บทที่ 10
การบริหารระบบ และจัดการเครือข่าย

การบริหารระบบเครือข่ายควรประกอบด้วยการวางแผน การคอนฟิก และการจัดการส่วนประกอบต่างๆ ของเครือข่าย ซึ่งส่วนประกอบต่างๆ เหล่านี้จะรวมถึงทรัพยากรณ์เครือข่ายทั้งที่อยู่ใกล้และไกล บัญชีผู้ใช้ และอุปกรณ์ต่างๆ ที่เชื่อมต่อเข้ากับระบบ จุดประสงค์หลักของการบริหารจัดการระบบเครือข่ายก็คือ เพื่อให้ผู้ใช้ได้รับประโยชน์สูงสุดจากเครือข่ายนั้นเอง

สิ่งที่สำคัญที่สุดในการดูแลระบบเครือข่ายคือ การจัดทำเอกสารข้อมูลเกี่ยวกับเครือข่ายเริ่มตั้งแต่การวางแผน ออกแบบ จนกระทั่งการใช้งาน แต่สิ่งนี้เป็นสิ่งที่ผู้ดูแลระบบส่วนใหญ่จะละเลยกัน เราควรคิดว่าการจัดทำเอกสารนี้เป็นเหมือนวัคซีนชนิดหนึ่งที่จะป้องกันความผิดพลาดต่างๆ ที่จะเกิดขึ้นอย่างแน่นอน จุดประสงค์ของการจัดทำเอกสารก็เพื่อความต่อเนื่องของเครือข่ายในขณะที่กำลังจัดทำเอกสารควรระลึกไว้เสมอว่าผู้ดูแลระบบคนใหม่ต้องการที่จะทราบข้อมูลอะไรบ้างในกรณีที่ถ้าหากเราไม่สามารถดูแลระบบได้ ตัวอย่างเช่น รหัสผ่านสำหรับผู้ดูแลระบบควรเก็บไว้ในที่ปลอดภัยควรมีคนอื่นที่มีความสำคัญและเกี่ยวข้องทราบว่าอยู่ที่ไหนเอกสารควรเริ่มด้วยคอนฟิกกุเรชั่นของเครือข่ายปัจจุบันซึ่งรวมถึงผังระบบทั้งหมด ตำแหน่งอุปกรณ์เครือข่ายต่างๆ และค่าคอนฟิกของแต่ละอุปกรณ์นั้นๆความเพียงพอในการใช้งานฮาร์ดแวร์และซอฟต์แวร์ และแนวโน้มความจำเป็นในการขยายเครือข่ายในอนาคตอันไกล เป็นต้น

เอกสารควรประกอบด้วยผังการวางสายสัญญาณ ตำแหน่งของอุปกรณ์เครือข่าย เช่น เราท์เตอร์ สวิตซ์ฮับ รูปแบบการเชื่อมต่อกันของอุปกรณ์ และความมีศูนย์เก็บเอกสารคู่มือต่างๆ ของอุปกรณ์ และอีกอย่างควรมีเอกสารเกี่ยวกับการเปลี่ยนแปลงและเพิ่มเติมของเครือข่ายด้วย

แบบอ้างอิงการบริหารเครือข่ายของ ISO

องค์การมาตรฐานนานาชาติ ISO ได้กำหนดแบบอ้างอิงการบริหารเครือข่ายเพื่อเป็นแนวทางสำหรับการบริหารเครือข่ายอย่างเป็นระบบ ซึ่งแบบอ้างอิงประกอบด้วย 5 หัวข้อเรื่องดังนี้

- การบริหารประสิทธิภาพ (Performance Management) : จุดประสงค์หลักของการบริหารประสิทธิภาพของเครือข่าย ก็เพื่อให้อุปกรณ์เครือข่ายทำงานได้เต็มประสิทธิภาพและมีแบนด์วิธเพียงพอต่อความต้องการ การบริหารประสิทธิภาพของเครือข่ายนั้นจะเกี่ยวข้องกับการมอนิเตอร์

การประเมิน และการปรับค่าคอนฟิกต่างๆ เพื่อให้การใช้แบนด์วิธและทรัพยากรอื่นๆ มีประสิทธิภาพ ซึ่งจะเกี่ยวข้องกับการทำบัญชีคอมพิวเตอร์และอุปกรณ์เครือข่าย การตรวจวัด รายงานวิเคราะห์ปริมาณการใช้ (Utilization) และอัตรส่งผ่านข้อมูล (Throughput) ของอุปกรณ์เครือข่ายต่างๆ เช่น ลิงค์ ฮับ สวิตซ์ เราท์เตอร์ โฮส และไฟร์วอลล์ เป็นต้นไปจนถึงเส้นทางข้อมูลผ่านอุปกรณ์เครือข่ายต่างๆ

- การบริหารข้อผิดพลาด (Fault Managements) : จุดประสงค์ของการบริหารข้อผิดพลาดของเครือข่ายคือ การเฝ้าระวัง การเก็บล๊อก (Log) การแจ้งเตือน การตรวจเช็ค และการแก้ไขข้อผิดพลาดต่างๆ ที่เกิดขึ้นในเครือข่าย ซึ่งขั้นตอนนี้จะมีบางส่วนที่คาบเกี่ยวกันกับการบริหารประสิทธิภาพของเครือข่าย แต่ข้อแตกต่างก็ คือ การบริหารข้อผิดพลาดนั้นจะเน้นที่การแก้ปัญหาหรือข้อผิดพลาดของเครือข่ายได้ทันเวลา เช่น สายสัญญาณขาด สวิตซ์เสียและเราท์เตอร์เสีย เป็นต้น ในขณะที่การบริหารประสิทธิภาพจะเน้นที่ประสิทธิภาพการใช้งานของเครือข่ายโดยรวม
- การบริหารคอนฟิกกูเรชัน (Configuration Management) : การบริหารค่าคอนฟิกกูเรชันต่างๆ ของอุปกรณ์ในเครือข่าย เช่น หมายเลข IP เวอร์ชันของซอฟต์แวร์ที่ใช้ในแต่ละเซิร์ฟเวอร์ ค่าคอนฟิกของเราท์เตอร์ สวิตซ์ ผังการเชื่อต่อของอุปกรณ์ต่างๆ เป็นต้น
- การบริหารบัญชีผู้ใช้ (Accounting Management) : การควบคุมการใช้งานทรัพยากรเครือข่ายของผู้ใช้ ซึ่งอาจใช้เพื่อการเก็บค่าบริการ ฟังก์ชันอาจรวมถึงการจัดการบัญชีผู้ใช้ การพิสูจน์ทราบตัวตน การกำหนดสิทธิ และการควบคุมการเข้าถึงทรัพยากรต่างๆ เป็นต้น
- การบริหารการรักษาความปลอดภัย (Security Management) : การควบคุมการเข้าใช้ทรัพยากรเครือข่ายให้เป็นไปตามนโยบายที่ได้กำหนดไว้

การจัดการบัญชีผู้ใช้

ก่อนเริ่มใช้งานระบบเครือข่ายนั้น ควรต้องมีการวางแผนเกี่ยวกับการที่จะอนุญาตให้ใครเข้าใช้ระบบเครือข่ายได้บ้าง ผู้ดูแลระบบต้องกำหนดวิธีการที่เป็นรูปแบบเดียวกันตลอดในการที่ผู้ใช้จะเข้าใช้เครือข่าย การเข้าใช้ระบบนั้นไม่ใช่แค่การล็อกอินเข้าใช้แต่ละเครื่องคอมพิวเตอร์เท่านั้น แต่รวมถึงการเข้าใช้ทรัพยากรที่มีอยู่ในเครือข่ายนั้นๆ ด้วย ระบบจัดการบัญชีผู้ใช้ที่นิยมทั่วไป เช่น ไมโครซอฟท์แอ็คทีฟไดเร็คทอรี (Active Directory).NDS (Novell Directory Service) หรือแม้กระทั่งของโอเพ่นซอร์ส อย่างเช่น

Open DAP เป็นต้น ระบบเหล่านี้จะใช้เป็นฐานข้อมูลที่จัดเก็บบัญชีผู้ใช้ของเครือข่าย โดยก่อนที่จะเริ่มเข้าใช้เครือข่ายก็ควรบังคับให้ทุกคนล็อกอินที่ระบบนี้ก่อน เพื่อพิสูจน์ทราบสิทธิของผู้ใช้คนนั้น หลังจากล็อกอินไปแล้วก็จำเป็นจะต้องเก็บล็อกเพื่อคำนวณออกมาเป็นข้อมูลทางด้านสถิติ หรืออาจใช้สำหรับการเก็บค่าบริการ เช่น การเข้าใช้งานอินเทอร์เน็ตซึ่งอาจมีแบนด์วิธที่จำกัด เป็นต้น

บัญชีผู้ใช้ในเครือข่ายที่สามารถจัดการได้มีจะมีอยู่ 2 ประเภทคือ บัญชีผู้ใช้ (UserAccount) บัญชีกลุ่มผู้ใช้ (Group Account)

บัญชีผู้ใช้ (User Account)

หนึ่งในมุมมองที่สำคัญของความปลอดภัยในเครือข่ายคือ รหัสผ่าน (Password) ถ้ารหัสผ่านยากต่อการเดาก็ยิ่งทำให้เครือข่ายมีความปลอดภัยมากขึ้นเท่านั้น ควรจะแนะนำให้ผู้ใช้กำหนดรหัสผ่านของตัวเองโดยใช้หลักการดังต่อไปนี้

- ไม่ควรใช้คำที่อยู่ในพจนานุกรม
- ไม่ควรใช้วันเดือนปีเกิด ชื่อญาติสนิท สัตว์เลี้ยง หรือข้อมูลเกี่ยวกับตัวเอง
- ต้องกำหนดความยาวอย่างต่ำ 8 อักษร
- ในรหัสผ่านควรมีทั้งตัวอักษร ตัวเลข ลัญลักษณ์พิเศษรวมอยู่ด้วย
- เก็บรายชื่อรหัสผ่านที่ใช้แล้ว
- ควรมีการเปลี่ยนรหัสผ่านบ่อยๆ

รหัสผ่านควรเป็นสิ่งที่จำง่ายโดยไม่ต้องเขียนโน้ตเพื่อเตือนความจำ อย่างไรก็ตามรหัสผ่านนี้จะต้องยากต่อการเดาโดยผู้อื่น วิธีหนึ่งที่ใช้กันมากในการบุกรุกเข้าระบบคือ การใช้คำในพจนานุกรมแทนรหัสผ่าน รหัสผ่านที่ยาวจะช่วยให้การบุกรุกยาวขึ้น

โปรแกรมสำหรับสร้างบัญชีผู้ใช้ซึ่งจะมาพร้อมกับระบบปฏิบัติการที่ติดตั้งหรือไดเร็คทอรีเซอร์วิสที่ใช้ เช่น สำหรับ Windows 2000/2003/2008 ก็จะมีเครื่องมือสำหรับการจัดการบัญชีผู้ใช้

บัญชีกลุ่มผู้ใช้ (Group Account)

การแบ่งผู้ใช้ออกเป็นกลุ่มนั้นก็เพื่อความสะดวกในการจัดการ ผู้ใช้ถูกกำหนดสิทธิในการเข้าถึงทรัพยากรต่างๆ ด้วยบัญชีกลุ่ม แทนที่จะกำหนดสิทธิให้กับผู้ใช้แต่ละคน ผู้ใช้ที่เป็นสมาชิกในกลุ่มเดียวกันก็จะมีสิทธิเท่ากัน ประโยชน์ของการจัดเป็นกลุ่มนี้ไม่ใช่แค่ความสะดวกเท่านั้น แต่ยังเป็นการป้องกันการลืมกำหนดสิทธิให้แก่ผู้ใช้แต่ละคน โดยเฉพาะถ้าเป็นผู้ใช้ที่สำคัญเช่นผู้จัดการบริษัท เป็นต้น

ระบบปฏิบัติการเครือข่ายส่วนใหญ่จะสร้างบัญชีกลุ่มผู้ใช้ไว้ให้แล้ว รวมทั้งกำหนดสิทธิให้แต่ละกลุ่มด้วย ซึ่งกลุ่มผู้ใช้บางกลุ่มมีสิทธิที่จะทำหน้าที่แทนผู้ดูแลระบบได้บางอย่าง เช่น การสร้างบัญชีใหม่การแบ็คอัพข้อมูล เป็นต้น ซึ่งการทำเช่นนี้จะเป็นการแบ่งเบาหน้าที่ความรับผิดชอบของผู้ดูและระบบได้ผู้ดูแลระบบสามารถกำหนดให้ใช้แต่ละคนเป็นสมาชิกในบัญชีกลุ่มผู้ใช้เหล่านี้ได้เลย นอกจากนี้ผู้ดูแลระบบยังสามารถสร้างบัญชีกลุ่มผู้ใช้ขึ้นมาใหม่ก็ได้ โดยจะกำหนดให้กลุ่มมีสิทธิตามความเหมาะสม

สำหรับเครือข่ายขนาดใหญ่นั้นในปัจจุบันนิยมใช้ได้เร็คทอรีเซอร์วิสเข้ามาใช้เช่น อีไดเร็คทอรี (Directory) ของโนเวลล์ และแอ็คทีฟไดเร็คทอรีของไมโครซอฟท์ เป็นต้น ไดเร็คทอรีเซอร์วิสต่างๆ จะมีเครื่องมือที่ช่วยให้การจัดการเกี่ยวกับบัญชีผู้ใช้ได้ง่าย

การจัดการทรัพยากร

จุดประสงค์หลักของเครือข่ายคือ เพื่อการใช้ทรัพยากรอย่างคุ้มค่า ไม่ว่าทรัพยากรนั้นจะเป็นฐานข้อมูลลูกค้า หรือแม้กระทั่งเครื่องพิมพ์เลเซอร์ก็ตาม การจัดการทรัพยากรเหล่านี้เป็นงานที่ใช้เวลาค่อนข้างมากสำหรับผู้ดูแลระบบ การจัดการทรัพยากรเริ่มจากการตั้งชื่อให้กับเซิร์ฟเวอร์โฮสต์ เครื่องพิมพ์ บัญชี และทรัพยากรอื่นๆ หลังจากที่ได้ติดตั้งทรัพยากรเรียบร้อยแล้วขั้นต่อไปเป็นการกำหนดสิทธิให้ผู้ใช้ที่เข้ามาใช้ทรัพยากรเหล่านั้น โดยการกำหนดให้เป็นกลุ่มของ ผู้ใช้

ดิสก์โควตา

ดิสก์โควตา (Disk Quota) เป็นนโยบายที่กำหนดข้อจำกัดเกี่ยวกับพื้นที่ที่ผู้ใช้แต่ละคนสามารถใช้ในฮาร์ดดิสที่ติดตั้งบนไฟล์เซิฟเวอร์ เนื่องจากว่าโดยธรรมชาติแล้วผู้ใช้แต่ละคนจะเก็บไฟล์ต่างๆ ไว้ในฮาร์ดดิส และขนาดพื้นที่ที่เก็บ ไฟล์เหล่านี้จะเพิ่มขึ้นเรื่อยๆ จนกระทั่งไม่มีพื้นที่เหลือ และถ้าฮาร์ดดิสที่ใช้เก็บไฟล์ต่างๆ เป็นของส่วนรวมหรือที่ใช้ร่วมกันจึงจำเป็นต้องมีการกำจัดพื้นที่ของแต่ละคนให้แน่นอน

ไม่อย่างนั้นจะไม่ว่าฮาร์ดดิสชนิดความจุมากเท่าไร พื้นที่จะถูกใช้หมดในไม่ช้าเพราะระบบปฏิบัติการเครือข่ายบางตัวจะมีฟีเจอร์นี้อยู่แล้ว อย่างไรก็ตามยังมีซอฟต์แวร์จากบริษัทอื่นที่สามารถนำมาใช้ได้

ไฟล์และไดเร็คทอรี

โดยทั่วไปแล้วไฟล์และไดเร็คทอรีที่เก็บไฟล์นั้นไว้จะไม่ถือว่าเป็นทรัพยากรเครือข่ายผู้ใช้จะเข้าถึงและใช้ไฟล์ประจำ ระบบปฏิบัติการเครือข่ายโดยทั่วไปจะมีฟังชั่นที่ใช้ในการจัดการไฟล์ต่างๆ ได้โดยการกำหนดสิทธิของกลุ่มผู้ใช้ที่สามารถเข้าถึงไฟล์ได้ แต่สำหรับผู้ใช้ที่ใช้เครื่องพีซีที่ใช้วินโดวส์95/98/Me มีสิทธที่จะเข้าถึงไฟล์ทุกอย่างที่อยู่ในเครื่องนั้น แต่ถ้าเป็นวินโดวส์เซฟเวอร์แล้วก็จำเป็นต้องมีการจัดการเกี่ยวกับสิทธิ์ของผู้ใช้ในการเข้าถึงไฟล์หรือโฟล์เดอร์

การพิมพ์

จุดประสงค์ที่สำคัญอย่างหนึ่งของการเชื่อมต่อคอมพิวเตอร์เป็นเครือข่าย โดยเฉพาะองค์กรขนาดเล็กคือ เพื่อสามารถใช้งานเครื่องพิมพ์ เนื่องจากเครื่องพิมพ์ที่มีคุณภาพดีจะมีราคาแพงข้อควรระวังคือ ถ้าเครื่องพิมพ์เสียการทำงานจะทำได้ไม่เต็มที่และเมื่อเครือข่ายขยายใหญ่ขึ้นความหลากหลายของเครื่องพิมพ์ก็จะเพิ่มมากขึ้น

มีซอฟต์แวร์หลายตัวที่อำนวยความสะดวกในการจัดการเกี่ยวกับเครื่องพิมพ์ ข้อเสียของซอฟต์แวร์ประเภทนี้คือ จะเป็นซอฟต์แวร์ของบริษัทที่สาม และจะใช้งานได้กับคอมพิวเตอร์บางยี่ห้อเท่านั้น ซอฟต์แวร์บางประเภทสามารถจัดการเครื่องพิมพ์ผ่านทางเว็บเพจได้

แบนด์วิธ

ปัจจุบันเกือบทุกองค์กรมีความจำเป็นอย่างยิ่งที่ต้องเชื่อมต่อเข้ากับอินเทอร์เน็ตเพื่อใช้ประโยชน์ทั้งทางตรงและทางอ้อม บางองค์กรมีเซิร์ฟเวอร์ที่ให้บริการอินเทอร์เน็ต เช่น เว็บเซิร์ฟเวอร์ เมลล์เซิร์ฟเวอร์เป็นต้น แต่ค่าใช้จ่ายในการเชื่อมต่อเข้ากับอินเทอร์เน็ตนั้นอาจสูงมากและส่วนใหญ่ แบนด์วิธอาจไม่เพียงพอต่อความต้องการของผู้ใช้ ดังนั้นการให้บริการนี้จำเป็นอย่างยิ่งที่ต้องมีการควบคุมโดย นอกจากการติดตั้งไฟร์วอลล์ซึ่งเป็นอุปกรณ์ด้านการรักษาความปลอดภัยพื้นฐานแล้ว ก็อาจจำเป็นต้องติดตั้งอุปกรณ์สำหรับการควบคุมแบนด์วิธของผู้ใช้แต่ละคนด้วย

ปัญหาทั่วไปเกี่ยวกับระบบเครือข่าย

ที่ผ่านมาเราพอจะทราบแล้วว่าระบบเครือข่ายเป็นสิ่งที่ซับซ้อนมาก ซึ่งประกอบด้วยชิ้นส่วนเล็กๆ ที่ผลิตโดยหลายบริการ โดยประกอบร่วมกันจนกลายเป็นระบบเครือข่าย ซึ่งบางทีอาจทำให้เราสับสนในบางส่วนได้ แต่ก็เป็นเรื่องธรรมดาที่อะไรก็แล้วแต่ที่ซับซ้อนมักจะเกิดปัญหาจากความซับซ้อนของมันเองเครือข่ายก็เช่นกัน ที่อาจมีบางส่วนที่จะเป็นสาเหตุของปัญหาซึ่งจะมีผลต่อระบบโดย รวมได้การวางแผนอย่างรัดกุม การออกแบบที่ดี และการติดตั้งขั้นตอนอย่างถูกต้องจะลดเวลาที่ใช้ในการซ่อมบำรุงระบบได้อย่างมาก อย่างไรก็ตามก็คงจะต้องมีปัญหาเกิดขึ้นกับระบบอย่างแน่นอน โดยเฉพาะปัญหาเกี่ยวกับประสิทธิภาพของเครือข่าย ดังนั้นผู้ดูแลระบบจำเป็นอย่างยิ่งที่ต้องเข้าใจปัญหาที่อาจเกิดขึ้นต้องเรียนรู้และเครื่องมือที่จะช่วยและการแก้ปัญหาเหล่านี้ด้วย

ฮาร์ดแวร์ของเครือข่าย

สายสัญญาณทุกประเภทจะมีข้อจำกัดอยู่ ไม่ว่าจะเป็นสายคู่เกลียวบิด (UTP) สายไฟเบอร์หรือระบบไร้สายก็ตาม จะมีข้อจำกัดเกี่ยวกับความยาวของสายที่ใช้ระยะทาง การใช้งานสายสัญญาณเหล่านี้เกินข้อจำกัด ไม่ว่าจะเป็นเพียงเล็กน้อยก็ตามอาจจะก่อให้เกิดปัญหาต่อประสิทธิภาพได้ เนื่องจากข้อมูลที่ส่งไปจะกลายเป็นขยะได้เมื่อมาถึงปลายทาง หรืออาจจะส่งไม่ถึงเลยก็ได้ ปัญหาที่เกิดจากสาเหตุนี้จะยากต่อการวินิจฉัย เช่น การใช้สายสัญญาณยาวกว่าข้อกำหนดการใช้ฮับหรือสวิตช์มากกว่าจำนวนที่กำหนด หรือการเทอร์มิเนตสายโคแอ็กซ์ไม่ถูกต้อง เป็นต้นสิ่งต่างๆ เหล่านี้อาจจะไม่ทำให้ทั้งระบบล่มเลยทีเดียว แต่จะมีผลต่อความเร็วและความเสถียรภาพของเครือข่าย ซึ่งเป็นอาการที่ยากยิ่งต่อการค้นหาสาเหตุ การที่ดีที่สุดที่จะป้องกันปัญหานี้คือ ทำความเข้าใจ และทำความคุ้นเคยกับข้อจำกัดเกี่ยวกับความยาวของสายสัญญาณแต่ละประเภทที่ใช้และข้อจัดอื่นๆ ด้วย และกำกับดูแลไม่ให้เกินที่มาตรฐานกำหนดในช่วงของการออกแบบและติดตั้งระบบ

เน็ตเวิร์คทราฟฟิก

เนื่องจากระบบเครือข่ายได้เปลี่ยนแปลงวิธีการทำงานของผู้ใช้ ทำให้การใช้งานเครือข่ายของผู้ใช้แต่ละคนเพิ่มมากขึ้นและการไหลเวียนของแพ็คเกจข้อมูลในเครือข่ายหรือเน็ตเวิร์คทราฟฟิก (Network Traffic) เพิ่มขึ้นเมื่อด้วย ไม่ว่าจะเนื่องมาจากการใช้แอพพลิเคชั่นที่ต้องการแบนด์วิธสูง ปัญหาเนื่องมาจากฮาร์ดแวร์ หรือการเพิ่มจำนวนผู้ใช้เครือข่าย หรือการเพิ่มปริมาณการไหลเวียนของแพ็คเกจเป็นเรื่อง

ธรรมดาในเครือข่ายสมัยใหม่ เครือข่ายส่วนใหญ่จะถูกออกแบบเผื่อไว้สำหรับการไหลเวียนของแพ็คเกจที่สูง แต่เมื่อปริมาณแพ็คเกจเพิ่มมากขึ้น และผลที่เกิดขึ้นไม่เป็นไปตามที่คาดไว้ ประเด็นต่างๆ ที่เกี่ยวกับปริมาณการไหลเวียนของแพ็คเกจในเครือข่ายสามารถทำให้ลดประสิทธิภาพของเครือข่ายได้

การชนกันของข้อมูล

อีเธอร์เน็ตเป็นเครือข่ายแบบ LAN ที่นิยมกันมากที่สุดในปัจจุบัน อีเธอร์เน็ตจะเป็นโปรโตคอล CSMA/DC เพื่อแข่งกันเข้าใช้ช่องส่งสัญญาณ ซึ่งโปรโตคอลนี้จะมีการแพร่สัญญาณรบกวนที่เรียกว่า โคลลิชั่น (Collision) เมื่อมีการส่งข้อมูลพร้อมกันมากกว่าหนึ่งแหล่ง

เมื่อมีเวิร์คสเตชันจำนวนมากขึ้นพยายามที่จะส่งข้อมูลผ่านเครือข่าย การเพิ่มขึ้นของการชนกันของข้อมูลเป็นสิ่งที่หลีกเลี่ยงไม่ได้ เนื่องจากถ้าเกิดการชนกันของข้อมูลขึ้นมาทุกๆ สถานที่ที่กำลังส่งข้อมูลจะต้องหยุดการส่งชั่วขณะ ดังนั้นการเกิดการชนกันเป็นจำนวนมากๆ เป็นสิ่งที่ไม่ดีอย่างแน่นอนบางครั้งการชนกันของข้อมูลเกิดขึ้นสูงมากจนอาจทำให้แต่ละสถานที่ไม่สามารถส่งข้อมูลได้เลยก็มี

ถ้าหากตรวจพบว่ามีการชนกันของข้อมูลมากขึ้น เครือข่ายอาจถูกใช้งานมากเกินไป ซึ่งสามารถแก้ปัญหาได้โดยการเปลี่ยนไปใช้สายสัญญาณที่มีประสิทธิภาพดีกว่าหรือมีแบนด์วิธที่สูงกว่า หรือจะแยกเครือข่ายออกเป็นหลายๆ เซ็กเมนต์ (Segment) หรือโดยการใช้สวิตช์ก็ได้

การใช้โปรโตคอลที่มีประสิทธิภาพต่ำ

โปรโตคอลจะมีเครือข่ายแต่ละประเภทจะมีวิธีการแรกเปลี่ยนข้อมูล และการจัดการเกี่ยวกับที่อยู่ (Address-Resolution) ที่ต่างกัน ซึ่งโปรโตคอลบางประเภทอาจมีประสิทธิภาพต่ำหลายตัวก็มีการเซ็ตอัปและการจัดการที่ง่ายโดยการใช้วิธีไดนามิกเนมมิ่งโซลูชั่น (Dynamic Naming Solution) ซึ่งจะมีการส่งแพ็คเกจแบบแพร่กระจาย ทำให้จำนวนแพ็คเกจในเครือข่ายเพิ่มมากขึ้น เช่น โปรโตคอล Apple Talk ที่ใช้ในแมคอินทอชเป็นต้น ส่วนโปรโตคอล IPX/SPX ที่ใช้กับเน็ตแวร์ก็เช่นกัน ก็จะส่งSAP Servie Advertisement Protocol) แบบแพร่กระจายถี่มาก ส่วนโปรโตคอล NetBEUI ที่ใช้ในระบบวินโดวส์ก็จะมีการส่งข้อมูลแบบแพร่กระจายมากเช่นกัน

วิธีการแก้ปัญหาการส่งข้อมูลแบบแพร่กระจายนี้ก็มีหลายวิธีเช่น การคอนฟิกเวิร์คสเตชันให้มีการส่งข้อมูลแบบแพร่กระจายให้น้อยที่สุด หรือการกองแพ็คเจแบบแพร่กระจายในระดับเราท์เตอร์หรือการเปลี่ยนไปใช้โปรโตคอลที่มีการส่งข้อมูลแบบแพร่กระจายน้อยลง เป็นต้น

ข้อจำกัดของฮาร์ดแวร์

เมื่อมีแพ็คเกจในเครือข่ายเพิ่มมากขึ้น ทำให้ฮาร์ดแวร์ต้องทำงานหนักมากยิ่งขึ้น ซึ่งจะมีผลกระทบกับอุปกรณ์เครือข่ายที่ฉลาด เช่น เราท์เตอร์ที่จะต้องเช็คเฮดเดอร์ของทุกๆ แพ็กเกจเพื่อดูข้อมูลเกี่ยวกับการจัดการเส้นทางข้อมูล ถ้าจำนวนแพ็คเกจมากเกินไปเราท์เตอร์ก็จะทำงานไม่ทันได้ เช่นกัน หรือบางทีเราท์เตอร์อาจจะส่งแพ็กเกจที่เป็นขยะได้เช่นกัน

การป้องกันปัญหานี้ก็มีหลายวิธีเช่น การใช้เราท์เตอร์ที่ทำหน้าที่เป็นเราท์เตอร์อย่างเดียวไม่ใช่คอมพิวเตอร์ที่ใช้งานอย่างอื่นด้วยและก็เป็นเราท์เตอร์ด้วย และอีกอย่างการใช้เราท์เตอ์ในการแบ่งเครือข่ายใหญ่ๆ เป็นเครือขายย่อยๆ หลายเครือข่ายจะช่วยลดโหลดของเราท์เตอร์ได้ แต่จะทำให้การจัดเส้นทางของข้อมูลของเราท์เตอร์ซับซ้อนยิ่งขึ้น

ข้อมูลขยะ

แพ็กเกจข้อมูลที่เป็นขยะอาจเกิดขึ้นเนื่องจากฮาร์ดแวร์ที่ชำรุด ซึ่งจะเป็นเรื่องธรรมดาตัวอย่าง เช่น อีเธอร์เน็ตการ์ดที่ชำรุดอาจจะส่งแพ็กเกจเป็นจำนวนมาก ทำให้เครือข่ายเต็มไปด้วยแพ็กเกจที่เสียเหล่านี้ ซึ่งบางทีเครือข่ายอาจล่มได้เช่นกัน เนื่องจากนี้แพ็กเกจที่เป็นขยะอาจเกิดขึ้นเนื่องจากคลื่นลบกวน นอกจากนั้นอุปกรณ์เครือข่ายเช่น ฮับ สวิตซ์ และเราท์เตอร์บางครั้งอาจจะส่งแพ็กเกจที่เป็นขยะได้เช่นกัน ในกรณีที่จำมีแพ็กเกจมากเกินความสามารถของอุปกรณ์เหล่านี้

การถูกโจมตี

การโจมตีเครือข่ายผ่านทางอินเทอร์เน็ตมักจะพบเห็นมากยิ่งขึ้นการโจมตีแบบหนึ่งคือ Dos (Denial-of-Serice) เป็นการโจมตีด้วยการส่งแพ็กเกจจำนวนมากไปยังเซฟเวอร์หรือเครือข่ายซึ่งจำทำให้เซิร์ฟเวอร์หรือเครือข่ายที่ถูกโจมตีนี้ไม่สามารถอบสนองได้ ภัยคุกคามอีกอย่างหนึ่งที่ส่วนใหญ่คงได้เจอมาแล้วคือ ไวรัส เวิร์ม โทรจันฮอร์ส ซึ่งเป็นโปรแกรมคอมพิวเตอร์ที่มีจุดมุ่งหมายเพื่อทำลายระบบคอมพิวเตอร์นั่นเอง ปัจจุบันไวรัสได้มีวิวัฒนาการอย่างมาก โดยจะใช้เครือข่ายเป็นช่องทางในการโจมตี

การโจมตีเครือข่ายและระบบคอมพิวเตอร์ส่วนใหญ่เกิดขึ้นเนื่องจากเป็นจุดอ่อนของโปรโตคอล TCP/IP ช่องโหว่ในระบบปฏิบัติการ และซอฟแวร์ที่พัฒนาขึ้นในโดยที่ไม่ได้ให้ความสำคัญด้านการรักษาความปลอดภัย การป้องกันปัญหานี้สามารถทำได้โดยการติดตั้งแพทช์ (Patch) หรือเซอร์วิสแพ็ค (Serivice Pack) หรือฮ็อตฟิกส์ (Hoffixes) ล่าสุดของระบบปฏิบัติการนั้นๆ และโดยการใช้เครื่องมือวิเคราะห์ข้อผิดพลาดของเครือข่ายเพื่อตรวจเช็คปัญหาดังกว่าได้

ปัญหาเกี่ยวกับการแอดเดรส

ถึงแม้ว่าเครือข่ายจะถูกออกแบบให้มีแบนด์วิธสูงและจำนวนแพ็กเก็ตไหลเวียนในเครือข่ายมีน้อยซึ่งจะทำให้เวิร์คเสตชันสามารภส่งข้อมูลได้อย่างรวดเร็ว อย่างไรก็ตามถ้าแพ็กเก็ตที่เวิร์ตสเตชันพยายามที่อยู่ในเกณดี เช่น ระบบ DNS (Domain Name Service) หรือ WINS เป็นต้นส่วนใหญ่แล้วปัญหาเกี่ยวกับที่อยู่นี้เกิดจากการเซตค่าต่างๆ ไม่ถูกต้อง

เครื่องมือพื้นฐานสำหรับดูแลระบบเครือข่าย

โดยปกติอุปกรณ์เครือข่าย เช่น เร้าท์เตอร์ สวิตซ์ หรือแม้กระทั่งระบบปฏิบัติการที่รองรับการทำงานผ่านเครือข่ายอย่างเช่น วินโดวส์ และลีนุกซ์ มักจะมีเครื่องมือพื้นฐานสำหรับการบริหารจัดการเครือข่าย หรือมีไว้สำหรับตรวจเช็คและแก้ปัญหาของเครือข่ายเบื้องต้นแต่การใช้เคริ่องมือนี้อาจจำเป็น ต้องมีความรู้ทางด้านเครือข่ายเพื่อจะได้เข้าใจและสามารถค้นหาต้นเหตุของปัญหาได้

Ping

ปิง Ping อาจเป็นเครื่องมือแรกและเป็นเครื่องมือที่สำคัญมากที่สุดที่จะใช้ในการวิเคราะห์ปัญหาของเครือข่ายที่ใช้โปรโตคอล TCP/IP ปิงเป็นเครื่องมือที่ใช้สำหรับทดสอบว่าโฮสต์นั้นๆ ยังเชื่อมต่อกับเครือข่ายอยู่หรือไม่ซึ่งปิงจะส่งแพ็กเกตไปยังโฮสต์ดังกล่าวเพื่อถามว่า *คุณยังอยู่หรือเปล่า* ถ้าโฮสต์นั้นยังเชื่อมต่อกับเครือข่ายอยู่ก็จะส่งแพ็กเกจกลับมาบอกว่า *ยังอยู่* ปิงจะวัดเวลาตั้งแต่เริ่มส่งแพ็กเกจออกไปและเมื่อแพ็กเกจตอบรับจากโฮสต์แล้วรายงานระยะเวลาดังกล่าว ปิงไม่ได้บอกว่าโฮสต์ยังคงเชื่อมต่ออยู่กับเครือข่ายอยู่หรือไม่เท่านั้น มันยังสามารถวัดได้ว่าการสื่อสารระหว่าง 2 เครื่องใช้เวลานานเท่าใดซึ่งข้อมูลนี้สามารภใช้ในการตรวจตอบการเชื่อมต่อของโฮสต์กับเครือข่ายและประสิทธิภาพของเครือข่าย

Traceroute

Tracert ทำงานโดยการส่งแพ็กเกต ICMP (Internet Contro Message Protocol) ด้วย TTL (Time to live) เพิ่มขึ้นทุกๆ ครั้งที่ส่งโดยจะเริ่มต้นที่ TTL มีค่าเท่ากับ 1 ก่อนเวิร์คสเตชั่นจะส่งแพ็กเกตไปเรื่อยๆ จนกระทั่ง TTL มีค่าเท่ากับค่าที่กำหนดหรือจนกระทั่งโฮสต์ไปทางตอบกลับดังนั้นคำสั่ง Tracert จะเริ่มโดยการส่งแพ็กเกตพิเศษนี้ไปไปยังเกตเวย์ของเครือข่ายก่อนถ้าเกตเวย์ทำงานปกติจะส่งแพ็กเกจตอบรับมายังเครื่องส่งแล้วโฮสต์ต้นทางก็จะส่งแพ็กเกจไปยังเราท์เตอร์ถัดไปตามเส้นทางไปยังโฮสต์ปลายทางซึ่งเราท์เตอร์ตัวถัดไปก็จะทำเช่นเดียวกันกับเกตย์เวย์ขบวนการนี้จะทำไปเรื่อยๆ จนกระทั่งโฮสต์ปลายทางได้รับแพ็กเกตแล้วตอบกลับหรือจำนวนฮ็อปที่เกินกำหนดไว้ โดยมาตรฐานแล้วฮ็อปที่สูงสุดคือ 30 อ็อปซึ่งเป็นค่าที่ได้จากโครงสร้างของอินเทอร์เน็ตในปัจจุบัน

Netstat

Netstat เป็นเครื่องมือที่จะช่วยในการเฝ้าดูพฤติกรรมของเครือข่าย Nestat เป็นเครื่องมือที่ใช้แสดงเกี่ยวกับโปรโตคอล TCP/IP เช่น IP ICM TCP และ UPD ข้อมูลเหล่านี้สามารถนำไปใช้ในการวิเคราะห์สาเหตุของสิ่งที่เกิดโดยการแยกออกได้ว่า ปัญหาเหล่านี้เกิดจากแอพพลิเคชันใด หรือเป็นปัญหาของเครือข่ายใด

Sniffer

เครื่องมือวิเคราะห์โปรโตคอล (Protocol Analyzer) หรือบางทีเรียกว่า แพ็กเก็ตสนิฟเฟอร์ (Packet Sniffer) เป็นอีกเครื่องมือหนึ่งที่ใช้สำหรับวิเคราะห์การไหลเวียนข้อมูลในเครือข่ายเครื่องมือนี้สามารถสำหรับ

- ตรวจจับเฟรมข้อมูลที่วิ่งบนเครือข่าย
- แสดงข้อมูลที่อยู่ในแต่ละเฟรมที่ตรวจจับได้หรือกรองเฟรมข้อมูลเหล่านี้ได้
- สามารถแก้ไขข้อมูลที่อยู่ในแต่ละเฟรมแล้วค้อยส่งต่อได้
- แสดงสถิติของอุปกรณ์เครือข่าย หรือโปรโตคอลที่มีการส่งข้อมูลมากที่สุด
- รายงานการวิเคราะห์ทราฟฟิกในรูปแบบที่อ่านได้ง่าย

Network Scanner

Ping เป็นเครื่องมือพื้นฐานที่ใช้ทดสอบการเชื่อมต่อเข้ากับเครือข่ายของเครื่องใดเครื่องหนึ่งแต่ถ้าเราต้องการทราบว่าเครือข่ายมีโฮสต์หรืออุปกรณ์ใดเชื่อมต่ออยู่บ้างนั้น ก็จำเป็นต้องใช้เครื่องมือช่วยในการสแกนเครือข่าย ปัจจุบันมีเครื่องมือประเภทนี้มากมายทั้งที่ดาวน์โหลดใช้งานได้ฟรีหรือเป็นซอฟต์แวร์ที่ต้องซื้อ ซึ่งจะแตกต่างกันในเรื่องของประสิทธิภาพและฟังก์ชั่นต่างๆ สแกนเนอร์ที่นิยม เช่น

- Angry IP Scanner
- SoftPerfect Network Scanner
- GFI LANguard Security Scanner
- NMAP

เครื่องมือเหน่านี้จะช่วยในการเก็บข้อมูลเกี่ยวกับโฮสต์ หรืออุปกรณ์เครือข่ายที่มีหมายเลขไอพี

Cable Analyzer

เครือข่ายที่วิ่งด้วยความเร็วสูง เช่น อีเธอร์เน็ตความสูง (Fast Ethernet) ที่แบนด์วิธที่ 100 Mbps และกิกะบิตอีเธอร์เน็ต (Gigabit Ethernet) ที่มีแบนด์วิธที่ 1000 Mbps ส่วนใหญ่จะมีปัญหาเกี่ยวกับสายสัญญาณ ซึ่งเครือข่ายแต่ละประเภทจะมีข้อจำกัดที่เกี่ยวกับสายสัญญาณ โดยส่วนใหญ่จะเป็นข้อกำจัดในเรื่องความยาวของสายสัญญาณและคลื่นรบกวน เช่น อีเธอร์เน็ตความเร็วสูงจะกำจัดการใช้สายสัญญาณ แบบยูทีพี (UTP Cat 5) ไม่เกิน 100 เมตร ถ้ามีการใช้สายสัญญาณเกินข้อจำกัดนี้อาจทำให้การส่งข้อมูลมีปัญหา เช่น บางเฟรมจะไม่สามารถส่งถึงปลายทางได้ ซึ่งเป็นการยากต่อการวิเคราะห์หาสาเหตุได้

เคเบิลอะนาไลเซอร์นี้จะใช้เมื่อการติดตั้งสายสัญญาณครั้งแรก เมื่อเสร็จแล้วจะไม่ค่อยให้ความสนใจมากนัก อีกอย่างปัญหาที่เกิดขึ้นอาจมีสาเหตุเนื่องมาจากสายสัญญาณเสื่อมคุณภาพ เมื่อใช้งานไปนานๆ ทำให้ไม่สามารถรองรับการส่งข้อมูลในอัตราความเร็วสูงได้ เคเบิลอะนาไลเวอร์สามารถใช้ตรวจสอบประสิทธิภาพของสายสัญญาณได้

Wireless Scanner

ในการดูแลระบบไวร์เลสแลนนั้นก็จำเป็นต้องมีเครื่องมือที่ช่วยในการวิเคราะห์ และสามารถเชื่อมต่อกับเครือข่ายไวร์เลสแลนได้ โดยเครื่องมือเหล่านี้จะสามารถกำหนด ESSID. คีย์การเข้ารหัส และการกำหนดค่าคอนฟิกของช่องสัญญาณของแอ็กเซสพอยต์ อัตราการรับส่งข้อมูลและค่าวัดประสิทธิภาพของเครือข่ายไร้สาย

เครื่องมือที่นิยมใช้ เช่น Network Stumbler เป็นเครื่องมือที่ใช้งานง่ายการทำงานของมันคือมันจะบรอดคาสต์ไคลเอนท์โพรบ (Client probe) และรายงานทุกแอ็กเซสพอยที่ตอบกลับและพยายามจะดักจับ ESSID และข้อมูลที่เกี่ยวกับแอ็กเซสพอยต์นั้นๆ เมื่อสามารถเชื่อมต่อกับแอ็กเซสพอยต์ได้แล้ว Network Stumbler ก็จะสามารถค้นหาไคลเอนท์ที่อยู่ใน BSS เดียวกันได้นอกจากนี้เน็ตสตัมเบลอสามารถเชื่อมต่อเครือข่ายแบบเปิด (Open network) ที่ใช้ WEP คีย์ได้ ถึงแม้ว่าเน็ตสตัมเบลอจะไม่มีฟีเจอร์ในการดักจับแพ็กเก็ต อย่างไรก็ตามการดักจับแพ็กเก็ตนั้นสามารภทำได้โดยการใช้เน็ตเวิร์คไดรเวอร์ที่รองรับการทำงานแบบโพรมิสซัยมโหมด (Promiscuous mode) ได้

ระบบบริหารจัดการเครือข่าย

ตามที่กล่าวมาแล้วข้างต้น หน้าที่ของบริการเครือข่าย เฝ้าระวังทดสอบ ตรวจเช็คสภาพคอนฟิก และควบคุมทั้งฮาร์ดแวร์และซอฟต์แวร์ของเครือข่าย อย่างที่ทราบกันดีแล้วว่าส่วนต่างๆ ของเครือข่ายนั้นจะอยู่กระจัดกระจายทั่วไป ทำให้ยากต่อการที่จะรวบรวมข้อมูล หรือจัดการอุปกรณ์เครือข่าย ที่อยู่ห่างไกลจากที่ทำงาน ระบบบริหารเครือข่ายจะช่วยให้งานของผู้บริหารเครือข่ายง่ายขึ้น โดยระบบนี้จะอนุญาตให้บริหารเครือข่ายสามารถทำงานได้จากที่ศูนย์กลางองค์ประกอบระบบบริหารจัดการเครือข่าย

โครงสร้างของระบบบริหารเครือข่ายประกอบด้วย 3 ส่วนคือ

- อุปกรณ์เครือข่ายที่ต้องการจัดการ (Managed Devices)
- เอเจนต์ (Agent)
- ระบบบริหารจัดการเครือข่าย (Network management System หรือ NMS)

อุปกรณ์เครือข่ายที่ต้องการจัดการ คือ อุปกรณ์เครือข่ายที่ติดตั้งเอเจนต์ SNMP ซึ่งเอเจนต์จะทำหน้าที่รวบรวมและจัดเก็บข้อมูลของอุปกรณ์และรับส่งข้อมูลนี้กับ NMS โดยใช้โปรโจคอล SNMPอุปกรณ์เครือข่ายที่ต้องการจัดการ เช่น เราท์เตอร์ แอ็กเซสเซิร์ฟเวอร์ สวิตซ์ ฮับคอมพิวเตอร์ หรือเครื่องพิมพ์ เป็นต้น

เอเจนต์เป็นซอฟต์แวร์ที่ติดตั้งอุปกรณ์เครือข่ายที่ต้องการจัดการ ซึ่งซอฟต์แวร์นี้จะจัดการข้อมูลของอุปกรณ์และแปลงให้สามารถใช้งานได้กับโปรโตคอล SNMP ส่วน NMS เป็นเซิร์ฟเวอร์ที่มอนิเตอร์และควบคุมอุปกรณ์เครือข่ายอีกทีหนึ่ง

MIB (Management Information Bass) เป็นฐานข้อมูลที่เก็บรวบรวมข้อมูลเกี่ยวกับการบริหารเครือข่าย และมีการเก็บแบบเป็นลำดับชั้น MIB สามารถแอ็กเซสได้โดยใช้โปรโตคอลจัดการระบบเช่น SNMP ฐานข้อมูลจะประกอบด้วยออบเจ็กต์ (Object) โดยแต่ละออบเจ็กต์จะมีหมายเลขประจำ (Object ID) ซึ่งเป็นค่าหนึ่งที่บอกคุณสมบัติ หรือสถานะของอุปกรณ์ที่ถูกจัดการนั้นๆ และแต่ละออบเจ็กต์ก็อาจมีหลายหน่วย (Instance) หรือตัวแปรอีกด้วย

โปรโตคอล SNMP และ RMON

SNMP (Simple Network Management Protocol) เป็นโปรโตคอลในเลเยอร์แอพพลิเคชันที่ใช้สำหรับแลกเปลี่ยนข้อมูลเกี่ยวกับการบริหารเครือข่ายระหว่างอุปกรณ์เครือข่ายต่างๆ โปรโตคอลนี้เป็นส่วนหนึ่งในชุดโปรโตคอล TCP/IP ซึ่งจะช่วยให้ผู้ดูแลระบบสามารถจัดการประสิทธิภาพ, วิเคราะห์ปัญหา และให้ข้อมูลเพื่อสำหรับการวางแผนเพื่อการขยายเครือข่ายในอนาคต

โปรโตคอล SNIMP ได้พัฒนามาแล้ว 2 เวอร์ชันคือ SNMPv1 และ SNMPv2 ซึ่งทั้งสองเวอร์ชั่นมีหลายฟีเจอร์ที่เหมือนกัน แต่เวอร์ชั่น 2 จะมีส่วนที่ขยายเพิ่ม ส่วนเวอร์ชั่น 3 (SNMPv3)กำลังอยู่ในระหว่างการพัฒนา

RMON (Remote Monitoring) เป็นมาตรฐานที่ใช้สำหรับเฝ้าดู หรือมอนิเตอร์เครือข่ายซึ่งเป็นเครื่องมือที่ช่วยให้ผู้ดูและระบบสามารถทำงานได้ง่ายขึ้น มาตรฐาน RMON ได้กำหนดสถิติต่างๆ และฟังก์ชันที่สามารถแลกเปลี่ยนได้ระหว่างโปรแกรมเมเนเจอร์ (Console Manager) และเน็ตเวิร์คโพรบ

(Network Monitoring) ดังนั้น RMON จึงสามารถให้ข้อมูลกับผู้ดูแลระบบที่เกี่ยวกับการวิเคราะห์ค้นหาจุดบกพร่อง (Fault Diagnosis) และสามารถปรับต่างเพื่อเพิ่มประสิทธิภาะให้กับเครือข่ายได้

RMON มีการพัฒนาอยู่ 2 เวอร์ชันคือ เวอร์ชัน 1 (RMON1 หรือ RMONv1) และเวอร์ชัน 2 (RMON2 หรือ RMONv2) โดย RMON1 จะกำหนดกลุ่มของ MIB อยู่ 10 กลุ่มสำหรับการมอนิเตอร์เครือข่ายพื้นฐาน ซึ่งฟีเจอร์นี้มักจะพบในอุปกรณ์เครือข่ายโดยทั่วไป ส่วน RMON2 เป็นส่วนขยายของ RMON1 ซึ่งจะเน้นบริหารจัดการโปรโตคอลที่อยู่เหนือกว่าเลเยอร์ MAC (MediumAccess Control) โดยRMON2 จะเน้นที่ทราฟฟิกในระดับ IP และระดับแอพพลิเคชัน ซอฟต์แวร์ที่ใช้โปรโตคอล RMON2 สามารถมอนิเตอร์ทราฟฟิกในทุกๆ เลเยอร์ ซึ่งจะแตกต่าง ROMON1 ที่มอเตอร์ได้เฉพราะทราฟฟิกในระดับ MAC เลเยอร์หรือต่ำกว่า

ซอฟต์แวร์บริหารจัดการเครือข่าย

ระบบบริหารเครือข่าย หรือ NMS (Network Management System) เป็นแอพพลิเคชันที่รันบนเซิร์ฟเวอร์ที่อยู่ศูนย์ควบคุมเครือข่าย NMS เป็นศูนย์ควบคุมการบริการเครือข่ายซึ่งทำหน้าที่รวบรวม จัดเก็บ วิเคราะห์ และแสดงข้อมูลเกี่ยวกับการบริหารเครือข่าย นอกจากนี้ยังเป็นเครื่องมือสำหรับผู้บริหารเครือข่ายที่ใช้จัดการกับอุปกรณ์เครือข่าย และข้อมูลต่างๆ ที่เกี่ยวกับเครือข่ายนี้จะจัดเก็บใน MIB (Management Information Base) ซึ่งจัดเก็บไว้ที่ NMS และอุปกรณ์แต่ละตัว

ระบบบริหารเครือข่าย NMS ที่นิยมใช้งานมีหลายบรษัท ซึ่งส่วนใหญ่ก็เป็นบรษัทที่ผลิตอุปกรณ์เครือข่าย เช่น Cisco, 3COM, Nortel ซึ่งซฮฟต์แวร์นี้จะมีมาพร้อมกับอุปกรณ์เครือข่ายที่จัดซื้อจะใช้ได้กับเฉพาะอุปกรณ์ที่ผลิตโดยบริษัทเท่านั้น แต่ก็ยังมีซอฟต์แวร์ไปทั่วที่สามารถใช้ได้กับฮาร์ดแวร์ที่รองรับมาตรฐาน SNMP

Tivoli NetView

IBM Tivoli NetView มีความสามารถคือ เรียนรู้ระบบเครือข่าย TCP/IP แสดงโทโปโลยีของเครือข่าย จัดการอีเวนต์และแทรบ (TRAP) ของ SNMP มอนิเตอร์การใช้งานเครือข่าย และเก็บรวบรวมข้อมูลเกี่ยวกับประสิทธิภาพของอุปกรณ์เครือข่าย

CiscoWorks

CiscoWorks เป็นซอฟต์แวร์ NMS ของซิสโก้ที่ใช้สำหรับการบริหารจัดการอุปกรณ์ของซิสโก้เอง CiscoWork มีหลายโมดูลสำหรับการบริหารจัดการอุปกรณ์เครือข่ายที่มีฟังก์ชันที่แตกต่างกันเมื่อใดก็ตามที่เครือข่ายที่ส่วนใหญ่ใช้ผลิตภัณฑ์ของซิสโก้ เครื่องมือนี้ก็จะมีประโยชน์มากสำหรับดูแลเครือข่าย

HP OpenView

HP OpenView เป็น NMS ที่ได้รับความนิยมมากที่สุดในปัจจุบัน ซึ่งสามารถจัดการเครือข่าย ระบบแอพพลิเคชัน และเซอร์วิสในเครือข่าย OpenView จะแบ่งการจัดการออกเป็นโมดูลโดยแยกเป็นไลเซนต์ที่ต้องซื้อเพิ่มเติม การทำงานของ OpenView ก็จะเหมือน NMS ทั่วไปที่ใช้โปรโตคอล SNMP เพื่อเรียกดูข้อมูลของอุปกรณ์เครือข่ายหรือเซิร์ฟเวอร์ นอกจากนั้นยังใช้เทคนิคพูลลิง เพื่อมอมิเตอร์เซอร์วิสต่างๆ ที่กำหนดโดยผู้ดูแลระบบ

JFFNMS

JFFNMS เป็น nsm ที่ออกแบบสำหรับการมอนิเตอร์เครือข่ายโดยใช้โปรโตคอล SNMP, Syslog, Tacacs ดังนั้น JFFNMS สามารถมอนิเตอร์อุปกรณ์เครือข่ายที่รองรับโปรโคอล SNMP เช่น เซิร์ฟเวอร์ เราท์เตอร์ สวิตช์ หรือแม้กระทั่ง TCP port ที่เปิดให้ เป็นโอเพ่นซอร์สที่เขียนโดยใช้ภาษา PHP และฐานข้อมูล MYSQL หรือ PostgreSQL ซึ่งมิเตอร์เฟสเป็นเว็บทำให้ผู้ดูแลระบบสามารภเข้ามาดูในข้อมูลจากที่ใดก็ได้ในเครือข่าย

OpenNMS

OpenNMS เป็น NMS ระดับเอ็นเตอร์ไพรส์และโอเพ่นซอร์สซอฟแวร์ด้วย OpenNMS เป็นเครื่องมือที่เขียนโดยใช้ภาษา JAVA และอินเตอร์เฟสจะเป็นเว็บเบส ซึ่งภาษา JSP ในการสร้างเว็บเพจนั่นนั่นเอง OpenNMS ก็มีฟังก์ชันเหมือน NMS ทั่วไปกล่าวคือ OpenNMS จะใช้โปรโตคอลSNMP ในการมอนิเตอร์และบริหารจัดการเครือข่าย

MRTHG

MRTHG เป็นเครื่องมือที่ใช้สำหรับการมอนิเตอร์ดูทราฟฟิกหรือแบนด์วิธของลิงค์ในเครือข่าย MRTG เป็นโอเพ่นซอร์สที่พัฒนาโดย Tobi Oetiker และ Dave Rand

โดยการทำงานของ MRTG จะมีการสร้างเว็บเพจที่ประกอบด้วยภาพ (กราฟ) ชนิด PNGโดยภาพดังกล่าวจะแสดงถึงปริมาณของทราฟฟิกบนเครือข่าย ซึ่งการใช้งานส่วนใหญ่ก็จะนำมาไปมอนิเตอร์ดูทราฟฟิกตามพอร์ตต่างๆ ของเราท์เตอร์หรือสวิตซ์ ว่ามีทราฟฟิกหนาแน่นขนาดไหน

RRDtool-CACTI

RRDTOOL (ROUND ROBIN DATABASE) เป็นเครื่องมือมาตรฐานสำหรับการเก็บล็อกแล้วสร้างกราฟจากข้อมูลสถิติได้จากล็อก นอกจากแบนด์วิธของเครือข่าย RRDTOOL ยังสามารถสร้างกราฟประเภทอื่น เช่น อุณหภูมิของห้อง, โหลดของเซิร์ฟเวอร์ เช่น CPU, RAM เป็นต้น