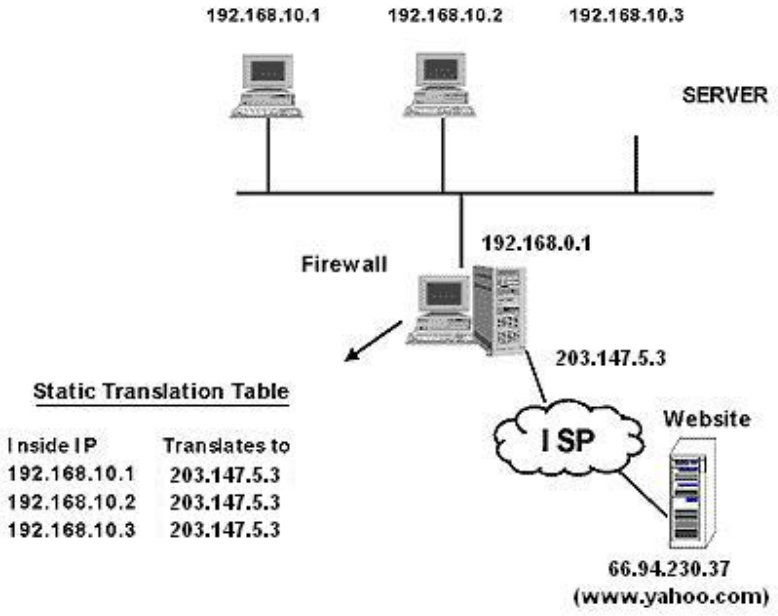


รูปที่ ๖ แสดง ไอพีแอดเดรส ของเครือข่ายภายในกับเครือข่ายภายนอก

จากรูปที่ ๖ จะเห็นว่าบรรดาเครื่องพีซีและเซิร์ฟเวอร์ต่าง ๆ ที่อยู่เครือข่ายภายใน จะใช้แอดเดรสส่วนตัว (private address) ของมันเอง รวมทั้งสามารถใช้แอดเดรสสาธารณะ (แอดเดรสที่จดทะเบียนถูกต้อง) ในการสื่อสารระหว่างกันเป็นการภายในได้ แต่ไม่ว่าจะใช้แอดเดรส อะไรก็ตาม หากต้องการติดต่อออกไปนอกเครือข่าย จะต้องผ่านการแปลแอดเดรสเสียก่อนที่จะออกจากเครือข่ายเสมอ

สมมุติว่า มีพีซีเครื่องหนึ่งซึ่งมีไอพีแอดเดรสภายในเบอร์ ๑๙๒.๑๖๘.๑๐.๑ ทำการส่งข่าวสารไปที่อินเตอร์เนต โดยอ้างแอดเดรสที่ ๖๖.๙๔.๒๓๐.๓๗ (www.yahoo.com) ซึ่งแอดเดรสนี้เป็นแอดเดรสบนอินเตอร์เนต ลักษณะนี้ packet ที่วิ่งออกจาก PC นั้นจะมี แอดเดรส ต้นทางเป็น ๑๙๒.๑๖๘.๑๐.๑ ในกรณีนี้เมื่อ packet วิ่งมาถึง NAT Router ก็จะถูกแปลงเป็น ๑๙๒.๑๖๘.๐.๑ ซึ่งเป็น ไอพีแอดเดรส ที่ผู้จัดการเครือข่ายได้กำหนดขึ้นให้สอดคล้องกับไอพีภายนอก (๒๐๓.๑๔๗.๕.๓) ลักษณะนี้จะเห็นได้ว่า แอดเดรสภายในจะสอดคล้องกับแอดเดรสภายนอกอย่างแน่นอนตายตัว และทุกครั้งที่ติดต่อออกไปที่ภายนอก ก็จะต้องใช้แอดเดรสเดิมเสมอ

และเมื่อมีการตอบกลับมาจากเว็บไซต์ที่อยู่บนอินเตอร์เนต ตัว NAT Router จะใช้กระบวนการย้อนกลับ โดย Router จะอ่านค่า แอดเดรสปลายทาง ที่อยู่บน packet ที่ส่งตรงมาจากเว็บไซต์ (๖๖.๙๔.๒๓๐.๓๗) จากนั้นก็จะทำการพิสูจน์เครื่องพีซีภายในที่เว็บไซต์นี้ต้องการติดต่อด้วย จากนั้นก็กำหนดไอพีแอดเดรสเพื่อติดต่อกับเครื่องพีซีนั้น ๆ ต่อไป (ดูรูปที่ ๗)



รูปที่ ๗ แสดง ลักษณะการอ้างแอดเดรส และ MAP แอดเดรส แบบ Static

ข้อดีและข้อเสียของการใช้ Static NAT

แม้ Static NAT จะเป็นระบบที่เรียบง่ายและตรงไปตรงมาก็ตาม แต่ก็มีจุดด้อยหลายประการ ที่ทำให้ Static NAT กลายเป็นระบบที่เหมาะสำหรับ เครือข่ายที่มีข้อจำกัดมากมาย แต่ไม่เหมาะกับเครือข่ายใหญ่ ด้วยเหตุผลหลายประการดังนี้

- ต้องการการดูแลอย่างมาก การ Map แอดเดรส โดยวิธีการของ Static Map นี้ จะไม่มีการเปลี่ยนแปลงเลขหมาย ไอพีแอดเดรส โดยอัตโนมัติ หากมีการเปลี่ยนแปลง แอดเดรส ภายในหรือภายนอกเกิดขึ้น เช่น หากต้องการเพิ่มหรือแก้ไข แอดเดรส ใดๆ แล้ว ผู้ดูแลเครือข่ายจะต้องเข้ามาจัดตั้งตารางการแปลแอดเดรส กันใหม่ และเป็นเรื่องน่าเสียดาย หากเกิดความผิดพลาดขณะที่มีการจัดตั้งตารางการแปลแอดเดรส
- มีการใช้งาน แอดเดรส อย่างมาก ในเครือข่ายขนาดใหญ่ การใช้ แอดเดรส ภายในและภายนอกแบบชนิดหนึ่งต่อหนึ่ง นี้ ทำให้กิน แอดเดรสภายนอกค่อนข้างมาก หากมีเครื่องคอมพิวเตอร์ภายในเครือข่ายเป็นจำนวนมาก เพราะต้องกำหนด ๑ เครื่องต่อหนึ่ง ไอพีแอดเดรส ที่ถูกต้อง
- มีการเลือกเส้นทางที่แน่นอนตายตัว ในกรณีที่มีการเชื่อมต่อกับอินเตอร์เนตแบบหลาย ๆ Connection เช่น เชื่อมต่อพร้อมกันหลาย ISP เมื่อมีการใช้ Static NAT เกิดขึ้น ระบบนี้จะเลือกเส้นทางที่แน่นอนตายตัว ตามที่ Static NAT กำหนดไว้

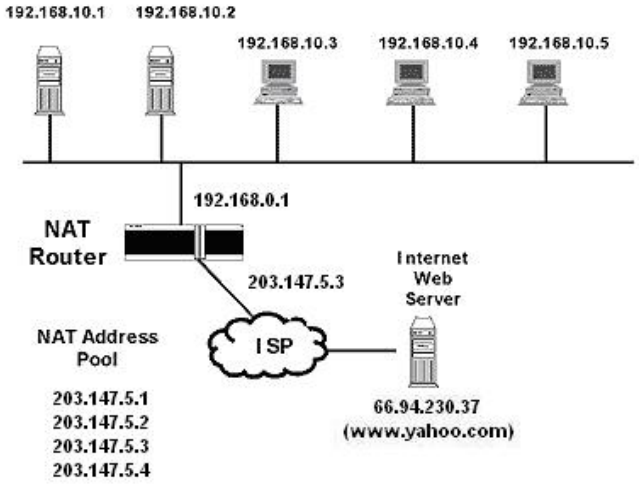
จุดด้อยของ Static NAT มิได้หมายความว่า ระบบนี้ไม่เหมาะสมกับเครือข่ายสมัยใหม่ในปัจจุบัน แต่ Static NAT เหมาะสำหรับระบบเครือข่ายขนาดเล็ก ต่อไปนี้ เป็นรายละเอียดที่แสดงถึงข้อดีของการใช้ Static NAT มีดังนี้

- จำกัดความต้องการใช้ NAT ภายในเครือข่ายที่ซึ่งมีการจำกัดจำนวนของ PC ที่ใช้ NAT ระบบ Static NAT ดูจะเป็นเครื่องมืออันทรงประสิทธิภาพที่จะควบคุมการ Access ไปที่ภายนอก หมายความว่า การจำกัดจำนวนคอมพิวเตอร์ที่จะออกไปที่อินเตอร์เนต ทำได้โดยการจำกัดไอพีแอดเดรส สำหรับที่จะออกไปที่ Internet เท่านั้นเอง สำหรับเครือข่ายใดที่ส่วนใหญ่มีการสื่อสารเฉพาะภายใน และมีบางครั้งที่มี Access ไปที่ภายนอกบ้าง เป็นจำนวนน้อย ระบบนี้ จึงเป็นระบบที่ดีกว่า
- การบริหารจัดการเครือข่าย ปัจจุบันมีระบบเครือข่ายอยู่มากมายที่ต้องการบริหารจัดการกับ Traffic ภายนอก เพื่อต้องการดูว่ามีคอมพิวเตอร์เครื่องใดบ้างที่ติดต่อกับภายนอก ทั้งนี้ก็เพื่อให้ง่ายต่อการตรวจสอบที่มาของปัญหา ว่ามาจากเครือข่ายภายในหรือภายนอก การใช้ Static NAT จะช่วยให้สามารถติดตามดูได้ว่า คอมพิวเตอร์แต่ละเครื่องมี Traffic ไปไหนมาไหนบ้าง

- สามารถเข้ากันได้กับ Application โดยทั่วไป มี Application บางตัวที่ฝัง ไอพีแอดเดรส ไว้ที่ช่องเก็บข้อมูลของ IP Datagram ซึ่งการทำเช่นนี้ จะทำให้ NAT โดยทั่วไปไม่สามารถสังเกตเห็น แอดเดรส ที่อยู่ในช่องนี้ ซึ่งหมายความว่า Application บางรายการไม่สามารถทำงานได้ตามปกติภายใต้ NAT แต่ Static NAT สามารถถูกจัด Configure ให้ทำงานร่วมกับ Application Level Gateway เพื่อตรวจสอบ IP Datagram ดังกล่าวได้

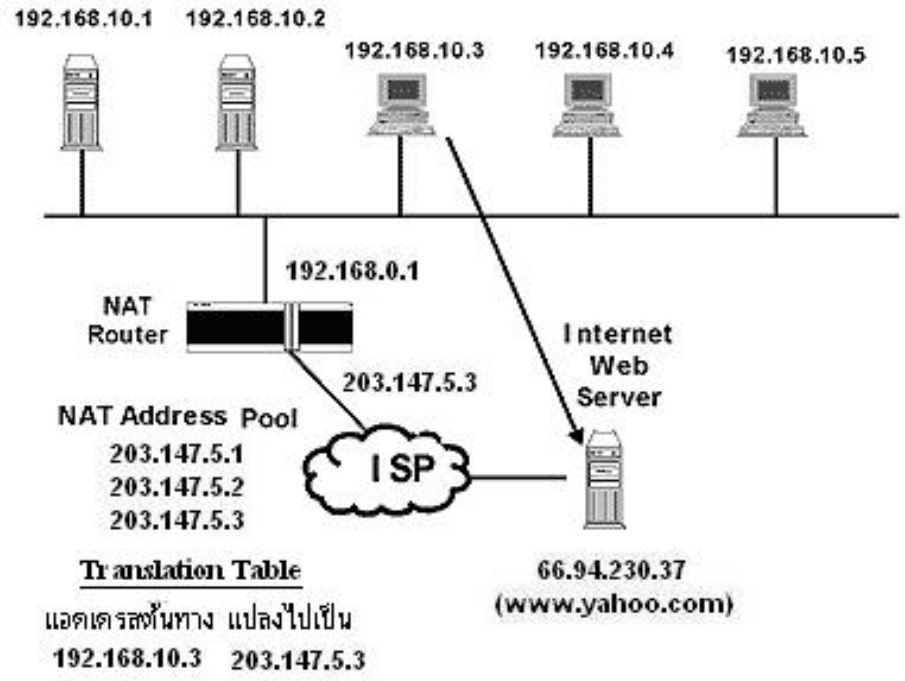
๒. Dynamic NAT

Dynamic NAT เป็นแบบตรงกันข้าม ที่มีการนำเอาไอพีแอดเดรสจากกลุ่มของไอพีแอดเดรสที่แชร์หรือร่วมใช้งานกัน หรือที่เรียกว่าแอดเดรส Pool มาทำการแปลจากแอดเดรส Pool ภายใน ให้เป็น Address Pool สำหรับเครือข่ายภายนอก หรือในทางกลับกัน รูปแบบนี้จะต้องได้รับการจัด Configure โดยผู้ดูแลระบบเครือข่าย แต่หลังจากที่จัด Configure เป็นที่เรียบร้อยแล้ว Router ที่สนับสนุน NAT จะเป็นผู้จ่ายไอพีแอดเดรสให้กับคอมพิวเตอร์อย่างเหมาะสม และเพื่อให้เกิดความรวดเร็วในการทำงาน ผู้บริหารจัดการเครือข่ายจะต้องทำการ Map ระยะของไอพีแอดเดรส หากเป็นไปได้ (ลักษณะนี้ คล้าย ๆ กับการทำงานของ DHCP Server ที่ไม่ได้กำหนดเครื่อง PC แต่ละเครื่องให้มีไอพีแอดเดรสที่ตายตัว โดยผู้จัดการเครือข่ายจะกำหนดแอดเดรสขึ้นมาจำนวนหนึ่ง เป็นระยะหรือช่วงของแอดเดรส อาทิเช่น ๒๐๓.๑๔๗.๕.๑ - ๒๐๓.๑๔๗.๕.๖๓ เป็นต้น) ดังนั้นใครที่เข้ามาที่เครือข่ายก่อน ก็จะได้รับแจกแอดเดรสไปใช้งานก่อน โดยเครื่องคอมพิวเตอร์ จะไม่ได้รับ IP ที่ซ้ำกัน ข้อแตกต่างกันระหว่าง NAT กับ DHCP Server ตรงที่ไอพีแอดเดรสของ NAT เป็นไอพีแอดเดรสที่ได้รับการจดทะเบียนแล้ว เพื่อแจกให้กับเครื่องคอมพิวเตอร์ที่เข้าๆ ออกๆ บนเครือข่าย ไปยังภายนอก (ดูรูปที่ ๘)



รูปที่ ๘ แสดงตัวอย่างการทำงานของ Dynamic NAT

หาก Static NAT เป็นส่วนที่เรียกว่าหัวในเหรียญบาท Dynamic NAT ก็จะถือได้ว่าเป็นส่วนก้อยของเหรียญ เช่นกัน ตรงที่ว่า Dynamic NAT มีการกำหนดแอดเดรสให้กับภายนอกแบบพลวัตร หมายความว่าแทนที่จะใช้ระบบกำหนดแอดเดรสภายในกับภายนอกแบบหนึ่งต่อหนึ่ง Dynamic NAT จะกำหนดว่าแอดเดรสที่ใช้จะเปลี่ยนแปลงไปเรื่อย ๆ และจะมีการเปลี่ยนแปลงทุกครั้งที่คอมพิวเตอร์ภายในเครือข่าย มีการสถาปนาการเชื่อมต่อกับคอมพิวเตอร์ภายนอกเครือข่าย หรืออาจมีการเปลี่ยนเป็นระยะ ๆ ก็เป็นได้ (ดูรูปที่ ๙)



รูปที่ ๙ แสดงการ Map แอดเดรส ของ PC เครื่องต่อไป ด้วย Dynamic NAT

ในเวลาเดียวกัน IP Datagram ที่มาจากคอมพิวเตอร์เครื่องที่สองบนเครือข่ายที่ส่งข่าวสารไปที่เครือข่ายภายนอก จะได้รับการปฏิบัติในทำนองเดียวกันโดย NAT Router ตัวอย่างเช่น NAT Router อาจแปลไอพีแอดเดรสต้นทางซึ่งอยู่ใน IP Header ที่ติดต่อออกไปเพื่อต้องการใช้งาน FTP Application จาก PC ที่ใช้ แอดเดรส ๑๙๒.๑๖๘.๑๐.๔ ไปที่แอดเดรสต่อไปใน NAT Address Pool ซึ่งประกอบด้วยแอดเดรสจำนวนหนึ่ง (เช่น ๒๐๓.๑๔๗.๕.๑ – ๒๐๓.๑๔๗.๕.๓) ซึ่งต่อมา NAT Router จะแปลแอดเดรส ๑๙๒.๑๖๘.๑๐.๔ ให้ เป็น ๒๐๓.๑๔๗.๕.๓ ส่วน PC อีกเครื่องหนึ่งคือ ๑๙๒.๑๖๘.๑๐.๕ จะได้รับการแปลเป็น ๒๐๓.๑๔๗.๕.๒ หากเครื่องพีซีทั้งสองต้องการติดต่อกับเครือข่ายภายนอก (ดูรูปที่ ๙)

เมื่อพีซีแต่ละเครื่องได้เสร็จสิ้นจากภารกิจในการสื่อสารข้อมูลกับเครือข่ายภายนอกแล้ว NAT Router ก็จะเรียกแอดเดรส ภายนอกคืนกลับเข้าไปที่ Address Pool เพื่อให้ผู้อื่นใช้ต่อไป

ความง่ายในการดูแลเครือข่ายที่ใช้ NAT

- เนื่องจากเราสามารถใช้ non-routable address ในเครือข่ายภายใน ซึ่งสามารถใช้ได้อย่างมากมาย จึงทำให้ลดค่าใช้จ่ายสำหรับ routable address ลงไปได้
- สามารถแบ่งเครือข่ายให้เล็กลงได้อย่างง่าย และการเพิ่มเข้า-ลดออกของเครื่องคอมพิวเตอร์ในเครือข่ายก็ไม่มีผลกระทบต่อระบบ
- NAT device รุ่นใหม่ ๆ สามารถทำหน้าที่เป็น DHCP server ได้ด้วย
- NAT device บางยี่ห้อ สามารถจำกัดการเข้าถึงอินเทอร์เน็ตได้ เช่น ให้ใช้เฉพาะ HTTP เท่านั้น
- มี traffic logging คือมีการบันทึกข้อมูลลงล็อกไฟล์ ทำให้สามารถตรวจสอบรายงานการใช้งานได้
- NAT device บางตัวสามารถทำ routing ได้ด้วย ซึ่งทำให้เราสามารถสร้างเครือข่ายที่เป็น sub-network ได้

NAT สามารถทำงานได้ในหลายโหมด (Mode)

เมื่อ NAT ทำงานใน outbound mode ทำให้ผู้ที่อยู่ภายนอกไม่สามารถส่ง packet เข้ามาได้ ถ้าไม่มีการเริ่มส่งจากเครือข่ายภายในก่อน การทำงานในลักษณะนี้ยังมีจุดอ่อนในเรื่องของความปลอดภัยดังต่อไปนี้ คือ

๑. ถ้า internal side user เรียกใช้เว็บที่มีโค้ดที่เป็นอันตราย (malicious code) เช่น IIS web server ที่ติดไวรัส Nimda หรือ malicious ActiveX code หรือ malicious Java code ซึ่งตัว NAT device เองจะไม่สามารถป้องกันอันตรายในลักษณะนี้ได้

๒. มีโปรแกรมบางตัวที่อยู่ในเครื่องของ internal side พยายามส่ง packet ออกไป external side เช่น ม้าโทรจัน ซึ่งในกรณีนี้ NAT ก็ไม่สามารถป้องกันได้เช่นเดียวกัน

๓. NAT ไม่ได้ปกป้องข้อมูลภายใน internal host เสมอไป เราสามารถตรวจสอบล็อกไฟล์ในบางเซิร์ฟเวอร์ (เช่น Windows Streaming Media Server) ซึ่งสามารถค้นพบว่า มีข้อมูลของ non-routable address และเวอร์ชั่นของระบบปฏิบัติการปรากฏอยู่

๔. มีความเป็นไปได้ที่จะมีการสร้าง IP packet ปลอม เพื่อหลอก NAT device ว่า packet นี้ถูกเริ่มสร้างจาก internal IP address จากนั้นตัว NAT device ก็จะ forward packet นี้ไปยัง internal network

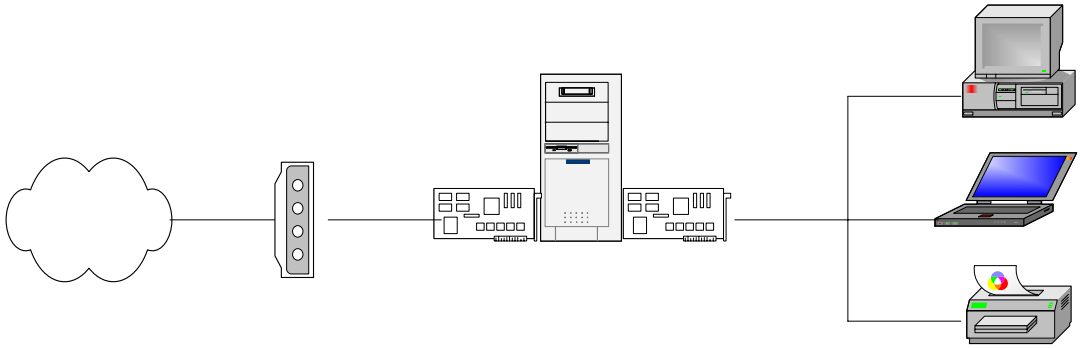
๕. และแน่นอนที่สุด NAT ไม่สามารถป้องกันไวรัสได้

เมื่อ NAT ทำงานใน bi-directional mode หรือ PAT mode ตัว NAT device จะมีตารางซึ่งใช้เก็บข้อมูลเพื่อ map external address, port ไปเป็น internal address, port ซึ่งในกรณีนี้จะอนุญาตให้เราเซ็ทอัพ internet IP address, port ได้ที่ external side ของ NAT device จากนั้นก็จะทำ statically map ไปยัง private address, port ซึ่งอยู่ที่ internal side ของ NAT device ยกตัวอย่างเช่น เราสามารถตั้งเว็บเซิร์ฟเวอร์ที่ internal side โดยมี IP address เป็น ๑๙๒.๑๖๘.๐.๒ ที่พอร์ต ๘๐ และมีค่า internet IP address เป็น ๒๐๓.๑๔๗.๕.๓ พอร์ต ๘๐ ที่ external side เมื่อมี request จากภายนอกเข้ามายัง external address ที่พอร์ต ๘๐ มันจะถูกส่งต่อไปยังพอร์ต ๘๐ ของ internal address และเมื่อมี request มาที่พอร์ตอื่นนอกเหนือจาก ๘๐ แล้ว ข้อมูลนั้นจะถูกทิ้งไป

คุณพร้อมหรือยังที่จะใช้ NAT

การที่เทคโนโลยี ADSL (Asymmetric Digital Subscriber Line) เริ่มเข้ามามีบทบาทเพิ่มมากขึ้น เนื่องจากมีข้อดีคือทำให้ผู้ใช้สามารถใช้สายโทรศัพท์ได้ในเวลาเดียวกับการเชื่อมต่อเครือข่ายอินเตอร์เน็ต และเริ่มมีการแข่งขันในเรื่องอินเตอร์เน็ตความเร็วสูงมากขึ้น ผู้ให้บริการอินเตอร์เน็ตต่างนำกลยุทธ์ การลด แลก แจก แถม ADSL Modem และนำเสนอการให้บริการต่างๆ ทำให้องค์กรที่ทำธุรกิจขนาดกลางและขนาดเล็ก (SME) มีทางเลือกในการประยุกต์ใช้ static NAT เพื่ออำนวยความสะดวกในการเชื่อมต่อเครือข่ายอินเตอร์เน็ต หรือแม้กระทั่งการใช้งานภายในบ้านเองก็ยากที่จะปฏิเสธความต้องการใช้ NAT บางบ้านอาจจะมีความจำเป็นที่จะต้องมีเครือข่ายขนาดเล็กภายในบ้าน (Home Networking) เพื่อรองรับการเชื่อมต่อเครือข่ายอินเตอร์เน็ตสำหรับเครื่องคอมพิวเตอร์ของคุณพ่อ คุณแม่ และคุณลูก หรือแม้ว่าระบบปฏิบัติการวินโดวส์ในปัจจุบันจะมีฟังก์ชันการใช้งานอินเตอร์เน็ตร่วมกัน (Internet Connection Sharing – ICS) เป็นตัวเลือกเสริมให้ติดตั้งสำหรับใช้งาน แต่การใช้ NAT ก็เป็นทางเลือกหนึ่งที่ไม่ควรมองข้าม เพราะสามารถจัดตั้งได้โดยง่าย สามารถเชื่อมต่ออินเตอร์เน็ตได้อย่างปลอดภัย และประหยัด โดยสามารถใช้เครื่องคอมพิวเตอร์เพียงเครื่องเดียวที่ทำหน้าที่เป็นได้ทั้ง NAT และ Firewall ซึ่ง

ใช้ LAN Card ๒ ชุด ทำหน้าที่แยกการเชื่อมต่อทางกายภาพของระบบเครือข่ายภายในบ้านออกจากเครือข่ายภายนอก ที่มีการเชื่อมต่ออินเตอร์เน็ตผ่าน ADSL Modem ระบบเครือข่ายในลักษณะดังกล่าวนี้มีโครงสร้างการเชื่อมต่ออย่างง่าย ดังแสดงตามรูปที่ ๑๐



รูปที่ ๑๐ การใช้ NAT กับระบบเครือข่ายภายในบ้าน

คำถามคือ NAT มีความปลอดภัยเพียงพอหรือไม่

มีหลายคนที่ยังเข้าใจผิดเรื่อง NAT โดยมักจะคิดว่าถ้ามี NAT แล้วก็ไม่จำเป็นต้องมีไฟร์วอลล์ ซึ่งจริง ๆ แล้ว NAT ยังมีช่องโหว่ที่ต้องพิจารณาอีก ในกรณีที่ NAT ทำงานใน bi-directional mode นั้น จะต้องมีการเปิดพอร์ตสำหรับให้บริการเสมอ เช่น ๒๐-๒๑ (FTP), ๒๓(TELNET), ๒๕ (SMTP), ๕๓ (DNS), ๘๐ (HTTP), ๑๑๐ (POP), ๑๔๓ (IMAP) ซึ่งพอร์ตเหล่านี้เป็นที่รู้จักกันดี และมี exploit code ที่รันได้บนพอร์ตเหล่านี้ ซึ่งมักจะมีช่องโหว่อยู่เสมอ และ NAT ไม่สามารถป้องกันอันตรายในลักษณะนี้ได้เลย นอกจากนี้ NAT device ยังมีข้อเสียที่การเก็บข้อมูลลงล็อกไฟล์ ซึ่งการโจมตีดังที่กล่าวไปข้างต้นนั้น NAT device (บางยี่ห้อ) จะไม่บันทึกข้อมูลลงล็อกไฟล์เลย ดังนั้นเราอาจจะโดนโจมตีโดยไม่รู้ตัวก็เป็นได้ นอกจากนั้นการที่ user ใน internal network รันโปรแกรมบนเครื่องตัวเอง ซึ่งโปรแกรมนั้นอาจจะเป็นม้าโทรจันก็เป็นไปได้ จากนั้นม้าโทรจันก็จะส่ง packet ออกไป external network ซึ่ง NAT ก็จะปล่อยให้ packet ผ่านไปได้เพราะถือว่าเป็นการ request จาก internal side ในกรณีนี้ก็จะเห็นได้ว่า NAT ไม่ได้ช่วยอะไรได้เลย

บทสรุป

การใช้ NAT เป็นทางเลือกอย่างหนึ่งในการเชื่อมต่อเครือข่ายอินเตอร์เน็ตสำหรับเครื่องคอมพิวเตอร์หลาย ๆ เครื่อง ที่นับว่ามีค่าใช้จ่ายในการดำเนินการค่อนข้างต่ำ และมีความปลอดภัยในระดับหนึ่ง ถึงแม้ว่า NAT จะไม่ใช่ทางเลือกที่ดีสำหรับการรักษาความปลอดภัยให้กับระบบเครือข่ายขนาดใหญ่ แต่ก็สามารถป้องกันข้อมูลด้าน internal network ได้โดยการปิดทุกพอร์ตที่เราไม่ได้ตั้งใจเปิดไว้ และก็ง่ายต่อการจัดตั้ง จึงมีความเหมาะสมสำหรับระบบเครือข่ายภายในบ้าน (Home Networking) หรือระบบเครือข่ายในองค์กรขนาดเล็กสำหรับธุรกิจ SME เพื่อช่วยให้คอมพิวเตอร์หลาย ๆ เครื่องในระบบเครือข่ายภายในสามารถเชื่อมต่ออินเตอร์เน็ตได้ในเวลาเดียวกัน อย่างไรก็ตามจากจุดอ่อนต่างๆ ของ NAT ดังที่กล่าวมาแล้วข้างต้น จะเห็นได้ว่าหากต้องการให้เครื่องคอมพิวเตอร์ในระบบเครือข่ายภายในมีความปลอดภัยสูง ยังจำเป็นที่จะต้องมีไฟร์วอลล์ การจัดตั้ง DMZ zone และ Intrusion Detection System ซึ่งได้รับการออกแบบให้เหมาะสมกับทรัพยากรที่มีอยู่ พร้อมกับการได้รับการดูแลจากผู้ดูแลระบบที่มีความรู้ความสามารถเพียงพออย่างสม่ำเสมอ