บทที่ 8
การรักษาความปลอดภัยระบบเครือข่าย

การวางแผนสำหรับความปลอดภัยเป็นส่วนประกอบสำคัญอย่างหนึ่งของการออกแบบระบบเครือข่าย การดำเนินงานตามแผน การติดตั้งอุปกรณ์รักษาความปลอดภัยให้กับระบบเครือข่ายนั้นง่ายยิ่งกว่าการฟื้นฟูระบบเครือข่ายจากการที่ข้อมูลสูญหาย ในสภาวะแวดล้อมการใช้งานระบบเครือข่ายจะต้องแน่ใจได้ว่าข้อมูลที่สำคัญจะต้องปลอดภัยและยังคงเป็นความลับต่อผู้ที่ไม่ได้รับอนุญาตให้ใช้งาน การสร้างความปลอดภัยให้กับข้อมูลที่สำคัญ จึงนับว่ามีความสำคัญเท่ากับการปกป้องระบบเครือข่ายจากความเสียหายที่อาจเกิดขึ้นโดยตั้งใจ หรือไม่ได้ตั้งใจ

การรักษาความปลอดภัยของระบบเครือข่ายจำเป็นต้องมีความสมดุลระหว่างการช่วยให้ผู้ใช้ที่ได้รับสิทธิการใช้งานสามารถเข้าถึงข้อมูลได้โดยง่าย กับการป้องกันไม่ให้ผู้ใช้ที่ไม่ได้รับสิทธิการใช้งานสามารถเข้าถึงข้อมูลได้ ในการสร้างความสมดุลนี้จึงเป็นหน้าที่ของผู้บริหารระบบเครือข่าย

8.1 การวางแผนสำหรับความปลอดภัยของระบบเครือข่าย

บางครั้งอาจมีการนำระบบการรักษาความปลอดภัยระบบเครือข่ายมาผนวกใช้ภายหลังจากที่เริ่มมีข้อมูลสำคัญในระบบเครือข่ายโดยไม่มีการวางแผนล่วงหน้า ดังนั้นหากต้องการให้มั่นใจว่าข้อมูลที่มีค่าเหล่านั้นจะปลอดภัยจึงควรมีการวางแผนการรักษาความปลอดภัยระบบเครือข่ายตั้งแต่เริ่มจัดตั้งระบบเครือข่าย สิ่งที่นับว่าเป็นภัยต่อระบบการรักษาความปลอดภัยให้กับข้อมูลในระบบเครือข่ายมีอยู่ 4 ประการคือ

- การสอดแนมเข้าไปในระบบเครือข่ายโดยไม่ได้รับอนุญาต
- การแทรกแซงของกระแสไฟฟ้า
- การโจรกรรมข้อมูล
- ความเสียหายที่เกิดขึ้นโดยตั้งใจหรือไม่ได้ตั้งใจ

ถึงแม้ว่าสิ่งต่างๆ ที่เป็นภัยต่อระบบการรักษาความปลอดภัยให้กับข้อมูลในระบบเครือข่ายเหล่านี้ จะส่งผลกระทบต่อระบบเครือข่าย แต่การรักษาความปลอดภัยของข้อมูลก็ไม่ได้เป็นตัวกำหนดการทำงาน หรือสนับสนุนความต้องการในการใช้งานระบบเครือข่ายอย่างถูกต้องสมบูรณ์เสมอไป ดังนั้นงานของผู้บริหารระบบเครือข่ายก็คือการสร้างความมั่นใจว่าระบบเครือข่ายจะยังคงมีความน่าเชื่อถือ และปลอดภัยจากภัยต่างๆ เหล่านี้

8.1.1 ระดับของการรักษาความปลอดภัย

การพิจารณาขยายระดับของการรักษาความปลอดภัยขึ้นอยู่กับสภาวะแวดล้อมที่ระบบเครือข่ายดำเนินงานอยู่ ตัวอย่างเช่นระบบเครือข่ายที่จัดเก็บข้อมูลการเงินที่สำคัญของลูกค้าในระบบเครือข่ายธนาคาร จำเป็นต้องมีระดับการรักษาความปลอดภัยให้กับข้อมูลเหล่านั้นสูงกว่าระบบเครือข่ายท้องถิ่นที่ใช้ในการแบ่งปันการใช้เครื่องพิมพ์ร่วมกัน เพื่อพิมพ์เอกสารต่างๆ ขององค์กร

8.1.2 การกำหนดนโยบาย

การสร้างความปลอดภัยในระบบเครือข่ายจำเป็นต้องสร้างระเบียบวินัย กฎเกณฑ์ และนโยบายต่างๆ เพื่อป้องกันการเกิดสิ่งที่ไม่คาดคิด ก้าวแรกในการนำไปสู่ความเชื่อมั่นในความปลอดภัยของข้อมูลคือการดำเนินการตามนโยบายที่เตรียมการไว้ นโยบายต่างๆ เหล่านี้จะช่วยแนะนำผู้บริหารระบบและผู้ใช้เกี่ยวกับการเปลี่ยนแปลงต่างๆ ในการพัฒนาระบบเครือข่ายอันเกิดจากสิ่งที่คาดหวังและไม่ได้คาดหวังไว้

8.1.3 การป้องกัน

วิธีการที่ดีที่สุดในการวางนโยบายให้กับระบบการรักษาความปลอดภัยให้กับข้อมูล คือการป้องกันไว้ก่อน (**Proactive**) เป็นการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลได้ การวางระบบจะเน้นไปที่การป้องกันล่วงหน้า ซึ่งจำเป็นต้องให้ผู้บริหารระบบเครือข่ายสามารถใช้เครื่องมือ และทราบวิธีการรักษาความปลอดภัยข้อมูลตามนโยบายที่กำหนดอย่างถ่องแท้

8.1.4 การตรวจสอบความถูกต้อง

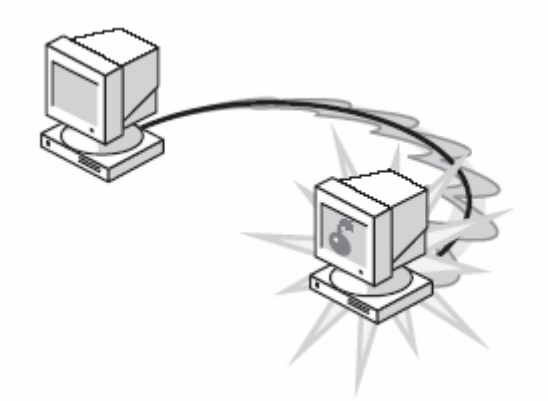
ในการ **logon** เข้าไปในระบบเครือข่าย ผู้ใช้จะต้องใส่ชื่อบัญชีผู้ใช้และรหัสผ่านอย่างถูกต้อง ระบบการรับรองความถูกต้องของรหัสผ่านจึงเป็นด่านแรกในการป้องกันผู้ใช้ที่ไม่ได้รับอนุญาตให้ใช้งานระบบเครือข่าย เนื่องจากรหัสผ่านจะถูกเชื่อมโยงกับบัญชีผู้ใช้งานระบบเครือข่าย สิ่งสำคัญในการรับรองความถูกต้อง คือต้องไม่มอบความไว้วางใจจนเกินไปจนกระทั่งนำไปสู่กระบวนการอันจะทำให้ระบบการรักษาความปลอดภัยเกิดความล้มเหลว เช่น ในระบบเครือข่ายแบบ **Peer-to-Peer** ผู้ใช้สามารถ **logon** เข้าสู่ระบบโดยบัญชีผู้ใช้งานและรหัสผ่านส่วนตัว ดังนั้นผู้ใช้งานนั้นจะสามารถเข้าไปใช้ทรัพยากรใดๆ ที่ได้รับการแบ่งปันให้ใช้งานบนระบบเครือข่ายได้

การตรวจสอบความถูกต้องของชื่อบัญชีผู้ใช้งานและรหัสผ่านจะทำงานได้ในการรักษาความปลอดภัยบนระบบเครือข่ายแบบ **Server-Based** โดยมีการตรวจสอบความเข้ากันได้ของชื่อบัญชีผู้ใช้งานกับรหัสผ่านจากฐานข้อมูลของระบบการรักษาความปลอดภัยบนระบบเครือข่าย ดังนั้นสิ่งที่สำคัญที่สุดในการรักษาความปลอดภัยคือความร่วมมือจากผู้ใช้ที่จะต้องรักษาสิทธิในการใช้งานระบบเครือข่ายของตนเอง โดยไม่มอบชื่อบัญชีผู้ใช้และรหัสผ่านให้กับผู้อื่นเพื่อเข้ามาใช้งานในระบบเครือข่าย

8.1.5 การฝึกฝน

ความผิดพลาดที่เกิดจากความไม่ตั้งใจอาจนำไปสู่ความล้มเหลวของระบบการรักษาความปลอดภัยได้ ดังนั้นผู้ใช้ที่ได้รับการฝึกฝนเป็นอย่างดีจะสร้างความเสียหายให้กับระบบเครือข่ายได้น้อยกว่าผู้ใช้ที่ไม่มีประสบการณ์การใช้งาน การพัฒนาตนเองจึงเป็นสิ่งสำคัญที่ช่วยให้ความผิดพลาดโดยไม่ได้ตั้งใจเกิดขึ้นน้อยลง ซึ่งอาจเป็นสาเหตุให้แหล่งทรัพยากรข้อมูลที่สำคัญถูกทำลายโดยบังเอิญอย่างถาวร

ผู้บริหารระบบเครือข่ายควรสร้างความมั่นใจว่าทุกคนที่ใช้ระบบเครือข่ายมีความคุ้นเคยกับขั้นตอนการปฏิบัติงานและระบบการรักษาความปลอดภัย โดยผู้บริหารระบบอาจหาแนวทางการพัฒนาอย่างง่ายและชัดเจนมาแนะนำให้กับผู้ใช้ และอธิบายในสิ่งที่ผู้ใช้จำเป็นต้องทราบ และกำหนดให้ผู้ใช้รายใหม่ได้รับการฝึกอบรมที่เหมาะสมตามระดับการใช้งานและสิทธิที่ได้รับ



รูปที่ 8 – 1 การฝึกฝนของผู้ใช้ช่วยลดความผิดพลาดราคาแพง

8.2 อุปกรณ์การรักษาความปลอดภัย

ขั้นแรกในการรักษาความปลอดภัยให้กับข้อมูลคือการเตรียมอุปกรณ์การรักษาความปลอดภัยในระบบเครือข่ายให้พร้อม การสร้างสภาวะแวดล้อมทางกายภาพที่ดีที่สุดสำหรับระบบเครือข่ายจึงนับว่ามีความสำคัญ สำหรับขอบเขตของระบบการรักษาความปลอดภัยข้อมูลจะขึ้นอยู่กับขนาดขององค์กร ความสำคัญของข้อมูล และแหล่งข้อมูลที่มี การที่ระบบเครือข่ายแบบ **Peer-to-Peer** ไม่มีนโยบายการรักษาความปลอดภัย ผู้ใช้จึงต้องเป็นผู้รับผิดชอบในความปลอดภัยของเครื่องคอมพิวเตอร์และข้อมูลภายในเครื่องคอมพิวเตอร์ของตนเอง สำหรับการรักษาความปลอดภัยในระบบเครือข่ายแบบ **Server-Based** จึงเป็นหน้าที่ของผู้บริหารระบบเครือข่าย

8.2.1 ความปลอดภัยของเครื่องเซิร์ฟเวอร์

ในระบบเครือข่ายขนาดใหญ่ที่มีเครื่องเซิร์ฟเวอร์เป็นศูนย์รวมในการจัดเก็บข้อมูลของผู้ใช้แต่ละคนและเป็นศูนย์รวมในการจัดเก็บข้อมูลที่สำคัญขององค์กรเป็นจำนวนมาก จึงมีความจำเป็นที่จะต้องจัดตั้งระบบการรักษาความปลอดภัยให้กับเครื่องเซิร์ฟเวอร์โดยเฉพาะ

ตามปกติผู้บริหารระบบเครือข่ายจะเป็นผู้ดำเนินการแก้ไขปัญหาทางเทคนิคเมื่อเครื่องเซิร์ฟเวอร์มีปัญหาซึ่งพวกเขาเหล่านั้นอาจจะทราบหรือไม่ทราบว่าพวกเขากำลังทำอะไรอยู่ วิธีที่ดีที่สุดในการดูแลป้องกันเครื่องเซิร์ฟเวอร์คือการล็อคเครื่องเซิร์ฟเวอร์ไว้ในห้องคอมพิวเตอร์โดยเฉพาะ และจำกัดการเข้าถึงข้อมูลในเครื่องเซิร์ฟเวอร์ต่างๆ ตามความจำเป็น การพิจารณาจัดตั้งอุปกรณ์การรักษาความปลอดภัยให้กับเครื่องเซิร์ฟเวอร์ จะขึ้นอยู่กับขนาดขององค์กรและความสำคัญของข้อมูล บางองค์กรอาจต้องการเพียงการล็อคเครื่องเซิร์ฟเวอร์ไว้ในตู้เก็บของขนาดใหญ่ในสำนักงาน แต่บางองค์กรอาจจะต้องสร้างห้องโดยเฉพาะสำหรับจัดเก็บเครื่องเซิร์ฟเวอร์

8.2.2 ความปลอดภัยของสายเคเบิล

สายเคเบิลที่ใช้พื้นฐานของลวดทองแดง เช่นสายโคแอ็กเชียล ข้อมูลจะเดินทางไปตามสายเคเบิลในรูปแบบของสัญญาณทางไฟฟ้า ดังนั้นข้อมูลอาจถูกตรวจจับโดยอุปกรณ์ตรวจจับทางอิเล็กทรอนิกส์ได้ จึงเป็นช่องทางหนึ่งที่บุคคลภายนอกอาจเจาะเข้าไปในสายเคเบิลเพื่อดักจับข้อมูลโดยตรงจากสายสัญญาณข้อมูลพื้นฐาน การพิจารณาเส้นทางการวางสายเคเบิลที่มีข้อมูลสำคัญจึงควรอยู่ในเส้นทางที่สามารถเข้าถึงได้โดยผู้ที่ได้รับสิทธิการเข้าถึงโดยถูกต้องเท่านั้น การวางแผนอย่างเหมาะสมจะทำให้ผู้ที่ไม่ได้รับสิทธิการเข้าถึงอย่างถูกต้องไม่สามารถเข้าไปถึงสายเคเบิลเหล่านั้นได้

เช่นการเดินสายเคเบิลตามรูปแบบของการรักษาความปลอดภัย (Security Model) ตามมาตรฐานการเดินสายในอาคาร จะแนะนำให้เดินสายเคเบิลภายในโครงสร้างของอาคารผ่านช่องว่างใต้ฝ้าเพดาน หรือวางท่อตามกำแพงและพื้น

8.3 ความปลอดภัยของข้อมูล

หลังจากการดำเนินการรักษาความปลอดภัยให้กับส่วนประกอบทางกายภาพแล้ว ผู้บริหารระบบเครือข่ายจะต้องทำให้มั่นใจได้ว่าแหล่งข้อมูลของระบบเครือข่ายจะปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตให้ใช้ระบบ หรือเกิดความเสียหายขึ้นโดยบังเอิญหรือไตร่ตรองไว้ก่อนได้ นโยบายในการมอบหมายความรับผิดชอบ การอนุญาต และให้สิทธิการใช้งานแหล่งข้อมูลบนระบบเครือข่ายจึงเป็นหัวใจสำคัญของการรักษาความปลอดภัยในระบบเครือข่าย รูปแบบการรักษาความปลอดภัยที่ได้รับการพัฒนาขึ้นเพื่อรักษาข้อมูลให้ปลอดภัยมี 2 รูปแบบ คือการแบ่งปันการใช้ทรัพยากรโดยมีรหัสผ่านและการกำหนดสิทธิการใช้งาน รูปแบบนี้เรียกว่า "**Share-level Security**" (สำหรับการดำเนินงานโดยใช้ **Password Protected Shares**) และเรียกว่า "**User-level Security**" (สำหรับการดำเนินงานโดยใช้ **Access Permission**)

8.3.1 การแบ่งปันการใช้ทรัพยากรโดยมีรหัสผ่าน

ในรูปแบบของการรักษาความปลอดภัยโดยใช้ **Password Protected Shares** จะมีการกำหนดรหัสผ่าน (**Password**) ให้กับแหล่งข้อมูลที่ใช้ร่วมกันบนระบบเครือข่าย การเข้าถึงแหล่งข้อมูลดังกล่าวจะได้รับการอนุญาตก็ต่อเมื่อผู้ใช้ใส่รหัสผ่านที่ถูกต้องเท่านั้น โดยทั่วไปในระบบปฏิบัติการเครือข่ายจะจัดให้มีเครื่องมือเหล่านี้ อย่างไรก็ตามในระบบปฏิบัติการของเครื่องคอมพิวเตอร์ได้มีการพัฒนาให้สามารถรองรับการจัดตั้งระบบเครือข่ายแบบ **Peer-to-Peer** จึงมีคุณสมบัติเหล่านี้ในระดับที่น่าพึงพอใจ เช่นในระบบปฏิบัติการ **Windows 98** จะสามารถแบ่งปันการใช้ข้อมูลในไดเร็กทอรี่ได้ในรูปแบบต่างๆ ดังนี้

8.3.1.1 Read Only

ถ้าผู้ใช้กำหนดการแบ่งปันการใช้งานในรูปแบบ **Read Only** ผู้ใช้ที่มีสิทธิในการใช้งานระบบเครือข่ายจะสามารถ **access** เข้าไปยังไฟล์ต่างๆ ในไดเร็กทอรี่นั้นได้ พวกเขาจะสามารถเปิดดูเอกสาร คัดลอกมายังเครื่องของตนเองและพิมพ์เอกสารเหล่านั้นออกมาได้ แต่พวกเขาเหล่านั้นจะไม่สามารถทำการเปลี่ยนแปลง ปรับปรุง และแก้ไขเอกสารต้นฉบับซึ่งอยู่ในเครื่องคอมพิวเตอร์ของผู้อื่นได้

8.3.1.2 Full

ถ้าผู้ใช้กำหนดการแบ่งปันการใช้งานในรูปแบบ **Full** ผู้ใช้ที่มีสิทธิในการใช้งานระบบเครือข่ายจะสามารถ **access** เข้าไปยังไฟล์ต่างๆ ในไดเร็กทอรี่นั้นได้ และมีสิทธิในการกระทำกับไฟล์เหล่านั้นได้อย่างเต็มที่ นั่นคือสามารถเรียกดู คัดลอก ปรับปรุง แก้ไข ลบหรือเพิ่มไฟล์เข้าไปในไดเร็กทอรี่นั้นได้

8.3.1.3 Depend on Password

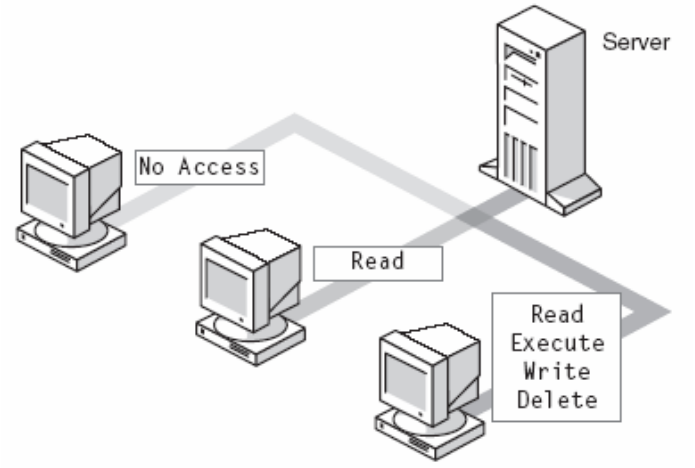
ถ้าผู้ใช้กำหนดการแบ่งปันการใช้งานในรูปแบบ **Depend on Password** ผู้ใช้ที่มีสิทธิในการใช้งานระบบเครือข่ายจะสามารถ **access** เข้าไปยังไฟล์ต่างๆ ในไดเร็กทอรี่นั้นได้ก็ต่อเมื่อผู้ใช้นั้นใส่รหัสผ่านได้อย่างถูกต้อง นอกจากนั้นผู้ที่เป็นเจ้าของทรัพยากรยังสามารถระบุได้ว่าเมื่ออนุญาตให้เข้ามายังทรัพยากรของตนเองแล้ว จะให้สิทธิในการใช้งานอย่างไร คือ **Read Only** หรือ **Full Access**

8.3.2 การกำหนดสิทธิการใช้งาน

การรักษาความปลอดภัยโดยกำหนดสิทธิการใช้จะเกี่ยวข้องกับการมอบหมายสิทธิการใช้งานให้กับผู้ใช้แต่ละคนตามระดับของการรักษาความปลอดภัย ในขณะที่ผู้ใช้ต้องการที่จะ **access** เข้าไปยังระบบเครือข่าย ผู้ใช้จะต้องพิมพ์รหัสผ่านที่ได้รับมอบ จากนั้นเครื่องเซิร์ฟเวอร์จะทำการตรวจสอบความถูกต้องของรหัสผ่าน จากข้อมูลที่มีอยู่ในระบบฐานข้อมูลการรักษาความปลอดภัยในเครื่องเซิร์ฟเวอร์ และอนุญาตหรือปฏิเสธการเข้าถึงแหล่งทรัพยากรที่แบ่งปันการใช้ร่วมกันบนระบบเครือข่าย การรักษาความปลอดภัยโดยกำหนดสิทธิการใช้งานจะมีระดับในการรักษาความปลอดภัยที่สูงกว่าการใช้รหัสผ่าน และการให้สิทธิการใช้งานจะทำได้ง่ายกว่าจึงเป็นที่นิยมใช้มากกว่าในองค์กรขนาดใหญ่

8.3.3 ความปลอดภัยของแหล่งข้อมูล

หลังจากที่ผู้ใช้ได้รับการตรวจสอบสิทธิการใช้งานอย่างถูกต้อง และได้รับอนุญาตให้เข้าไปในระบบเครือข่ายแล้ว ระบบการรักษาความปลอดภัยจะจัดให้ผู้ใช้เหล่านั้นเข้าไปยังแหล่งทรัพยากรที่เหมาะสม การที่ผู้ใช้มีรหัสผ่านและได้รับการอนุญาตให้เข้าไปใช้ข้อมูลได้ จึงเปรียบเหมือนรั้วของระบบการรักษาความปลอดภัยซึ่งทำหน้าที่คุ้มกัน ดูแล แหล่งทรัพยากรแต่ละแห่ง โดยมีประตูเข้าได้หลายทาง ผู้ใช้จะได้รับสิทธิในการเข้าถึงข้อมูลได้เฉพาะทางประตูเข้าที่ได้รับอนุญาตเท่านั้น นอกจากนั้นผู้บริหารระบบเครือข่ายจะสามารถตัดสินใจได้ว่าผู้ใช้คนใดจะได้รับอนุญาตให้มีสิทธิการใช้งานที่พิเศษมากขึ้นในการเข้าถึงแหล่งข้อมูล โดยวิธีการควบคุมการให้สิทธิ **(Permission Control)**



รูปที่ 8 – 2 วิธีการควบคุมการให้สิทธิการเข้าถึงแหล่งข้อมูล

คุณสมบัติการกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลของระบบปฏิบัติการเครือข่ายที่แตกต่างกัน จะใช้ชื่อเรียกไม่เหมือนกัน ตารางที่ 8 – 1 เป็นตัวอย่างการให้สิทธิโดยทั่วไปของระบบปฏิบัติการ **Windows NT Server**

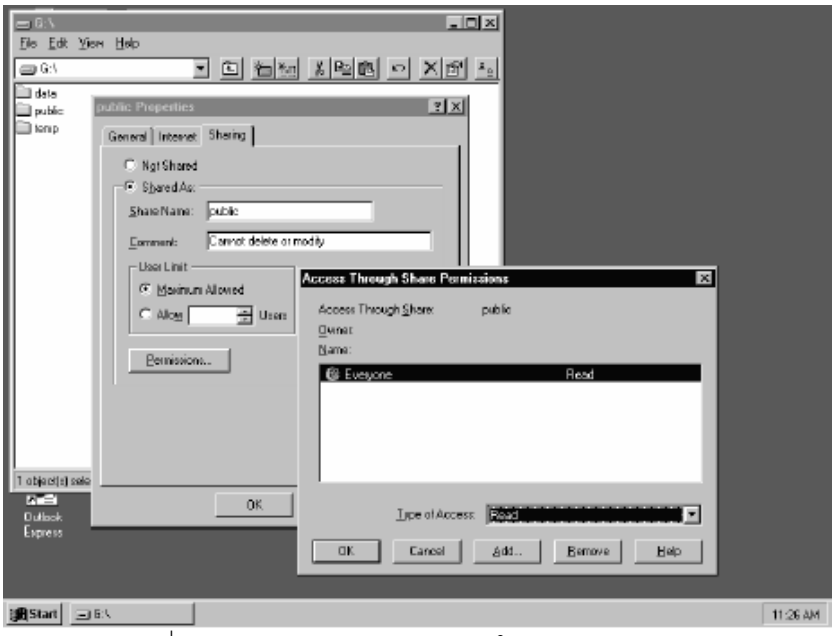
ตารางที่ 8 – 1 **Windows NT Server Permission**

Permission	Functionality
Read	Reads and copies files in the shared directory.
Execute	Runs (executes) the files in the directory.
Write	Creates new files in the directory.
Delete	Deletes files in the directory.
No Access	Prevents the user from gaining access to directories, files, or resources.

8.3.4 การกำหนดสิทธิสำหรับกลุ่มผู้ใช้

งานของผู้บริหารระบบเครือข่ายจะรวมถึงการกำหนดสิทธิการใช้งานที่เหมาะสมให้กับผู้ใช้แต่ละราย ซึ่งอาจมีผู้ใช้หลายรายที่ได้รับสิทธิในการเข้าถึงข้อมูล และแหล่งทรัพยากรอย่างอื่นในระดับเดียวกัน วิธีการดำเนินการที่มีประสิทธิภาพอย่างหนึ่งคือการกำหนดสิทธิผ่านกลุ่มบัญชีผู้ใช้งาน วิธีการนี้จะมีประโยชน์เป็นอย่างมากในองค์กรขนาดใหญ่ที่มีผู้ใช้งานระบบเครือข่ายเป็นจำนวนมาก

การกำหนดให้ผู้ใช้แต่ละรายอยู่ในกลุ่มบัญชีผู้ใช้ที่เหมาะสมจะมีความสะดวกในการบริหารจัดการมากกว่าการกำหนดสิทธิให้กับผู้ใช้แต่ละราย เช่นการกำหนดให้กลุ่ม **Everyone** มีสิทธิในระดับ **Read Acces** สำหรับการ **access** เข้าไปยัง **Public Directory** เป็นต้น รูปที่ 8 – 3 แสดงให้เห็นการใช้เครื่องมือใน **Windows NT Server** กำหนดสิทธิให้กับกลุ่มผู้ใช้ **Everyone** ตามตัวอย่าง



รูปที่ 8 – 3 **Group Permission** ใน **Windows NT**

ตัวอย่างเช่น ผู้บริหารระบบเครือข่ายอาจจะสร้างกลุ่มผู้ตรวจสอบ **(Reviewer)** ให้ได้รับสิทธิในการเข้าไปยังไฟล์ข้อมูลของนักเรียนได้โดยสมบูรณ์ และมอบสิทธิในการเข้าไปถึงไฟล์ข้อมูลของนักเรียนได้เพียง **Read** ให้กับกลุ่มของคณะกรรมการ **(Faculty)** ดังนั้นคณะกรรมการการศึกษาจะสามารถเข้าไปอ่านไฟล์ของนักเรียนได้แต่ไม่สามารถทำการปรับปรุงแก้ไข หรือลบไฟล์เหล่านั้นได้

8.4 การเพิ่มระดับการรักษาความปลอดภัย

ผู้บริหารระบบเครือข่ายอาจจะพิจารณาเพิ่มระดับการรักษาความปลอดภัยให้กับระบบเครือข่ายได้หลายวิธี ทั้งนี้ขึ้นอยู่กับนโยบายการรักษาความปลอดภัย และความต้องการความปลอดภัยของข้อมูลในระบบเครือข่าย วิธีการต่างๆ เหล่านี้เป็นตัวเลือกที่ดีในการเพิ่มระดับการรักษาความปลอดภัยให้กับระบบเครือข่าย

8.4.1 จัดตั้งไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ (Firewall) หรือกำแพงไฟเป็นระบบการรักษาความปลอดภัยที่ผสมผสานระหว่างฮาร์ดแวร์กับซอฟต์แวร์ที่ใช้ในการปกป้องระบบเครือข่ายขององค์กรจากภัยคุกคามภายนอก ซึ่งมาจากเครือข่ายอื่นหรือเครือข่ายอินเตอร์เน็ต โดยไฟร์วอลล์จะป้องกันการติดต่อโดยตรงจากเครื่องคอมพิวเตอร์ในเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอก และในทางกลับกันก็จะป้องกันไม่ให้ผู้บุกรุกจากภายนอกสามารถ access เข้ามายังเครื่องคอมพิวเตอร์ในระบบเครือข่ายภายในองค์กรได้โดยตรง การติดต่อระหว่างระบบเครือข่ายจะต้องมีเส้นทางผ่านพร็อกซี่เซิร์ฟเวอร์ (Proxy Server) ซึ่งเป็นส่วนประกอบหนึ่งของไฟร์วอลล์ นอกจากนั้นไฟร์วอลล์ยังมีหน้าที่ในการตรวจสอบกิจกรรมต่างๆ ของระบบเครือข่าย บันทึกปริมาณการขนส่งข้อมูลผ่านระบบเครือข่าย และบันทึกข้อมูลเกี่ยวกับความพยายามที่จะเข้ามาในระบบอย่างไม่ถูกต้อง

พร็อกซี่เซิร์ฟเวอร์จะมีหน้าที่ในการจัดการกับการขนส่งแพ็กเก็ตข้อมูลระหว่างระบบเครือข่ายภายในองค์กรกับเครือข่ายอินเตอร์เน็ต โดยตัดสินใจว่ามีความปลอดภัยหรือไม่ที่จะให้ข้อมูลหรือไฟล์จากเครือข่ายอินเตอร์เน็ตถูกส่งผ่านเข้ามายังระบบเครือข่ายขององค์กร ทำการกลั่นกรอง และยกเลิกการร้องขอซึ่งผู้บริหารระบบเครือข่ายพิจารณาแล้วว่าไม่เหมาะสม รวมทั้งการร้องขอเข้าไปยังข้อมูลโดยผู้ใช้ซึ่งไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

8.4.2 ตรวจสอบการใช้งานระบบเครือข่าย

การพิจารณาทบทวนบันทึกเหตุการณ์ต่างๆ ที่เกิดขึ้นกับเครื่องเซิร์ฟเวอร์ เรียกว่า “การตรวจสอบ (Auditing)” กระบวนการนี้จะเป็นการเฝ้าติดตามกิจกรรมในระบบเครือข่ายของบัญชีผู้ใช้ต่างๆ การตรวจสอบควรเป็นงานประจำวันของระบบการรักษาความปลอดภัยให้กับเครือข่ายขององค์กร การตรวจสอบจะช่วยให้ผู้บริหารระบบเครือข่ายสามารถระบุกิจกรรมต่างๆ ที่เกิดขึ้นโดยไม่ได้รับการอนุญาตอย่างถูกต้อง และทำให้ทราบข้อมูลดังต่อไปนี้

- ความพยายามในการ logon เข้ามายังระบบเครือข่าย
- การติดต่อหรือขาดการติดต่อกับแหล่งทรัพยากรระบบเครือข่ายที่กำหนด
- การยุติการติดต่อ
- การใช้งานบัญชีผู้ใช้ไม่ได้
- การเปิด-ปิดไฟล์
- การสร้างหรือลบไฟล์ในไดเร็กทอรี่ที่ได้รับอนุญาต
- การปรับปรุงไดเร็กทอรี่
- เหตุการณ์ต่างๆ ที่เกิดขึ้นกับเครื่องเซิร์ฟเวอร์
- การเปลี่ยนรหัสผ่าน
- การเปลี่ยนปัจจัยในการ logon ของผู้ใช้

จะเห็นได้ว่าบันทึกการตรวจสอบจะช่วยให้ผู้บริหารระบบเครือข่ายสามารถระบุวิธีที่ระบบเครือข่ายถูกใช้งาน และวิเคราะห์ความพยายาม logon ที่ผิดปกติ และสามารถบอกได้ว่ากำลังมีผู้ใช้งานซึ่งไม่มีสิทธิพยายามที่จะเจาะเข้ามาในระบบเครือข่ายภายในองค์กร เพื่อที่จะได้วางแผนการป้องกันระบบเครือข่ายได้อย่างมีประสิทธิภาพ

8.4.3 การใช้เครื่องคอมพิวเตอร์ไร้ดิสก์ (Diskless Computer)

เครื่องคอมพิวเตอร์ไร้ดิสก์ หมายถึงเครื่องคอมพิวเตอร์ที่ไม่มีฟล้อปี้ดิสก์หรือฮาร์ดดิสก์ แต่สามารถทำงานทุกอย่างได้ตามปกติเหมือนกับเครื่องคอมพิวเตอร์ที่มีดิสก์ไดร์ฟทุกประการ ยกเว้นการบันทึกข้อมูลลงดิสก์ การใช้เครื่องคอมพิวเตอร์ไร้ดิสก์เป็นทางเลือกอย่างยอดเยี่ยมสำหรับการรักษาความปลอดภัยระบบเครือข่าย เพราะผู้ใช้จะไม่สามารถทำการดาวน์โหลดข้อมูลที่มีอันตรายเข้ามาในระบบได้

เครื่องคอมพิวเตอร์ไร้ดิสก์ไม่ต้องการ **Boot Disk** แต่จะทำการติดต่อกับเครื่องเซิร์ฟเวอร์ตลอดเวลา และทำการ **logon** ด้วย **ROM Boot chip** ชนิดพิเศษซึ่งติดตั้งอยู่กับการ์ดเชื่อมต่อระบบเครือข่ายของเครื่องคอมพิวเตอร์ เมื่อเปิดเครื่อง **ROM Boot chip** จะส่งสัญญาณออกไปยังเครื่องเซิร์ฟเวอร์ว่าพร้อมที่จะทำงาน และเครื่องเซิร์ฟเวอร์จะทำการจัดส่งข้อมูลหน้าจอแสดงการ **logon** ให้กับเครื่องคอมพิวเตอร์นั้นโดยเฉพาะ เมื่อผู้ใช้ต้องการเข้ามาใช้งานระบบเครือข่ายก็เพียงแต่พิมพ์ชื่อบัญชีผู้ใช้และรหัสผ่าน และหลังจาก **logon** เสร็จเรียบร้อยคอมพิวเตอร์ไร้ดิสก์เครื่องนั้นจะถูกเชื่อมโยงเข้ากับระบบเครือข่าย

ถึงแม้ว่าการใช้คอมพิวเตอร์ไร้ดิสก์ในระบบเครือข่ายจะช่วยให้ระดับของการรักษาความปลอดภัยสูงขึ้น แต่ก็มีข้อเสียคือการที่ไม่มีดิสก์ไดร์ในตัวเองจะทำให้ไม่สามารถจัดเก็บแอพพลิเคชั่น (**Application**) และข้อมูลไว้ได้เอง การดำเนินกิจกรรมทุกอย่างจะต้องถูกกระทำบนระบบเครือข่าย ความหนาแน่นในการขนส่งข้อมูลจะเพิ่มตามขึ้นมา ดังนั้นระบบเครือข่ายจึงจำเป็นต้องมีความสามารถในการจัดการกับความต้องการที่เพิ่มขึ้นตลอดเวลา

8.4.4 การเข้ารหัสข้อมูล (Data Encryption)

การใช้ยูทิลิตี้โปรแกรม **Data Encryption** จะทำให้ข้อมูลมีความหมายคลุมเครือก่อนที่จะส่งเข้าไปบนระบบเครือข่าย จึงไม่สามารถอ่านข้อมูลเหล่านั้นได้อย่างถูกต้องถึงแม้ว่าจะสามารถเจาะสายเคเบิลเข้าไปดักจับข้อมูลนั้นในขณะที่ทำการส่งผ่านสายเคเบิลระบบเครือข่ายได้ก็ตาม แต่เมื่อข้อมูลที่มีความหมายคลุมเครือเหล่านั้นเดินทางมาถึงเครื่องคอมพิวเตอร์ปลายทาง รหัสข้อมูลเดียวกันที่ใส่ไว้ในเครื่องคอมพิวเตอร์ปลายทางจะช่วยในการถอดรหัสและทำการแปลข้อมูลเหล่านั้นให้มีความหมายอย่างถูกต้อง ระบบการรักษาความปลอดภัยโดยการเข้ารหัสข้อมูลที่ดีที่สุดจะเป็นฮาร์ดแวร์ซึ่งมีหน้าที่ในการเข้ารหัสและถอดรหัสโดยเฉพาะ แต่ก็มีราคาแพง

มาตรฐานโดยทั่วไปของการเข้ารหัสข้อมูลคือ **DES (Data Encryption Standard)** ที่ได้รับการพัฒนาโดยบริษัท **IBM** ถูกนำมาใช้เป็นครั้งแรกในปี ค.ศ.**1975** โดยรัฐบาลกลางของประเทศสหรัฐอเมริกา มาตรฐานนี้จะกำหนดรายละเอียดในการเข้ารหัสข้อมูลที่ส่งบนระบบเครือข่ายคอมพิวเตอร์ พร้อมทั้งอธิบายคำจำกัดความต่างๆ โดยที่จะต้องใช้ **DES** ในการ **access** เข้าไปยังข้อมูล ทั้งด้านผู้ส่งและผู้รับ อย่างไรก็ตามภายหลังได้ยกเลิกมาตรฐาน **DES** เนื่องจากตรวจพบว่ามีการดักรับสัญญาณข้อมูลที่เข้ารหัสเหล่านั้นได้

ในปัจจุบันรัฐบาลกลางของประเทศสหรัฐอเมริกาได้ใช้มาตรฐานใหม่ที่เรียกว่า **CCEP (Commercial COMSEC Endorsement Program)** ซึ่งกำหนดโดยองค์กรมาตรฐานสากล หรือ **NSA (The National Security Agency)** ในมาตรฐานนี้ได้อนุญาตให้ผู้จำหน่ายมีสิทธิในการร้องขอการเข้าร่วมในการผลิตอุปกรณ์การสร้างระบบการรักษาความปลอดภัยที่เหมาะสมจะเข้าร่วมใน **CCEP** และเมื่อได้รับการรับรอง จะทำให้ระบบเครือข่ายมีความปลอดภัยมากยิ่งขึ้นถ้าผู้บริหารระบบเครือข่ายเลือกใช้ผลิตภัณฑ์จากผู้จำหน่ายรายที่ได้รับการรับรอง

8.5 ไวรัสคอมพิวเตอร์ (Computer Virus)

ไวรัสคอมพิวเตอร์กลายเป็นส่วนหนึ่งในชีวิตการใช้งานบนระบบเครือข่าย การพบเห็นรายงานข่าวเกี่ยวกับไวรัสคอมพิวเตอร์ตัวใหม่ล่าสุด หรือคำเตือนเกี่ยวกับผลกระทบที่เกิดจากไวรัสตัวนั้นๆ เริ่มที่จะเป็นเรื่องปกติธรรมดาที่เกิดขึ้นในโลกยุคปัจจุบัน ไวรัสคอมพิวเตอร์เป็นกลุ่มของโปรแกรมคอมพิวเตอร์ หรือโปรแกรมเล็กๆ เพียงไม่กี่บิตที่ซ่อนตัวอยู่ในโปรแกรมคอมพิวเตอร์หรือข้อมูลข่าวสารบนระบบเครือข่าย เมื่อเครื่องคอมพิวเตอร์ติดไวรัส ซึ่งโดยมากจะเข้าไปฝังตัวอยู่ใน **Boot Sector** ของอุปกรณ์จัดเก็บข้อมูล เช่นฟล็อปปี้ดิสก์หรือฮาร์ดดิสก์ หรือในหน่วยความจำ **RAM** จุดประสงค์หลักของไวรัสคอมพิวเตอร์คือการเพิ่มจำนวนของตัวมันเองให้มากที่สุดเท่าที่จะทำได้ และเข้าไปทำลายโปรแกรมระบบปฏิบัติการหรือโปรแกรมประยุกต์ที่ติดไวรัส ไวรัสคอมพิวเตอร์จะกลายเป็นสิ่งที่คอยรบกวนผู้ใช้งานตลอดเวลาเพราะอาจจะเข้าไปทำลายไฟล์ข้อมูลที่สำคัญของผู้ใช้ และอาจจะส่งผลกระทบจนถึงกับทำให้ระบบเครือข่ายล่มทั้งระบบก็เป็นได้

ไวรัสคอมพิวเตอร์ถูกจัดแบ่งตามวิธีการเพิ่มจำนวนของตัวเองออกเป็น 2 ประเภทคือ **Boot Sector Virus** เมื่อเครื่องคอมพิวเตอร์ติดไวรัสประเภทนี้ ในขณะที่เริ่มทำการ **Boot** เครื่อง ไวรัสจะเริ่มดำเนินการ และสร้างความเสียหายให้กับฮาร์ดดิสก์ และเมื่อมีการ **access** เข้ามายังฮาร์ดดิสก์ที่ติดไวรัส จะทำให้ไวรัสเกิดการเคลื่อนย้ายไปยังคอมพิวเตอร์เครื่องอื่นและเพิ่มจำนวนของตัวเองลงไปในไดร์ฟใหม่นั้นๆ และเข้าไปทำลาย **Boot Sector** ของไดร์ฟใหม่และจะติดต่อไปจนทั่วระบบเครือข่าย ซึ่งหากไม่มีการแก้ไขปัญหาเหล่านี้อย่างถูกต้องจะส่งผลให้เครื่องคอมพิวเตอร์ทั้งหมดในระบบเครือข่ายเกิดความเสียหาย ซึ่งหมายถึงระบบเครือข่ายล่ม

ไวรัสคอมพิวเตอร์อีกประเภทหนึ่งคือ **File Infector** ไวรัสประเภทนี้จะติดอยู่กับไฟล์หรือโปรแกรมประยุกต์ ไวรัสประเภทนี้จะถูกกระตุ้นให้มีการทำงานเมื่อเปิดโปรแกรมนั้นขึ้นมาใช้งาน หรือมีการเรียกใช้ไฟล์ที่ติดไวรัสมาใช้งาน ตัวอย่างของไวรัสประเภท **File Infector** มีดังต่อไปนี้

- **Companion Virus :** เป็นไวรัสที่แฝงตัวอยู่ในโปรแกรมประยุกต์ โดยใช้ชื่อตามโปรแกรมจริง **Companion Virus** จะถูกกระตุ้นให้ทำงานโดยใช้ส่วนต่อขยายที่ไวรัสสร้างขึ้นเอง เช่นในการเปิดโปรแกรม **wordprocessor.exe** เมื่อมีคำสั่งให้ดำเนินการ ไวรัสชื่อ “**wordprocessor.com**” จะดำเนินการในส่วนของไวรัส เนื่องจากไฟล์ **.com** จะทำงานก่อนไฟล์ **.exe**
- **Macro Virus :** เป็นไวรัสที่ตรวจพบได้ยาก ที่ได้ชื่อนี้เพราะไวรัสประเภทนี้ถูกเขียนขึ้นในลักษณะเป็นมาโครของโปรแกรมประยุกต์นั้นๆ โดยมากมักจะเขียนในโปรแกรมประยุกต์ที่ได้รับความนิยม เช่นโปรแกรม **Microsoft Word** วัตถุประสงค์ของไวรัสประเภทนี้คือเมื่อผู้ใช้เปิดไฟล์ที่ได้รับมาจากที่อื่นด้วยโปรแกรมประยุกต์ของตนเอง จะทำให้ไวรัสนั้นติดเข้ามาในโปรแกรมประยุกต์และทำให้ไฟล์อื่นติดไวรัสเข้าไปด้วย ไฟล์ในเครื่องคอมพิวเตอร์ที่ติดไวรัสจึงเกิดความเสียหาย
- **Polymorphic Virus :** ไวรัสประเภทนี้จะทำการเปลี่ยนแปลงลักษณะของตัวเองทุกครั้งที่ถูกทำซ้ำ จึงทำให้คุณสมบัติของไวรัสแตกต่างไปจากเดิม ยากที่จะตรวจพบ
- **Stealth Virus :** ไวรัสประเภทนี้จะใช้วิธีการซ่อนพรางตัวเองให้รอดพ้นจากการถูกตรวจพบ เมื่อโปรแกรม **Antivirus** พยายามที่จะค้นหาไวรัสจำพวกนี้ **Stealth Virus** จะเข้าขัดขวางกระบวนการตรวจสอบ โดยส่งข้อมูลผิดๆ ออกมาระบุว่า ไม่มีไวรัส

8.5.1 การเพิ่มจำนวนของไวรัส

ไวรัสคอมพิวเตอร์ไม่ได้สร้างตัวขึ้นมาเอง และไม่มีการแพร่กระจายอยู่ในอากาศ ดังนั้นการติดไวรัสจึงเกิดจากการแลกเปลี่ยนบางอย่างระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง ในช่วงแรกๆ ของการติดไวรัสคอมพิวเตอร์มักจะเกิดจากการแลกเปลี่ยนข้อมูลด้วยการใช้ฟล็อปปี้ดิสก์ ดังนั้นเครื่องคอมพิวเตอร์เครื่องหนึ่งที่ติดไวรัสจะสามารถแพร่ไวรัสไปยังเครื่องคอมพิวเตอร์เครื่องอื่นในองค์กรได้

การเติบโตอย่างรวดเร็วของระบบเครือข่าย **LAN, WAN** และเครือข่ายอินเตอร์เน็ต เป็นการเปิดเส้นทางใหม่สำหรับการแพร่กระจายไวรัสอย่างรวดเร็ว ในขณะที่เครื่องคอมพิวเตอร์เครื่องใดๆ สามารถที่จะเชื่อมโยงเข้ากับเครื่องคอมพิวเตอร์เครื่องอื่นในระบบเครือข่ายอินเตอร์เน็ต ผลที่ตามมาคือการสร้างไวรัสก็เพิ่มมากขึ้นด้วย และผู้สร้างไวรัสบางรายยังจัดให้มีซอฟต์แวร์ที่ง่ายต่อการนำไปเผยแพร่ และคำแนะนำในการสร้างไวรัส วิธีแพร่ขยายไวรัสที่เพิ่งจะมีขึ้นเมื่อไม่นานมานี้คือการส่งไวรัสผ่านบริการจดหมายอิเล็กทรอนิกส์ หรืออีเมลล์ **(E-mail)** การที่ผู้ใช้เปิดข้อความในอีเมลล์ที่มีไวรัส จะทำให้ไวรัสนั้นขยายตัวเองเข้ามาในเครื่องคอมพิวเตอร์ของผู้นั้น

8.5.2 ผลกระทบที่เกิดจากไวรัส

ไวรัสอาจจะเป็นสาเหตุให้เกิดผลร้ายต่อเครื่องคอมพิวเตอร์ ซึ่งอาจเป็นการทำให้เครื่องคอมพิวเตอร์ไม่สามารถบูทได้ ข้อมูลในเครื่องคอมพิวเตอร์ถูกทำให้เสียหาย ฮาร์ดดิสก์ถูกทำลาย อาการที่เกิดบ่อยที่สุดของการติดไวรัสคอมพิวเตอร์ในระบบเครือข่ายแบบ **Peer-to-Peer** ที่นับว่าบอบบางที่สุด คือเครื่องเวิร์กสเตชั่นเครื่องหนึ่งหรือมากกว่าติดไวรัส และทำให้ทรัพยากรที่แบ่งปันการใช้ร่วมกันถูกทำลาย จึงทำให้ระบบเครือข่ายเกิดความเสียหายในการทำงาน สำหรับระบบเครือข่ายแบบ **Server-Based** เครื่องเซิร์ฟเวอร์มักจะมีการป้องกันการติดไวรัสแบบ **Built-in** ระบบเครือข่ายแบบนี้จึงมีแนวโน้มในการติดไวรัสที่เครื่องเวิร์กสเตชั่นมากกว่าเครื่องเซิร์ฟเวอร์

8.5.3 การป้องกันไวรัส

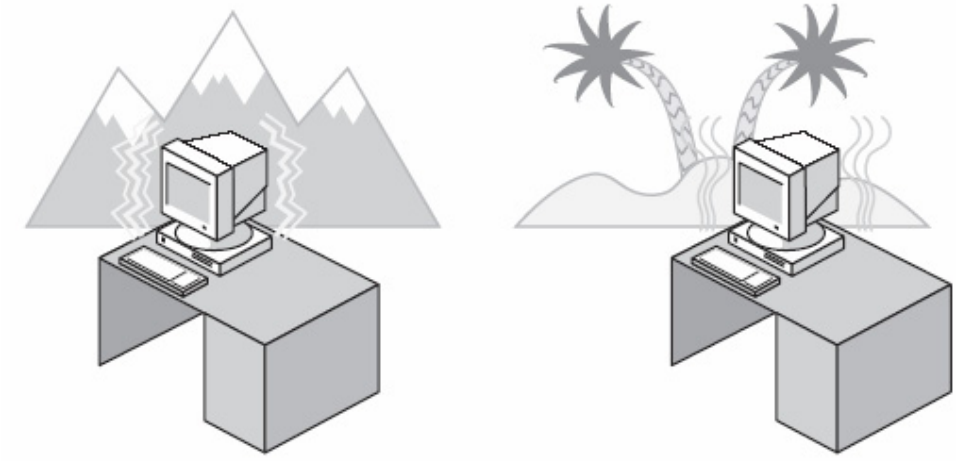
ความเสียหายที่เกิดจากไวรัสคอมพิวเตอร์เริ่มที่จะเป็นเรื่องปกติมากขึ้นทุกวันจึงควรนำเรื่องนี้มาใส่ใจในขั้นตอนของการพัฒนาการรักษาความปลอดภัยให้กับระบบเครือข่าย แผนการต่อต้านไวรัสที่มีประสิทธิภาพเป็นส่วนสำคัญในการวางแผนการใช้งานระบบเครือข่าย ถึงแม้ว่าในปัจจุบันจะไม่มีซอฟต์แวร์ที่สามารถป้องกันไวรัสทั้งหมดได้ แต่การเลือกใช้ซอฟต์แวร์ **Antivirus** ที่ดีจะช่วยได้ระดับหนึ่ง นอกจากนั้นผู้บริหารระบบเครือข่ายยังอาจวางแผนให้มีการเตรียมจัดส่วน **Download** ให้กับผู้ใช้ระบบเครือข่าย เพื่อทำการดาวน์โหลด **Update Antivirus** ไปทำการปรับปรุงในเครื่องคอมพิวเตอร์ของตนเอง ซึ่งอย่างน้อยซอฟต์แวร์จำพวกนี้ก็สามารถช่วยเตือนเกี่ยวกับการติดไวรัส ป้องกันไม่ให้ไวรัสทำงาน ลบไวรัสออก หรืออาจจะซ่อมแซมความเสียหายที่เกิดจากไวรัสนั้นได้

การป้องกันผู้ที่ไม่ได้รับสิทธิในการใช้งานระบบเครือข่าย เป็นหนทางที่ดีที่สุดในการหลีกเลี่ยงการติดไวรัส สำหรับการใช้ฟล็อปปี้ดิสก์ การป้องกันการเขียนข้อมูลเป็นหนทางหนึ่งที่ใช้ป้องกันการแพร่กระจายของไวรัสได้ เนื่องจากการป้องกันไวรัสเป็นหัวใจสำคัญในการรักษาความปลอดภัยให้กับระบบเครือข่าย ดังนั้นผู้บริหารระบบจึงต้องกำหนดมาตรการการป้องกันที่เหมาะสม เช่นกำหนดรหัสผ่าน และสิทธิการใช้งานของผู้ใช้ในระบบ รวมทั้งมีนโยบายซึ่งระบุกฎเกณฑ์การป้องกันไวรัสในเครื่องลูกข่าย และเครื่องแม่ข่ายของระบบ และมีการอบรมให้กับผู้ใช้

8.6 สภาวะแวดล้อมในการใช้งานระบบเครือข่าย

อุปกรณ์อิเล็กทรอนิกส์ส่วนมาก รวมถึงเครื่องคอมพิวเตอร์จะสามารถปฏิบัติงานได้อย่างน่าเชื่อถือเป็นเวลาหลายปี โดยมีการบำรุงรักษาเพียงเล็กน้อย ผลกระทบทางลบที่เกิดจากสภาวะแวดล้อมการนำเครื่องคอมพิวเตอร์ไปใช้งานบนดวงจันทร์เพียงไม่กี่วันแล้วนำกลับมาใช้งานบนโลกจะไม่เป็นสิ่งที่น่าตื่นเต้นเร้าใจ แต่หากใช้งานเครื่องคอมพิวเตอร์โดยไม่มีการบำรุงรักษาเลยจะทำให้เกิดการเสื่อมถอยลงอย่างช้าๆ และต่อเนื่อง จะส่งผลกระทบอย่างร้ายแรงต่อระบบเครือข่าย

เครื่องคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ในระบบเครือข่ายก็เป็นเช่นเดียวกับคน หากได้รับผลกระทบจากสภาวะแวดล้อมมากๆ เป็นเวลานาน ก็จะทำให้เกิดความผิดพลาดในการทำงานได้ ดังนั้นเครื่องคอมพิวเตอร์และอุปกรณ์ของระบบเครือข่ายก็ต้องการสภาวะแวดล้อมในการทำงานที่เหมาะสม โดยมากเครื่องคอมพิวเตอร์จะได้รับการติดตั้งในสภาวะแวดล้อมที่มีการควบคุม การประเมินสภาวะแวดล้อมว่าจะส่งผลกระทบต่อเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่ายหรือไม่นั้น ก้าวแรกในการศึกษาเรื่องนี้คือการพิจารณาสภาพแวดล้อมของที่ตั้งทางภูมิศาสตร์ ระบบเครือข่ายที่ติดตั้งในบริเวณอาร์คติก จะถูกควบคุมโดยสภาวะแวดล้อมที่แตกต่างจากระบบเครือข่ายที่ติดตั้งในบริเวณป่าเขตร้อนเป็นอย่างมาก ดังแสดงตามรูปที่ 8 – 4



รูปที่ 8 – 4 สภาวะแวดล้อมที่แตกต่างมีผลกระทบต่อเครื่องคอมพิวเตอร์

โดยทั่วไปเรามักจะคิดว่าสภาวะแวดล้อมของเครื่องคอมพิวเตอร์จะเหมือนกับสภาวะแวดล้อมในสำนักงานทั่วไป สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลหรือเครื่องเวิร์กสเตชั่น ซึ่งเป็นเพียงองค์ประกอบส่วนหนึ่งของระบบเครือข่าย อย่าลืมว่าการเดินสายสัญญาณที่จำเป็นต้องเดินออกไปนอกอาคาร ไม่ว่าจะวางสายไว้บนดินหรือโยงไปกลางอากาศโดยไม่มีสิ่งห่อหุ้ม ปัจจัยทางสภาวะแวดล้อมจึงมีส่วนในการส่งผลกระทบต่อส่วนประกอบต่างๆ ของระบบเครือข่าย ซึ่งจะนำไปสู่การเสื่อมสภาพของระบบเครือข่ายในที่สุด ดังนั้นการวางแผนการบำรุงรักษาระบบเครือข่ายจึงเป็นสิ่งสำคัญที่ต้องคำนึงถึง โดยที่องค์ประกอบของระบบเครือข่ายทั้งระบบจะต้องได้รับการดูแลอย่างทั่วถึง

ความเสียหายอันเนื่องจากการกระตุ้นของสภาวะแวดล้อม โดยมากจะมีลักษณะเป็นการเสื่อมสภาพอย่างช้าๆ เป็นเวลานาน มากกว่าความเสียหายที่เกิดขึ้นในทันทีทันใด ในลักษณะเดียวกับตะปูเหล็กที่ถูกทิ้งไว้ข้างนอกจะค่อยๆ เป็นสนิม และกลายเป็นสิ่งที่ใช้งานไม่ได้ และผุพังไปในที่สุด ในทำนองเดียวกันระบบเครือข่ายที่ดำเนินงานภายใต้สภาวะแวดล้อมที่ไม่ดีอาจจะทำงานได้เป็นเวลาหลายปี แต่อย่างไรก็ตามปัญหาการทำงานไม่ต่อเนื่องจะเริ่มเกิดขึ้น และความถี่ของการเกิดปัญหาก็จะเพิ่มมากขึ้น จนกระทั่งในที่สุดระบบเครือข่ายนั้นก็ไม่สามารถใช้งานได้อีกต่อไป

8.7 การสร้างสภาวะแวดล้อมที่ถูกต้อง

ในองค์กรขนาดใหญ่ ผู้บริหารจะต้องจัดเตรียมสภาวะแวดล้อมในการทำงานอย่างปลอดภัยและสะดวก มีการกำหนดกฎเกณฑ์สำหรับสภาวะแวดล้อมในการทำงานของมนุษย์ แต่ยังไม่มีการกำหนดกฎเกณฑ์ในเรื่องของสภาวะแวดล้อมของระบบเครือข่าย จึงเป็นหน้าที่ของผู้บริหารระบบเครือข่ายที่จะกำหนดนโยบายในการควบคุม ดูแล อุปกรณ์ระบบเครือข่าย และดำเนินการจัดการเกี่ยวกับการสร้างสภาวะแวดล้อมที่เหมาะสมกับการทำงานของระบบเครือข่าย

สภาวะแวดล้อมที่ดีสำหรับอุปกรณ์ระบบเครือข่าย คือสภาพที่เหมือนกับสภาวะแวดล้อมที่ดีสำหรับมนุษย์ อุปกรณ์อิเล็กทรอนิกส์ส่วนใหญ่จะได้รับการออกแบบมาเพื่อให้สามารถทำงานได้ภายใต้ของเขตของอุณหภูมิและความชื้นเดียวกับที่ทำให้มนุษย์ปกติมีความรู้สึกสบาย

8.7.1 อุณหภูมิ

ปัจจัยพื้นฐานของสภาวะแวดล้อมซึ่งควบคุมได้คือ อุณหภูมิ โดยทั่วไปจะมีความจำเป็นต้องทำการควบคุมอุณหภูมิให้กับอุปกรณ์ระบบเครือข่าย เนื่องจากอุปกรณ์อิเล็กทรอนิกส์จะสร้างความร้อนจากการทำงานตามปกติ อุปกรณ์อิเล็กทรอนิกส์หลายประเภทที่ได้รับการออกแบบให้มีพัดลมระบายอากาศสำหรับรักษาอุณหภูมิในการทำงานให้ได้ตามขอบเขตที่ได้รับการออกแบบ อย่างไรก็ตามถ้าห้องซึ่งอุปกรณ์เหล่านั้นติดตั้งมีอุณหภูมิสูงมากจนเกินไป จนกระทั่งพัดลมระบายอากาศไม่สามารถที่จะควบคุมอุณหภูมิของอุปกรณ์เหล่านั้นให้อยู่ภายในขอบเขตที่กำหนดได้ จะส่งผลให้อุปกรณ์อิเล็กทรอนิกส์ไม่สามารถทำงานได้ตามปกติ

สภาพแวดล้อมซึ่งมีการเปลี่ยนแปลงอุณหภูมิระหว่างร้อนกับเย็นเป็นช่วงๆ เป็นสภาพแวดล้อมที่แย่ที่สุดสำหรับอุปกรณ์อิเล็กทรอนิกส์ ช่วงห่างระหว่างการเปลี่ยนแปลงอุณหภูมิอย่างสูงสุดนี้จะทำให้ส่วนประกอบที่เป็นเหล็กเกิดการขยายตัวและหดตัว ซึ่งจะนำไปสู่ความล้มเหลวในการทำงานของอุปกรณ์ และส่งผลให้ระบบเครือข่ายล่มในที่สุด การพิจารณาติดตั้งเครื่องปรับอากาศที่สามารถควบคุมอุณหภูมิให้คงที่ได้ จึงเป็นทางเลือกอย่างหนึ่งสำหรับห้องซึ่งจัดเก็บเครื่องเซิร์ฟเวอร์และอุปกรณ์ระบบเครือข่ายที่สำคัญ

8.7.2 ความชื้น

ปัจจัยที่เกี่ยวข้องกับความชื้นมีผลกระทบทางลบต่ออุปกรณ์อิเล็กทรอนิกส์ 2 ประการคือ ความชื้นสูงทำให้เกิดการกัดกร่อน ซึ่งโดยมากมักเกิดกับจุดสัมผัสทางไฟฟ้า เช่นจุดเชื่อมต่อสายเคเบิลเข้ากับการ์ดเชื่อมต่อระบบเครือข่าย เหตุการณ์เช่นนี้จะเกิดขึ้นอย่างค่อยเป็นค่อยไป นอกจากนั้นการกัดกร่อนยังเพิ่มความต้านทานให้กับจุดสัมผัสเหล่านั้น ซึ่งอาจส่งผลให้อุณหภูมิบริเวณนั้นสูงขึ้น และอาจตามมาด้วยความล้มเหลวในการทำงานของอุปกรณ์ หรือหากโชคร้ายอาจทำให้เกิดไฟไหม้ได้ ในอาคารที่มีความชื้นต่ำ จะทำให้เกิดไฟฟ้าสถิตขึ้น และอาจทำลายอุปกรณ์อิเล็กทรอนิกส์ของระบบเครือข่ายได้

เนื่องจากเราแทบจะไม่สามารถควบคุมความชื้นได้ ผู้บริหารระบบเครือข่ายจำเป็นต้องตระหนักถึงผลที่จะตามมาของการที่ความชื้นสูงหรือต่ำมาก และดำเนินมาตรการป้องกันที่เหมาะสมกับสถานการณ์ที่เกิดขึ้น อุปกรณ์อิเล็กทรอนิกส์โดยมากจะทำงานได้ภายใต้ความชื้นสัมพัทธ์ **50 – 70%** อย่างไรก็ตามหากระบบเครือข่ายมีความสำคัญต่อองค์กรเป็นอย่างมาก อาจจะต้องจำเป็นต้องติดตั้งเครื่องปรับอากาศที่มีความสามารถในการควบคุมความชื้นได้

8.7.3 ฝุ่นละออง

แน่นอนว่าเครื่องคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ทำงานได้ไม่ดีในสภาพแวดล้อมที่มีฝุ่นละอองมาก ละอองฝุ่นจะถูกดึงดูดโดยไฟฟ้าสถิตเข้าไปยังอุปกรณ์อิเล็กทรอนิกส์ การสะสมของฝุ่นเป็นจำนวนมากจะส่งผลกระทบ 2 อย่างคือ ฝุ่นจะเป็นตัวกั้นกระแสไฟฟ้าให้ไหลไม่สะดวก จึงทำหน้าที่เป็นเหมือนฉนวน ซึ่งส่งผลให้อุปกรณ์นั้นมีความร้อนสูงมากขึ้น และถ้าฝุ่นจับกระแสไฟฟ้าไว้มากจนกระทั่งกลายเป็นสื่อนำไฟฟ้า ดังนั้นการมีฝุ่นมากจนเกินไปอาจทำให้เกิดไฟฟ้าลัดวงจรได้

8.7.4 ปัจจัยมนุษย์

ในการออกแบบระบบเครือข่าย เราสามารถควบคุมควบคุมจำนวนของปัจจัยสภาวะแวดล้อมทางกายภาพให้กับเครื่องคอมพิวเตอร์ได้อย่างสมบูรณ์ การเข้ามาใช้งานของมนุษย์จะนำมาซึ่งความเปลี่ยนแปลงซึ่งเป็นข้อจำกัดของระบบเครือข่าย ลองวาดภาพสำนักงานแห่งใหม่ที่มีสภาพแวดล้อมในการทำงานอย่างเหมาะสม มีเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่ทันสมัย มีเครื่องพิมพ์อยู่บนโต๊ะเป็นส่วนกลาง เมื่อเริ่มมีพนักงานเข้ามาทำงาน ไม่ช้าสำนักงานแห่งนี้ก็จะเต็มไปด้วยต้นไม้ รูปภาพ ถ้วยกาแฟ หนังสือ และเอกสารต่างๆ พนักงานบางคนอาจจะตั้งรูปภาพไว้ด้านบนของจอคอมพิวเตอร์ ดันเครื่องคอมพิวเตอร์เข้าไปติดกับผนัง เพราะไม่ได้ตระหนักถึงความต้องการในการระบายอากาศ การเปลี่ยนแปลงที่เกิดขึ้นจากฝีมือมนุษย์นี้จะทำให้อุณหภูมิภายในอุปกรณ์สูงขึ้นจนไม่เหมาะสม อาจส่งผลให้อุปกรณ์ทำงานล้มเหลว นอกจากนั้นธรรมชาติในการทำงานของมนุษย์ที่ต้องมีการดื่มน้ำ หรือเครื่องดื่มเย็นๆ หากทำหกใส่คีย์บอร์ดหรือเครื่องคอมพิวเตอร์อาจทำให้เกิดความเสียหายต่อเครื่องคอมพิวเตอร์ได้ หรือเมื่ออุณหภูมิภายนอกเริ่มเย็นจำเป็นต้องเปิดฮีตเตอร์ ซึ่งมีท่อส่งความร้อน อาจทำให้เครื่องคอมพิวเตอร์มีความร้อนสูงเกินไปจนทำให้เกิดความเสียหายได้

8.7.5 ปัจจัยซ่อนเร้น

องค์ประกอบของระบบเครือข่ายหลายๆ ส่วน เป็นสิ่งที่มองเห็นได้ยาก จึงไม่ค่อยได้รับความสนใจ โดยมากจึงมักจะคิดว่าทุกสิ่งยังทำงานได้เป็นอย่างดี สายเคเบิลซึ่งเป็นส่วนประกอบหนึ่งของระบบเครือข่าย อาจทำให้เกิดปัญหาขึ้นกับระบบเครือข่ายได้ โดยเฉพาะอย่างยิ่งสายที่เดินอยู่บนพื้น ซึ่งมีคนเดินเหยียบไปมาตลอดเวลา ส่วนสายเคเบิลที่เดินอยู่ในช่องใต้เพดานก็อาจเกิดความเสียหายโดยบังเอิญในระหว่างการซ่อมแซมหลังคาได้

แมลงและสัตว์ทุกชนิดที่ใช้ฟันแทะวัตถุต่างๆ ได้ นับว่าเป็นปัจจัยซ่อนเร้นอีกอย่างหนึ่ง มีความเป็นไปได้ที่แขกผู้ไม่ได้รับเชิญเหล่านี้จะเข้ามาแทะ กัด หรือรับประทานส่วนประกอบของระบบเครือข่ายเป็นอาหารเย็น หรือนำส่วนของสายเคเบิลไปทำรัง

8.7.6 ปัจจัยทางอุตสาหกรรม

เครื่องคอมพิวเตอร์ไม่ได้ถูกจำกัดไว้สำหรับใช้งานเฉพาะในสำนักงาน ในโรงงานอุตสาหกรรมสมัยใหม่จะใช้เครื่องคอมพิวเตอร์ในการควบคุมอุปกรณ์ต่างๆ ในการผลิต การรวมระบบเครือข่ายไว้ในสภาพแวดล้อมนี้จะทำให้สามารถควบคุมและตรวจสอบกระบวนการในการผลิตได้จากส่วนกลาง หรืออาจจะสามารถทำการต่อโทรศัพท์กลับไปแจ้งผู้ซึ่งทำหน้าที่บำรุงรักษาระบบได้เมื่อเกิดปัญหาขึ้น

พัฒนาการของกระบวนการผลิตในภาคอุตสาหกรรม นำไปสู่การเพิ่มขีดความสามาถในการผลิต แต่สำหรับผู้บริหารระบบเครือข่ายแล้วการปฏิบัติงานของระบบเครือข่ายภายใต้สภาวะแวดล้อมเช่นนี้ นับว่าเป็นสิ่งที่ท้าทายเป็นอย่างมาก ประเด็นที่จำเป็นต้องกล่าวถึงเมื่อระบบเครือข่ายต้องทำงานในโรงงานอุตสาหกรรมประกอบด้วย

- สัญญาณรบกวน
- การรบกวนของคลื่นแม่เหล็กไฟฟ้า
- ความสั่นสะเทือน
- สภาวะแวดล้อมที่ทำให้เกิดการกัดกร่อน และการระเบิด
- พนักงานที่ไม่ได้รับการฝึก และไม่มีความชำนาญ

บ่อยครั้งที่อาจจะไม่มีการควบคุมสภาวะแวดล้อมด้านอุณหภูมิและความชื้นในโรงงานอุตสาหกรรมในส่วนที่เกี่ยวข้องกับการผลิต และในบรรยากาศอาจมีสิ่งเจือปนโดยสารเคมีที่มีฤทธิ์ในการกัดกร่อนสูง ซึ่งอาจทำลายเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่ายได้ภายในเวลาเพียงไม่กี่เดือน สภาวะแวดล้อมในการผลิตที่ต้องใช้อุปกรณ์หนักซึ่งมีมอเตอร์ไฟฟ้าขนาดใหญ่อาจทำให้เกิดการรบกวนทางคลื่นแม่เหล็กไฟฟ้าที่ก่อความเสียหายให้กับระบบปฏิบัติงานของเครื่องคอมพิวเตอร์และระบบเครือข่าย ดังนั้นเพื่อทำให้ปัญหาที่เกิดจากการทำงานของระบบเครือข่ายภายใต้สภาวะแวดล้อมการผลิตในโรงงานอุตสาหกรรมมีน้อยที่สุดเท่าที่จะทำได้ จึงควรจะ

- ติดตั้งอุปกรณ์ระบบเครือข่ายในส่วนที่แยกต่างหาก และมีการระบายอากาศออกไปข้างนอก
- พิจารณาใช้เคเบิลใยแก้วนำแสงเป็นสายสัญญาณเพื่อช่วยลดการแทรกแซงของคลื่นแม่เหล็กไฟฟ้า และป้องกันปัญหาการสึกกร่อนของสายเคเบิล
- ติดตั้งระบบสายดินอย่างเหมาะสม
- จัดให้มีการฝึกฝนพนักงานที่จำเป็นต้องใช้อุปกรณ์ เพื่อให้แน่ใจถึงความสมบูรณ์ของระบบ

8.8 การป้องกันข้อมูลที่สำคัญ

องค์กรขนาดใหญ่เป็นจำนวนมากจะมีแผนการฟื้นฟูความเสียหายอย่างครอบคลุม เพื่อรักษาการปฏิบัติและสร้างใหม่หลังจากความหายนะที่เกิดขึ้นตามธรรมชาติ เช่นแผ่นดินไหว พายุ และอื่นๆ อย่างไรก็ตามเมื่อเปรียบเทียบกับความหายนะทางธรรมชาติแล้ว การฟื้นฟูความเสียหายของระบบเครือข่ายจะเป็นมากกว่าการนำฮาร์ดแวร์ใหม่มาดำเนินการจัดตั้งระบบเครือข่าย ข้อมูลที่สำคัญซึ่งเป็นหัวใจหลักในการทำงานขององค์กรเหล่านั้นจะต้องได้รับการปกป้องเช่นกัน ความเสียหายของระบบเครือข่ายที่ทำให้ไซต์ล่มมีสาเหตุมาจากเหตุการณ์ต่างๆ ดังต่อไปนี้

- ส่วนประกอบของระบบเครือข่ายเกิดความเสียหาย
- ไวรัสคอมพิวเตอร์เข้ามาทำลายระบบ
- การลบข้อมูล หรือเปลี่ยนแปลงข้อมูลให้ผิดไปจากความจริง
- เพลิงไหม้ ไม่ว่าจะถูกลอบวางเพลิง หรืออุบัติเหตุ
- ภัยพิบัติทางธรรมชาติ เช่นฟ้าผ่า น้ำท่วม พายุทอร์นาโด และแผ่นดินไหว
- กระแสไฟฟ้าขัดข้องเป็นเวลานาน
- ขโมยส่วนประกอบของระบบเครือข่าย หรือพวกชอบทำลาย

เมื่อเกิดเหตุการณ์ต่างๆ ที่สร้างความเสียหายให้กับระบบเครือข่ายแล้ว ระยะเวลาที่ใช้ในการฟื้นฟูระบบเครือข่ายโดยนำข้อมูลที่สำรองไว้มาใช้งานจะเป็นสิ่งที่กำหนดอนาคตของบริษัท ถ้าใช้เวลานานอาจเกิดการสูญเสียอย่างร้ายแรงในการผลิต และหากไม่มีข้อมูลสำรองผลที่เกิดจะร้ายแรงยิ่งกว่า ซึ่งหมายถึงการสูญเสียเงินเป็นจำนวนมหาศาล การป้องกันข้อมูลสูญหายสามารถทำได้โดยใช้ระบบสำรองข้อมูลด้วยเทป (**Tape Backup**) หรือออปติคอลดิสก์ (**Optical Disc**) การใช้อุปกรณ์สำรองไฟฟ้าฉุกเฉิน (**Uninterruptible Power Supply**) หรือ **UPS** และการสร้างระบบที่คงทนต่อความเสียหาย (**Fault Tolerant**) การเลือกใช้วิธีการสำรองข้อมูลที่สำคัญของระบบเครือข่ายจะขึ้นอยู่กับว่าข้อมูลนั้นมีค่าต่อองค์กรเพียงใด

8.9 การสำรองข้อมูล (Data Backup)

วิธีธรรมดาที่สุดและถูกที่สุด ในการหลีกเลี่ยงความเสียหายจากการสูญเสียข้อมูล คือการจัดการโดยกำหนดการสำรองข้อมูลเป็นช่วงๆ ซึ่งเก็บข้อมูลสำรองไว้นอกไซต์งาน การใช้เทปแบ็คอัพเป็นหนึ่งในวิธีการจำนวนน้อยที่ใช้โดยทั่วไปและประหยัด ในการทำให้แน่ใจว่าข้อมูลยังคงปลอดภัยและใช้การได้

วิศวกรเครือข่ายที่มีประสบการณ์แนะนำว่า ระบบสำรองข้อมูลควรจะใช้เป็นด่านแรกในการต่อต้านความสูญหายของข้อมูล ยุทธวิธีสำรองข้อมูลที่ปลอดภัยทำให้ความเสี่ยงในการสูญเสียข้อมูลเหลือน้อยที่สุด โดยการรักษาข้อมูลสำรองในปัจจุบัน ซึ่งเป็นสำเนาของไฟล์ที่มีอยู่ ดังนั้นไฟล์สำรองนั้นจะถูกนำมาใช้ในการฟื้นฟูระบบเครือข่ายได้ ถ้าเกิดความเสียหายขึ้นกับข้อมูลดั้งเดิม (**Original Data**) ในการสำรองข้อมูลจะต้องมี

- อุปกรณ์ที่เหมาะสม
- กำหนดการปกติสำหรับการสำรองข้อมูลในช่วงต่างๆ
- ความแน่ใจว่าไฟล์ข้อมูลสำรองนั้นเป็นข้อมูลปัจจุบัน
- บุคคลที่ได้รับมอบหมายให้ทำให้แน่ใจว่ากำหนดการนี้ได้รับการทำจนสำเร็จ

อุปกรณ์นั้นโดยมากจะประกอบด้วยเทปไดร์ฟ (**Tape Drive**) และเทปคาสเซ็ตมากกว่า **1** ชุด หรือสื่ออย่างอื่นในการจัดเก็บข้อมูลปริมาณมาก เช่นออปติคอลดิสก์ รายจ่ายใดๆ ที่เกิดขึ้นในการสำรองข้อมูลนี้ จะเป็นค่าใช้จ่ายที่จะน้อยที่สุดเมื่อเทียบกับคุณค่าของสิ่งที่จะได้รับการคุ้มครองในเหตุการณ์การสูญเสียข้อมูล

8.9.1 การจัดทำระบบสำรองข้อมูล

กฎธรรมดาอย่างง่าย ถ้าคุณไม่สามารถทำงานต่อไปได้โดยปราศจากข้อมูลนั้นก็ทำสำรองไว้ แม้ว่าคุณจะสำรองข้อมูลในดิสก์ทั้งหมด หรือจะเลือกเฉพาะไดเร็กทอรี่หรือไฟล์ ขึ้นอยู่กับว่าคุณจะต้องการปฏิบัติการหลังจากสูญเสียข้อมูลที่สำคัญเร็วแค่ไหน การสำรองข้อมูลไว้ทั้งหมดทำให้การฟื้นฟูโครงสร้างของดิสก์ทำได้ง่ายขึ้นมาก แต่ถ้ามีข้อมูลเป็นจำนวนมาก ก็อาจต้องการเทปหลายชุด (**Multiple Tapes**) การสำรองข้อมูลเฉพาะไฟล์และไดเร็กทอรี่ของแต่ละบุคคลอาจต้องการเทปน้อยกว่า แต่ก็ต้องการผู้บริหารในการฟื้นฟูโครงสร้างของดิสก์ที่เสียหายด้วยมือ

ข้อมูลที่สำคัญมากๆ ควรจะได้รับการสำรองไว้ ตามกำหนดเป็นรายวัน รายสัปดาห์ หรือรายเดือน ขึ้นอยู่กับว่าข้อมูลนั้นสำคัญแค่ไหน และได้รับการปรับปรุงให้ทันสมัยบ่อยแค่ไหนที่จะเป็นการดีที่สุด ถ้าทำการสำรองข้อมูลในขณะที่มีการใช้งานระบบน้อยผู้ใช้ควรได้รับการแจ้งเมื่อจะมีการทำการสำรองข้อมูล เพื่องดใช้งานเครื่องเซิร์ฟเวอร์ในขณะที่มีการสำรองข้อมูลของเครื่องเซิร์ฟเวอร์

8.9.2 การเลือกเทปไดร์ฟ

เนื่องจากการสำรองข้อมูลโดยส่วนมากจะถูกทำโดยใช้เทปไดร์ฟ (**Tape Drive**) ดังนั้นขั้นแรกคือการเลือกเทปไดร์ฟที่เหมาะสม โดยมีลำดับความสำคัญของปัจจัยต่างๆ เช่น

- มีข้อมูลจำนวนเท่าไรที่ต้องทำการสำรองข้อมูล
- ความจำเป็นของระบบเครือข่ายที่ต้องการ การสำรองข้อมูลที่เชื่อถือได้ ความสามารถของการสำรองข้อมูลและความเร็ว
- ต้นทุนของเทปไดร์ฟ และระบบปฏิบัติการที่ใช้

เทปไดร์ฟที่ดีควรมีความสามารถอย่างพอเพียงในการสำรองข้อมูลของเครื่องเซิร์ฟเวอร์ซึ่งใหญ่ที่สุดในระบบเครือข่าย แต่ควรจะมีการป้องกันความผิดพลาดและการทำแก้ไขข้อผิดพลาดให้ถูกต้องระหว่างการสำรองข้อมูลและฟื้นฟูการปฏิบัติงาน

8.9.3 วิธีการสำรองข้อมูล

ตารางที่ 8 – 2 อธิบายรายละเอียดของวิธีการในการสำรองข้อมูลแบบต่างๆ สำหรับนโยบายในการสำรองข้อมูลที่มีประสิทธิภาพจะต้องใช้การผสมผสานกันของวิธีต่างๆ

ตารางที่ 8 – 2 วิธีการสำรองข้อมูล

Method	Description
Full backup	Backs up and marks selected files, whether or not they have changed since the last backup.
Copy	Backs up all selected files without marking them as being backed up.
Incremental backup	Backs up and marks selected files only if they have changed since the last time they were backed up.
Daily copy	Backs up only those files that have been modified that day, without marking them as being backed up.
Differential backup	Backs up selected files only if they have changed since the last time they were backed up, without marking them as being backed up.

เทปสามารถทำการสำรองข้อมูลบนพื้นฐานของวงรอบ 2 สัปดาห์ ขึ้นอยู่กับว่ามีเทปให้ใช้มากเพียงใด ไม่มีกฎตายตัวในการกำหนดวงรอบการสำรองข้อมูล อย่างไรก็ตามในวันแรกของวงรอบผู้บริหารระบบอาจจะทำการสำรองข้อมูลด้วยวิธี **Full Backup** และตามด้วยจำนวนข้อมูลสำรองที่เพิ่มขึ้นในวันต่อๆ มา เมื่อวงจรทั้งหมดเสร็จสิ้นกระบวนการสำรองข้อมูลก็เริ่มขึ้นอีกครั้ง อีกวิธีหนึ่งคือกระบวนการทำสำรองข้อมูลในลักษณะที่กำหนดเวลาไว้ล่วงหน้า

8.9.4 การทดสอบและจัดเก็บ

ผู้บริหารระบบที่มีประสบการณ์จะทดสอบระบบสำรองข้อมูลก่อนที่จะกระทำ โดยจะทำการสำรองข้อมูล ลบข้อมูล ฟื้นฟูข้อมูล และพยายามใช้ข้อมูล ผู้บริหารควรทดสอบขั้นตอนการสำรองข้อมูลอย่างสม่ำเสมอ เพื่อตรวจความถูกต้องว่าสิ่งที่คาดหวังว่าจะได้รับจากการสำรองข้อมูลจริงๆ มากกว่านั้น ขั้นต่อนการฟื้นฟูควรได้รับการทดสอบเพื่อทำให้แน่ใจว่าไฟล์ที่สำคัญสามารถได้รับการฟื้นฟูอย่างรวดเร็ว

ผู้บริหารระบบควรทำสำเนาเทปแต่ละอันไว้ 2 ชุด โดยชุดหนึ่งเก็บไว้ในไซต์ และอีกชุดหนึ่งเก็บไว้ในสถานที่ปลอดภัยนอกไซต์ จำไว้ว่าถึงแม้เทปที่ใช้จัดเก็บจะเป็นวัตถุกันไฟที่สามารถป้องกันไฟไหม้ได้ แต่ความร้อนจากไฟจะทำลายข้อมูลที่ถูกเก็บไว้ในเทป นอกจากนั้นหลังจากใช้เทปบันทึกข้อมูลซ้ำเป็นเวลานาน จะทำให้สูญเสียความสามารถในการเก็บข้อมูล ให้ทำการสำรองข้อมูลนั้นขึ้นมาอย่างสม่ำเสมอเพื่อความมั่นใจในการมีข้อมูลสำรองเก็บไว้

8.9.5 การรักษาบันทึกการสำรองข้อมูล

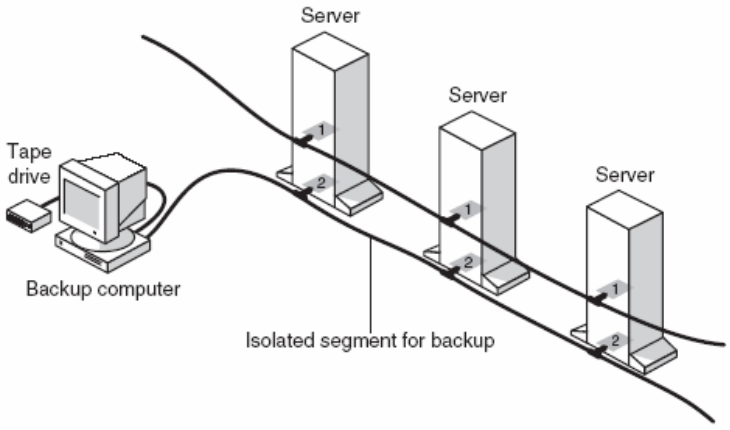
การรักษาบันทึกการสำรองข้อมูลทั้งหมดนั้นสำคัญและเป็นประโยชน์สำหรับการฟื้นฟูไฟล์ในภายหลัง สำเนาของบันทึกควรถูกเก็บไว้กับเทปแบ็คอัพชุดที่เก็บไว้ที่ไซต์ บันทึกดังกล่าวควรจะเก็บข้อมูลดังนี้

- วันที่ที่ทำการสำรองข้อมูล
- หมายเลขของชุดเทป (Tape – Set)
- คอมพิวเตอร์เครื่องใดที่ได้รับการสำรองข้อมูล
- ไฟล์ใดได้รับการสำรองข้อมูล
- ใครเป็นผู้ทำการสำรองข้อมูล
- สถานที่จัดเก็บข้อมูลสำรอง

8.9.6 การติดตั้งระบบการสำรองข้อมูล

เทปไดร์ฟสามารถต่อเข้ากับกับเครื่องเซิร์ฟเวอร์หรือเครื่องคอมพิวเตอร์เวิร์กสเตชั่นได้ในลักษณะของอุปกรณ์ต่อพ่วงหรือเป็นอุปกรณ์ติดตั้งภายใน แต่ถ้าติดตั้งระบบการสำรองข้อมูลไว้ที่เครื่องเซิร์ฟเวอร์ การนำข้อมูลสำรองนั้นมาฟื้นฟูระบบเครือข่ายจะทำได้รวดเร็วกว่า เพราะข้อมูลเหล่านั้นไม่ต้องเดินทางผ่านระบบเครือข่าย

ถึงแม้ว่าการสำรองข้อมูลข้ามระบบเครือข่ายจะเป็นวิธีการที่มีประสิทธิภาพดีที่สุดในระบบการสำรองข้อมูลที่สามารถทำได้หลายหนทาง แต่ภาระในการขนส่งข้อมูลจำนวนมากผ่านระบบเครือข่ายจะทำให้ประสิทธิภาพในการทำงานของระบบเครือข่ายลดลง ดังนั้นจึงควรทำการสำรองข้อมูลในขณะที่ระบบเครือข่ายมีการทำงานน้อย เช่นในเวลากลางคืน นอกจากนั้นการจัดให้เครื่องเซิร์ฟเวอร์หลายๆ เครื่อง ตั้งรวมกันอยู่ในที่เดียวกัน โดยมีเครื่องสำหรับทำการสำรองข้อมูลโดยเฉพาะ และใช้เส้นทางในการสำรองข้อมูลแยกต่างหาก โดยใช้การ์ดเชื่อมต่อระบบเครือข่ายอีกการ์ดหนึ่งแยกจากกัน จะสามารถลดปริมาณการขนส่งข้อมูลบนระบบเครือข่ายลงได้ ดังแสดงตามรูปที่ 8 – 5

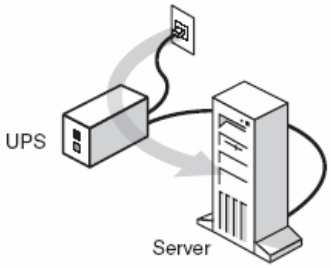


รูปที่ 8 – 5 การใช้เส้นทางอื่นในการสำรองข้อมูล

8.10 เครื่องสำรองไฟฟ้าฉุกเฉิน (Uninterruptible Power Supply – UPS)

UPS เป็นอุปกรณ์ซึ่งเป็นตัวกลางในการจัดส่งพลังงานไฟฟ้าจากภายนอกเข้ามายังเครื่องคอมพิวเตอร์ ซึ่งได้รับการออกแบบมาเพื่อช่วยในระบบการเก็บรักษาข้อมูลของเครื่องเซิร์ฟเวอร์ หรืออุปกรณ์ไฟฟ้าอย่างอื่น ที่ไม่ต้องการให้เหตุการณ์กระแสไฟฟ้าขัดข้องมาทำลายการรักษาความปลอดภัยของระบบ **UPS** จะช่วยให้มีพลังงานไฟฟ้าส่งไปยังระบบที่เชื่อมต่ออยู่อย่างเพียงพอ และไม่ขาดตอน ถึงแม้ว่าไฟฟ้าจะดับก็ตาม อย่างไรก็ตามการใช้ **UPS** จะช่วยเหลือได้ในช่วงเวลาที่จำกัดเท่านั้นผู้บริหารระบบเครือข่ายจะต้องดำเนินการอย่างอื่น เพื่อรักษาข้อมูลที่สำคัญไว้ในขณะที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้อง ระบบปฏิบัติการเครือข่ายส่วนใหญ่จะจัดให้มียูทิลิตี้ในการเชื่อมต่อกับ **UPS** โดยจะควบคุมการ **Shut down** เครื่องเซิร์ฟเวอร์อย่างปลอดภัย แหล่งพลังงานของ **UPS** ส่วนใหญ่จะเป็นแบตเตอรี่ ที่ทำการประจุไฟฟ้าในขณะที่ยังมีกระแสไฟฟ้าตามปกติ แต่อย่างไรก็ตามในระบบขนาดใหญ่อาจจะใช้เครื่องยนต์ดีเซลเป็นแหล่งสำรองไฟฟ้าฉุกเฉินในกรณีที่เกิดกระแสไฟฟ้าขัดข้อง

ระบบ **UPS** ที่ดีจะต้องป้องกันไม่ให้มีผู้ใช้สามารถ **access** เข้ามายังเครื่องเซิร์ฟเวอร์ได้ และต้องสามารถส่งข้อความเตือนในเรื่องต่างๆ ที่เกี่ยวข้องกับการจ่ายพลังงานไปยังผู้บริหารระบบเครือข่ายผ่านทางเครื่องเซิร์ฟเวอร์ได้ โดยมาก **UPS** จะถูกติดตั้งอยู่ระหว่างแหล่งจ่ายพลังงานกับเครื่องเซิร์ฟเวอร์ ดังแสดงตามรูปที่ 8 – 6



รูปที่ 8 – 6 การใช้ **UPS** กับเครื่องเซิร์ฟเวอร์

8.10.1 ชนิดของระบบ UPS

ระบบ **UPS** ที่ดีจะมีการทำงานในลักษณะออนไลน์ และประจุกระแสไฟฟ้าเข้าไปในแบตเตอรี่ของตัวเองให้เต็มอยู่ตลอดเวลา และเมื่อมีเหตุผิดปกติขึ้นกับระบบไฟฟ้าหลัก จะต้องจ่ายพลังงานให้กับระบบได้โดยอัตโนมัติ นอกจากนั้นยังมีระบบ **UPS** ที่มีการทำงานแบบ **Stand-by** ซึ่งจะเริ่มมีการทำงานเมื่อเกิดเหตุการณ์ผิดปกติของแหล่งพลังงานหลัก ระบบ **UPS** ชนิดนี้จะมีราคาถูกกว่าแบบออนไลน์ แต่จะมีความน่าเชื่อถือต่ำกว่า

8.10.2 การติดตั้งระบบ UPS

การตอบคำถามต่อไปนี้ จะช่วยให้ผู้บริหารระบบเครือข่ายตัดสินใจได้ว่าระบบ **UPS** แบบใด จึงจะเหมาะสมกับความต้องการของระบบเครือข่าย

- **UPS** จะต้องให้พลังงานพื้นฐานที่ระบบเครือข่ายต้องการได้หรือไม่
- ต้องการให้ **UPS** สนับสนุนอุปกรณ์ระบบเครือข่ายได้กี่ส่วน
- ต้องการให้ **UPS** ติดต่อกับเครื่องเซิร์ฟเวอร์ผ่านระบบเครือข่ายเพื่อการบริหารจัดการได้หรือไม่
- อายุการใช้งานของแบตเตอรี่ใน **UPS** ยาวนานเพียงใด

- ต้องการให้ **UPS** ป้องกันการรบกวนเครื่องเซิร์ฟเวอร์และอุปกรณ์ต่อพ่วง จากคลื่นแม่เหล็กไฟฟ้าหรือไม่
- ต้องการให้ **UPS** เตือนผู้บริหารระบบเครือข่ายก่อนที่พลังงานสำรองจะหมดไปหรือไม่

8.11 ระบบ Fault Tolerant

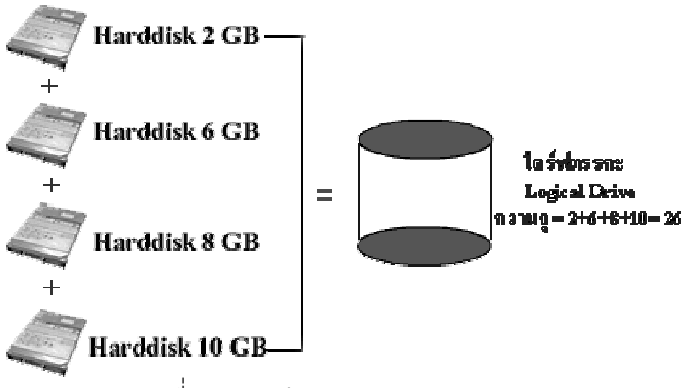
ระบบ **Fault Tolerant** เป็นระบบที่จัดตั้งขึ้นมาเพื่อปกป้องข้อมูลโดยการทำข้อมูลซ้ำแล้วนำไปเก็บไว้ในแหล่งอื่น เช่นในส่วนอื่นของดิสก์ ในดิสก์ตัวอื่น หรือบนเครื่องคอมพิวเตอร์เครื่องอื่นในระบบเครือข่าย เมื่อข้อมูลหลักที่ใช้งานเกิดความเสียหาย จะสามารถเข้าไปเรียกข้อมูลจากที่อื่นมาใช้งานได้โดยอัตโนมัติ ข้อมูลเหล่านี้อาจจะเป็นข้อมูลที่เกินความจำเป็นแต่ก็มีประโยชน์ในระบบที่ไม่ต้องการให้ระบบเครือข่ายล่ม

ระบบ **Fault Tolerant** ไม่ควรถูกนำมาใช้เพื่อทดแทนระบบการสำรองข้อมูลตามปกติของเครื่องเซิร์ฟเวอร์และการสำรองข้อมูลในฮาร์ดดิสก์ การวางแผนในการสำรองข้อมูลที่ดีจะสามารถรับประกันได้ว่าจะสามารถฟื้นฟูระบบจากความเสียหายหรือถูกทำลายได้อย่างดี ทางเลือกอย่างหนึ่งของระบบ **Fault Tolerant** ที่นับว่าเป็นมาตรฐานอย่างหนึ่งคือ **RAID (Redundant Array of Independent Disks)** ซึ่งจัดแบ่งระดับการทำ **RAID** ตามผลการทำงาน ความน่าเชื่อถือ และค่าใช้จ่ายในการลงทุน มีวิธีการต่างๆ ในการจัดตั้งระบบ **Fault Tolerant** อาทิเช่น **Disk Striping, Disk Mirroring, Sector Sparing, Mirrored Drive Array** และ **Clustering**

8.11.1 RAID (Redundant Array of Independent Disks)

ในปี **1987 Patterson, Gibson** และ **Katz** ซึ่งทำงานที่ **University of California Berkeley** ได้ตีพิมพ์บทความเกี่ยวกับ **A Case for Redundant Arrays of Inexpensive Disks (RAID)** โดยกล่าวถึงชนิดของดิสก์อาเรย์ประเภทต่างๆ โดยเรียกชื่อย่อว่า **RAID** หลักการพื้นฐานของ **RAID** มาจากแนวคิดที่ว่าเมื่อเอาดิสก์ที่มีความจุน้อยหลายๆ ตัวมารวมกัน ประสิทธิภาพที่ได้จากการใช้งานจะมากกว่าใช้ดิสก์ขนาดใหญ่เพียงตัวเดียว โดยเมื่อเอาดิสก์มารวมกันแล้วคอมพิวเตอร์จะต้องเห็นว่าเป็นดิสก์ขนาดใหญ่ตัวเดียว (เป็น **Logical Drive**) ต่อมา **RAID** ได้เปลี่ยนคำจำกัดความเป็น **Redundant Array of independent disks** คือระบบเผื่อแบบอาเรย์ของดิสก์ที่เป็นอิสระต่อกัน คือ การนำฮาร์ดดิสก์หลายๆ ตัวมาต่อกัน เช่น **5** ตัว ข้อดีคือได้ความจุเพิ่มขึ้น แต่ถ้าดิสก์ตัวใดตัวหนึ่งพังก็จะเสียข้อมูลในฮาร์ดดิสก์ตัวนั้นไป แต่จะป้องกันได้มากกว่า ถ้าหากเพิ่มฮาร์ดดิสก์เข้าไป **3** ตัว แล้วใช้ระบบการจัดแบ่งเก็บข้อมูลในแต่ละตัวพร้อมกัน ในแต่ละตัวก็จะมีข้อมูลที่ซ้ำกัน หรือมีการเก็บ **Parity** ของอีกตัวไว้ ถ้าเกิดพังไป ข้อมูลในตัวที่พังก็ยังคงมีเก็บ “สำรองเผื่อเสีย” ไว้ การแก้ไขทำได้โดยเปลี่ยนฮาร์ดดิสก์ แล้วถ่ายข้อมูลในฮาร์ดดิสก์ตัวที่พังไปที่ฝากไว้กับฮาร์ดดิสก์ตัวอื่นมาลง ทั้งหมดนั้นเรียกว่าระบบ **Fault Tolerance** ซึ่งหมายถึง “ระบบที่คงทนต่อความเสียหาย” คือแทนที่เมื่อฮาร์ดดิสก์พังไปตัวหนึ่งก็ต้อง “**Down**” เครื่องเซิร์ฟเวอร์เพื่อซ่อมทำ ซึ่งส่งผลให้ระบบต้องหยุดชะงัก เพื่อป้องกันความเสียหายดังกล่าว จะต้องสร้างระบบให้คงทนต่อความเสียหาย เมื่อฮาร์ดดิสก์พังไปแล้วหนึ่งตัว ระบบยังทำงานต่อไปเหมือนไม่มีอะไรเกิดขึ้น โดยวิธีการนี้จะต้องใช้ **RAID** ซึ่งเป็นหัวใจของการสร้าง “ดิสก์ที่คงทนต่อความเสียหาย” ปัจจุบันการนำ **RAID** มาใช้งานนั้นจะเกี่ยวกับเซิร์ฟเวอร์เป็นส่วนใหญ่ เมื่อระบบเครือข่ายถูกพัฒนาขึ้นใช้ ความสำคัญของระบบจัดเก็บข้อมูล **(Storage System)** ก็ทวีความสำคัญขึ้น เพราะถ้าหากฮาร์ดดิสก์ในเซิร์ฟเวอร์ชำรุดใช้งานไม่ได้ นอกจากจะสูญเสียข้อมูลที่เก็บไว้ในฮาร์ดดิสก์ไปทั้งหมดแล้ว ยังจะต้องเสียเวลาเพื่อรอให้การซ่อมแซมแล้วเสร็จ ซึ่งหมายถึงการสูญเสียโอกาสทางธุรกิจ

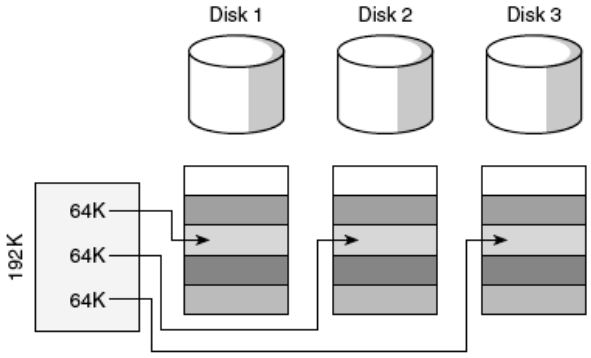
ระบบ **RAID** จะประกอบไปด้วยฮาร์ดดิสก์หลายๆ ตัวรวมเป็นระบบ **RAID** ย่อยๆ **1** ระบบ แต่ไดร์ฟเหล่านั้นกลับถูกเก็บซ่อนจากผู้ใช้เสมือนหนึ่งว่าเป็นฮาร์ดดิสก์เพียงไดร์ฟเดียว ดังนั้นจึงสามารถขยายความจุได้อย่างมหาศาล ถึงกว่า **1,000 GB** ซึ่งตัวไดร์ฟเสมือนนี้ จะถูกสร้างและควบคุมโดยระบบปฏิบัติการ ซึ่งได้มีการติดตั้งโปรแกรมจัดการ **RAID** มาไว้ในตัว ซอฟต์แวร์ **RAID** ไม่ได้จัดการเฉพาะสร้างตัวไดร์ฟเสมือนเท่านั้น แต่ยังควบคุมการเข้าถึงไดร์ฟเหล่านี้ด้วยว่าจะเข้าถึงด้วยเส้นทางและวิธีใดจึงจะเหมาะสมและรวดเร็วที่สุด ระบบ **RAID** จะสามารถตั้งค่าได้หลากหลายเพื่อประสิทธิภาพที่แตกต่างกันไป ตั้งแต่ในเรื่องของความจุสูงสุด หรือแม้กระทั่งความทนทานต่อความผิดพลาด ก่อนอื่นเราต้องเข้าใจหลักการของฮาร์ดแวร์ก่อน นั่นคือการที่จะรวมเอาฮาร์ดดิสก์หลายตัวมารวมไว้ได้นั้น จะต้องพึ่งพา **RAID Controller Board** ซึ่งจะทำหน้าที่เป็นเสมือนโครงข่ายหลักที่ทำงานอยู่เบื้องหลัง และยังเป็นช่องสำหรับต่อดิสก์หลายๆ ตัวเข้าไว้อีกด้วย นอกจาก **RAID Controller** จะมีคำสั่งในการ **input/output** สำหรับระบุตำแหน่งของไดร์ฟต่างๆ ในช่องใส่แล้ว ยังทำหน้าที่ให้ไดร์ฟย่อยๆ เหล่านี้เป็นอิสระต่อกัน นั่นหมายความว่าจะช่วยให้สามารถ ถอดเปลี่ยน หรือเคลื่อนย้ายไดร์ฟเหล่านี้ให้ราบรื่นยิ่งขึ้น นอกจากนี้ **RAID controller** ยังคอยดูแลความมั่นคงในการทำงานของไดร์ฟแต่ละตัว หากพบปัญหาว่าไดร์ฟตัวไหนมีโอกาสได้รับความเสียหาย ยังสามารถโอนย้ายข้อมูลที่มีความเสี่ยงเหล่านั้น ไปอยู่ในไดร์ฟอื่นที่ปลอดภัยกว่า เพื่อป้องกันปัญหาข้อมูลสูญหาย (เราเรียกระบบนี้ว่ามีความทนทานต่อความเสียหาย หรือมีระบบ **Fault Tolerance**) และในหัวข้อต่อๆ ไป คือคำอธิบายถึงระดับของ **RAID** ซึ่งจะขึ้นอยู่กับประสิทธิภาพการทำงานที่แตกต่างกัน



รูปที่ 8 – 7 หลักการทำงานของ **RAID**

8.11.2 RAID 0 (Disk Striping)

คือการทำ **Disk Striping** คำว่า "**Stripe**" มีความหมายว่าลายยาวบนผืนผ้า ซึ่งใช้เปรียบเทียบการเก็บข้อมูลของ **RAID 0** โดยแยกข้อมูลออกเป็นแถบ ขนาดบล็อกละ **64K** เท่าๆ กัน และแบ่งการจัดเก็บไว้ในอุปกรณ์การจัดเก็บข้อมูลทางกายภาพหลายๆ ส่วน การทำเช่นนี้จะไม่มีข้อมูลที่ถูกทำซ้ำเพิ่มขึ้นมาจากเดิม การทำ **Disk Striping** จะผสมผสานพื้นที่ต่างๆ มากกว่า **1** พื้นที่จากเนื้อที่ว่างเข้าเป็นไดร์ฟทางตรรกะ (**logical drive**) เดียวกัน แล้วกระจายการจัดเก็บข้อมูลลงไปยังไดร์ฟทั้งหมดพร้อมกันในเวลาเดียวกัน ข้อมูลที่เข้ามาจะถูกแตกออกที่ **RAID Controller** และถูกเขียนลงฮาร์ดดิสก์ที่นำมาต่อในลักษณะ "ขนาน" นี้ก็จะเกิดขึ้นเช่นเดียวกันในกรณีของการอ่านข้อมูลด้วย ดังนั้นการอ่านและการเขียนข้อมูลของ **RAID 0** ที่มีการนำเอาฮาร์ดดิสก์ **3** ตัวมาต่อเชื่อมกันก็จะมีความเร็วเป็น **3** เท่าของการใช้ฮาร์ดดิสก์เพียงตัวเดียว ดังแสดงตามรูปที่ 8 – 8



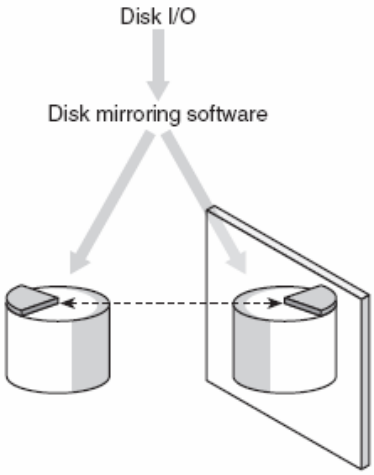
รูปที่ 8 – 8 **RAID 0**

รูปที่ 8 – 8 แสดงให้เห็นฮาร์ดดิสก์ 3 ตัว ในการเริ่มสร้าง **Stripe Set** ข้อมูลทั้งหมดจะมี **192 K** โดยข้อมูล **64K** ชุดแรกจะถูกเขียนในแถวบน **Disk1** ข้อมูล **64K** ชุดที่สองจะถูกเขียนลงบน **Disk2** และข้อมูล **64K** ชุดสุดท้ายจะถูกเขียนไว้บน **Disk3** การทำ **Stripe** แก่ดิสก์มีข้อดีอยู่หลายอย่างคือสามารถสร้างพาร์ทิชัน ขนาด **1** หน่วยใหญ่ จากพาร์ทิชันขนาดเล็กหลายๆ หน่วย ซึ่งจะทำให้สามารถใช้พื้นที่การใช้งานของดิสก์ได้มีประสิทธิภาพมากยิ่งขึ้น โดยเฉพาะอย่างยิ่งการทำงานกับ **Disk Controller** มากกว่า **1** ตัว

อย่างไรก็ตาม แม้ความเร็วในการอ่านและเขียนจะเพิ่มขึ้น แต่ **RAID 0** ก็ยังมีข้อเสียอยู่ตรงที่ไม่มี **Fault Tolerance** หรือ กระบวนการตรวจสอบความผิดพลาดของข้อมูล นั่นคือถ้าฮาร์ดดิสก์ตัวใดตัวหนึ่งมีอาการเสียเกิดขึ้น นั่นหมายความว่าข้อมูลทั้งหมดก็จะใช้ไม่ได้ตามไปด้วย ดังนั้น **RAID 0** จึงเหมาะสำหรับระบบที่ไม่ใหญ่นัก และให้ความสำคัญกับเรื่องความเร็วของการส่งผ่านข้อมูลจำนวนมาก และไม่ค่อยให้ความสำคัญของความผิดพลาดของข้อมูลมากเท่าไหร่ เพราะถ้าข้อมูลเกิดผิดพลาดก็สามารถแก้ไขได้ทันที และสามารถทำการ แบ็คอัพได้ทุกครั้งหลังทำงานเสร็จแล้ว นอกจากนั้น **Stripe set** ยังสามารถรวบรวมพื้นที่จากไดร์ฟต่างชนิดกันได้ เช่น **SCSI (Small Computer System Interface), ESDI (Enhanced Small Device Interface)** และแบบ **IDE (Integrated Device Electronic)** เป็นต้น

8.11.3 RAID 1 (Disk Mirroring)

คือการทำ **Disk mirroring** โดยการทำสำเนาซ้ำ **(duplicate)** ข้อมูลในพาร์ทิชันหนึ่งๆ แล้วนำไปจัดเก็บไว้ในดิสก์อีกลูกหนึ่ง ดังนั้นจะมีข้อมูลที่เหมือนกันอยู่ 2 ชุดตลอดเวลา และแยกจัดเก็บไว้ในดิสก์คนละตัวกัน การทำเช่นนี้จะทำให้พาร์ทิชันจะมีขนาดเท่ากัน ดิสก์ที่ใช้จึงต้องมีขนาดเท่ากัน วิธีการนี้เป็นวิธีที่ง่ายที่สุดในการป้องกันความเสียหายที่เกิดจากการมีข้อมูลเพียงชุดเดียวอยู่ในดิสก์ตัวเดียว วิธีการทำ **Mirror** นี้นับได้ว่าเป็นการสำรองข้อมูลวิธีหนึ่ง แต่จะมีข้อดีกว่าการสำรองข้อมูลตามปกติเพราะจะทำการอัพเดทข้อมูลชุดสำเนา พร้อมกับข้อมูลจริงตลอดเวลา จึงเป็นระบบการสำรองข้อมูลอย่างต่อเนื่อง สำหรับการดำเนินการจะใช้วิธีการ **Duplex** เพื่อสลับการจัดส่งข้อมูลชุดเดียวกันไปเก็บไว้ในดิสก์ทั้งสองตัว ดังแสดงตามรูปที่ 8 – 9



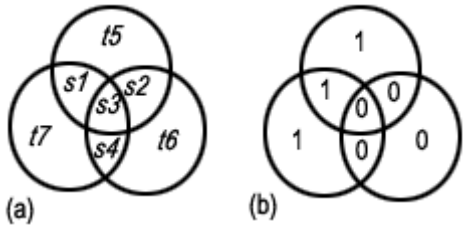
รูปที่ 8 – 9 **RAID 1**

RAID 1 มีลักษณะโครงสร้างภายในตามชื่อของมัน ก็คือจะมีฮาร์ดดิสก์ 2 ตัวที่เก็บข้อมูลเหมือนกันทุกประการ (**100% Data Redundancy**) เราจึงถือได้ว่าฮาร์ดดิสก์ตัวหนึ่งเสมือนเป็น "เงา" ของอีกตัวได้ และในยามที่ข้อมูลในฮาร์ดดิสก์ตัวใดตัวหนึ่งเกิดความผิดพลาดขึ้นข้อมูลของฮาร์ดดิกส์อีกตัวก็จะถูกก๊อปปี้ทับข้อมูลที่ผิดพลาดนั้น ระบบนี้จึงเป็นระบบที่มีประสิทธิภาพในการตรวจจับและแก้ไขข้อผิดพลาด (**Error Checking/Correction**) สูงที่สุดเพราะข้อมูลจะเสมือนมีการแบ๊คอัพไว้ตลอดเวลา และด้วยการที่มันต้องแบ๊คอัพอยู่ตลอดเวลานี่เองที่ทำให้ **RAID1** มีประสิทธิภาพในการเขียนข้อมูลช้ากว่าฮาร์ดดิกส์ตัวเดียวโดดๆ เสียอีก อย่างไรก็ตามข้อเสียอันนี้ก็ถูกชดเชยด้วยประสิทธิภาพในการอ่านที่เพิ่มมากขึ้นกว่าฮาร์ดดิกส์ตัวเดียว 2 เท่าทำให้เราสามารถนำ **RAID1** ไปใช้งานที่คำนึงถึงความเร็วในการอ่านมากกว่าความเร็วในการเขียน ข้อมูลงานประเภทที่ว่าได้แก่งาน **Web Server** หรือ **FTP Server** ระดับกลางหรือจะนำไปใช้กับงานที่ต้องการความแน่นอนของข้อมูล สูงๆ เช่นงานด้านการเงิน การบัญชี งานจำพวกนี้ไม่ต้องการส่งผ่านข้อมูลที่รวดเร็วเหมือนงานใน **RAID 0** แต่ต้องการความแน่นอนของข้อมูลมากกว่า มีข้อควรระวังข้อหนึ่งเกี่ยวกับการใช้ **RAID 1** ก็คือถ้าเราใช้ซอฟท์แวร์ **Windows NT/2000** เป็นตัวควบคุมการทำงานของ **RAID 1** หรือใช้ **RAID Controller** ที่ไม่รองรับคุณสมบัติ **Mirroring** จะทำให้ไปหน่วงการทำงานของซีพียู และทำให้ประสิทธิภาพการทำงานลดลงอย่างมาก ดังนั้นควรจะใช้ฮาร์ดแวร์ **RAID Controller** เป็นตัวควบคุมการทำงานจะดีกว่า

8.11.4 RAID 2 (Hamming Code ECC)

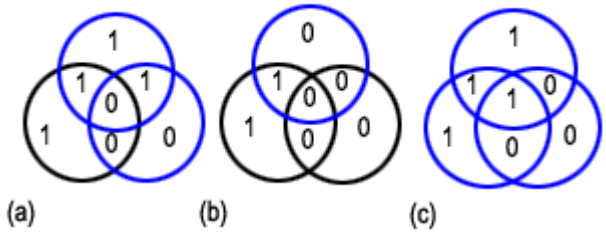
RAID 2 เป็น **RAID** ชนิดแรกที่มีการใช้เทคโนโลยีในการตรวจจับความผิดพลาดของข้อมูล โดยอาศัยการเข้ารหัสแบบ **Hamming Code ECC** (**Error Checking/Correction**) ก่อนที่จะพูดถึงวิธีการเข้ารหัสแบบ **Hamming Code** เราไปดูการตรวจจับความผิดพลาดของข้อมูลโดยการใช้บิต **Parity** กันก่อน ข้อมูลที่ถูกส่งเข้ามาเก็บในฮาร์ดดิสก์ แต่ละตัวสำหรับ **RAID 2** นั้น จะมีลักษณะเป็นขบวนของบิตเลขฐานสอง ซึ่งแน่นอนว่าในระหว่างการส่งผ่านข้อมูล โอกาสที่ข้อมูลที่เป็นขบวนบิตนี้จะผิดพลาดที่บิตใดบิตหนึ่งย่อมเกิดขึ้นได้ จึงได้มีการคิดวิธีเติมบิต **Parity** เข้าไปที่ท้ายขบวนบิตข้อมูล (**1 Word**) โดยบิตที่เติมเข้าไปนี้จะเป็น "**0**" หรือ "**1**" ก็ขึ้นกับว่าเราจะใช้การตรวจจับเป็น แบบ **Even Parity** หรือ **Odd Parity** ลองดูตัวอย่างต่อไปนี้

สมมติขบวนบิตที่เข้ามาเป็นดังนี้ **1 0 0 1 0 0 1** ถ้าใช้ วิธี **Even Parity** ในการตรวจจับความผิดพลาด บิต **Parity** ที่จะถูกเติมเข้าไปต่อจากขบวนบิตข้อมูลจะต้อง ทำให้ผลรวมแบบเลขฐานสองของทุกบิต (รวมบิตที่เพิ่มเข้าไปด้วย) มีค่าเท่ากับ **"0"** (วิธีจำง่ายๆ **0 + 0 = 1, 1 + 1 = 0, 0 + 1** และ **1 + 0 = 1**) จากตัวอย่างผลรวมของขบวนบิตข้อมูล (ยังไม่รวมบิต **Parity**) มีค่าเป็น **1+0+0+1+0+0+1 = 1** เพราะฉะนั้นบิต **Parity** ที่ถูกเติมเข้าไปก็คือ **"1"** เพื่อทำให้ผลรวมของทุกบิตทั้งหมด จะกลายเป็น **1 0 0 1 0 0 1 1**



รูปที่ 8 – 10

ส่วนในกรณีของ **Odd Parity** บิต **Parity** ที่จะถูกเติมเข้าไปจะต้องเข้าไปทำให้ผลรวมของทุกบิต (รวมบิต **Parity** ด้วย) มีค่าเป็น **"1"** และเมื่อปลายทางได้รับข้อมูลที่ผ่านการเติมบิต **Parity** มาแล้วก็จะสามารถตรวจสอบได้ว่าข้อมูลที่ได้รับมาผิดพลาด หรือไม่ ยกตัวอย่างสมมติว่าเกิดผิดพลาดขึ้นที่บิตที่ **3** ทำให้ข้อมูลที่ผ่านการทำ **Even Parity** มาแล้วผิดพลาดเป็น **1 0 1 1 0 0 1 1** ทางฝั่งรับจะรู้ได้ทันทีว่าข้อมูลนี้ผิดพลาด โดยดูจากผลบวกของทุกบิต **1+0+1+1+0+0+1+1 = 1** ซึ่งขัดกับการทำ **Even Parity** ที่ผลรวมของทุกบิตจะต้องเป็น **"0"** ทางฝั่งรับก็อาจจะส่งสัญญาณตอบกลับไปที่ฝั่งส่ง ให้ทำการส่งข้อมูลมาใหม่อีกครั้ง



รูปที่ 8 – 11

สำหรับวิธีเติมบิต **Parity** ที่ได้อธิบายข้างต้นนี้ยังมีข้อเสียอยู่ตรงที่ถ้าเกิดบิตข้อมูลเกิดการผิดพลาดพร้อมกัน **2** บิต ทางฝั่งรับจะไม่สามารถตรวจจับความผิดพลาดได้เลย เช่นสมมติว่าบิตที่ **2** และ **3** เกิดการผิดพลาดเป็น **1 1 1 1 0 0 1 1** ผลรวมของบิตทั้งหมดก็ยังเป็น **"0"** อยู่ดี แม้จะเกิดความผิดพลาดขึ้น และข้อเสียอีกประการก็คือวิธีเติมบิต **Parity** นี้ ทำได้เฉพาะสำหรับการตรวจจับความผิดพลาดเท่านั้น แต่ไม่สามารถระบุได้ว่าบิตใดเกิดความผิดพลาดขึ้น จึงทำการแก้ไขข้อมูลให้ถูกต้องไม่ได้ ด้วยเหตุนี้จึงต้องมีการคิดค้นวิธีที่จะ เข้ามาแก้ปัญหาเหล่านี้ วิธีที่ว่าก็คือวิธีการเข้ารหัสข้อมูล ซึ่งมีอยู่หลายวิธีด้วยกัน แต่ที่นำมาใช้ใน **RAID 2** จะเป็นวิธีการเข้ารหัสแบบ **Hamming Code**

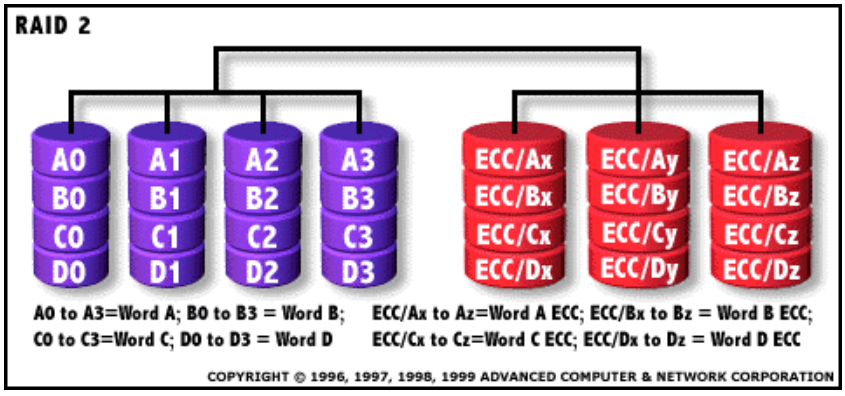
หลักการของการเข้ารหัสก็คือ ขบวนบิตข้อมูลจำนวน **k** บิต จะถูกเข้ารหัสให้กลายเป็นรหัสคำ (**Code Word**) ที่มีความยาว **n** บิต โดยจะมีการเติมบิตที่ใช้ในการตรวจสอบ (**Check Bits**) **n - k** บิตต่อท้ายบิตข้อมูล โดยบิตที่ใช้ในการตรวจสอบนี้จะมีความสัมพันธ์กับบิตข้อมูลด้วยส่วนจะสัมพันธ์ในรูปแบบไหนก็ขึ้นอยู่กับว่าใช้การเข้ารหัสแบบใด ในส่วนของการเข้ารหัสแบบ **Hamming Code** นี้จะอาศัยการสร้างบิตตรวจสอบจากวิธีการนี้ ในการเข้ารหัสแบบ **Hamming Code** จะใช้ขบวนบิตข่าวสาร **4** บิต และจะมีการเติมบิตที่ใช้ในการตรวจสอบเข้าไป **3** บิต รวมเป็น **7** บิต สมมติให้ **s1 - s4** แทนขบวนบิตข้อมูล และ **t5-t7** แทนบิตตรวจสอบ ดังนั้นขบวนบิตทั้งหมดหลังจากการทำการ เข้ารหัสแล้วจะเป็นดังนี้ **s1-s2-s3-s4-t5-t6-t7** บิต **t5-t7** หาได้จากวิธีในรูปที่ **8 – 10**

หลักการหาก็คือว่าทั้ง **t5, t6** และ **t7** จะต้องมีค่าที่ทำให้ผลรวมของบิตในแต่ละวงกลมเป็น **Even** (**"0"**) อย่างตัวอย่างใน รูปที่ **8 – 10 (b)** ถ้า **s = 1 0 0 0** บิต **t5** ก็ต้องเป็นบิตที่ทำให้ผลรวมของ **s1-s2-s3-t5** เป็น **"0"** ดังนั้น **t5** จึงเป็นบิต **"1"** ก็ทำในลักษณะเดียวกัน ดังนั้นขบวนบิตหลังจากผ่านการเข้ารหัสก็จะเป็น **1 0 0 0 1 0 1**

ตารางที่ **8 – 2** แสดงขบวนบิตข้อมูลที่เป็นไปได้ทั้งหมดกับขบวนบิตหลังผ่านการเข้ารหัส

s	t	s	t	s	t	s	t
0000	0000000	0100	0100110	1000	1000101	1100	1100011
0001	0001011	0101	0101101	1001	1001110	1101	1101000
0010	0010111	0110	0110001	1010	1010010	1110	1110100
0011	0011100	0111	0111010	1011	1011001	1111	1111111

สำหรับการเข้ารหัสโดยวิธี **Hamming Code** นี้ จะได้เปรียบวิธีเติมบิต **Parity** ตรงที่ทางฝั่งรับสามารถระบุได้ว่าบิต ใดเกิดความผิดพลาดขึ้นจึงทำให้เราสามารถแก้ไขความผิดพลาดที่เกิดขึ้นได้ แต่มีข้อแม้ว่าข้อผิดพลาดนั้นต้องมีเพียงบิตเดียว และต้องไม่ใช่บิต **s3** ลองพิจารณาดูรูปที่ **8 – 10** สมมติว่าใช้ขบวนบิตที่ผ่านการเข้ารหัสมาแล้วเหมือนตัวอย่างที่แล้วคือ **1 0 0 0 1 0 1** แล้วเกิดความผิดพลาดที่บิต **s2** ทำให้ข้อมูลเปลี่ยนเป็น **1 0 1 0 1 0 1** หรือเขียนเป็นไดอะแกรมได้ตามรูปที่ **8 – 10 (a)** จะเห็นได้ ว่าจะมีเฉพาะวงกลมเส้นประเท่านั้นไม่เป็นไปตาม **Even Parity** ดังนั้นบิตที่เป็นไปได้ที่จะทำให้เกิดความผิดพลาดกับวงกลม ทั้งสองวงก็คือบิต **s3 = 0** และ **s2 = 1** แต่เราจะตัดการพิจารณาบิต **s3** ออกไปเพราะบิต **s3** อยู่ในอาณาเขตของวงกลมเส้นทึบด้วย สาเหตุก็เนื่องมาจากว่าถ้าบิต **s3** เกิดความผิดพลาด มันก็จะไปส่งผลกระทบต่อ **Even Parity** ของวงกลมเส้นทึบด้วย จึงเหลือบิตให้พิจารณาเพียงบิตเดียวคือ **s2** เพราะฉะนั้นทางฝั่งรับก็จะรู้ได้ทันทีว่าบิต **s2** เป็นบิตผิดพลาด ก็จะมีการแก้ไขเกิด ขึ้นโดยการกลับบิตจาก **"1"** เป็น **"0"** ส่วนรูปที่ **8 – 10 (b)** บิตที่ผิดพลาดจะเป็นบิต **t5** ซึ่งเป็นการตรวจสอบที่เพิ่มเข้าไป จากรูปจะเห็นได้ว่า ถ้าบิตตรวจสอบเกิดความผิดพลาด ทางฝั่งรับจะรู้ได้ทันทีว่าเป็นบิตไหน เพราะวงกลมเส้นประจะเกิดขึ้นแค่วงเดียว และบิต **s1, s2** และ **s3** ก็อยู่ในอาณาเขตของวงกลมทึบด้วย ดังนั้นจึงมีเพียงบิตเดียวที่อยู่ในวงกลมเส้นประล้วนๆ นั้นคือบิต **t5** ในรูปที่ **8 – 10 (c)** จะเป็นไดอะแกรมแสดงจุดบอดของวิธี **Hamming Code** เพราะถ้าบิตตรงกลางวงกลมบิต **s3** เกิดผิดพลาดขึ้นทางฝั่งรับจะไม่มีทางรู้ได้เลยว่าบิตใดผิดพลาด เพราะวงกลมทั้งสามวงเป็นเส้นประหมด โดยทางฝั่งรับจะตีความว่าข้อมูลที่ได้รับเกิดการผิดพลาด แต่จะไม่มีการแก้ไขใดๆ เกิดขึ้น ต้องให้ทางฝั่งส่งทำการส่งข้อมูลมาใหม่เท่านั้น



รูปที่ 8 – 12 RAID 2

ทางฝั่งรับข้อมูลจะมีตารางข้อมูลในตารางที่ 8 – 2 เอาไว้เพื่อถอดรหัสเอาข้อมูลออกมา เช่นเดียวกับทางฝั่งส่ง ใน **RAID 2** นั้น ฮาร์ดดิสก์แต่ละตัวจะเก็บข้อมูลที่เข้ามาทีละบิตๆ ดูรูปที่ 8 – 11 **A0-A3** จะแทนข้อมูล **1** เวิร์ด โดยทั้ง **4** บิตนี้จะผ่านการเข้ารหัสแบบ **Hamming Code** โดยการเติมบิตตรวจสอบ **ECC/Ax, ECC/Ay** และ **ECC/Az** เข้าไป ทำให้ **RAID 2** มีความสามารถ ในการแก้ไขความผิดพลาดได้ แต่ข้อเสียที่เราเห็นได้อย่างชัดเจนของ **RAID 2** ก็คือการที่มันต้องใช้ฮาร์ดดิสก์ เพื่อเก็บบิตตรวจ สอบเกือบๆเท่ากับจำนวนฮาร์ดดิสก์ที่ใช้เก็บข้อมูล เพราะยิ่งขนาด **word** ของข้อมูลเล็กเท่าไหร่สัดส่วนระหว่างฮาร์ดดิสก์ทั้งสอง ชนิดก็ยิ่งเกือบจะเท่าๆกัน ดูจากรูปที่ 8 – 11 นั่นก็หมายความว่า เราต้องเสียค่าใช้จ่ายอีกประมาณเกือบเท่าตัวในการเก็บบิตตรวจสอบ ซึ่งเป็นเรื่องที่ค่อนข้างสิ้นเปลืองทีเดียว

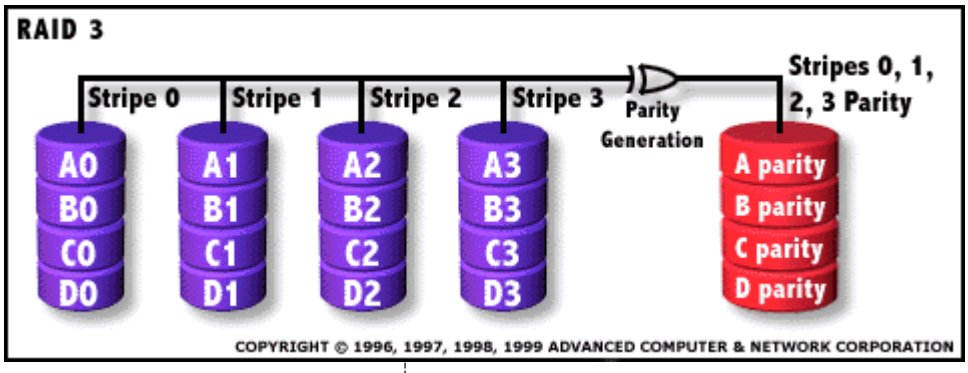
8.11.5 RAID 3 (Parallel Transfer with Parity)

เป็นการทำ **Disk Striping** โดย **ECC** จะถูกเก็บในรูปแบบของบิต **Parity** โดยโครงสร้างจะมีลักษณะการต่อฮาร์ดดิสก์เป็นแบบ **Stripe** เช่นเดียวกับ **RAID 0** และข้อมูลที่เข้ามาแต่ละครั้งจะถูกแยกเก็บไว้ที่ฮาร์ดดิสก์แต่ละตัว ส่วนดิสก์แต่ละตัวจะเก็บข้อมูลกี่บิตหรือกี่ไบต์ก็ขึ้นอยู่ที่การกำหนด (ข้อมูลที่เก็บอยู่ใน **A0, A1, A2, ...** ตามรูปที่ 8 – 13 ว่าเป็น **1** เวิร์ด) จากรูปที่ 8 – 13 ข้อมูลที่เข้ามาก็จะถูกแบ่งย่อยเพื่อเก็บไว้ที่ **A0, A1, A2, A3, B0, ...** จนกว่าจะเก็บข้อมูลได้หมด ลักษณะการต่อฮาร์ดดิสก์ตามรูปที่ 8 – 13 เป็นการต่อที่เรียกว่า **4+1** คือมีฮาร์ดดิสก์สำหรับเก็บข้อมูล **4** ตัว และเก็บ **Parity** ที่ได้จากการคำนวณทางคณิตศาสตร์ของข้อมูลในแถวนั้นๆ อีก **1** ตัวการคำนวณหา **Parity** นั้นจะอาศัยวิธีการทางคณิตศาสตร์ง่ายๆ คือการนำเอาลอจิก **XOR** เข้ามาช่วย โดยเงื่อนไขของการ ทำ **XOR** เป็นดังที่แสดงในตารางที่ 8 – 3

ตารางที่ 8 – 3

XOR Example		
A XOR B		Result
0	0	0
1	0	1
0	1	1
1	1	0

สาเหตุที่นำลอจิก **XOR** มาใช้ก็เนื่องมาจากคุณสมบัติที่ว่า ถ้านำข้อมูลเวิร์ด **A** และ **B** มา **XOR** กันได้ผลลัพธ์ตัวหนึ่ง แล้วเกิดเหตุการณ์ที่เวิร์ด **A** หรือ **B** อันใดอันหนึ่งเกิดสูญหายไป เราสามารถสร้างเวิร์ดที่หายไปนั้นให้กลับมาเหมือนเดิมได้ โดยการ **XOR** ผลลัพธ์กับเวิร์ดที่ยังเหลืออยู่ดังตัวอย่างต่อไปนี้ สมมติให้ข้อมูล **word A** คือ **0 1 1 0** และ **word B** คือ **1 1 0 0** ทั้งสองเวิร์ดเมื่อนำมา **XOR** กันจะได้ผลลัพธ์ **1010** สมมติให้ **word A** เกิดการสูญหาย เราสามารถสร้าง **word A** ได้โดยนำผลลัพธ์มา **XOR** กับ **word B** จะได้ **0 1 1 0** ซึ่งก็คือ **word A** นั่นเอง จากเหตุผลข้างต้นจึงมีการนำลอจิก **XOR** มาสร้าง **Parity** ขึ้นมาโดย **A Parity = A0 XOR A1 XOR A2 XOR A3** (แถว **B, C** และ **D** ก็เป็นแบบเดียวกัน) และถ้าข้อมูลจากฮาร์ดดิสก์ตัวใดเกิดสูญหาย ก็สามารถสร้างเวิร์ดข้อมูลนั้นขึ้นมาใหม่ได้ด้วยการนำ **A Parity** มา **XOR** กับ **word** ข้อมูลที่ยังเหลืออยู่ สมมติให้เวิร์ดข้อมูลเป็นดังนี้ **A0= 1010, A1= 0011, A2 = 0001** และ **A3 = 1000** ดังนั้น **A Parity** จะมีค่าเท่ากับ **0000** และสมมติให้ข้อมูล **A2** เกิดสูญหายอันเนื่องมาจากฮาร์ดดิสก์ตัวที่ **3** เกิดปัญหาเราจะสร้างข้อมูล **A2** กลับคืนมาได้โดยนำ **A Parity 0000 XOR** กับเวิร์ดข้อมูลที่ยังเหลืออยู่ซึ่งก็คือ **A0, A1** และ **A3** จะได้ผลลัพธ์คือ **0001** ซึ่งก็คือ **word A2** นั่นเอง

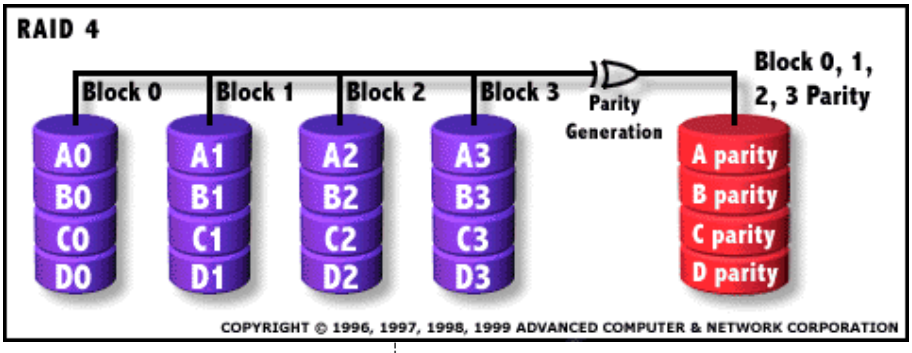


รูปที่ 8 – 13 RAID 3

แม้ว่า **RAID 3** จะมีข้อดีในการอ่านและเขียนข้อมูลได้อย่างรวดเร็ว เพราะต่อฮาร์ดดิสก์เป็นแบบ **Stripe** และใช้ฮาร์ดดิสก์ในการเก็บ **Parity** เพียงแค่ตัวเดียว แต่ถ้านำ **RAID 3** ไปใช้กับงานที่ข้อมูลที่มีการผ่านเข้าออกเป็นจำนวนเล็กน้อยในแต่ละครั้ง แต่ลักษณะการเขียนข้อมูลมีการกระจายไปทั่วทั้งฮาร์ดดิสก์ จะส่งผลให้เกิดเวลาคอขวดขึ้นที่ฮาร์ดดิสก์ตัวที่เก็บ **Parity** เพราะไม่ว่าข้อมูลจะไปปรากฏอยู่ในกลุ่มของเวิร์ดข้อมูลแถวไหน **RAID 3** ก็จะมีการสร้าง **Parity** ขึ้นมาตลอด ซึ่งแม้ว่าข้อมูลเราจะมีขนาดเล็ก แต่ **RAID 3** ก็จำเป็นต้องเสียเวลาไปสร้าง **Parity** ขึ้นมาตลอด ซึ่งแม้ว่าข้อมูลเราจะมีขนาดเล็ก แต่ **RAID 3** ก็จำเป็นต้องเสียเวลาไปสร้าง **Parity** ขึ้นในทุกๆ แถวที่ข้อมูลนั้นไปอยู่ ยิ่งข้อมูลกระจายไปอยู่แถวต่างๆมากขึ้น จำนวน **Parity** ก็จะมากขึ้นตาม และในแต่ละครั้งของการที่จะเขียนข้อมูลใหม่ลงไป **RAID 3** จำเป็นจะต้องรอให้ **Parity** ถูกเขียนให้เสร็จก่อนที่ข้อมูลเวิร์ดต่อไปจะถูกเขียน (เป็นลักษณะของการทำงานแบบ **Synchronous**) ยกตัวอย่าง ตามรูปที่ **8 – 13** ถ้าเราต้องการเขียนข้อมูลลงที่ **word A0** ฮาร์ดดิสก์ที่ต้องใช้ในการเขียนจะมีอยู่ **2** ตัวคือฮาร์ดดิสก์ตัวที่ **1** และฮาร์ดดิสก์ตัวที่ **5** จะเห็นได้ว่า ก่อนที่ **word B2** จะถูกเขียน จะต้องรอจนกว่าฮาร์ดดิสก์ตัวที่ **5** จัดการ **Parity** ของ **word A1** ให้เสร็จก่อนเวลาที่เกิดนี้แหละที่เป็นเวลาคอขวด ยิ่งมีการกระจายการเขียนข้อมูลไปหลายๆแถวเมื่อใด ก็ยิ่งต้องเสียเวลารอมากขึ้นเท่านั้น ฉะนั้นงานที่เหมาะจะเอา **RAID 3** ไปใช้งานก็ควรจะเป็นงานที่ต้องการการอ่านข้อมูลจำนวนมากในเวลารวดเร็ว เพราะการอ่านจะไม่ไปยุ่งกับส่วนของ **Parity** ถ้าข้อมูลไม่สูญหาย เช่นงานด้านการผลิตหรือตัดต่อ **Video**

8.11.6 RAID 4 (Independent Data Disks with Shared Parity Disk)

เป็นการทำ **Disk Striping** เป็นบล็อกข้อมูลขนาดใหญ่ แล้วนำมาเขียนลงบนดิสก์แต่ละตัวในรูปแบบของอาเรย์ (**array**) โดยไม่ต้องกระจายไปเก็บเป็นข้อมูลชุดเล็กๆ และมีดิสก์ส่วนหนึ่งแยกไว้ต่างหากสำหรับจัดเก็บข้อมูลบิต **parity** สำหรับใช้ตรวจสอบความถูกต้องของข้อมูล แต่ละครั้งที่ทำการเขียนข้อมูล บิต **parity** จะถูกอ่านออกไปจากดิสก์ส่วนนี้และถูกปรับปรุงให้ตรงกับค่าที่ถูกต้อง การทำเช่นนี้จะทำให้เกิด **overhead** เนื่องจากวิธีการ **Block Interleaving** จะทำงานกับบล็อกข้อมูลขนาดใหญ่ได้ดีกว่า **Transaction Based Processing** หลักการทำงานของ **RAID 4** จะเหมือนกับ **RAID 3** แทบทุกประการจะต่างกันก็ตรงที่ข้อมูลแต่ละเวิร์ดใน **RAID 3** นั้น จะมีขนาดกี่บิตหรือกี่ไบต์ก็อยู่กับการกำหนด แต่ใน **RAID 4** เวิร์ดข้อมูลจะเก็บในรูปของบล็อกข้อมูล (**1 Sector**) เพราะฮาร์ดดิสก์ส่วนใหญ่จะอ่านข้อมูลแต่ละครั้งจะอยู่ในรูปของบล็อก โดยขนาดของบล็อกจะมีตั้งแต่ **512** ไบต์ ถึง **8 KB** ขึ้นกับระบบปฏิบัติการที่ใช้ รูปที่ **8 – 14** แสดงการทำงานของ **RAID 4** ในการเปลี่ยนมาใช้การเก็บข้อมูลเป็นบล็อกนี้จะช่วยให้จำนวนครั้งในการเก็บข้อมูลและกระบวนการเปรียบเทียบ **XOR** น้อยลง ซึ่งจะส่งผลให้เวลาในการกู้หรือเก็บข้อมูลสั้นลงตามไปด้วย อย่างไรก็ตามเวลาคอขวดอย่างที่เกิดใน **RAID 3** ก็ยังคงมีอยู่เช่นเดิม



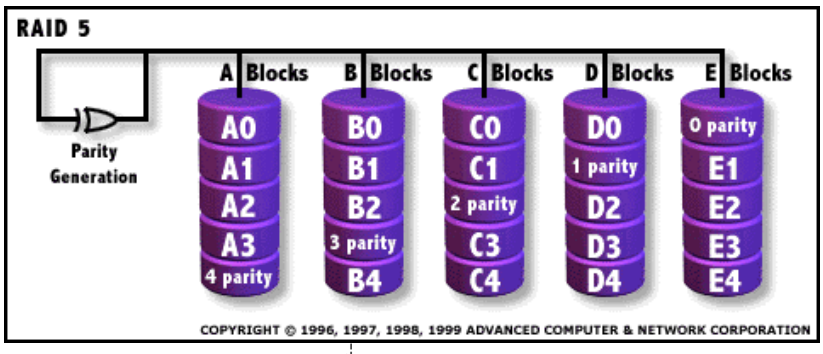
รูปที่ **8 – 14 RAID 4**

8.11.7 RAID 5 (Independent Data Disk with Distributed Parity Block)

RAID 5 จะมีการเก็บข้อมูลเป็นบล็อกเช่นเดียวกับใน **RAID 4** ข้อเสียที่สำคัญที่สุดของ **RAID 3** และ **4** ก็คือเรื่องเวลาคอขวดที่เกิดจากการเขียนส่วน **Parity** ดังที่ได้ยกตัวอย่างไปแล้ว สำหรับ **RAID 5** จะมีการแก้ไขปัญหานี้โดยการนำเอาส่วนของ **Parity Block** ไปกระจายอยู่ในฮาร์ดดิสก์แต่ละตัว ไม่แยกมาเก็บโดดๆ เหมือนใน **RAID 3** การกระทำเช่นนี้จะลดเวลาคอขวดได้อย่างไร จะขอเปรียบเทียบกับตัวอย่างที่ได้ยกไปในหัวข้อ **RAID 3** นั่นคือการเขียนข้อมูลที่ **Word A0** และ **B1** ในกรณีของ **RAID 5** การเขียนข้อมูลลง **Word A0** จะใช้ฮาร์ดดิสก์ **2** ตัว คือตัวที่ **1** และ **5** ส่วน **Word B1** จะใช้ตัวที่ **2** และ **4** จะเห็นได้ว่าไม่ต้องไปเสียเวลารอให้ **RAID 5** ทำส่วนของ **Parity** ให้เสร็จก่อนเหมือน **RAID 3** เพราะเราสามารถเขียนทั้ง **Word A0** และ **B1** ไปได้พร้อมๆ กัน นี่จึงเป็นที่มาของการกระจายส่วนของ **Parity Block** ให้อยู่ในฮาร์ดดิสก์ทุกตัว

อย่างไรก็ตามการมี **Parity Block** เช่นใน**RAID 3, 4** หรือ **5** จะส่งผลกระทบต่อการเขียนข้อมูลค่อนข้างมากเช่นกัน เพราะถ้าเปรียบเทียบระหว่าง **RAID 5** กับ **RAID 0** จะทำได้ง่าย เพราะจะเป็นการเขียนลงฮาร์ดดิสก์เพียงตัวเดียว แต่ในกรณีของ **RAID 5** จำนวนบล็อกที่ต่ำสุดที่จะถูกเขียนจะไม่ใช่ **1 Block** แล้ว เช่นในรูปที่ **8 – 15** การเขียนข้อมูลลงใน **Block B2** ข้อมูลเก่าที่อยู่ใน **Block B 2** และ **Parity Block 2** จะต้องถูกอ่าน

ขึ้นมาก่อน แล้วนำมาเก็บไว้ในหน่วยความจำแคช แล้วนำข้อมูลใน **Block B2** มาทำการ **XOR** กับ **Parity** ผลที่ได้ก็คือข้อมูลของบล็อกที่เหลือในแถวนั้นที่ได้ถูกนำมา **XOR** กันแล้ว หลังจากอ่านข้อมูลเก่าเสร็จ ข้อมูลใหม่ก็จะถูกเขียนลงไปที่ **BlockB2** จากนั้นก็จะมีการคำนวณ **Parity** ใหม่อีกครั้งโดยการนำเอาข้อมูลใหม่ไป **XOR** กับผลที่ได้จากการอ่านในครั้งแรกก่อน แล้วจึงจะมีการเขียน **Parity** ลงใน **Parity Block** จะเห็นได้ว่าต้องใช้กระบวนการอ่านและเขียนถึง **4** ครั้งกับการเขียนข้อมูลเพียงบิตเดียวดังนั้นจึงมีการนำหน่วยความจำแคชมาใช้กับตัว **RAID 5 Controller** เพื่อช่วยเพิ่มความเร็วในการเขียนข้อมูลให้เร็วมากขึ้น (จาก **5–12 ms** เหลือ **0.5 ms**) โดยมีขนาดประมาณ **64 – 256 MB** การนำหน่วยความแคชมาใช้นี้ส่งผลให้ประสิทธิภาพในการทำงานของ **RAID 5** ดีกว่า **RAID 0**



รูปที่ 8 – 15 **RAID 5**

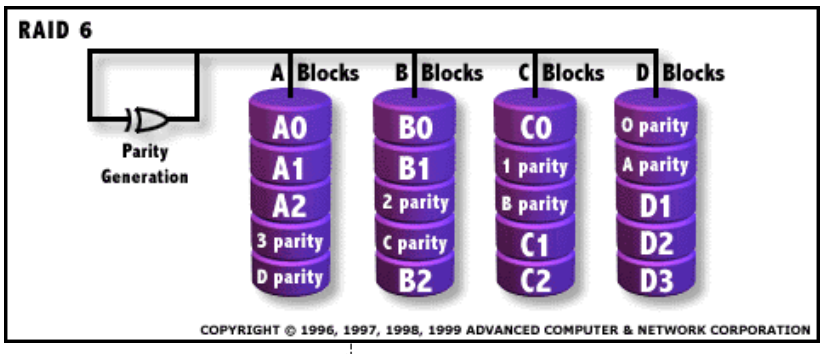
นอกจากนั้น **RAID 5** ยังมาพร้อมกับคุณสมบัติ "**Hot Swap**" นั่นคือสามารถสลับสับเปลี่ยนฮาร์ดดิสก์ที่ดีกับฮาร์ดดิสก์ที่เสียได้ในขณะที่ระบบกำลังทำงานอยู่ สาเหตุก็เพราะ **RAID5** สามารถสร้างข้อมูลที่หายไปกลับมาใหม่ได้โดยอาศัย **Parity Block** ที่เก็บอยู่ในฮาร์ดดิสก์ตัวอื่นนั่นเอง สำหรับงานที่เหมาะกับการนำ **RAID 5** ไปใช้งานก็ได้แก่งานที่ไม่ต้องการปริมาณการเขียนข้อมูลมากนักแต่จะถูกอ่านข้อมูลมากกว่า และข้อมูลที่เก็บก็มีขนาดใหญ่มากเกินกว่าที่จะลงทุนทำฮาร์ดดิสก์เงาเพื่อแบ็คอัพข้อมูลเช่นใน **RAID 1** เช่นงานจำพวก **File Server, Database Server, WWW, E-mail** หรือ **News Server** หรือ **Intranet Servers**

นอกจาก **RAID** ระดับมาตรฐานทั้ง **5** ระดับข้างต้น ยังมี **RAID** ระดับย่อยๆ ซึ่งเกิดขึ้นตามความต้องการที่แตกต่างกันออกไป จึงต้องมีการออกแบบระบบ **RAID** เพื่อตอบสนองความต้องการที่เกิดขึ้นนี้ เช่น **RAID 6** จะให้ความสำคัญกับความป้องกันความเสียหายในระดับสูงมากๆ **RAID 10** (หรือที่รู้จักกันในนามของ **RAID** ระดับ **0&1**) จะพุ่งเป้าไปที่ความสามารถในด้าน **input/output** และการปกป้องความเสียหาย **RAID 53** จะเป็นส่วนผสมของ **RAID** ระดับ **0** และ **3** เพื่อความสามารถในการเขียนและอ่านข้อมูล อย่างไรก็ตามคุณยังสามารถออกแบบระบบ **RAID** เพื่อตอบสนองการทำงานที่เฉพาะเจาะจงของคุณเองได้ ซึ่งด้วยศักยภาพและความยืดหยุ่นที่มีอยู่ในการออกแบบ **RAID** นี้ จะช่วยให้คุณพบทางออกที่ตรงตามความต้องการ

8.11.8 RAID 6 (Independent Data Disks with Two Independent Distributed Parity Schemes)

RAID 6 นั้นจะมีพื้นฐานการทำงานเหมือนกับ **RAID 5** แทบทุกประการ เพียงแต่ว่า **RAID 6** มีการเพิ่ม **Fault Tolerance** ให้มากขึ้นกว่า **RAID 5** โดยการเพิ่ม **Parity Block** เข้าไปอีก **1** ชุด ดังรูปที่ 8 – 16 เพื่อยอมให้สามารถทำการสลับเปลี่ยนฮาร์ดดิสก์ได้พร้อมกัน **2** ตัว ในยามที่เกิดเหตุเสียขึ้นพร้อมกัน และด้วยการที่มี

Parity Block เพิ่มขึ้นนี้จึงส่งผลให้การเขียนข้อมูลช้ายิ่งกว่าใน **RAID 5** อีก นอกจากนั้นการเพิ่มจำนวน **Parity Block** ก็ยังส่งผลให้จำนวนฮาร์ดดิสก์ที่ใช้เพิ่มขึ้นอีกด้วย สมมติว่าใช้ฮาร์ดดิสก์สำหรับเก็บข้อมูล **n** ตัว จะต้องจัดหาฮาร์ดดิสก์มาสำหรับการต่อแบบ **RAID 6** นี้ **n+2** ตัว ดังนั้นงานที่จะนำ **RAID 6** ไปใช้ก็ควรจะเป็นงานประเภท **Mission Critical** หรืองานที่ต้องการเสถียรภาพของข้อมูลในระดับสุดยอดจริงๆ ถึงจะคุ้มค่าต่อการลงทุน



รูปที่ 8 – 16 RAID 6

8.11.9 RAID 10 (Mirroring with striped subsets)

RAID 10 ความจริงแล้วก็คือการรวมเอาโครงสร้างของ **RAID 0** และ **1** เข้าด้วยกันนั่นเอง การรวมกันนี้จะส่งผลให้การเข้าถึงข้อมูลจะรวดเร็วขึ้น (คุณสมบัติของ **RAID 0**) ในขณะเดียวกันก็จะมีการแบ็คอัพข้อมูลไปด้วยตลอดเวลา (คุณสมบัติของ **RAID 1**) ลักษณะของโครงสร้าง **RAID 10** จะเป็นดังรูปที่ 8 – 17 นั่นคือฮาร์ดดิสก์แต่ละตัวก็จะมีฮาร์ดดิสก์เงาอยู่คู่กัน โดยข้อมูลของฮาร์ดดิสก์แต่ละคู่ก็จะส่งออกมาในลักษณะขนานกัน และจากโครงสร้างของ **RAID 10** นี้ จึงมีชื่อเรียก **RAID 10** อีกอย่างว่าเป็น **RAID** ที่มีลักษณะ 2 มิติ

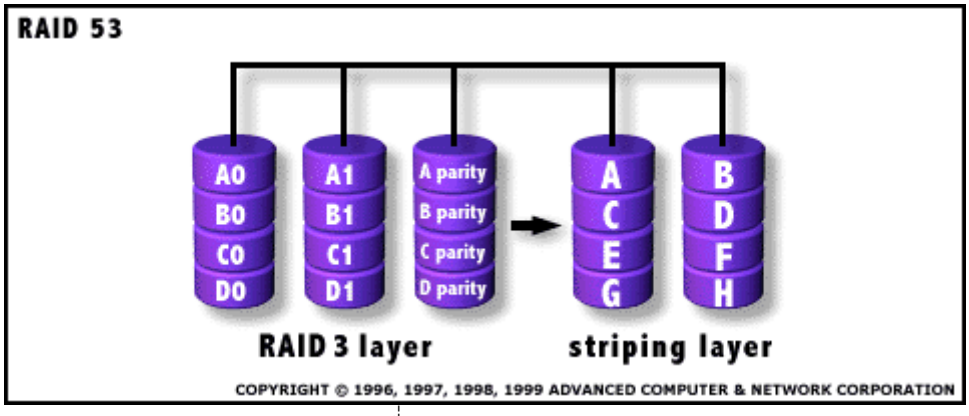
รูปที่ 8 – 17 RIAD 10

จากการที่ **RAID10** ต้องมีฮาร์ดดิสก์เงาคู่กับฮาร์ดดิสก์หลักทุกตัว จะทำให้การเพิ่มจำนวนฮาร์ดดิสก์ในอนาคตทำได้ค่อนข้างลำบาก เพราะยิ่งเพิ่มจำนวนฮาร์ดดิสก์เก็บข้อมูลมากขึ้นเท่าใด ก็ต้องเพิ่มฮาร์ดดิสก์แบ็คอัพมากขึ้นเป็นเงาตามตัว เพราะฉะนั้นงานที่จะนำ **RAID 10** ไปใช้จึงควรเป็นงานประเภท **Database Server** ที่ต้องการ

ประสิทธิภาพในการอ่าน/เขียนข้อมูลสูงๆ และมี **Fault Tolerance** ดี แต่มีความจุข้อมูลไม่สูงมากนัก และไม่ต้องการคุณสมบัติด้าน **Scalability** มากเท่าใด

8.11.10 RAID 53 (High I/O + Data Transfer Performance)

RAID 53 นั้น ถ้าพิจารณาจากพื้นฐานการทำงานแล้วน่าที่จะเรียกว่า **RAID 30** มากกว่า เพราะเป็นการนำเอาการจัดเรียงแบบ **Stripe** อย่างใน **RAID 0** มาใช้ โดยข้อมูลแต่ละส่วนจะใช้โครงสร้างแบบ **RAID 3** (ดูรูปที่ 8 – 18 ประกอบ) ดังนั้น **RAID 53** จึงมีอัตราการส่งข้อมูลสูงอันเนื่องมาจากโครงสร้าง **RAID 0** และมี **Fault Tolerance** ในระดับเดียวกับ **RAID 3** ด้วยคุณสมบัติ ดังกล่าว **RAID 53** จึงมักถูกนำไปใช้กับงานที่เคยใช้กับ **RAID 3** มาก่อน แต่ต้องการเพิ่มความเร็วในการส่งผ่านข้อมูลให้มากขึ้น แต่ต้องตระหนักเสมอว่า **RAID 53** นี้ยังคงมีรูปแบบการทำงานแบบ **Synchronous** ดังนั้นปัญหาเรื่องเวลาคอขวดก็จะยังคงมีอยู่เหมือนกับ **RAID 3**



รูปที่ 8 – 18 RAID 53

8.11.11 การจัดทำเซ็กเตอร์สำรอง (Sector Sparing)

การจัดทำเซ็กเตอร์สำรอง หรือที่เรียกว่า "**Hot Fixing**" เป็นคุณสมบัติเพิ่มเติมของระบบปฏิบัติการเครือข่ายที่มีในปัจจุบัน เช่น **Windows 2000 Server** นั่นคือหากระบบปฏิบัติการตรวจพบว่ามีส่วนหนึ่งส่วนใดของฮาร์ดดิสก์เกิดความเสียหาย จะทำการคัดลอกข้อมูลจากเซ็กเตอร์ที่เสียหายทั้งหมดไปจัดเก็บไว้ในเซ็กเตอร์ส่วนที่ดีในขณะที่เครื่องเซิร์ฟเวอร์กำลังทำงาน ดังแสดงตามรูปที่ 8 – 19

รูปที่ 8 – 19 การสำรองข้อมูลในเซ็กเตอร์ที่เสียหาย

คุณสมบัตินี้เป็นการเพิ่มความสามารถในการฟื้นฟูระบบเครือข่ายในระบบไฟล์ไฟล์โดยอัตโนมัติ ถ้าระหว่างการส่งข้อมูลเข้า-ออกจากดิสก์ ระบบปฏิบัติการตรวจพบว่ามีเซ็กเตอร์ซึ่งได้รับความเสียหาย **Fault Tolerant Driver** จะพยายามเคลื่อนย้ายข้อมูลซึ่งอยู่ในเซ็กเตอร์ที่เสียหายนั้นไปจัดเก็บในเซ็กเตอร์ที่ดี และวางแผนในการ

ซ่อมแซมเซ็กเตอร์ในส่วนที่เกิดความเสียหาย ถ้าสามารถกู้คืนเซ็กเตอร์ที่เกิดความเสียหายได้ ระบบไฟล์ก็จะไม่ถูกเปลี่ยนแปลงไปจากเดิม การทำเซ็กเตอร์สำรองนี้สามารถทำได้เฉพาะอุปกรณ์จำพวก **SCSI** สำหรับอุปกรณ์จำพวก **ESID** และ **IDE** จะไม่สามารถทำเซ็กเตอร์สำรองได้

ระบบปฏิบัติการ เช่น **Microsoft Windows 2000 Server** จะมียูทิลิตี้ในรูปแบบของเครื่องมือสำหรับให้ผู้บริการระบบเครือข่ายใช้ในการตรวจสอบเซ็กเตอร์ต่างๆ ของฮาร์ดดิสก์ นอกจากนั้นยังมียูทิลิตี้ในการเตือนผู้บริหารระบบเครือข่ายทราบถึงความบกพร่องทั้งหมดของเซ็กเตอร์ และข้อมูลทั้งหมดอาจจสูญหายได้ ถ้าระบบการทำสำเนาข้อมูลซ้ำเกิดความล้มเหลว

8.11.12 การเพิ่มประสิทธิภาพของ Fault Tolerant

ระบบปฏิบัติการเครือข่ายที่ทันสมัยส่วนใหญ่จะมียูทิลิตี้สำหรับดำเนินการแก้ไขความเสียหาย หรือความบกพร่องของดิสก์ เช่นใน **Windows NT Server** จะมี **Disk Administrator** ไว้สำหรับสร้างระบบ **Fault Tolerant** ในรูปแบบของ **GUI (Graphic User Interface)** ซึ่งจะช่วยให้สามารถทำการสร้างพาร์ทิชัน และจัดการกับพาร์ทิชันเหล่านั้นได้โดยง่าย นอกจากนั้นยังมีตัวเลือกในการย้ายดิสก์นั้นไปยัง **Controller** ตัวอื่น หรือเปลี่ยน **ID** ของดิสก์ โดยที่ระบบปฏิบัติการยังยอมรับว่าเป็นดิสก์ต้นฉบับสำหรับจัดเก็บข้อมูล โปรแกรม **Disk Administrator** ได้ถูกพัฒนาให้สามารถรองรับการจัดโครงสร้างในรูปแบบต่างๆ ได้ดังนี้

- **Stripe Set** เป็นการรวมพื้นที่ของดิสก์หลายๆ ตัวลงในพาร์ทิชันขนาดใหญ่ **1** อัน และกระจายการเก็บข้อมูลไปยังไดร์ฟต่างๆ เท่ากัน
- **Stripe Set with Parity** เป็นการรวมพื้นที่ของดิสก์หลายๆ ตัวลงในพาร์ทิชันขนาดใหญ่ **1** อัน และกระจายการเก็บข้อมูลไปยังไดร์ฟต่างๆ เท่ากัน และทำการจัดเก็บ **Parity** สำหรับตรวจสอบความถูกต้อง โดยการเพิ่ม **Fault Tolerant Parity Information**
- **Mirror Set** เป็นการทำพาร์ทิชัน **1** อัน ใส่ลงไปในดิสก์แยกต่างหาก
- **Volume Set** เป็นการรวมพื้นที่ของดิสก์หลายๆ ตัว เป็นโวลุ่มขนาดใหญ่

8.12 การทำคลัสเตอร์ (Clustering)

หากมองย้อนไปในอดีต **10 – 15** ปีผ่านมา ระบบประมวลผลแบบศูนย์กลางอย่างเครื่องคอมพิวเตอร์เมนเฟรมได้ถูกเคลื่อนย้ายมาสู่ระบบเปิดที่มีการประมวลผลแบบกระจายมากขึ้น **(Decentralized Environment)** ปัจจัยอย่างหนึ่งที่ผลักดันให้เกิดการประมวลผลแบบกระจาย ก็คือการกระจายระบบงานจะช่วยลดผลกระทบที่เกิดจากความเสียหาย หรือการหยุดให้บริการของระบบเครือข่าย โดยจะส่งผลกระทบเพียงกลุ่มเดียว อย่างไรก็ตามการกระจายงานก็จะทำให้เกิดความซับซ้อนในการบริหารจัดการเพิ่มมากขึ้นตามมา ความต้องการในการใช้บริการระบบเครือข่ายอย่างต่อเนื่องเพิ่มขึ้นตามลำดับ ถึงแม้ว่าผู้บริหารระบบจะพยายามเพิ่มองค์ประกอบทางฮาร์ดแวร์ รวมถึงการสร้างระบบสำรองมารอสำหรับใช้งานเมื่อจำเป็น แต่การกระจายระบบงานจะช่วยลดความรุนแรงที่เกิดจากความเสียหายของระบบคอมพิวเตอร์ได้ จากในอดีตที่ต้องใช้วิธีย้ายสายแพร์ที่ต่อดิสด์ไดร์ฟไปต่อกับดิสก์ตัวสำรอง เมื่อระบบการจัดเก็บข้อมูลได้พัฒนาขึ้นมาเป็นแบบ **Dual Hosting Storage** การย้ายสายแพร์ก็ไม่มีความจำเป็นอีกต่อไป จากนั้นจึงมีการพัฒนา

โปรแกรมขนาดเล็กที่ช่วยจัดการให้ระบบสำรองทำงานแทนระบบหลัก ตรงนี้ถือว่าเป็นยุคแรกของระบบ **FMS (Fail-over Management Software)** หรือการทำคลัสเตอร์นั่นเอง

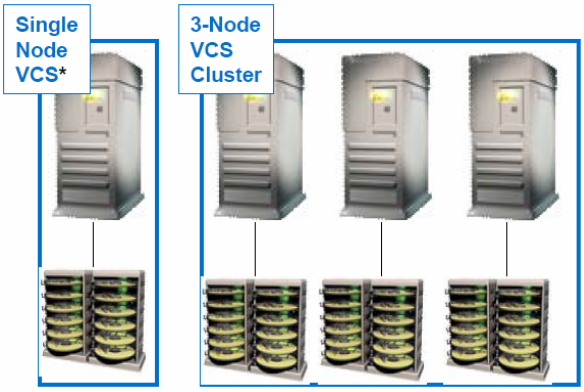
เทคโนโลยีการทำคลัสเตอร์ไม่ได้ถือกำเนิดขึ้นมาเพื่อแทนที่การทำงานของระบบ **Fault Tolerant** แต่ก็สามารถช่วยให้ประสิทธิภาพในการรักษาความปลอดภัยให้กับข้อมูลในระบบเครือข่ายได้อย่างยอดเยี่ยม คำว่า "คลัสเตอร์" หมายถึงกลุ่มของระบบที่มีการทำงานอย่างอิสระ โดยมีการทำงานร่วมกันเป็นระบบเดียว เมื่อระบบหนึ่งภายในกลุ่มล้มเหลว **Clustering Software** จะกระจายงานจากระบบที่ล้มเหลวไปยังระบบที่เหลือในคลัสเตอร์ สิ่งหนึ่งที่ต้องมีในแอพพลิเคชั่นที่ทำงานในลักษณะคลัสเตอร์ คือระบบการจัดเก็บข้อมูลที่มีเสถียรภาพและเป็นข้อมูลล่าสุด ณ จุดที่ระบบหลักล้มเหลว แอพพลิเคชั่นนั้นจะเรียกใช้งานระบบสำรองได้ ในหัวข้อนี้จะอธิบายรูปแบบของสถาปัตยกรรมคลัสเตอร์ซึ่งเป็นที่รู้จักในปัจจุบัน

8.12.1 Local Clustering

คือลักษณะของกลุ่มเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไป ที่ทำงานพร้อมกับซอฟต์แวร์จัดการเพื่อให้ **Application** ที่ดูแลนั้นสามารถให้บริการได้อย่างต่อเนื่อง ถึงแม้ว่าฮาร์ดแวร์หลักล้มเหลว สถาปัตยกรรมคลัสเตอร์แบบนี้ มีโครงสร้างอยู่ 2 รูปแบบ คือ **Shared Nothing Architecture** และ **Shared Data Architecture**

8.12.1.1 Shared Nothing Architecture

ถือว่าเป็นรูปแบบของคลัสเตอร์ในยุคแรก ที่ยังคงมีการใช้งานอยู่อย่างแพร่หลายพอสมควร กับแอพพลิเคชั่นที่มีลักษณะเป็น **Read-Only Type** เช่น **Web** จากรูปที่ 8 – 20 จะเห็นได้ว่า เครื่องเซิร์ฟเวอร์แต่ละเครื่องจะเชื่อมต่ออยู่กับอุปกรณ์การจัดเก็บข้อมูลของตัวเอง ไม่ยุ่งเกี่ยวกัน ข้อมูลจะถูกอัพเดทด้วยวิธีการ **Replicate** หรือใช้งานร่วมกันผ่าน **NAS (Network Attached Storage)** สำหรับโครงสร้างแบบนี้ โดยปกติแล้วข้อมูลที่ใช้งานร่วมกันจะอยู่ในรูปของไฟล์

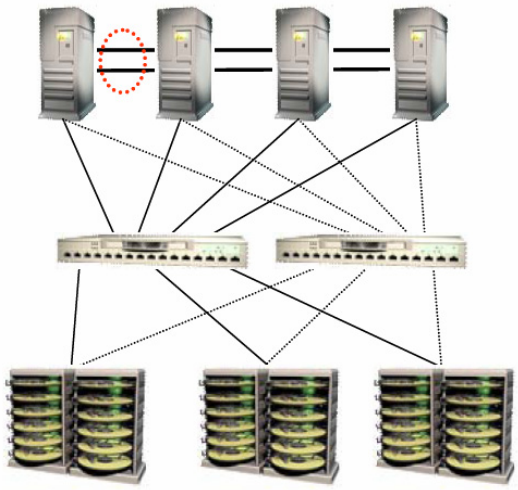


รูปที่ 8 – 20 Shared Nothing Architecture

8.12.1.2 Shared Data Architecture

โครงสร้างแบบนี้เป็นระบบคลัสเตอร์ที่ถูกเลือกใช้เป็นส่วนใหญ่ โดยเครื่องแต่ละเครื่องในกลุ่มจะมีการเชื่อมต่อเข้ากับอุปกรณ์จัดเก็บข้อมูลเดียวกัน ไม่ว่าจะเป็นแบบ **SCSI** หรือ **SAN** โดยดิสก์ที่เก็บข้อมูลของ **Application** ใน **Shared Storage** นี้ ในช่วงระยะเวลาหนึ่งจะถูก access ได้โดยคอมพิวเตอร์เพียงเครื่องเดียวที่ใช้

Application นั้นอยู่ ดังแสดงตามรูปที่ 8 – 21 จุดเด่นของโครงสร้างแบบนี้คือสามารถรองรับการทำคลัสเตอร์ของระบบจัดการฐานข้อมูลเชิงสัมพันธ์ (Relational Database Management System – RDBMS) ได้เป็นอย่างดี



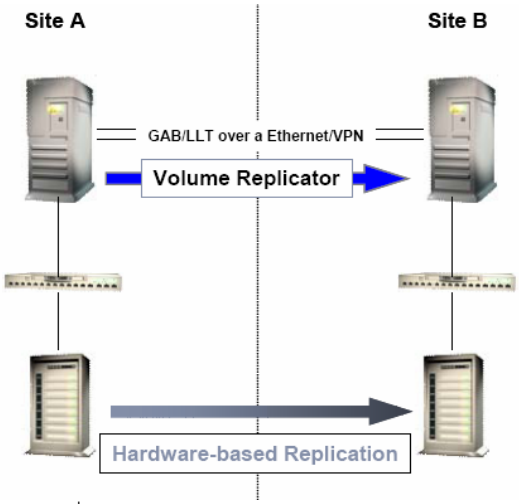
รูปที่ 8 – 21 Shared Data Architecture

8.12.2 Campus Clustering

ในบางกรณีการทำคลัสเตอร์แบบ Local Clustering อาจจะไม่เพียงพอต่อความต้องการขององค์กร หากองค์กรมีขนาดใหญ่ มีพื้นที่และอาคารในลักษณะที่เรียกว่า Campus เช่นในมหาวิทยาลัย เราสามารถออกแบบระบบให้สามารถครอบคลุมเหตุการณ์ความเสียหายได้มากกว่า Local Clustering จะรองรับได้ เช่นการทำคลัสเตอร์ในระยะไกลระหว่างอาคาร เป็นต้น Campus Clustering มีอยู่ 2 รูปแบบ คือ

8.12.2.1 แบบ Replicated Data Cluster

RDC หรือ Replicated Data Cluster เป็นโครงสร้างสถาปัตยกรรมประเภท Shared Nothing อีกรูปแบบหนึ่ง ข้อมูลล่าสุดของ Application ที่ทำคลัสเตอร์สามารถถูกอัพเดทถึงระบบงานสำรองโดยอาศัยเทคโนโลยี Replication ในโหมด Synchronous ดังนั้น Topology แบบนี้จึงถือว่าเป็นต้นแบบสำหรับการทำ DR (Site Fail-over) ดังแสดงตามรูปที่ 8 – 22

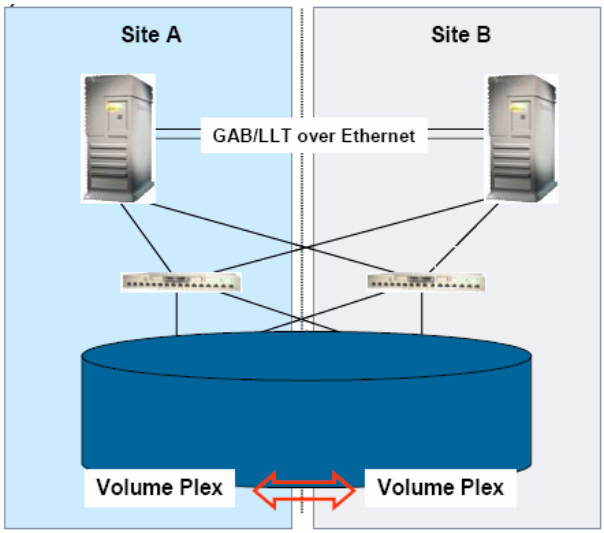


รูปที่ 8 – 22 Replicated Data Cluster

อย่างไรก็ตามการนำ **Topology** แบบ **Wide Area Clustering** มาใช้ในการทำ **Campus Cluster** อาจจะไม่เหมาะสมนัก เนื่องจากโอกาสที่จะต้องทำ **Fail-over** ในระดับ **LAN** จะมีค่อนข้างมากกว่าการทำ **DR (Site Fail-over)** เพราะการทำ **Fail-back** จะเกิดขึ้นได้ก็ต่อเมื่อมีการทำ **Resync** ข้อมูลที่เปลี่ยนแปลงในช่วง **Fail-over** เสร็จสมบูรณ์แล้วเท่านั้น

8.12.2.2 แบบ Stretch Cluster

การทำ **Stretch Cluster** ถือว่าเป็นส่วนขยายของ **Local Clustering** แบบ **Shared Data Architecture** ที่กล่าวมาแล้ว แต่สามารถรองรับความต้องการในด้าน **DR** เพิ่มขึ้นอีกระดับหนึ่ง โดยใช้พื้นฐานของเทคโนโลยี **SAN** ที่สามารถเชื่อมต่อได้ในระยะทางที่ไกลขึ้น (สนับสนุนได้ถึง **100** กม.) ทำให้สามารถวางโครงสร้าง **SAN** ครอบคลุมกลุ่มอาคารใน **Campus** ได้มากกว่า ดังแสดงตามรูปที่ 8 – 23

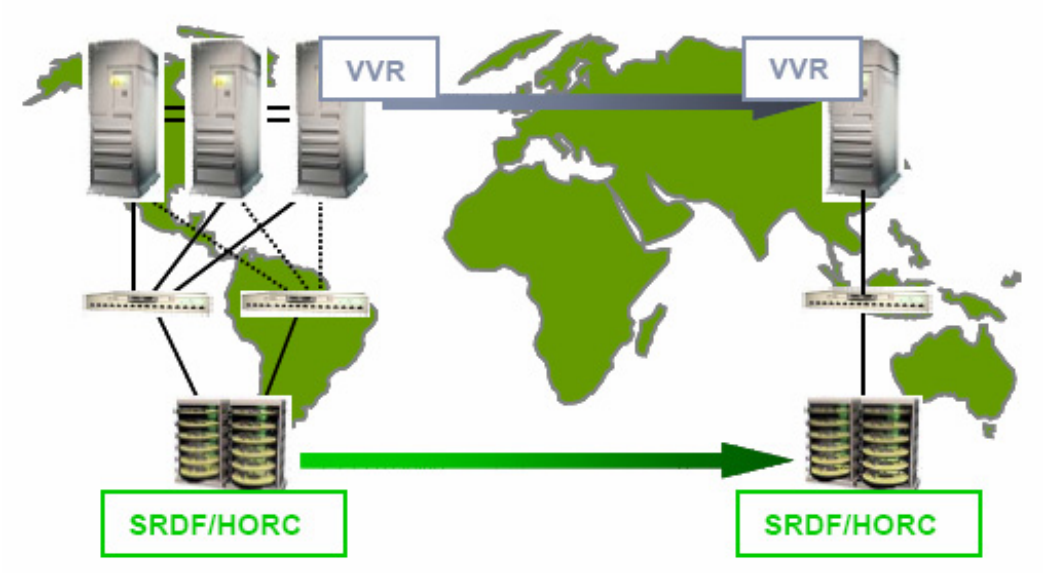


รูปที่ 8 – 23 Stretch Cluster

หากเกิดเหตุการณ์ความหายนะขึ้นที่อาคาร หรือ **Site1** ที่ทำให้ระบบงานบนไซต์หลักดังกล่าวล้มเหลว **Site2** ที่เหลืออยู่จะสามารถ **Fail-over** งานของ **Site1** ขึ้นมาได้พร้อมกับสถานะล่าสุดของข้อมูลจากชุด **Mirror** ที่เหลืออยู่ใน **Array** บน **Site2** ลักษณะการทำงานแบบนี้ไม่ต้องใช้เทคโนโลยี **Replication** เข้ามาเกี่ยวข้อง และในกลุ่มคลัสเตอร์สามารถมีสมาชิกในแต่ละไซต์ได้มากกว่า **1** โหนด อย่างไรก็ตามถึงแม้ว่าจะออกแบบคลัสเตอร์แบบนี้ให้เป็นแบบ **Multiple Site** แต่ในมุมมองของคลัสเตอร์ก็ยังถือว่าเป็นคลัสเตอร์กลุ่มเดียวกัน

8.12.3 Wide Area Clustering for DR

ถึงแม้ว่าการทำ **Stretch Cluster** จะสามารถคุ้มครองความเสียหายจากสภาพความหายนะ ได้เป็นส่วนใหญ่ แต่สำหรับองค์กรที่มีเครือข่ายอยู่ทั่วโลกในบางลักษณะภูมิประเทศองค์กรจะต้องการความมั่นใจมากขึ้น ระยะห่างระหว่างไซต์ที่ได้จากการทำ **Campus Clustering** อาจจะไม่เพียงพอ เช่นบางประเทศอาจมีการเกิดแผ่นดินไหวบ่อยครั้งและรุนแรง หรือมีความเสี่ยงต่อการเกิดวินาศกรรม จึงมีความจำเป็นต้องทำ **Wide Area Clustering** เพื่อรองรับเหตุการณ์การกู้คืนจากความหายนะโดยไม่มีขีดจำกัดการเชื่อมต่อ ดังแสดงตามรูปที่ 8 – 24



รูปที่ 8 – 24 **Wide Area Clustering**

นอกจากฟังก์ชันการดูแลจัดการกลุ่มคลัสเตอร์ที่กระจายอยู่ตามภูมิภาคต่างๆ แล้ว หากระบบงาน **Application** มีความสำคัญสูงมาก สำหรับโครงสร้างแบบ **Wide Area Clustering** จะสามารถกำหนดให้กลุ่มคลัสเตอร์ในภูมิภาคอื่นเข้ามา **Fail-over** งานนั้นๆ ได้ ถ้าคลัสเตอร์ในกลุ่มไม่สามารถทำงานได้อีกต่อไป การทำ **Wide Area Clustering** อาศัยการทำ **Replication** ในการอัพเดทข้อมูลเป็นหลัก

แบบฝึกหัดท้ายบท

1. จงอธิบายวิธีการโดยทั่วไป 2 วิธี ซึ่งผู้ใช้ที่ไม่มีสิทธิในการใช้ระบบเครือข่าย ใช้ในการ access เข้าไปยังระบบเครือข่ายโดยไม่ได้รับอนุญาต และบอกถึงวิธีการป้องกันสำหรับแต่ละวิธี
2. จงอธิบายความแตกต่างระหว่าง การแบ่งปันการใช้ทรัพยากรร่วมโดยมีรหัสผ่าน กับสิทธิการเข้าไปใช้งาน
3. ให้คำจำกัดความของการเข้ารหัสข้อมูล (Data Encryption) และ DES
4. ไฟร์วอลล์ (Firewall) คืออะไร และมีประโยชน์อย่างไรต่อระบบเครือข่าย
5. ให้ระบุไวรัสคอมพิวเตอร์ประเภทที่พบได้โดยทั่วไปมา 4 ประเภท และอธิบายวิธีการแพร่กระจายไวรัสเหล่านั้น
6. จงอธิบายวิธีการป้องกันไวรัสคอมพิวเตอร์บนระบบเครือข่ายมา 3 วิธี
7. จงอธิบายว่าความร้อน ความชื้น และฝุ่นละออง มีผลต่อประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์อย่างไร
8. ให้ระบุปัจจัยที่เกิดจากมนุษย์อย่างน้อย 3 ประการที่ส่งผลกระทบต่อประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์ ในสภาพแวดล้อมการทำงานของระบบเครือข่าย
9. มีปัจจัยซ่อนเร้นอะไรบ้างที่ส่งผลกระทบต่อประสิทธิภาพการทำงานของระบบเครือข่ายคอมพิวเตอร์ในสภาพแวดล้อมการใช้งานในโรงงานอุตสาหกรรม พร้อมทั้งแจกแจงวิธีการป้องกันในเบื้องต้น
10. ปัญหากรณีศึกษา

    บริษัทขนาดเล็กแห่งหนึ่งได้รับความเสียหายจากช่องโหว่ในการรักษาความปลอดภัยในระบบเครือข่ายแบบ Peer-to-Peer ของบริษัท โดยมีผู้บุกรุกเข้ามาขโมยข้อมูลทางด้านธุรกิจที่สำคัญของบริษัท ผู้บริหารจึงต้องการให้มีการรักษาความปลอดภัยมากขึ้นโดยปรับเป็นระบบเครือข่ายแบบ Server-based บริษัทนี้มีที่ตั้งอยู่ในรัฐแคลิฟอเนีย ซึ่งเกิดแผ่นดินไหวบ่อยและกระแสไฟฟ้าดับอยู่เป็นประจำ งานของคุณคือวางแผนการจัดตั้งระบบเครือข่ายเพื่ออุดช่องโหว่ในด้านการรักษาความปลอดภัย และเพิ่มความสามารถในการกู้คืนระบบจากความหายนะที่อาจเกิดขึ้นจากแผ่นดินไหว โดยเขียนรายการสิ่งที่ทำให้ข้อมูลมีความเสี่ยง และอุปกรณ์เพิ่มเติมที่ต้องการ

11. ในการจัดทำเซ็กเตอร์สำรอง มีวิธีการดำเนินการอย่างไร จงอธิบาย
12. ระบบสำรองไฟฟ้าฉุกเฉิน (UPS) ที่ดี จะต้องมีคุณสมบัติอย่างไร
13. จงอธิบายหน้าที่ของ RAID Controller มาพอเข้าใจ
14. จงอธิบายหลักการทำงานของ RAID 10 มาพอสังเขป
15. การเพิ่มประสิทธิภาพของระบบ Fault Tolerant โดยใช้โปรแกรม Disk Administrator ของ Windows NT Server จะทำอะไรเพิ่มเติมได้บ้าง จงอธิบาย

จงเติมคำลงในช่องว่างให้ถูกต้อง

16. ข้อพิจารณาอันดับแรกในการรักษาความปลอดภัยให้กับข้อมูลบนระบบเครือข่าย คือการทำให้มั่นใจว่าระบบการรักษาความปลอดภัยของระบบเครือข่าย _____
17. สิทธิการใช้งานระบบเครือข่าย มีชื่อเรียกอีกอย่างหนึ่งว่า _____

18. การใช้รหัสผ่านป้องกันการเข้าถึงทรัพยากรบนระบบเครือข่าย จะเกี่ยวข้องกับการกำหนด _____ ให้กับทรัพยากรที่แบ่งปันการใช้งานร่วมกันบนระบบเครือข่าย

19. ถ้ากำหนดให้ทรัพยากรนั้นๆ เป็นแบบ _____ ผู้อื่นในระบบเครือข่ายจะสามารถเปิดดูเอกสารและคัดลอกไปยังเครื่องของผู้ใช้นั้นได้ แต่จะไม่สามารถทำการปรับเปลี่ยนเอกสารต้นฉบับได้

20. วิธีการซึ่งมีประสิทธิภาพในการกำหนดสิทธิการใช้งานของผู้ใช้ ทำโดยการใช้ _____

21. เราสามารถเลือกประเภทของเหตุการณ์ที่เกิดขึ้นกับระบบเครือข่าย ที่จัดเก็บอยู่ใน _____ ของเครื่องเซิร์ฟเวอร์ เพื่อตรวจสอบการทำงานของระบบเครือข่ายโดยชื่อบัญชีผู้ใช้

22. ยูทิลิตี้ _____ จะทำการผสมข้อมูลให้ไม่สามารถอ่านได้ ก่อนที่จะส่งออกไปบนระบบเครือข่าย

23. คอมพิวเตอร์ที่ไม่มีดิสก์จะสื่อสารกับเครื่องเซิร์ฟเวอร์ และทำการ **logon** โดย _____ ซึ่งติดตั้งอยู่บนเครื่องคอมพิวเตอร์เวิร์กสเตชั่น

24. เงื่อนไขที่สำคัญในการตรวจสอบระบบเครือข่าย คือ _____ และ _____

25. _____ มีความจำเป็นในการป้องกันเครื่องคอมพิวเตอร์จากอุณหภูมิสูงเกินไป

26. สิ่งแรกในการป้องกันข้อมูลสูญหายคือการใช้ระบบ _____

27. Tape Drive มีประโยชน์สำหรับระบบ _____

28. การเก็บรักษา _____ ข้อมูลสำรองทั้งหมด มีความสำคัญต่อการกู้คืนระบบในอนาคต

29. การใช้ **UPS** ที่สามารถสั่งงานผ่านระบบเครือข่าย จะช่วยให้สามารถควบคุมการ **Shut down** _____ได้อย่างปลอดภัย

30. ระบบ **Fault Tolerant** จะป้องกันข้อมูลโดยการทำสำเนาข้อมูลไปเก็บไว้ _____

31. RAID 0 มีชื่อเรียกว่า _____ โดยจะทำการแบ่งข้อมูลออกเป็นแถบเล็กๆ ขนาด **64 K** และนำไปเก็บไว้ในดิสก์ทั้งหมดในอาเรย์

32. RAID 0 จะไม่มีคุณสมบัติ **Data** _____

33. Disk _____ จะทำสำเนาพาร์ทิชัน และเคลื่อนย้ายสำเนานั้นไปจัดเก็บบนดิสก์ตัวอื่นเพื่อให้มีข้อมูล **2** ชุดอยู่ตลอดเวลา

34. การทำ **RAID 5** จะต้องมีฮาร์ดดิสก์อย่างน้อย _____ ตัว

35. RAID 53 มีการทำงานแบบ _____

36. การเขียนบล็อกข้อมูลอย่างลงบนดิสก์แต่ละตัวในอาเรย์สมบูรณ์มีชื่อเรียกว่า **disk** _____

37. โครงสร้างที่สำคัญ **2** แบบ ของการจัดทำ **Local Clustering** คือ _____ และ _____

38. การทำคลัสเตอร์ ใช้ในการเรียกกลุ่มของ _____ ซึ่งทำงานร่วมกันเป็นระบบเดียว

39. Replicated Data Cluster (RDC) เป็นโครงสร้างสถาปัตยกรรมแบบ _____

40. เพื่อให้มั่นใจในความปลอดภัยของข้อมูลจึงมีความจำเป็นต้องจัดตั้ง _____ สำหรับองค์กรที่มีเครือข่ายอยู่ทั่วโลก