บทที่ 4

การออกแบบเครือข่ายคอมพิวเตอร์สำหรับกรมตำรวจ

การออกแบบเครือข่ายคอมพิวเตอร์สำหรับกรมตำรวจ ซึ่งมีการเชื่อมโยงกันระหว่างหน่วยงานต่างๆในเขตกรุงเทพมหานครและหน่วยงานที่อยู่ต่างจังหวัด หน่วยงานเหล่านี้ได้แก่

1. หน่วยงานที่อยู่ในบริเวณกรมตำรวจ
   1.1. ศูนย์ข้อมูลข่าวสารกรมตำรวจ (ศข.ส.)
   1.2. กองทะเบียนประวัติอาชญากร (ทว.)
   1.3. กองพิสูจน์หลักฐาน (พฐ.)
2. หน่วยงานที่อยู่นอกบริเวณกรมตำรวจแต่อยู่ในกรุงเทพมหานคร
   2.1. กองทะเบียน (ท.)
   2.2. กองบัญชาการตำรวจนครบาล (บช.น.)
   2.3. กองบังคับการตำรวจจราจรกลาง (บก.จร.)
   2.4. สถานีตำรวจนครบาลต่างๆ (สน.)
3. หน่วยงานที่อยู่ต่างจังหวัด
   3.1. สำนักงานตำรวจภูธรภาค 1-9 (ตร.ภาค)
   3.2. กองบังคับการตำรวจภูธรจังหวัด (บก.ภ.จว.)
   3.3. สถานีตำรวจภูธรอำเภอ (สภ.อ.)

1. การเชื่อมโยงระหว่างหน่วยงานที่อยู่ในบริเวณกรมตำรวจ

ศูนย์ข้อมูลข่าวสารกรมตำรวจ(ศข.ส) เป็นหน่วยงานหลักในการเก็บข้อมูลต่างๆทั้งหมด ความต้องการในการติดต่อสื่อสารกันเองภายในศูนย์ข้อมูลต้องการความเร็วไม่น้อยกว่า 10 เมกกะบิตต่อวินาทีซึ่งสามารถพิจารณาการออกแบบเครือข่ายภายในศูนย์ข้อมูลได้โดยให้เป็นเครือข่ายแบบ อีเทอร์เน็ต ซึ่งได้ความเร็วที่ 10 เมกกะบิตต่อวินาทีหรือ FDDI ที่ความเร็ว 100 เมกกะบิตต่อ

วินาที เมื่อพิจารณาดูจะเห็นว่า FDDI จะให้ความเร็วได้ถึง 100 เมกกะบิตต่อวินาทีแต่ในปัจจุบันเครือข่ายชนิดนี้ยังคงมีราคาค่อนข้างแพงอยู่มากเมื่อเทียบกับเครือข่ายชนิดอีเทอร์เน็ต ดังนั้นจึงให้ความสนใจไปที่เครือข่ายชนิดอีเทอร์เน็ต เมื่อพิจารณาใช้เครือข่ายชนิดนี้ปัญหาที่ตามมาคือการแย่งกันใช้สายสื่อสาร เนื่องจากวิธีการขอใช้สายสื่อสารเป็นแบบ carrier sense multiple access/ collision detection (CSMA/CD) จึงอาจทำให้ประสิทธิภาพของระบบเครือข่ายลดลงโดยเฉพาะอย่างยิ่งเมื่อมีจำนวนผู้ใช้มากๆ ขอใช้สายสื่อสารเพื่อใช้บริการจากไฟล์เซอร์ฟเวอร์ในกรณีของศูนย์ข้อมูลมีเซอร์ฟเวอร์ อยู่หลายตัวเช่นไฟล์เซอร์ฟเวอร์ อิมเมจเซอร์ฟเวอร์เป็นต้น ดังนั้นจึงนำอุปกรณ์สวิตชิ่งฮับ เข้ามาช่วยจัดการแบ่งส่วนการจราจรเพื่อช่วยลดการชนกันของการส่งข้อมูลโดยสวิตชิ่งฮับจะวางที่ศูนย์ข้อมูล และเชื่อมโยงกับเซอร์ฟเวอร์ต่างๆในศูนย์ข้อมูลในรูปแบบทางกายภาพแบบรูปดาว

กองทะเบียนประวัติอาชญากรและกองพิสูจน์หลักฐานซึ่งอยู่ในบริเวณใกล้กันกับศูนย์ข้อมูล แต่ละหน่วยงานก็มีความจำเป็นที่จะต้องใช้ข้อมูลข้อสนเทศจากแหล่งข้อมูลที่สำคัญคือศูนย์ข้อมูล ดังนั้นจึงต้องมีการเชื่อมโยงทั้งสองหน่วยงานนี้เข้ากับศูนย์ข้อมูลด้วย โดยการเชื่อมโยงนี้เป็นไปในแบบการเชื่อมโยงเครือข่ายภายในบริเวณเดียวกัน แต่ต้องไม่ลืมว่าทั้งกองทะเบียนประวัติอาชญากรและกองพิสูจน์หลักฐานก็ยังมีข้อมูลเฉพาะของแต่ละหน่วยงานเช่นกันหรือมีไฟล์เซอร์ฟเวอร์ของแต่ละหน่วยงาน นั่นหมายถึงว่าการใช้งานข้อมูลบางครั้งอาจจะไม่จำเป็นต้องติดต่อมายังศูนย์ข้อมูล แต่เมื่อมีการเชื่อมโยงเครือข่ายถึงกันจะทำให้การใช้สายสื่อสารเกิดการคับคั่งของการจราจรของข้อมูล เมื่อพิจารณาถึงตรงนี้จึงออกแบบให้ใช้บริดจ์เป็นอุปกรณ์ช่วยแบ่งส่วนการจราจรของข้อมูลในสายสื่อสาร แต่เนื่องจากมีการใช้อีเทอร์เน็ตสวิตชิ่งแล้วจึงช่วยลดภาระในการติดตั้งอุปกรณ์บริดจ์ไปได้

สิ่งสำคัญที่จะต้องพิ จารณาด้วยนั่นคืองานของแต่ละหน่วยงานในศูนย์ข้อมูล มีเซอร์ฟเวอร์ที่ให้บริการข้อมูลกราฟิกส์และโปรแกรมประยุกต์ ดังนั้นการใช้ 10 เมกกะบิตต่อวินาที อาจจะไม่สามารถรองรับความต้องการของผู้ใช้ได้ถ้ามีการเรียกใช้ข้อมูลชนิดกราฟิกส์ เมื่อประมาณต้นปีพ. ศ. 2538 ได้มีการเพิ่มประสิทธิภาพของเครือข่ายแบบ อีเทอร์เน็ต (IEEE 802.3) ให้สามารถทำงานที่ 100 เมกกะบิตต่อวินาทีได้ โดยเรียกว่า Fast อีเทอร์เน็ต (IEEE 802.3u) ซึ่งใช้สื่อนำสัญญาณได้ทั้งสายชนิด UTP (100BASE-T)และสายเคเบิลใยแก้ว (100BASE-F) ทั้งนี้ขึ้นอยู่กับระยะทางที่ใช้ระหว่างอุปกรณ์ทวนสัญญาณ ถ้าห่างกันมากๆ อาจใช้สายเคเบิลใยแก้วเป็นสื่อนำสัญญาณได้ แต่ถ้าระยะไม่ไกลนักหรือไม่เกิน 100 เมตรนั้น เสนอแนะให้ใช้สาย UTP category 5 หรือ CAT 5 เป็นสื่อนำสัญญาณ แต่การนำเทคโนโลยี Fast อีเทอร์เน็ต มาใช้เพื่อให้ได้ 100 เมกกะบิตต่อวินาที นั้นจะต้องใช้เน็ตเวอร์คอินเตอร์เฟสการ์ดชนิด 100 Mbp. ทั้งในคอมพิวเตอร์ที่เป็น เซอร์ฟเวอร์และไคล์

เอ็นต์ด้วย นอกจากนั้นยังต้องใช้อุปกรณ์ฮับที่ทำงานที่ 100 เมกกะบิตต่อวินาทีอีกด้วย และในกรณีที่ต้องการทรูพุตที่สูงสุดนั้น สามารถใช้ อีเทอร์เน็ตสวิตชิ่งที่สนับสนุน Fast อีเทอร์เน็ต (100 BaseT หรือ 100BaseF) โดยสามารถปรับให้ทำงานแบบฟูลดูเพล็กได้ รวมทั้งสายนำสัญญาณที่เหมาะสมจึงจะทำให้ระบบเครือข่ายทำงานที่ 100 เมกกะบิตต่อวินาทีได้เต็มที่

รูปที่ 4.1 แสดงถึงการเชื่อมโยงเครือข่ายท้องถิ่นภายในบริเวณกรมตำรวจ ซึ่งจะเชื่อมโยงระหว่างหน่วยงานหลักได้แก่ ศูนย์ข้อมูลข้อสนเทศ กองทะเบียนประวัติอาชญากร และกองพิสูจน์หลักฐาน ซึ่งส่วนประกอบของเครือข่ายมีดังนี้

1. ไฟล์เซอร์ฟเวอร์ มี 3 เครื่อง ได้แก่

1.1 กราฟิกส์เซอร์ฟเวอร์

ใช้เครื่องคอมพิวเตอร์ที่มีโปรเซสเซอร์ขนาด 32 บิตหรือ 64 บิต
หน่วยความจำหลัก 64 เมกกะไบต์ และฮาร์ดดิสก์ 5 กิกะไบต์
มีอุปกรณ์อ่านซีดีรอม อุปกรณ์อ่านบันทึกเทปขนาด 4 มิลลิเมตร และฟลอปปีดิสก์ขนาด 3.5 นิ้ว รวมทั้งเน็ตเวอร์กอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ตชนิดความเร็ว 100 เมกกะบิตต่อวินาที

1.2 ดาต้าเบสเซอร์ฟเวอร์

ใช้เครื่องคอมพิวเตอร์ที่มีโปรเซสเซอร์ขนาด 32 บิตหรือ 64 บิต
หน่วยความจำหลัก 128 เมกกะไบต์ และฮาร์ดดิสก์ 5 กิกะไบต์
มีอุปกรณ์อ่านซีดีรอม อุปกรณ์อ่านบันทึกเทปขนาด 4 มิลลิเมตร และฟลอปปีดิสก์ขนาด 3.5 นิ้ว รวมทั้งเน็ตเวอร์กอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ตชนิดความเร็ว 100 เมกกะบิตต่อวินาที

1.3 เซอร์ฟเวอร์สำหรับให้บริการโปรแกรมประยุกต์

ใช้เครื่องคอมพิวเตอร์ที่มีโปรเซสเซอร์ขนาด 32 บิตหรือ 64 บิต
หน่วยความจำหลัก 64 เมกกะไบต์ และฮาร์ดดิสก์ 5 กิกะไบต์
มีอุปกรณ์อ่านซีดีรอม และฟลอปปีดิสก์ขนาด 3.5 นิ้ว
รวมทั้งเน็ตเวอร์กอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ตชนิด
ความเร็ว 100 เมกกะบิตต่อวินาที

2. อีเทอร์เน็ตสวิตชิ่ง

2.1 มีสวิตชิ่งฮับชนิด 100BaseT สำหรับต่อสาย UTP จำนวน 20 ช่องสัญญาณ

2.2 มีสวิตชิ่งฮับชนิด 100BaseF สำหรับต่อเคเบิลใยแก้วจำนวน 8 ช่องสัญญาณ

3. เราเตอร์ ให้มีจำนวนช่องสัญญาณแบบอะซิงโครนัสอย่างน้อย 12 ช่องสัญญาณ หรือใช้เราเตอร์ชนิด 4 ช่องสัญญาณอะซิงโครนัส 3 ตัว

4. โมเด็ม 20 ตัว

5. เทอร์มินอลเซอร์ฟเวอร์ ชนิด 12 ช่องสัญญาณแบบอะซิงโครนัส 2 ตัว

6. อีเทอร์เน็ตสวิตชิ่งแบบ 5 ช่องสัญญาณ (10/100 เมกกะบิตต่อวินาที) สำหรับต่อให้แต่ละชั้นของศูนย์ข้อมูล จำนวน 4 ตัว

7. ฮับ 16 ช่องสัญญาณ ชนิด 10/100 เมกกะบิตต่อวินาที จำนวน 8-10 ตัว

8. เครื่องคอมพิวเตอร์ที่ใช้เป็นสถานีงาน จำนวน 60 ชุด ประกอบด้วย

8.1 มีโปรเซสเซอร์ขนาด 32 บิต

8.2 หน่วยความจำหลัก 8 เมกกะไบต์

8.3 ความจุของฮาร์ดดิสก์ 530 เมกกะไบต์

8.4 ฟลอปปีดิสก์ไดรว์ขนาด 3.5 นิ้ว

8.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต ชนิด 10/100 เมกกะบิตต่อวินาที

สำหรับที่กองทะเบียนประวัติอาชญากรและกองพิสูจน์หลักฐานถูกออกแบบให้เป็นเครือข่ายท้องถิ่นมีลักษณะดังต่อไปนี้ดังนี้

1. ไฟล์เซอร์ฟเวอร์ 1 เครื่อง

1.1 ใช้เครื่องคอมพิวเตอร์ที่มีโปรเซสเซอร์ขนาด 32 บิตหรือ 64 บิต

1.2 หน่วยความจำหลัก 64 เมกกะไบต์ และฮาร์ดดิสก์ 2 กิกะไบต์

1.3 มีอุปกรณ์อ่านซีดีรอม อุปกรณ์อ่านบันทึกเทปขนาด 4 มิลลิเมตร

1.4 ฟลอปปีดิสก์ขนาด 3.5 นิ้ว

1.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต
ชนิดความเร็ว 10/100 เมกกะบิตต่อวินาที

2. เครื่องคอมพิวเตอร์ที่ใช้เป็นสถานีงาน จำนวน 10 ชุด ประกอบด้วย

2.1 มีโปรเซสเซอร์ขนาด 32 บิต

2.2 หน่วยความจำหลัก 8 เมกกะไบต์

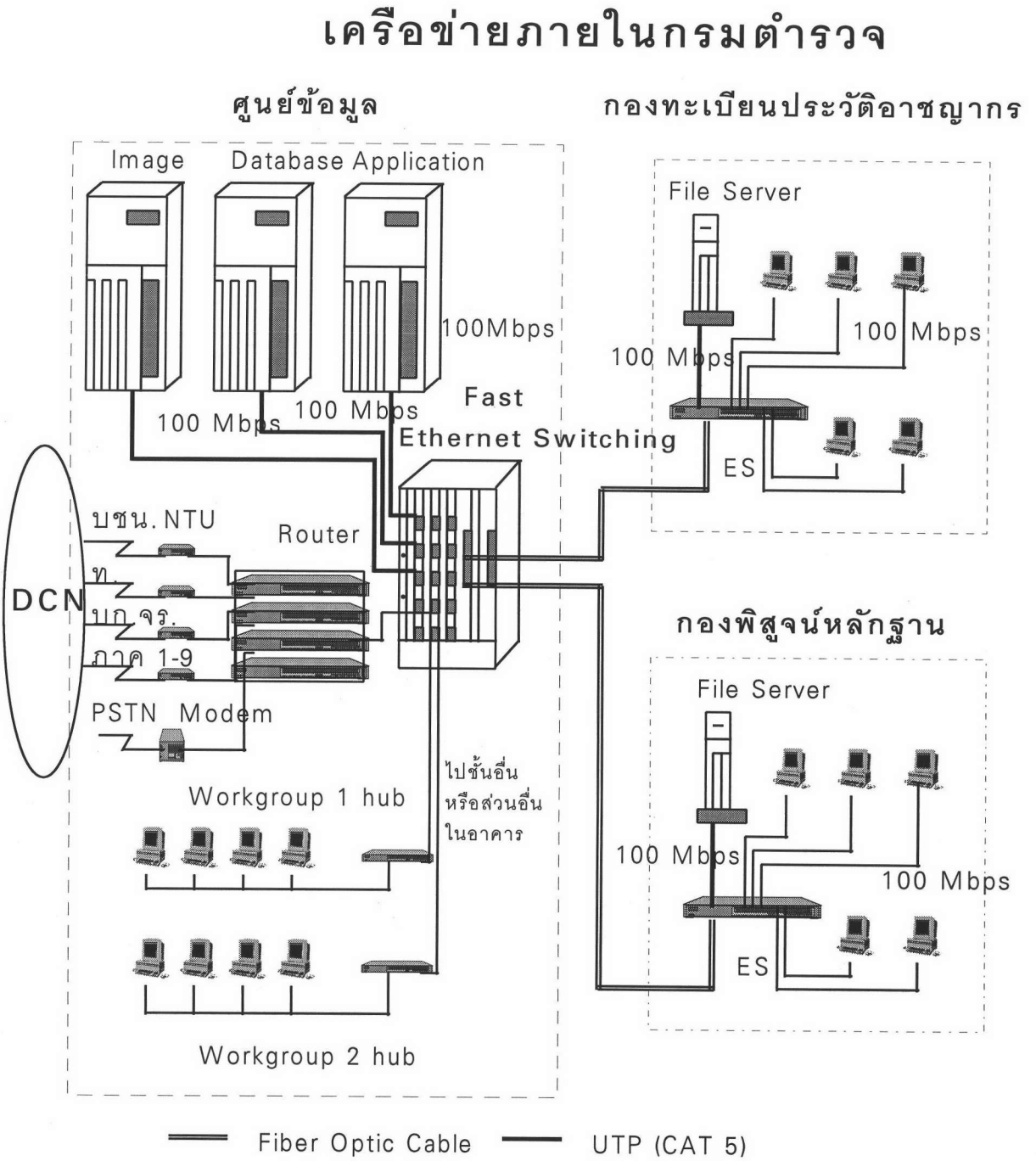
2.3 ความจุของฮาร์ดดิสก์ 530 เมกกะไบต์

2.4 ฟลอปปีดิสก์ไดรว์ขนาด 3.5 นิ้ว

2.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต ชนิด 10/100 เมกกะบิตต่อวินาที

3. อีเทอร์เน็ตสวิตชิ่งแบบ 5 ช่องสัญญาณ (10/100 เมกกะบิตต่อวินาที) 1 ตัว และมีช่องสัญญาณสำหรับเชื่อมต่อกับสายเคเบิลใยแก้วด้วย

4. ฮับ 16 ช่องสัญญาณ ชนิด 10/100 เมกกะบิตต่อวินาที จำนวน 1 ตัว

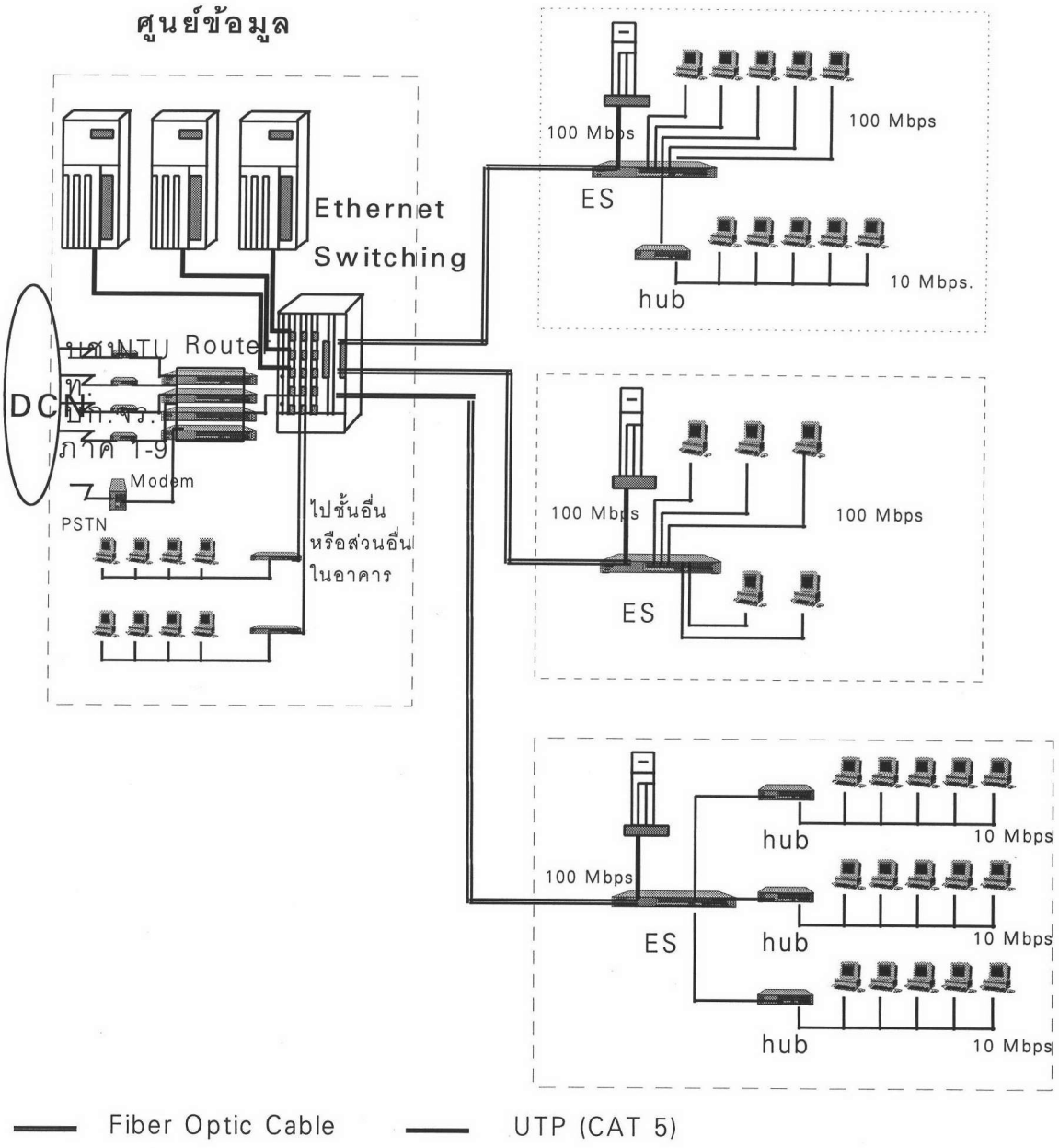


รูปที่ 4.1 แสดงการเชื่อมโยงระหว่างหน่วยงานในบริเวณกรมตำรวจ

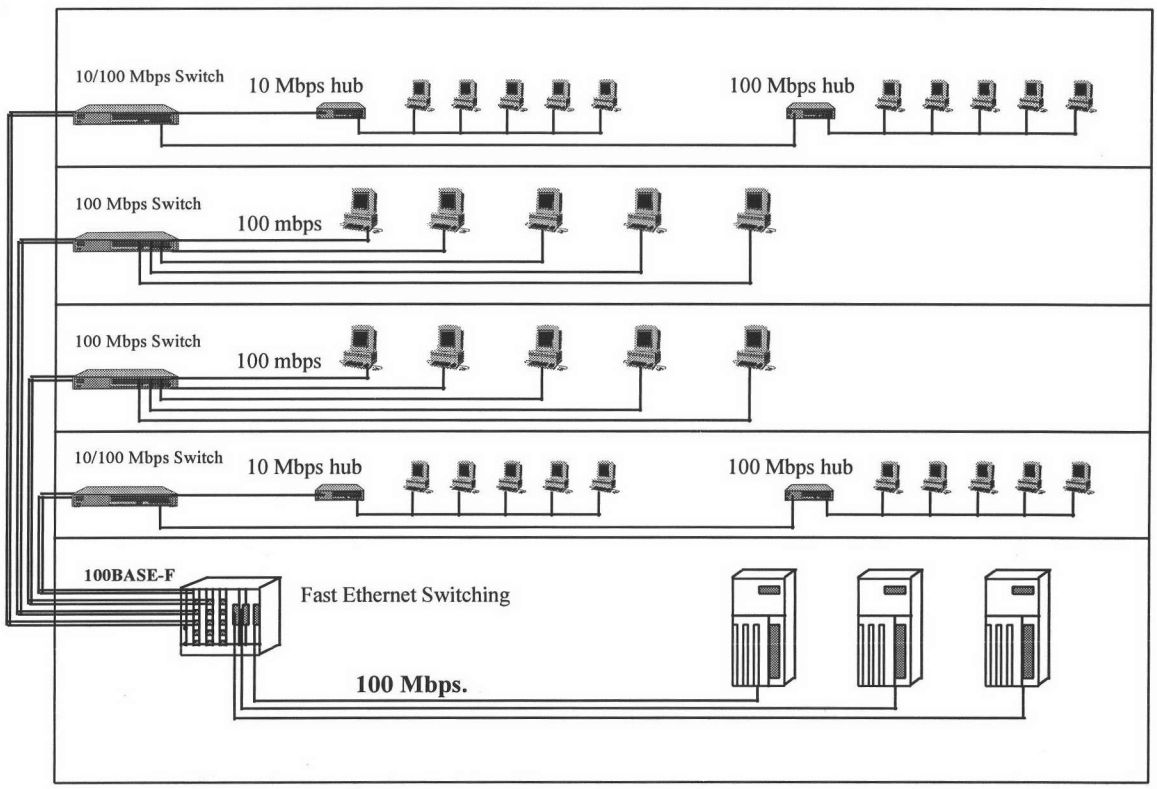
จากรูปที่ 4.1 แสดง Diagram ของเครือข่ายภายในบริเวณกรมตำรวจ เนื่องจากมี 3 หน่วยงานหลักที่ต้องมีการเชื่อมต่อเครือข่ายถึงกัน ได้แก่ ศูนย์ข้อมูล กองทะเบียนประวัติอาชญากร และกองพิสูจน์หลักฐาน โดยที่ศูนย์ข้อมูลจะเป็นที่ตั้งของเซอร์ฟเวอร์ทั้งหลายได้แก่กราฟิกส์เซอร์ฟเวอร์ ดาต้าเบสเซอร์ฟเวอร์ และเซอร์ฟเวอร์ที่ให้บริการโปรแกรมประยุกต์ นอกจากนี้ยังมีอุปกรณ์ที่ใช้ในการเชื่อมโยงไปยังหน่วยงานอื่นนอกบริเวณกรมตำรวจเช่น บก.จร.หรือสำนักงานตำรวจภูธรภาคทั้ง 9 ซึ่งเชื่อมโยงกันด้วยวงจรความเร็วสูง 64 กิโลบิตต่อวินาที อุปกรณ์เหล่านี้คือ เราเตอร์ และ เน็ตเวอร์คเทอร์มิเนตติงยูนิตหรือNetwork Terminating Unit (NTU) ซึ่งเป็นทรัพย์สินขององค์การโทรศัพท์ (เนื่องจากเช่าวงจรความเร็วสูง) ภายในศูนย์ข้อมูลจะมีการใช้เซอร์ฟเวอร์ทั้งหลายได้จากการต่อฮับออกมาจากอีเทอร์เน็ตสวิตชิ่งซึ่งจะทำให้มีลักษณะการทำงานเป็นกลุ่ม สายนำสัญญาณที่ใช้เชื่อมต่อระหว่างเซอร์ฟเวอร์กับอีเทอร์เน็ตสวิตชิ่งและฮับกับอีเทอร์เน็ตสวิตชิ่งนั้นพิจารณาให้ใช้สายคู่ตีเกลียวไม่หุ้มฉนวน (UTP) ตามข้อกำหนดของ EIA/TIA category 5(CAT 5) เนื่องจากเป็นสื่อคุณภาพสูงและเหมาะกับการส่งข้อมูลความเร็วสูงเช่น วิดีโอ ข้อมูลทางด้านกราฟิกส์ เป็นต้น

ในส่วนของกองทะเบียนประวัติอาชญากรก็มีเซอร์ฟเวอร์สำหรับหน่วยงานเองเช่นกัน ซึ่งที่หน่วยงานนี้มีการใช้ระบบงานที่เป็นระบบงานด้านกราฟิกส์และเชื่อมโยงกับศูนย์ข้อมูลโดยต่อสายสัญญาณเข้าไปที่ อีเทอร์เน็ตสวิตชิ่งแต่เนื่องจากสถานที่ตั้งของหน่วยงานอยู่ห่างกันค่อนข้างมาก การใช้สื่อเช่น UTP หรือ Coaxial จำเป็นต้องใช้อุปกรณ์ ทวนสัญญาณหลายช่วงเมื่อพิจารณาดูแล้วอาจเกินข้อกำหนดของ IEEE 802.3 ซึ่งจำกัดจำนวน อุปกรณ์ทวนสัญญาณในเครือข่าย ดังนั้นจึงใช้สายเคเบิลใยแก้วเป็นสื่อนำสัญญาณแทน โดยเชื่อมโยงระหว่างศูนย์ข้อมูลและกองทะเบียนประวัติอาชญากร การเชื่อมโยงนั้นใช้ทรานซิฟเวอร์ เพื่อเปลี่ยนจาก UTP ที่ ฮับ ด้านกองทะเบียนประวัติอาชญากรเป็นเคเบิลใยแก้วจากนั้นก่อนจะเข้าอีเทอร์เน็ตสวิตชิ่ง ก็ใช้ทรานซิฟเวอร์แปลงจากเคเบิลใยแก้วเป็น UTP เพื่อเข้าอีเทอร์เน็ตสวิตชิ่งต่อไป หรืออีกกรณีหนึ่งสามารถเชื่อมโยงสายเคเบิลใยแก้วจากอีเทอร์เน็ตสวิตชิ่งที่ศูนย์ข้อมูลซึ่งมีอุปกรณ์ที่ใช้สำหรับเชื่อมต่อกับสายเคเบิลใยแก้ว โดยตรงลากสายข้ามอาคารมายังกองทะเบียนประวัติอาชญากรเพื่อเข้ามาเชื่อมกับอีเทอร์เน็ตสวิตชิ่ง ที่มีอุปกรณ์หรือช่องสัญญาณสำหรับเคเบิลใยแก้วโดยเฉพาะก็สามารถทำได้ ซึ่งการเชื่อมโยงทั้งหมดนี้จะใช้อุปกรณ์ที่ทำงานที่ 100 เมกกะบิตต่อวินาทีทั้งหมด สำหรับการเชื่อมโยงเครือข่ายระหว่างศูนย์ข้อมูลกับกองพิสูจน์หลักฐานก็มีลักษณะเช่นเดียวกันกับการเชื่อมโยงระหว่างศูนย์ข้อมูลและกองทะเบียนประวัติอาชญากร

การเชื่อมโยงไปยังอาคารอื่นที่เกี่ยวข้อง



รูปที่ 4.2 แสดงการเชื่อมโยงไปยังอาคารอื่นที่เกี่ยวข้อง



รูปที่ 4.3 แสดงการเชื่อมโยงระหว่างชั้นต่างๆในอาคารศูนย์ข้อมูลข้อสนเทศ

2. การเชื่อมโยงระหว่างหน่วยงานที่อยู่นอกบริเวณกรมตำรวจแต่อยู่ในกรุงเทพฯ

หน่วยงานอื่นซึ่งอยู่นอกบริเวณกรมตำรวจแต่ยังคงอยู่ในกรุงเทพมหานครนั้นได้แก่ กองทะเบียน (ท.) กองบัญชาการตำรวจนครบาล (บช.น.) กองบังคับการตำรวจจราจรกลาง (บก.จร.) และสถานีตำรวจนครบาลต่างๆ (สน.) หน่วยงานเหล่านี้ก็มีความต้องการเรียกใช้ข้อมูลจากศูนย์ข้อมูลเช่นกัน ดังนั้นจึงมีความจำเป็นที่จะต้องเชื่อมโยงเครือข่ายระหว่างศูนย์ข้อมูลกับหน่วยงานต่างๆเหล่านี้ แต่เนื่องจากไม่ได้อยู่ในบริเวณใกล้เคียงกับศูนย์ข้อมูลที่พอจะทำการเชื่อมโยงเครือข่ายในลักษณะเครือข่ายท้องถิ่นได้แต่ความต้องการข้อมูลอย่างรวดเร็วยังคงมีอยู่ ดังนั้นการเชื่อมโยงเครือข่ายเข้าหาศูนย์ข้อมูลจึงต้องใช้วิธีเช่าสายสัญญาณความเร็วสูงจากผู้ให้บริการ โดยการเช่าสายสัญญาณส่งข้อมูลนั้นจะใช้ความเร็วในการส่ง 64 กิโลบิตต่อวินาที เชื่อมโยงศูนย์ข้อมูลกับกองทะเบียน กองบัญชาการตำรวจนครบาล และกองบังคับการตำรวจจราจรกลาง นอกจากนี้ยังต้องทำการสำรองสายส่งข้อมูลความเร็ว 9600 บิตต่อวินาที เอาไว้ด้วยเพื่อใช้ในกรณีฉุกเฉินถ้าหากสายความเร็วสูงไม่สามารถใช้งานได้ สำหรับการเชื่อมโยงศูนย์ข้อมูลกับสถานีตำรวจนครบาลนั้นใช้สายส่งข้อมูลความเร็ว 64 กิโลบิตต่อวินาที เช่นกัน และยังให้มีการใช้วงจรสายโทรศัพท์สื่อสารผ่านโมเด็มเพื่อให้สามารถเชื่อมโยงไปยังสถานีตำรวจนครบาลอื่นๆ หรือเชื่อมโยงเข้าสู่ศูนย์ข้อมูลข้อสนเทศโดยตรงรวมทั้งเป็นวงจรสำรองอีกด้วย

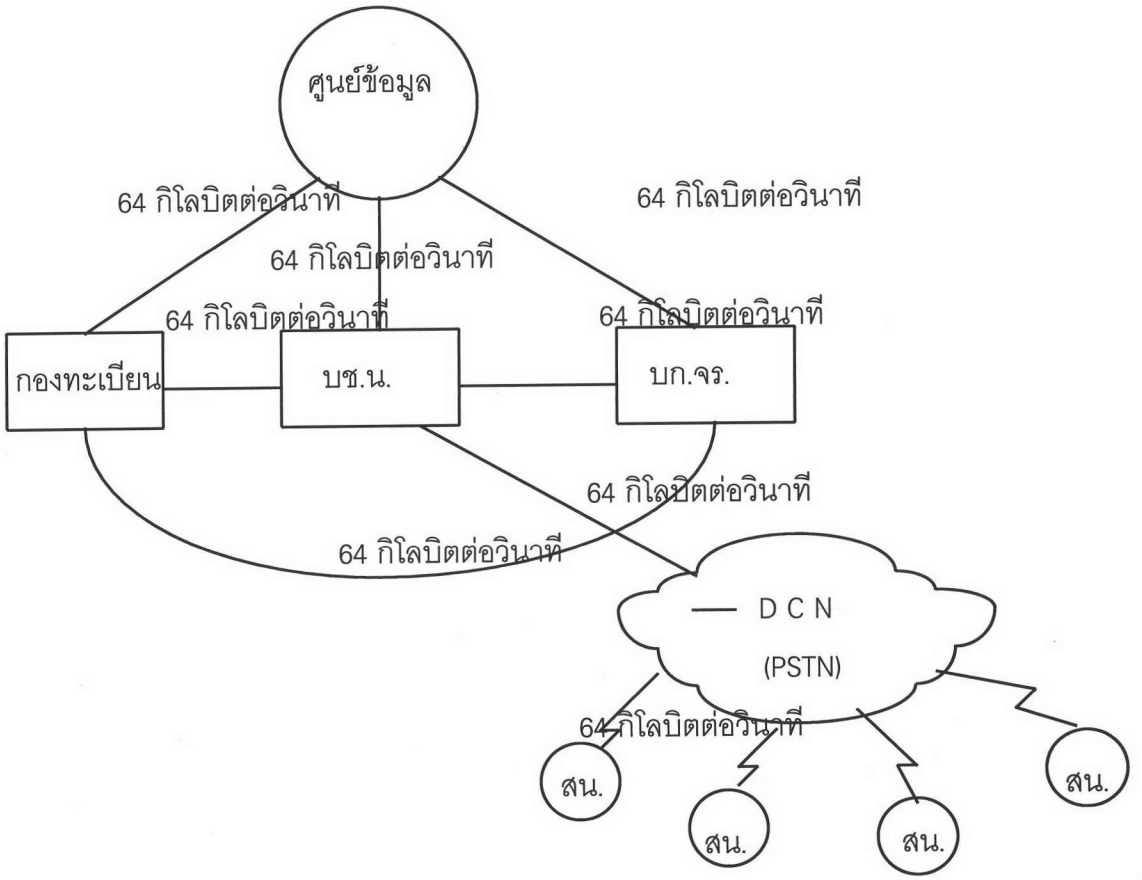
การเชื่อมโยงหน่วยต่างๆภายในเขตกรุงเทพมหานครกับศูนย์ข้อมูลข้อสนเทศนั้นจะต้องวางรีโมตเราเตอร์ไว้ที่ กองบังคับการตำรวจจราจร กองบัญชาการตำรวจนครบาล และกองทะเบียน โดยที่รีโมตเราเตอร์ทั้ง 3 นั้น ต้องเชื่อมโยงกับ เราเตอร์ ที่ศูนย์ข้อมูลข้อสนเทศด้วยสายส่งข้อมูลความเร็วสูงความเร็ว 64 กิโลบิตต่อวินาที เพื่อไม่ให้เกิดการหยุดชะงักในการใช้งานและต้องสามารถทำ Alternate route กับรีโมตเราเตอร์ชุดอื่นได้ กรณีที่รีโมตเราเตอร์ตัวใดตัวหนึ่งเกิดขัดข้องหรือมีปัญหาการใช้งาน หน่วยผู้ใช้ต่างๆสามารถใช้โมเด็มหมุนผ่านสายโทรศัพท์ไปยัง รีโมตเราเตอร์ อื่นๆในระบบได้ เพื่อไม่ให้เกิดการหยุดชะงักในการใช้งาน

การเชื่อมโยงเครือข่ายจากศูนย์ข้อมูลไปยังหน่วยงานอื่นที่มีรีโมตเราเตอร์ที่ตั้งอยู่นอกศูนย์ข้อมูลฯ สามารถทำได้โดยผ่านอุปกรณ์ เราเตอร์ ซึ่ง เราเตอร์ ที่จะนำมาใช้งานตรงนี้จะต้องเป็นอุปกรณ์ที่มีประสิทธิภาพสูง มีตัวจ่ายกระแสไฟสองชุดเพื่อแก้ปัญหาเกี่ยวกับกระแสไฟฟ้าโดยจะสามารถทำงานได้เมื่อตัวจ่ายกระแสไฟตัวใดตัวหนึ่งเสียไป รวมทั้งจะต้องมี Uninterruptable Power Supply (UPS) ด้วย สำหรับ เราเตอร์ นั้น ควรจะมีช่องสื่อสารแบบอนุกรมทั้งหมดรวมกันเท่ากับ 48 ช่องสัญญาณ โดยแบ่งการเชื่อมต่อแบบมาตราฐาน เป็น V.35 16 ช่อง ที่เหลืออีก 32 ช่องจะเป็นแบบ RS-232

ที่ศูนย์ข้อมูลข้อสนเทศ จะเชื่อมโยงไปยังหน่วยงานอื่นที่มีรีโมตเราเตอร์ โดยผ่านทาง เราเตอร์ ที่ติดตั้งอยู่ที่หน่วยงานทั้งสามให้มี หน่วยงานละเครื่อง โดยแต่เครื่องจะมีช่องสัญญาณแบบซิงโครนัส 2 ช่อง รวม 2 เครื่อง จะเป็น 4 ช่องสัญญาณ โดย 2 ช่องสัญญาณที่เครื่องหนึ่งจะเชื่อมโยงไปศูนย์ข้อมูลข้อสนเทศ และหน่วยงานข้างเคียงส่วนอีก 1 ช่องสัญญาณของอีกเครื่องจะเชื่อมกับหน่วยงานข้างเคียงที่เหลือ โดยการเชื่อมโยงจะมีความเร็วอย่างน้อย 64 กิโลบิตต่อวินาที

จากลักษณะการเชื่องโยงข้างต้นจะเห็นได้ว่า ถ้ามี เส้นทางใดเส้นทางหนึ่งหรืออุปกรณ์ เราเตอร์ ตัวใดตัวหนึ่งทั้ง รีโมต และศูนย์กลางเสียหาย เราเตอร์จะสามารถหาเส้นทางผ่านทาง Alternate route ซึ่งปัจจุบันนี้อุปกรณ์ เราเตอร์ สามารถหา Alternate route ที่จะใช้ได้โดยอัตโนมัติ โดยคุณสมบัติของโปรโตคอลจัดการเส้นทางส่งข้อมูล เช่น OSPF (Open Shortest Path First) เป็นต้น นอกจากนี้ จะมี เราเตอร์ ที่สามารถหาเส้นทางใหม่อยู่แห่งละ 2 เครื่อง จะทำให้ความน่าเชื่อถือของระบบสูงขึ้น โดยเมื่อมีเครื่องใดเสียหาย ก็จะมีอีกเครื่องหนึ่งทดแทน ซึ่งเมื่อเทียบกับการใช้เครื่องเดียวที่ให้จำนวนช่องสัญญาณเท่ากัน เมื่อเกิดความเสียหายกับเครื่องก็จะทำให้ระบบถูกตัดขาดทันที

สำหรับการเชื่อมโยงสถานีตำรวจนครบาลตามที่ต่างๆที่กระจายอยู่ในกทม.เข้าสู่กองบัญชาการตำรวจนครบาล สามารถทำได้โดย หน่วยงานที่เป็นระบบเครือข่ายท้องถิ่นที่เป็นไมโครคอมพิวเตอร์ การเชื่อมโยงจะเป็นลักษณะเครือข่ายท้องถิ่นเชื่อมโยงกับเครือข่ายท้องถิ่น โดยเชื่อมโยงผ่าน สายเช่า ความเร็ว 64 กิโลบิตต่อวินาที เข้าสู่ บชน. ที่อุปกรณ์ NTU แล้วเข้าสู่ อุปกรณ์เทอร์มินอลเซอร์ฟเวอร์ซึ่งทำหน้าที่เป็น เราเตอร์ แล้วเข้าสู่เซอร์ฟเวอร์ ของบชน. ต่อไป นอกจากจะใช้สายเช่าแล้ว ยังออกแบบให้มีการส่งข้อมูลทางสายโทรศัพท์สาธารณะผ่านโมเด็มเพื่อเป็นเส้นทางสำรองกรณีที่เส้นทางหลักไม่สามารถใช้งานได้



รูปที่ 4.4 แสดงการเชื่อมโยงหน่วยงานที่อยู่ในกรุงเทพกับศูนย์ข้อมูล

3. การเชื่อมโยงระหว่างสำนักงานตำรวจภาคกับศูนย์ข้อมูล

การเชื่อมโยงระหว่างสำนักงานตำรวจภาคจะมีลักษณะดังต่อไปนี้

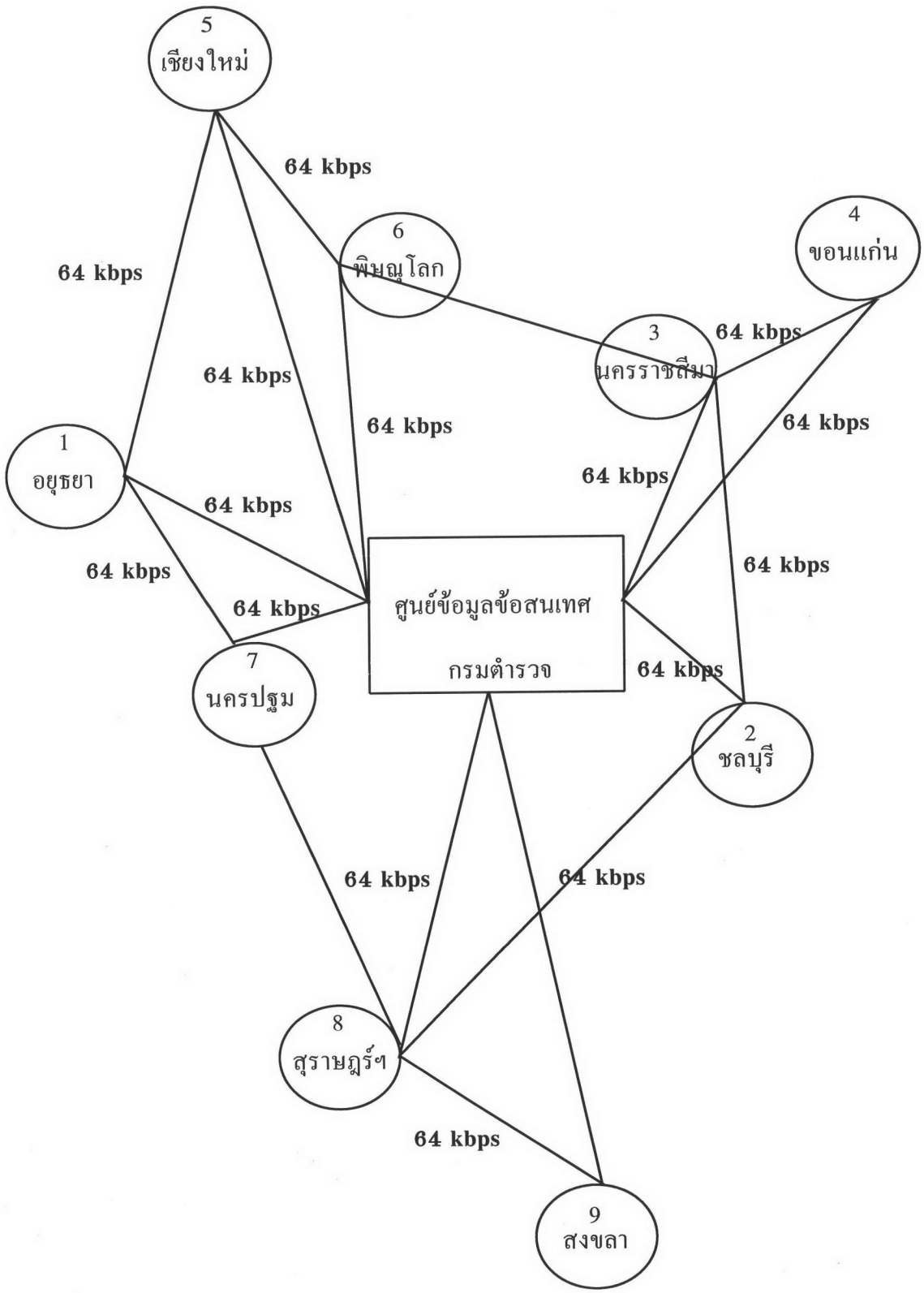
1. สำนักงานตำรวจภาค 1 กับ สำนักงานตำรวจภาค 5
2. สำนักงานตำรวจภาค 1 กับ สำนักงานตำรวจภาค 7
3. สำนักงานตำรวจภาค 5 กับ สำนักงานตำรวจภาค 6
4. สำนักงานตำรวจภาค 3 กับ สำนักงานตำรวจภาค 4
5. สำนักงานตำรวจภาค 3 กับ สำนักงานตำรวจภาค 6

6. สำนักงานตำรวจภาค 2 กับสำนักงานตำรวจภาค 3
7. สำนักงานตำรวจภาค 2 กับ สำนักงานตำรวจภาค 8
8. สำนักงานตำรวจภาค 7 กับ สำนักงานตำรวจภาค 8
9. สำนักงานตำรวจภาค 8 กับ สำนักงานตำรวจภาค 9

การเชื่อมโยงจากสำนักงานตำรวจภาคสู่ศูนย์ข้อมูล มีลักษณะเดียวกับการเชื่องโยงกับหน่วยงานต่างๆ ภายในกรุงเทพมหานครกับศูนย์ข้อมูล เพียงแต่สำนักงานตำรวจภาคอยู่กระจายกันตามจังหวัดต่างๆ 9 จังหวัด การเชื่อมเข้าต่อศูนย์ข้อมูลจะมีความเร็วอย่างน้อย 64 กิโลบิตต่อวินาที

รีโมต ไซต์ ตามสำนักงานตำรวจภาคต่างๆ จะเชื่องโยงเข้าศูนย์ข้อมูลผ่าน รีโมตเราเตอร์สู่ศูนย์กลาง และเช่นเดียวกันกับการเชื่อมโยงในกรุงเทพ จะมีรีโมตเราเตอร์อยู่ 2 เครื่องในแต่ละสำนักงานตำรวจภาค

นอกจากนี้ยังต้องพิจารณากรณีที่รีโมตเราเตอร์ตัวใดตัวหนึ่งเกิดขัดข้องหรือมีปัญหาการใช้งาน หน่วยผู้ใช้งานต่างๆต้องสามารถ หมุนผ่านสายโทรศัพท์สาธารณะไปยังรีโมตไซต์ ที่อยู่ใกล้เคียงได้อย่างมีประสิทธิภาพ โดยไม่ให้เกิดการหยุดชะงักของการทำงานรีโมตไซต์ทุกแห่งจะต้องสามารถเชื่อมโยงไปยัง ศูนย์กลาง ณ.ศูนย์ข้อมูลข้อสนเทศ หรือ รีโมต ไซต์ อื่นที่อยู่ใกล้เคียงด้วยสายส่งข้อมูลความเร็ว 64 กิโลบิตต่อวินาที เพื่อไม่ให้เกิดการหยุดชะงักของการใช้งาน และสามารถทำ Alternate Route ไปยัง รีโมตไซต์ อื่นได้ รูปต่อไปนี้แสดงเส้นทางการเชื่อมโยงระหว่างสำนักงานภาคทั้ง 9 กับ ศูนย์ข้อมูลที่กรมตำรวจ



รูปที่ 4.5 แสดงเส้นทางการเชื่อมโยงระหว่างสำนักงานภาคกับศูนย์ข้อมูล

4. การเชื่อมโยงระหว่างสำนักงานภาคกับกองบังคับการตำรวจภูธรจังหวัดและสภ.อ.เมือง

การเชื่อมโยงระหว่างสำนักงานภาคกับกองบังคับการตำรวจภูธรจังหวัดนั้นแบ่งการพิจารณาได้ 3 กลุ่มด้วยกัน คือ

4.1. กองบังคับการตำรวจภูธรจังหวัดที่มีสำนักงานภาคและสภ.อ.เมือง ตั้งอยู่ด้วย

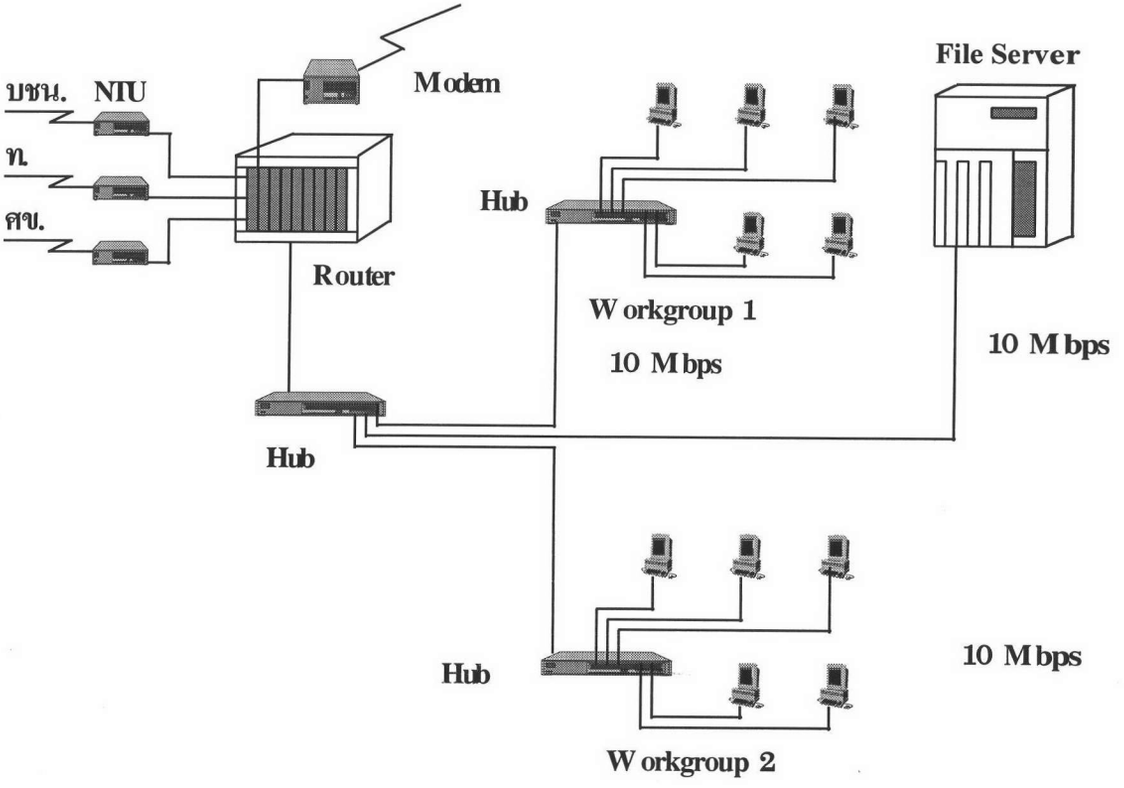
4.2 กองบังคับการตำรวจภูธรจังหวัดที่ไม่มีสำนักงานภาคตั้งอยู่แต่มีสภ.อ.เมือง ตั้งอยู่ด้วย

4.3. สภ.อ.อย่างเดียว

หน่วยงานที่มีรูปแบบตามข้อ 4.1 คือ มีทั้งสำนักงานตำรวจภาค กองบังคับการตำรวจภูธรจังหวัด และสภ.อ.อยู่ในบริเวณเดียวกันนั้น พิจารณาให้มีการสร้างเครือข่ายท้องถิ่น และมีการเชื่อมโยงเข้าสู่ศูนย์ข้อมูลด้วยสายส่งข้อมูลความเร็วสูง 64 กิโลบิตต่อวินาที. ตามรูปที่ 4.3 นอกจากนี้ยังมีสายส่งข้อมูลแบบผ่านสายโทรศัพท์สาธารณะด้วยความเร็ว 9600 บิตต่อวินาที สำรองไว้ในกรณีสายส่งข้อมูลความเร็วสูงไม่สามารถทำงานได้

หน่วยงานที่มีรูปแบบตามข้อ 4.2 คือมีกองบังคับการตำรวจภูธรจังหวัดและสภ.อ.อยู่ด้วยกันนั้น พิจารณาให้มีการสร้างเครือข่ายท้องถิ่นเช่นกันแต่การเชื่อมโยงจากกองบังคับการตำรวจภูธรจังหวัดไปยังสำนักงานตำรวจภาคนั้นให้ใช้เป็นสายส่งข้อมูลความเร็ว 64 กิโลบิตต่อวินาที แบบสายเช่าแต่ให้มีการสำรองสาย หมุนผ่านสายโทรศัพท์สาธารณะ ไว้ด้วยเช่นกัน

หน่วยงานที่มีรูปแบบตามข้อ 4.3 คือเป็นสภ.อ. โดยมากจะเป็นเครื่องคอมพิวเตอร์ส่วนบุคคลเพียงเครื่องเดียว (อาจจะมากกว่า 1 ตัวก็ได้) ให้เชื่อมโยงไปยังหน่วยงานอื่นโดยสายส่งข้อมูลแบบผ่านสายโทรศัพท์สาธารณะความเร็ว 9600 บิตต่อวินาทีด้วยโมเด็ม สภ.อ.สามารถเชื่อมโยงเข้าสู่ระบบได้ โดยผ่านเครือข่ายสาธารณะไปยังรีโมตเราเตอร์ของหน่วยงานที่สังกัดได้อย่างมีประสิทธิภาพ นอกจากนี้ในกรณีที่รีโมตเราเตอร์ที่ใช้งานอยู่เกิดขัดข้องหรือมีปัญหาในการใช้งาน สภ.อ.หรือจังหวัดยังสามารถ หมุนผ่านสายโทรศัพท์สาธารณะไปยังรีโมตไซต์ อื่นๆในระบบได้ เพื่อไม่ให้เกิดการหยุดชะงักในการใช้งาน



รูปที่ 4.7 แสดงเครือข่ายภายในกองบังคับการตำรวจจราจร

8.3 การออกแบบเครือข่ายท้องถิ่นภายในกองบัญชาการตำรวจนครบาล

ภายใน บชน. มีศูนย์ข้อมูลของหน่วยงานเองด้วย โดยศูนย์ข้อมูลที่นี่จะทำหน้าที่รวบรวมข้อมูลเกี่ยงกับคดีต่างๆที่ถ่ายโอนมาจากสถานีตำรวจนครบาลทั่วกรุงเทพ ซึ่งการโอนข้อมูลนี้จะทำด้วยการส่งข้อมูลผ่านสายเช่าความเร็ว 64 กิโลบิตต่อวินาทีและสามารถ หมุนผ่านสายโทรศัพท์สาธารณะ ผ่านทางโมเด็ม เข้ามาได้ในกรณีวงจร 64 กิโลบิตต่อวินาทีไม่สามารถใช้งานได้ ดังนั้นจึงต้องมีการเตรียมโมเด็มแบบหมุนผ่านสายโทรศัพท์สาธารณะไว้ให้ด้วย นอกจากนี้ยังต้องมี เร้าเตอร์ และ อุปกรณ์ Network Terminating Unit (NTU) ซึ่งเป็นของหน่วยงานที่ให้บริการเช่าสายสัญญาณความเร็วสูง (ซึ่งเราใช้ 64 กิโลบิตต่อวินาที) และเนื่องจากที่ บชน. ยังมีผู้ใช้งานเครื่องคอมพิวเตอร์มากพอสมควร ดังนั้นสามารถแยกกลุ่มผู้ใช้หรือกลุ่มของสถานีงานได้โดยใช้ฮับช่วยได้ ส่วนประกอบต่างๆภายในเครือข่ายได้ออกแบบให้มีลักษณะดังนี้

1. ไฟล์เซอร์ฟเวอร์ 1 เครื่อง

1.1 ใช้เครื่องคอมพิวเตอร์ที่มีโปรเซสเซอร์ขนาด 32 บิตหรือ 64 บิต

1.2 หน่วยความจำหลัก 64 เมกกะไบต์

1.3 ฮาร์ดดิสก์ 5 กิกะไบต์

1.4 ฟลอปปีดิสก์ขนาด 3.5 นิ้ว

1.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต ชนิดความเร็ว 10/100 เมกกะบิตต่อวินาที

1.6 เทปไดรว์ขนาด 4 มิลลิเมตร

1.7 ซีดีรอมไดรว์

2. เครื่องคอมพิวเตอร์ที่ใช้เป็นสถานีงาน จำนวน 40 ชุด ประกอบด้วย

2.1 มีโปรเซสเซอร์ขนาด 32 บิต

2.2 หน่วยความจำหลัก 8 เมกกะไบต์

2.3 ความจุของฮาร์ดดิสก์ 530 เมกกะไบต์

2.4 ฟลอปปีดิสก์ไดรว์ขนาด 3.5 นิ้ว

2.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต ชนิด 10/100 เมกกะบิตต่อวินาที

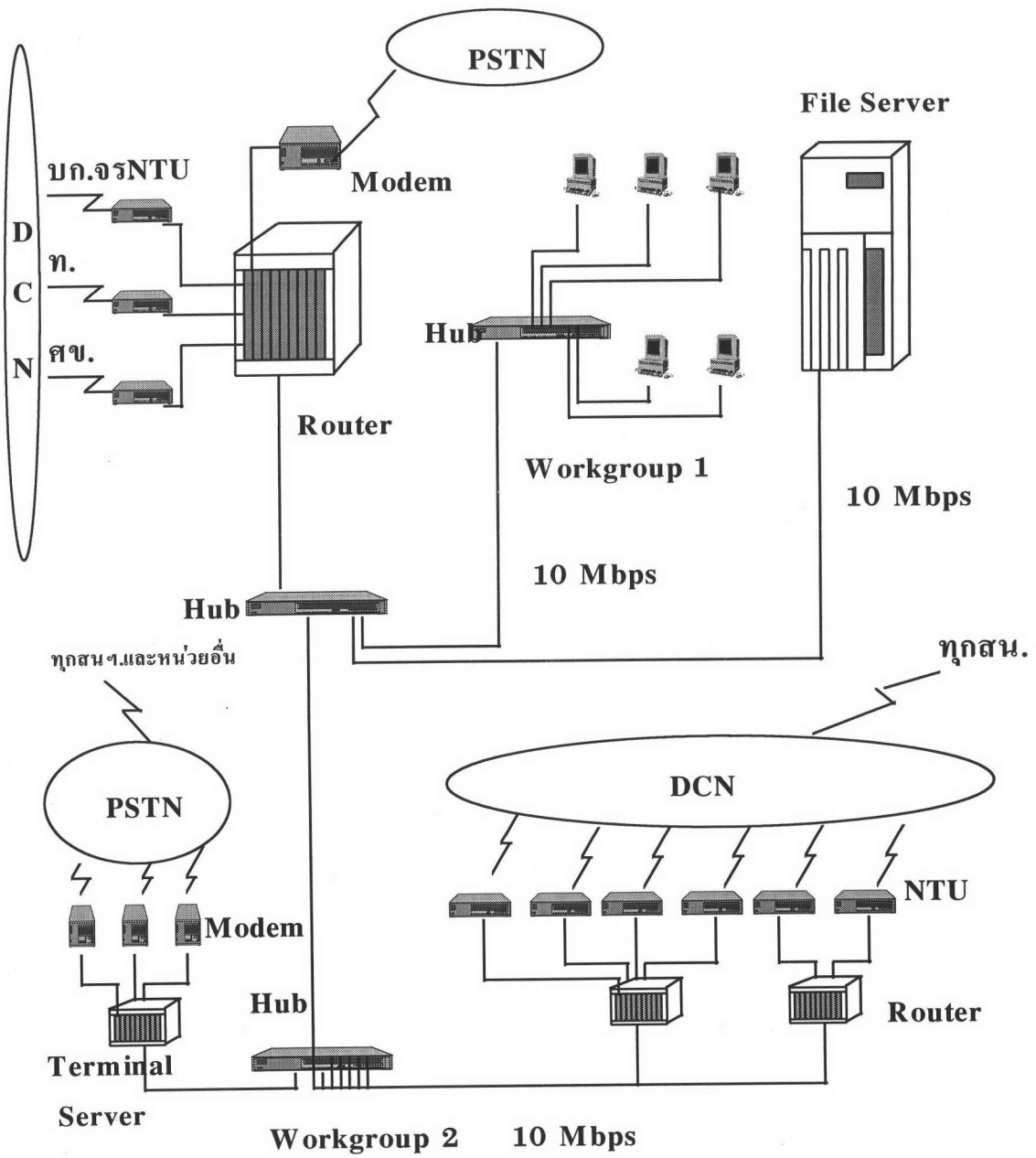
3. ฮับ 16 ช่องสัญญาณ ชนิด 10/100 เมกกะบิตต่อวินาที จำนวน 4 ตัว

4. เร้าเตอร์ ให้มีจำนวนช่องสัญญาณแบบอะซิงโครนัสอย่างน้อย 80 ช่องสัญญาณ หรือใช้เร้าเตอร์ชนิด 4 ช่องสัญญาณอะซิงโครนัส 20 ตัว

5. โมเด็ม 10 ตัว

6. เทอร์มินอลเซอร์ฟเวอร์สำหรับใช้ในการติดต่อระยะไกลกับโมเด็ม ให้มีช่องสัญญาณแบบอะซิงโครนัสจำนวน 16 ช่อง 1 ตัว

รูปต่อไปนี้แสดงเครือข่ายท้องถิ่นของกองบัญชาการตำรวจนครบาล



รูปที่ 4.8 แสดงเครือข่ายภายในกองบัญชาการตำรวจนครบาล

8.4 การออกแบบเครือข่ายภายในสถานีตำรวจ

สำหรับสถานีตำรวจไม่ว่าจะเป็นสถานีตำรวจนครบาลหรือสถานีตำรวจภูธร การใช้งานคอมพิวเตอร์ย่อมมีอยู่เช่นกัน แต่เมื่อพิจารณาถึงความจำเป็นเมื่อต้องการใช้ข้อมูลแข่งกับเวลาหรือความรีบด่วนในการเข้าถึงข้อมูลแล้วจะเห็นว่าสถานีตำรวจนครบาลอาจมีความต้องการใช้งานสูงกว่า แต่อย่างไรก็ตามการออกแบบเครือข่ายไว้ล่วงหน้าก็ไม่ใช่ว่าจะไม่มีประโยชน์ ดังนั้นจึงออกแบบให้สถานีตำรวจทั้งในเขตนครบาลและภูธรมีโครงสร้างของเครือข่ายภายในสำนักงานคล้ายกัน โดยใช้เครือข่ายแบบ อีเทอร์เน็ต โดยมีฮับเป็นอุปกรณ์ช่วยในการเชื่อมต่อกับคอมพิวเตอร์ในเครือข่ายท้องถิ่น (ซึ่งโดยความจำเป็นในการใช้งานแล้ว สถานีตำรวจบางแห่งสามารถใช้สายโคแอกเชียลแบบบางเป็นแบ็กโบนหรือทำตาม 10BASE2 ได้ด้วย แต่มีแนวโน้มจะให้เปลี่ยนเป็น UTP กับ ฮับ แทนซึ่งในการออกแบบนี้จะใช้สาย UTP และฮับ) โดยจะได้ความเร็วที่ 10 เมกกะบิตต่อวินาทีนอกจากนี้ยังมีการเชื่อมโยงกับหน่วยงานอื่นโดยใช้ หมุนผ่านสายโทรศัพท์สาธารณะ ผ่านโมเด็ม ดังนั้นในสน.จะมีอุปกรณ์ดังนี้

1. ไฟล์เซอร์ฟเวอร์ 1 เครื่อง

1.1 ใช้เครื่องคอมพิวเตอร์ที่มีโปรเซสเซอร์ขนาด 32 บิตหรือ 64 บิต

1.2 หน่วยความจำหลัก 32 เมกกะไบต์

1.3 ฮาร์ดดิสก์ 1 กิกะไบต์

1.4 ฟลอปปีดิสก์ขนาด 3.5 นิ้ว

1.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต
ชนิดความเร็ว 10/100 เมกกะบิตต่อวินาที

2. เครื่องคอมพิวเตอร์ที่ใช้เป็นสถานีงาน จำนวน 4 ชุด ประกอบด้วย

2.1 มีโปรเซสเซอร์ขนาด 32 บิต

2.2 หน่วยความจำหลัก 8 เมกกะไบต์

2.3 ความจุของฮาร์ดดิสก์ 530 เมกกะไบต์

2.4 ฟลอปปีดิสก์ไดรว์ขนาด 3.5 นิ้ว

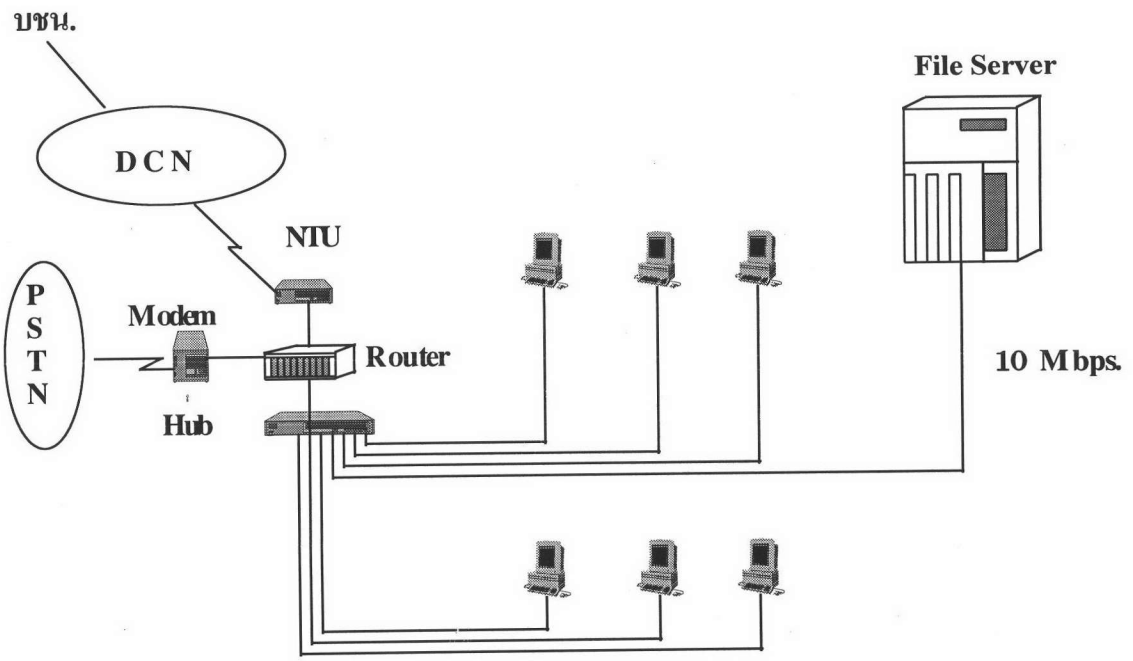
2.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต ชนิด 10/100 เมกกะบิตต่อวินาที

3. ฮับ 16 ช่องสัญญาณ ชนิด 10/100 เมกกะบิตต่อวินาที จำนวน 1 ตัว

4. เร้าเตอร์ ให้มีจำนวนช่องสัญญาณแบบอะซิงโครนัสอย่างน้อย 2 ช่องสัญญาณ หรือใช้เร้าเตอร์ชนิด 2 ช่องสัญญาณอะซิงโครนัส 1 ตัว

5. โมเด็ม 1 ตัว

รูปต่อไปนี้แสดงเครือข่ายภายในสน.



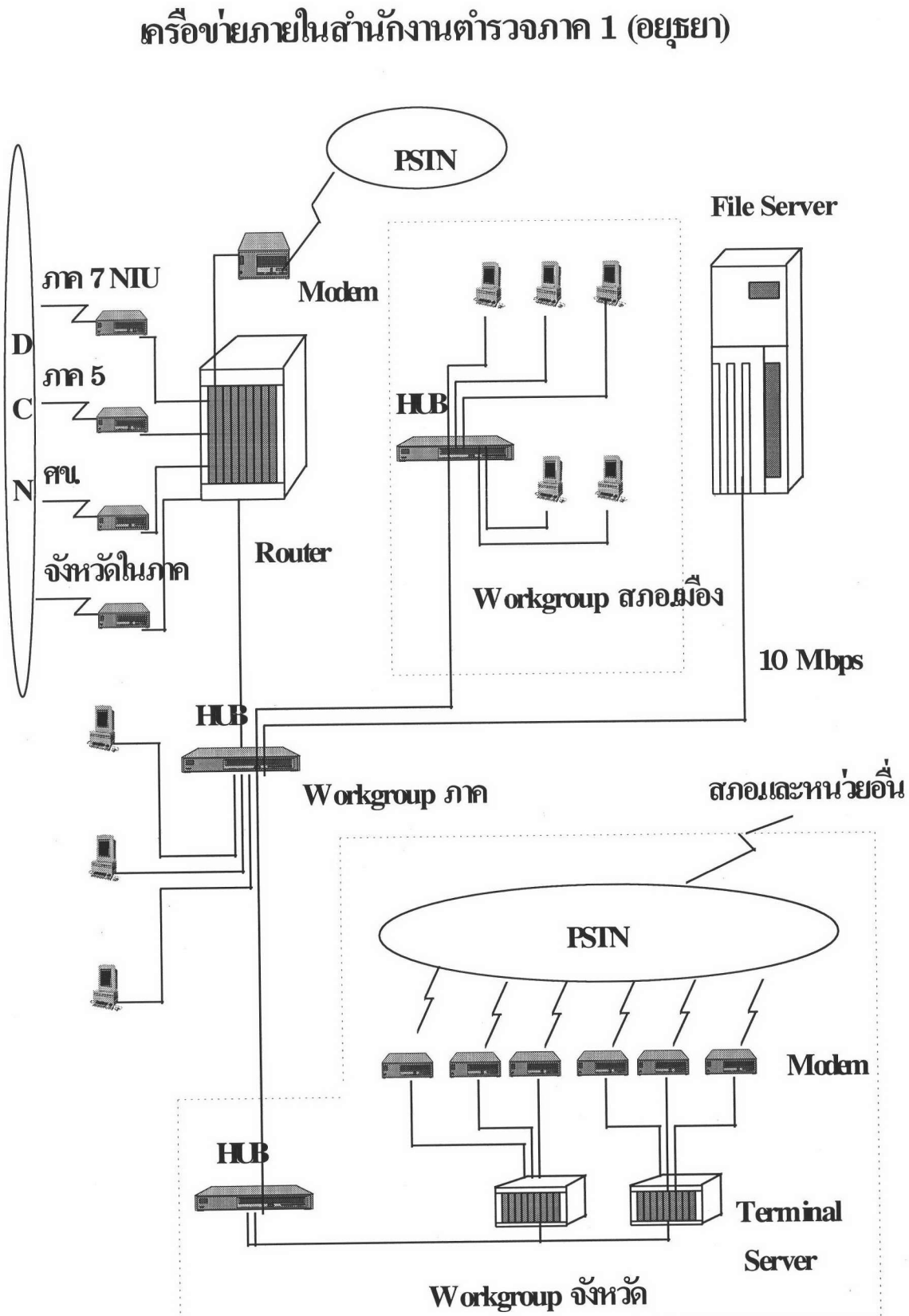
รูปที่ 4.9 แสดงเครือข่ายภายในสถานีตำรวจต่างๆ

8.5 การออกแบบเครือข่ายท้องถิ่นภายในสำนักงานตำรวจภาค

ภายในสำนักงานตำรวจภาคต่างๆทั้ง 9 ภาคนั้นจะมีลักษณะคล้ายกันคือจะเป็นที่ตั้งของกองกำกับการตำรวจภูธรจังหวัดและสถานีตำรวจภูธรอำเภอเมือง (สภ.อ.เมือง) ด้วย นอกจากนี้ความต้องการในการเชื่อมโยงไปยังศูนย์ข้อมูลที่กรมตำรวจในกรุงเทพและเชื่อมโยงไปยังสำนักงานภาคอื่นๆ ดังนั้นการออกแบบเครือข่ายภายในสำนักงานภาคทั้ง 9 นี้จะมีส่วนคล้ายกันมาก โดยจะใช้เครือข่ายแบบ อีเทอร์เน็ต ตามแบบ 10BaseT นั่นคือจะใช้ฮับเป็นอุปกรณ์กระจายสัญญาณไปสู่เครื่องคอมพิวเตอร์ในเครือข่ายและใช้สาย UTP เป็นสื่อนำสัญญาณ จากนั้นจะมีฮับเป็นอุปกรณ์ช่วยแยกกลุ่มของสถานีงานออกไปตามสายงาน ดังนั้นในเครือข่ายของตำรวจภูธรภาคจึงมีอุปกรณ์ดังนี้

1. ไฟล์เซอร์ฟเวอร์ 1 เครื่อง
    - 1.1 ใช้เครื่องคอมพิวเตอร์ที่มีโปรเซสเซอร์ขนาด 32 บิตหรือ 64 บิต
    - 1.2 หน่วยความจำหลั ก 64 เมกกะไบต์
    - 1.3 ฮาร์ดดิสก์ 5 กิกะไบต์
    - 1.4 ฟลอปปีดิสก์ขนาด 3.5 นิ้ว
    - 1.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ตชนิดความเร็ว10/100เมกกะบิตต่อวินาที
    - 1.6 เทปไดรว์ขนาด 4 มิลลิเมตร
    - 1.7 ซีดีรอมไดรว์
2. เครื่องคอมพิวเตอร์ที่ใช้เป็นสถานีงาน จำนวน 20 ชุด ประกอบด้วย
    - 2.1 มีโปรเซสเซอร์ขนาด 32 บิต
    - 2.2 หน่วยความจำหลัก 8 เมกกะไบต์
    - 2.3 ความจุของฮาร์ดดิสก์ 530 เมกกะไบต์
    - 2.4 ฟลอปปีดิสก์ไดรว์ขนาด 3.5 นิ้ว
    - 2.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต ชนิด 10/100 เมกกะบิตต่อวินาที
3. ฮับ 16 ช่องสัญญาณ ชนิด 10/100 เมกกะบิตต่อวินาที จำนวน 1 ตัว
   และ ฮับ 8 ช่องสัญญาณ จำนวน 2 ตัว
4. เราเตอร์ ให้มีจำนวนช่องสัญญาณแบบอะซิงโครนัส 11-14 ช่องสัญญาณ หรือใช้เราเตอร์ชนิด 4 ช่องสัญญาณอะซิงโครนัส 4 ตัว
5. โมเด็ม 10-12 ตัว
6. เทอร์มินอลเซอร์ฟเวอร์สำหรับใช้ในการติดต่อระยะไกลกับโมเด็ม ให้มีช่องสัญญาณ

แบบอะซิงโครนัสจำนวน 16 ช่อง 1 ตัว



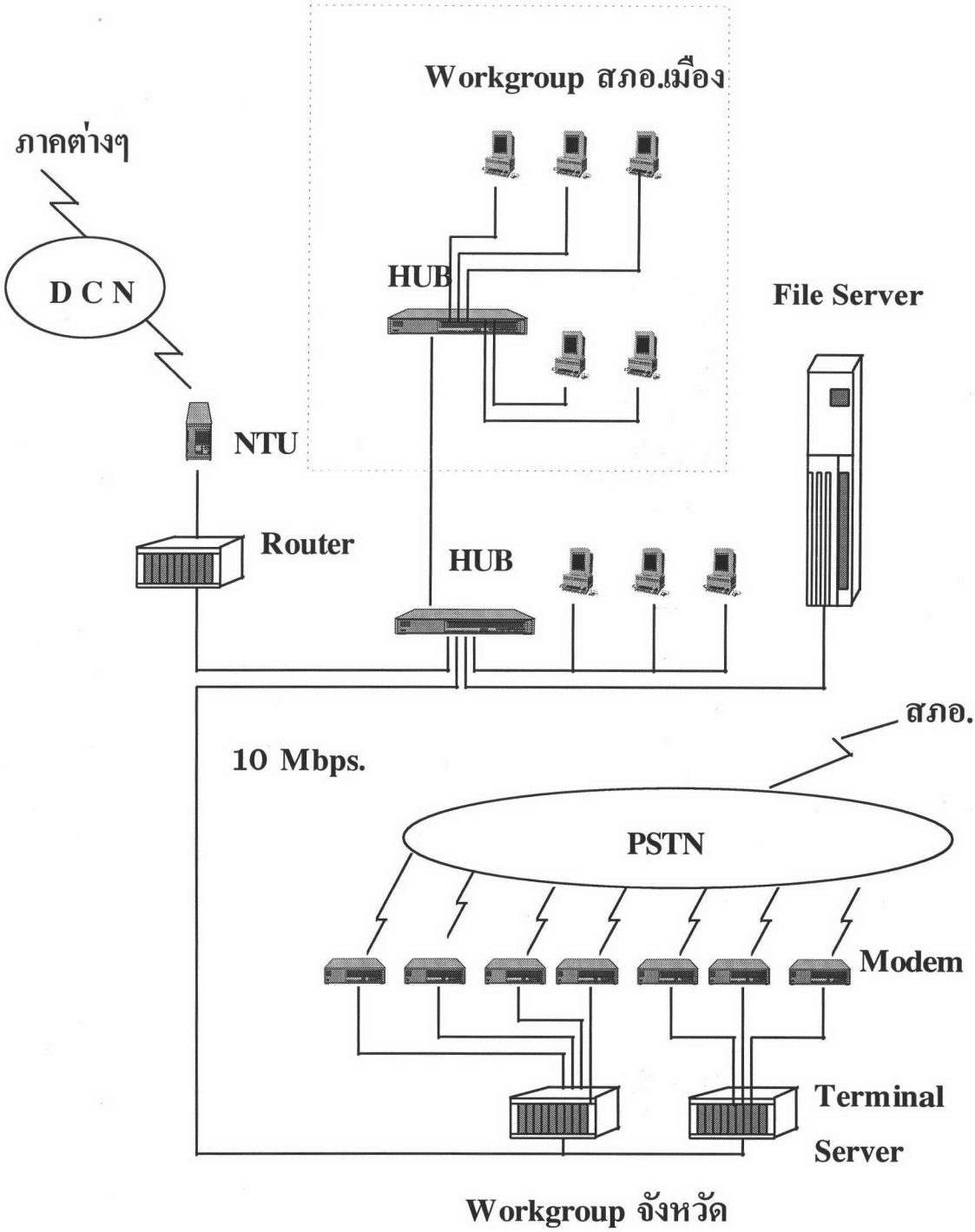
รูปที่ 4.10 แสดงตัวอย่างเครือข่ายภายในสำนักงานภาค 1

8.6 การออกแบบเครือข่ายภายในกองบังคับการตำรวจภูธรจังหวัด

เนื่องจากกองบังคับการตำรวจภูธรจังหวัดจะตั้งอยู่ในบริเวณเดียวกับสถานีตำรวจภูธรอำเภอเมืองหรือสภ.อ.เมือง ดังนั้นจึงมีความจำเป็นที่จะต้องมีเครือข่ายท้องถิ่นภายในสำนักงาน ซึ่งยังคงใช้เครือข่ายแบบ อีเทอร์เน็ต โดยใช้สายสัญญาณแบบ UTP สำหรับทำเป็นสื่อนำสัญญาณ โดยมีฮับเป็นอุปกรณ์ที่ใช้แยกกลุ่มการทำงานของสถานีงาน และที่หน่วยงานนี้จะมีโมเด็ม ไว้สำหรับเชื่อมโยงกับเครือข่ายอื่นด้วย แต่จะไม่มีการเชื่อมโยงด้วยวงจรความเร็วสูง (64 กิโลบิตต่อวินาที) ดังนั้นเครือข่ายในตำรวจภูธรจังหวัดจึงมีการออกแบบให้มีอุปกรณ์ต่างๆดังนี้

1. ไฟล์เซอร์ฟเวอร์ 1 เครื่อง
    1.1 ใช้เครื่องคอมพิวเตอร์ที่มีโปรเซสเซอร์ขนาด 32 บิตหรือ 64 บิต
    1.2 หน่วยความจำหลัก 32 เมกกะไบต์
    1.3 ฮาร์ดดิสก์ 1 กิกะไบต์
    1.4 ฟลอปปีดิสก์ขนาด 3.5 นิ้ว
    1.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต
        ชนิดความเร็ว 10/100 เมกกะบิตต่อวินาที
2. เครื่องคอมพิวเตอร์ที่ใช้เป็นสถานีงาน จำนวน 10 ชุด ประกอบด้วย
    2.1 มีโปรเซสเซอร์ขนาด 32 บิต
    2.2 หน่วยความจำหลัก 8 เมกกะไบต์
    2.3 ความจุของฮาร์ดดิสก์ 530 เมกกะไบต์
    2.4 ฟลอปปีดิสก์ไดรว์ขนาด 3.5 นิ้ว
    2.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต ชนิด 10/100 เมกกะบิตต่อวินาที
3. ฮับ 16 ช่องสัญญาณ ชนิด 10/100 เมกกะบิตต่อวินาที จำนวน 2 ตัว
4. เราเตอร์ ให้มีจำนวนช่องสัญญาณแบบอะซิงโครนัสอย่างน้อย 2 ช่องสัญญาณ หรือใช้เราเตอร์ชนิด 2 ช่องสัญญาณอะซิงโครนัส 1 ตัว
5. โมเด็ม 8-12 ตัว
6. เทอร์มินอลเซอร์ฟเวอร์สำหรับใช้ในการติดต่อระยะไกลกับโมเด็ม ให้มีช่องสัญญาณแบบอะซิงโครนัสจำนวน 16 ช่อง 1 ตัว

เครือข่ายภายในกองกำกับการตำรวจภูธรจังหวัดและสภอ.เมือง



รูปที่ 4.11 แสดงเครือข่ายภายในกองบังคับการตำรวจภูธรจังหวัด

5. การเชื่อมต่อไปยังหน่วยงานอื่นๆ

สำหรับหน่วยงานอื่นที่อยู่นอกกรมตำรวจเช่น กองการต่างประเทศ กองตรวจคนเข้าเมือง กองหนังสือเดินทางเป็นต้น ได้ออกแบบให้สามารถเชื่อมโยงกันได้โดยการเตรียมโมเด็มและสายวงจรโทรศัพท์เพื่อเปิดให้หน่วยงานอื่นๆสามารถเชื่อมโยงเข้าสู่เครือข่ายของกรมตำรวจได้ แต่ทั้งนี้จำเป็นจะต้องออกข้อบังคับเอาไว้เพื่อการป้องกันผู้ไม่ประสงค์และเป็นการรักษาความลับของกรมตำรวจด้วย

6. อุปกรณ์สื่อสารข้อมูลในเครือข่าย

อุปกรณ์ที่ใช้ในการเชื่อมโยงเครือข่ายระหว่างหน่วยงานต่างๆนั้นได้แก่ เราเตอร์ ซึ่งอุปกรณ์ดังกล่าว จะต้องมีคุณสมบัติดังนี้

1. สามารถรองรับแบ็กโบนแบบอีเทอร์เน็ตและเคเบิลใยแก้วที่ติดตั้งในกรมตำรวจ โดยมีความเร็วไม่ต่ำกว่า 10 กิโลบิตต่อวินาที
2. สามารถรองรับ เทอร์มินอลหรือไมโครคอมพิวเตอร์ที่เป็นสถานีงานทั้งหมดที่ติดตั้งในศูนย์ข้อมูล ในลักษณะของ อีเทอร์เน็ต
3. สามารถรองรับการเชื่อมต่อแบบอนุกรมความเร็วสูง ตามมาตรฐาน V. 35 ที่มีความเร็วในการรับส่งข้อมูลไม่ต่ำกว่า 64 กิโลบิตต่อวินาที จำนวนไม่น้อยกว่า 15 ช่องสัญญาณ
4. สามารถรองรับการเชื่อมต่อแบบอนุกรมตามมาตรฐาน V.21 ที่มีความเร็วในการรับส่งข้อมูลไม่ น้อยกว่า 9600 บิตต่อวินาที จำนวนไม่น้อยกว่า 30 ช่องสัญญาณ
5. สามารถรองรับโปรโตคอล TCP/IP, PPP ได้เป็นอย่างน้อย
6. สามารถรองรับโปรโตคอลการจัดการเส้นทางส่งข้อมูลแบบ RIP และ OSPF ได้
7. สามารถรองรับการจัดการในเครือข่ายตามมาตรฐาน SNMP
8. มีคุณสมบัติ Transparent Bridging
9. มีช่องสัญญาณสำหรับคอนโซล จำนวนอย่างน้อย 1 ช่องสัญญาณ
10. มีตัวจ่ายกระแสไฟสองชุด

สำหรับอุปกรณ์ที่ใช้ที่ รีโมต ไซต์ มีคุณสมบัติอย่างน้อยดังนี้

1. สามารถรองรับเทอร์มินอลและไมโครคอมพิวเตอร์ที่เป็นสถานีงานทั้งหมดในหน่วยงานที่ ไซต์

2. รีโมตเราเตอร์ที่ใช้ในกรุงเทพต้องสามารถรองรับเทอร์มินอล ของผู้ใช้งาน ในเขตกรุงเทพร่วมกับ ศูนย์กลาง ได้อย่างมีประสิทธิภาพ
3. มีการเชื่อมต่อแบบอนุกรมความเร็วสูง มาตราฐาน V.35 ที่มีความเร็วในการรับส่งข้อมูล ไม่น้อยกว่า 64 กิโลบิตต่อวินาที จำนวนไม่น้อยกว่า 3 ช่องสัญญาณ
4. สามารถรองรับโปรโตคอลทีซีพี/ไอพี และพีพีพี ได้เป็นอย่างน้อย
5. สามารถรองรับโปรโตคอลจัดการเส้นทางส่งข้อมูลแบบ อาร์ไอพี (RIP) และ โอเอสพีเอฟ (OSPF) เป็นอย่างน้อย
6. สามารถรองรับการจัดการเครือข่ายตามมาตราฐานเอสเอ็นเอ็มพี (SNMP) เป็นอย่างน้อยและอื่นๆที่ใช้ในระบบ
7. มีคุณสมบัติทรานแพเรนบริดจ์ (Transparent Bridging)
8. มีช่องสัญญาณสำหรับต่อกับคอนโซลจำนวนอย่างน้อย 1 ช่อง

อุปกรณ์ที่ใช้เป็นโมเด็มควรมีคุณสมบัติอย่างน้อยดังนี้

1. มีคุณสมบัติตามมาตรฐาน CCITT V.42 bis เป็นอย่างน้อย
2. มีคุณสมบัติ Error Correction ตามมาตรฐาน V.42
3. มีคุณสมบัติบีบอัดข้อมูล ตามมาตรฐาน V.42 bis
4. สามารถใช้งานได้ทั้ง 2/4 wire leased line และ หมุนผ่านสายโทรศัพท์สาธารณะ
5. มีคุณสมบัติ Automatic dial backup กรณีที่สายเช่า ไม่สามารถใช้งานได้
6. สามารถปรับความเร็วตั้งแต่ 1.2 กิโลบิตต่อวินาที - 14.4 กิโลบิตต่อวินาที ในการรับส่งข้อมูลได้อย่างอัตโนมัติ โดยขึ้นอยู่กับสภาพของสาย
7. สามารถใช้กับงานได้ทั้งแบบซิงโครนัสและอะซิงโครนัส
8. มีหน้าปัดถ์แสดงสถานะการทำงานและสัญญาณต่างๆได้อย่างถูกต้อง

<u>7. การจัดการเครือข่าย</u>

ระบบเครือข่ายที่ประสบความสำเร็จในการดำเนินงานนั้นมีความจำเป็นอย่างยิ่งที่จะต้องมีการดูแลเครือข่ายทั้งหมด ดังนั้นจึงต้องมีการจัดตั้งหน่วยงานที่เรียกว่า เน็ตเวอร์กแมเนจเมนต์เซ็นเตอร์ (Network Management Center หรือ NMC)

NMC ทำหน้าที่เป็นศูนย์ตรวจสอบ และควบคุมการทำงานของเครือข่ายทั้งหมด โดยต้องประกอบด้วยสถานีงานและจอภาพกราฟิกส์ขนาดใหญ่ พร้อมซอฟต์แวร์ที่เหมาะสมในการควบคุม

เครือข่าย NMC จะทำการติดต่อกับอุปกรณ์สื่อสารข้อมูลต่างๆในเครือข่าย โดยใช้โปรโตคอลตามแบบ SNMP ทำให้ NMC สามารถทราบถึงสถานะของเครือข่ายได้อย่างดีตลอดเวลา และยังสามารถใช้ข้อมูลเกี่ยวกับเครือข่ายที่มีเพื่อการตัดสินใจในการขยายระบบในอนาคตด้วย

ลักษณะเฉพาะของอุปกรณ์บริหารงานเครือข่าย เป็นดังนี้

1. เครื่องที่เป็นสถานีงาน จะต้องเป็นแบบคุณภาพสูง สามารถเปิดใช้งานได้ตลอด 24 ชม. ติดต่อกัน โดยมีคุณสมบัติอย่างต่ำดังนี้

1.1 ใช้ หน่วยประมวลผล แบบ 32 บิต หรือดีกว่า

1.2 มีจอภาพพร้อมอุปกรณ์ควบคุม แบบจอสี มีความละเอียดในการแสดงผลไม่น้อยกว่า 1024x768 จุดภาพ

1.3 มีจานแม่เหล็กแบบฟลอปปี ขนาด 3.5 นิ้ว ความจุ 1.44 เมกกะไบต์ อย่างน้อย 1 เครื่อง

1.4 มีจานแม่เหล็กแบบฮาร์ดดิสก์ ความจุไม่น้อยกว่า 1 กิกะไบต์

1.5 มีเทปความจุสูงไม่น้อยกว่า 4 กิกะไบต์ จำนวน 1 เครื่อง

1.6 มี อีเทอร์เน็ตอินเตอร์เฟสการ์ด เพื่อเชื่อมโยงกับเครือข่ายได้

1.7 มีความสามารถใช้ได้ดีกับซอฟต์แวร์ บริหารเครือข่าย

2. ซอฟต์แวร์ บริหารเครือข่าย จำนวน 1 ชุด 2 user licenses ซึ่งมีคุณสมบัติขั้นต่ำดังนี้

2.1 มีการแสดงผลเป็นแบบกราฟิกส์

2.2 สามารถช่วยติดตั้งและปรับแต่ง อุปกรณ์ เราเตอร์ และ สวิตชิ่งโหนด

2.3 สามารถค้นหาและตรวจสอบข้อผิดพลาด ของระบบเครือข่าย

2.4 สามารถเก็บสถิติการรับส่งข้อมูลเพื่อใช้ในการวิเคราะห์ระบบในเครือข่ายดังต่อไปนี้

2.4.1 จำนวนข้อมูลที่ส่งในแต่ละอินเตอร์เฟส

2.4.2 จำนวนข้อมูลผิดพลาด

2.4.3 เวลาที่มีข้อมูลส่งผ่านในระบบมากที่สุด

2.5 สนับสนุนโปรโตคอลในการบริหารเครือข่ายดังต่อไปนี้

2.5.1 เอสเอ็นเอ็มพี (SNMP)

2.5.2 เอ็มไอบี (MIB I Version 2 และ MIB II)

นอกจากการใช้ระบบคอมพิวเตอร์ช่วยในการดูแลระบบเครือข่ายแล้ว ยังมีความจำเป็นที่จะต้องใช้บุคคลากรในการจัดการเครือข่ายอีกด้วย โดยแบ่งออกเป็น

1. งานดูแลความเรียบร้อยของเครือข่าย

เจ้าหน้าที่ในส่วนนี้จะมีหน้าที่ในการตรวจตราดูแลความเรียบร้อยของเครือข่าย ได้แก่อุปกรณ์ต่างๆในเครือข่ายและคอยให้บริการช่วยเหลือหรือให้คำปรึกษาแก่เจ้าหน้าที่คนอื่นที่เป็นผู้ใช้ระบบตามที่ได้รับมอบหมายงาน เจ้าหน้าที่ในส่วนนี้ควรจะเป็นวิศวกรที่มีความชำนาญทางด้านเครือข่ายเป็นอย่างดี

2. งานวางแผนและพัฒนา

เจ้าหน้าที่ในส่วนนี้จะทำหน้าที่วางแผนงานรวมทั้งกำหนดมาตราการต่างๆ วางนโยบายและแผนงานในอนาคตของเครือข่ายคอมพิวเตอร์ของกรมตำรวจ ซึ่งควรจะสอดคล้องกับนโยบายของกรมตำรวจเองด้วย

3. งานฝึกอบรม

เจ้าหน้าที่ในส่วนนี้จะต้องทำหน้าที่จัดฝึกอบรมเจ้าหน้าที่ตำรวจซึ่งเป็นผู้ใช้งานเครือข่ายให้มีความรู้ความเข้าใจในระบบคอมพิวเตอร์รวมทั้งระบบเครือข่ายของกรมตำรวจ โดยจัดฝึกอบรมให้ผู้ใช้สามารถใช้งานเครือข่ายได้อย่างถูกต้อง มีระเบียบ และสามารถใช้งานเครือข่ายได้อย่างมีประสิทธิภาพเพื่อให้เกิดประโยชน์สูงสุด

4. งานให้คำปรึกษาทางเทคนิค

งานในส่วนนี้ทำหน้าที่เป็น Help desk หรือเจ้าหน้าที่ที่คอยรับโทรศัพท์หรือรับคำขอความช่วยเหลือจากผู้ใช้ระบบเครือข่าย คอยตอบและแก้ไขปัญหาต่างๆที่เกิดขึ้น ซึ่งสถานที่เกิดปัญหานั้นอาจอยู่ไกลไม่สามารถไปได้ทันที ดังนั้นจึงให้หน่วยงานนี้ช่วยแก้ปัญหาทางโทรศัพท์หรือทางใดก็ตามที่จะติดต่อกันได้ เช่นตอบปัญหาทางเทคนิคผ่านทางไปรษณีย์อิเล็คโทรนิคเป็นต้น

8.การออกแบบเครือข่ายท้องถิ่นภายในหน่วยงานต่าง

ภายในหน่วยงานต่างๆนอกเหนือจากศูนย์ข้อมูลแล้ว ยังมีการใช้งานคอมพิวเตอร์เช่นกัน บางหน่วยงานอาจมีการใช้คอมพิวเตอร์ช่วยงานหลายอย่าง มีจำนวนผู้ที่ต้องการใช้เครื่องมากมาย บางหน่วยงานก็ไม่จำเป็นจะต้องใช้งานเครื่องคอมพิวเตอร์มากนัก ดังนั้นการออกแบบเครือข่ายท้องถิ่นภายในหน่วยงานเหล่านี้จึงเป็นสิ่งที่จำเป็นและจะมองข้ามเสียมิได้

8.1. การออกแบบเครือข่ายท้องถิ่นในกองทะเบียน

เนื่องจากในกองทะเบียนมีการใช้งานในส่วนของหน่วยงานนี้เองและงานทะเบียนต้องการความเร็วในการประมวลผลพอสมควร รวมทั้งจำนวนผู้ใช้ก็มีจำนวนมาก ดังนั้นจึงออกแบบให้ใช้เครือข่ายแบบ อีเทอร์เน็ต ความเร็ว 10 เมกกะบิตต่อวินาทีโดยใช้ฮับเป็นอุปกรณ์เชื่อมโยงกับคอมพิวเตอร์ในเครือข่ายโดยใช้สายสัญญาณแบบยูทีพี (UTP) หรือ 10BaseT ซึ่งสามารถมีความยาวของแต่ละเซ็กเมนต์ได้ประมาณ 100 เมตร โดยแต่ละสถานีงานจะเชื่อมต่อกับฮับได้โดยตรง ถ้ามีการเชื่อมโยงไปยังชั้นต่างๆยังสามารถใช้อุปกรณ์ฮับได้ ดังนั้นในกองทะเบียนจึงประกอบไปด้วยอุปกรณ์ต่างๆดังนี้

1. ไฟล์เซอร์ฟเวอร์ 1 เครื่อง

1.1 ใช้เครื่องคอมพิวเตอร์ที่มีโปรเซสเซอร์ขนาด 32 บิตหรือ 64 บิต

1.2 หน่วยความจำหลัก 32 เมกกะไบต์

1.3 ฮาร์ดดิสก์ 1 กิกะไบต์

1.4 ฟลอปปีดิสก์ขนาด 3.5 นิ้ว

1.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต

ชนิดความเร็ว 10/100 เมกกะบิตต่อวินาที

2. เครื่องคอมพิวเตอร์ที่ใช้เป็นสถานีงาน จำนวน 10 ชุด ประกอบด้วย

2.1 มีโปรเซสเซอร์ขนาด 32 บิต

2.2 หน่วยความจำหลัก 8 เมกกะไบต์

2.3 ความจุของฮาร์ดดิสก์ 530 เมกกะไบต์

2.4 ฟลอปปีดิสก์ไดรว์ขนาด 3.5 นิ้ว

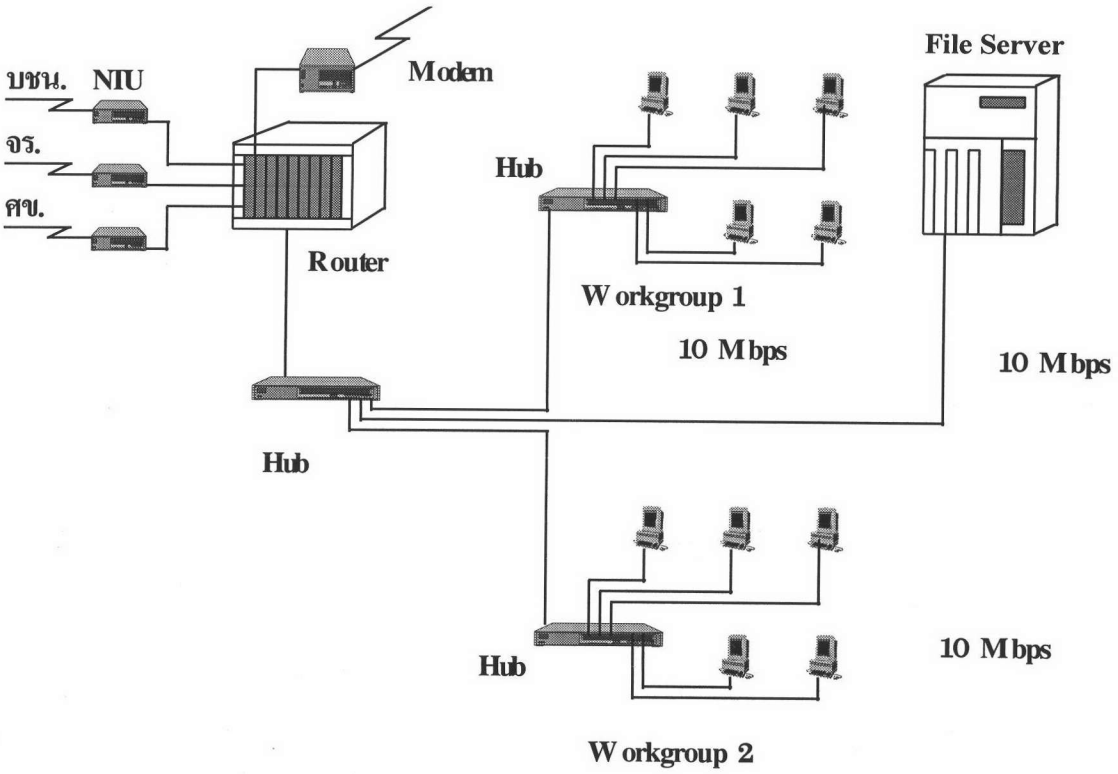
2.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต ชนิด 10/100 เมกกะบิตต่อวินาที

3. ฮับ 16 ช่องสัญญาณ ชนิด 10/100 เมกกะบิตต่อวินาที จำนวน 1 ตัว

4. เร้าเตอร์ ให้มีจำนวนช่องสัญญาณแบบอะซิงโครนัสอย่างน้อย 4 ช่องสัญญาณ หรือใช้เร้าเตอร์ชนิด 4 ช่องสัญญาณอะซิงโครนัส 1 ตัว

5. โมเด็ม 1 ตัว

เครือข่ายภายในกองทะเบียน



รูปที่ 4.6 แสดงเครือข่ายภายในกองทะเบียน

8.2 การออกแบบเครือข่ายท้องถิ่นภายในกองบังคับการตำรวจจราจร

มีลักษณะการใช้งานคอมพิวเตอร์ที่คล้ายกับกองทะเบียน การออกแบบเครือข่ายจึงคล้ายกัน ดังนี้

1. ไฟล์เซอร์ฟเวอร์ 1 เครื่อง

1.1 ใช้เครื่องคอมพิวเตอร์ที่มีโปรเซสเซอร์ขนาด 32 บิตหรือ 64 บิต

1.2 หน่วยความจำหลัก 32 เมกกะไบต์

1.3 ฮาร์ดดิสก์ 3 กิกะไบต์

1.4 ฟลอปปีดิสก์ขนาด 3.5 นิ้ว

1.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต

ชนิดความเร็ว 10/100 เมกกะบิตต่อวินาที

2. เครื่องคอมพิวเตอร์ที่ใช้เป็นสถานีงาน จำนวน 20 ชุด ประกอบด้วย

2.1 มีโปรเซสเซอร์ขนาด 32 บิต

2.2 หน่วยความจำหลัก 8 เมกกะไบต์

2.3 ความจุของฮาร์ดดิสก์ 530 เมกกะไบต์

2.4 ฟลอปปีดิสก์ไดรว์ขนาด 3.5 นิ้ว

2.5 เน็ตเวอร์คอินเตอร์เฟสการ์ดแบบอีเทอร์เน็ต ชนิด 10/100 เมกกะบิตต่อวินาที

3. ฮับ 16 ช่องสัญญาณ ชนิด 10/100 เมกกะบิตต่อวินาที จำนวน 1 ตัว

4. ฮับ 8 ช่องสัญญาณ ชนิด 10/100 เมกกะบิตต่อวินาที จำนวน 2 ตัว

5. เร้าเตอร์ ให้มีจำนวนช่องสัญญาณแบบอะซิงโครนัสอย่างน้อย 4 ช่องสัญญาณ หรือใช้เร้าเตอร์ชนิด 4 ช่องสัญญาณอะซิงโครนัส 1 ตัว

6. โมเด็ม 1 ตัว

รูปต่อไปนี้แสดงเครือข่ายท้องถิ่นของกองบังคับการตำรวจจราจร

เนื่องจากในสำนักงานต่างๆของกรมตำรวจรวมทั้งสถานีตำรวจด้วยนั้น จะมีสายโทรศัพท์ที่ใช้สำหรับเครื่องโทรสารหรือแฟกซ์ ดังนั้นจึงเสนอแนะให้ใช้คู่สายโทรศัพท์ที่ใช้สำหรับเครื่องโทรสารนั้นสำรองไว้ในกรณีฉุกเฉิน ถ้าสายโทรศัพท์สำรองเกิดเสียหาย

9. การจัดการด้านความปลอดภัยของระบบ

หน้าที่สำคัญอย่างหนึ่งในการจัดการเครือข่ายคือการรักษาความปลอดภัยของระบบ ผู้จัดการระบบจะต้องดูแลรักษาระบบเครือข่ายให้ปลอดภัยจากผู้ไม่หวังดีที่จะมาทำลายข้อมูลหรือดูข้อมูลที่เป็นความลับและการทำให้โปรแกรมหรือข้อมูลเสียหายโดยไวรัสคอมพิวเตอร์ การป้องกันระบบเครือข่ายจากผู้ใช้งานที่ไม่มีสิทธิ หมายถึงการจำกัดจำนวนของการเรียกใช้งานโดยผู้ใช้บนระบบเครือข่ายเองรวมทั้งการป้องกันไม่ให้ผู้ที่ไม่ได้เป็นเจ้าหน้าที่ที่มีสิทธิใช้งานในระบบเครือข่ายด้วย

9.1 การจำกัดจำนวนผู้ใช้บนเครือข่าย

ผู้ที่ทำหน้าที่เป็นผู้จัดการระบบเครือข่ายสามารถใช้คุณสมบัติพิเศษที่มีในระบบปฏิบัติการเครือข่ายในการจำกัดการเรียกใช้งานระบบแฟ้มข้อมูล จากผู้ใช้งานระบบโดยการซ่อนระบบแฟ้มข้อมูล นั้นไว้ ดังนั้นเวลาที่ผู้ใช้เหล่านั้นต้องการดูรายการของแฟ้มข้อมูล ก็จะมองไม่เห็นระบบแฟ้มข้อมูล ที่ทำการซ่อนไว้ เช่นเดียวกันถ้าหากผู้จัดการระบบเครือข่ายไม่ได้กำหนดสิทธิในการอ่าน ค้นหาข้อมูลหรือค้นหา ระบบแฟ้มข้อมูล ที่ระบุให้กับผู้ใช้งาน ผู้ใช้เหล่านั้นก็จะมองไม่เห็น ระบบแฟ้มข้อมูล นั้นๆได้ ผู้จัดการระบบเครือข่ายสามารถกำหนดรหัสผ่าน สำหรับให้ผู้ใช้งานแต่ละคนใส่ให้ถูกต้องเสียก่อนจึงจะเข้าสู่ระบบได้ และรหัสผ่านนี้จะแตกต่างกันไปบนเซอร์ฟเวอร์ แต่ละเครื่อง นั่นคือผู้ใช้แต่ละคนจะถูกจำกัดให้ทำงานได้เฉพาะบน เซอร์ฟเวอร์ ที่กำหนดไว้เท่านั้น มีวิธีการต่างๆที่ผู้จัดการระบบเครือข่ายสามารถใช้ในการป้องกันระบบโดยรหัสผ่านได้แก่

9.1.1 ห้ามผู้ใช้งานใส่รหัสผ่านไว้ในแฟ้มคำสั่งตามลำดับหรือสคริป สำหรับการเข้าสู่ระบบแบบอัตโนมัติ เนื่องจากจะทำให้รหัสผ่านสามารถอ่านได้จากผู้อื่น ดังนั้นจึงไม่ใช่รหัสลับอีกต่อไป

9.1.2 กำหนดให้ผู้ใช้งานตั้งรหัสผ่านตามความยาวที่กำหนด

9.1.3 กำหนดอายุของรหัสผ่าน เพื่อบังคับให้ผู้ใช้งานระบบต้องเปลี่ยนรหัสผ่านทันทีเมื่อถึงเวลาที่กำหนดนั่นคือเวลาที่รหัสผ่านหมดอายุนั่นเอง

9.1.4 ป้องกันไม่ให้ผู้ใช้งานตั้งรหัสผ่านเป็นชื่อเดิมซ้ำกันสองครั้งติดต่อกัน

9.1.5 แนะนำให้ผู้ใช้งานตั้งชื่อรหัสผ่านจากชื่อที่เดาได้ยากหรือไม่สามารถเดาได้

9.1.6 ป้องกันไม่ใช้ผู้ใช้งานใช้รหัสผ่านเดียวกันเข้าสู่ระบบจากสถานีงานหลายๆ เครื่องพร้อมกัน

9.1.7 กำหนดไม่ให้ผู้ใช้งานเข้าสู่ระบบตามวันและเวลาที่ระบุไว้เช่นวันหยุดราชการ (ใช้กับผู้ใช้งานบางคนหรือบางแผนก)

9.1.8 บนบางระบบปฏิบัติการของระบบเครือข่ายจะมีการทำการเข้ารหัสของรหัสผ่านได้ ทำให้ผู้ไม่หวังดีไม่สามารถอ่านรหัสผ่านที่เก็บไว้ในระบบได้

9.1.9 ผู้จัดการระบบเครือข่ายต้องคอยเตือนไม่ให้ผู้ใช้งานระบบทุกคนจดรหัสผ่านของตนเอาไว้บนกระดาษและติดเอาไว้ใกล้เครื่อง

9.1.10 มีการกำหนดระยะเวลา Timeout สำหรับการใช้งานระบบเครือข่ายเมื่อเปิดทิ้งไว้โดยไม่ใช้งาน

9.1.11ผู้จัดการระบบเครือข่ายจะต้องได้รับการแจ้งทุกครั้งที่เจ้าหน้าที่หรือผู้ใช้งานระบบเครือข่ายพ้นสภาพการเป็นเจ้าหน้าที่ของหน่วยงานเพื่อที่ผู้จัดการระบบเครือข่ายจะได้ทำการตัดสิทธิในการใช้งานออกจากระบบเครือข่ายด้วย

9.1.12 ผู้ใช้งานประเภทพนักงานชั่วคราว ควรจะถูกกำหนดให้มีบัญชีบนระบบเครือข่ายแบบที่มีอายุการใช้งานครั้งละไม่นานนัก

9.2 การป้องกันจากผู้ไม่มีสิทธิเข้าระบบเครือข่าย

ระบบการรักษาความปลอดภัยบนระบบเครือข่ายมักจะทำได้ยากในกรณีที่ระบบเครือข่ายนั้นเปิดโอกาสให้มีการเข้าสู่ระบบจากผู้ใช้งานระยะไกล การป้องกันโดยใช้รหัสผ่านเป็นการป้องกันได้ในระดับหนึ่ง นอกจากนี้เรายังสามารถเพิ่มการป้องกันได้โดยกำหนดจำนวนการใส่รหัสผ่าน ถ้าหากมีการใส่รหัสผ่านผิดเป็นจำนวนครั้งที่กำหนด ผู้ใช้คนนั้นก็จะถูกระงับสิทธิการใช้งานระบบ และจะต้องแจ้งให้ผู้จัดการระบบดำเนินการต่อไป ซึ่งจะช่วยให้การป้องการเข้าสู่ระบบของผู้ไม่ประสงค์ดีได้อีกขั้นหนึ่ง

นอกจากนี้ยังมีการป้องกันการใช้เข้าสู่ระบบจากระยะไกลอีกวิธีหนึ่งคือการใช้โมเด็มแบบ call-back โมเด็ม อุปกรณ์แบบนี้เป็น โมเด็ม ที่หลังจากรับการติดต่อแล้วจะกำหนดให้ใส่รหัสผ่าน จากนั้นจะมีการเรียกกลับไปยังผู้จะที่เข้าสู่ระบบให้ติดต่อและใส่รหัสผ่านตามช่วงเวลาสุ่มที่กำหนด call-back โมเด็ม จะมีการโปแกรมเก็บตารางต่างๆเช่น รายชื่อของผู้ใช้งานหมายเลขโทรศัพท์เอาไว้ ถ้าใส่รายละเอียดผิดก็จะตัดการติดต่อ สำหรับการป้องกันผู้ใช้ที่อยู่ในหน่วยงานอื่นที่ต้องการเข้าสู่ระบบเครือข่ายหรือผู้ใช้ที่อาจเข้ามาโดยผ่านระบบเครือข่ายอินเตอร์เน็ต (ซึ่งระบบเครือข่ายของเราอาจติดต่อกับผู้ให้บริการที่เป็นเกตเวย์ของอินเตอร์เน็ต) เรา

สามารถจัดหาระบบป้องกันจำพวก FireWall มาช่วยได้ ตารางต่อไปนี้แสดงถึงวิธีการลักลอบการใช้งานเครือข่ายและวิธีป้องกัน

องค์ประกอบในเครือข่าย	การกระทำ	การป้องกัน
ระบบปฏิบัติการ	การเข้าถึงโดยไม่ได้รับอนุญาต การแก้ไขระบบโดยไม่ได้รับอนุญาต ทำความเสียหายซอฟต์แวร์	กำหนดสิทธิในการเข้าระบบ ใช้รหัสผ่าน
โมเด็ม	ขโมยข้อมูล เข้าสู่ระบบโดย Hacker (แฮกเกอร์) ทำความเสียหายซอฟต์แวร์	ใช้ โมเด็มส่วนกลาง ใช้ โมเด็มชนิด call-back ใช้การเข้ารหัสข้อมูล
สถานีงาน	ใช้รหัสผ่านจากสถานีงานอื่นๆ เข้ามาใช้สถานีงานโดยพละการ	จำกัดการเข้าใช้สถานีงาน ใช้เคเบิลใยแก้ว เข้ารหัสและกำหนดอายุรหัสผ่าน
แผ่นดิสก์	ขโมยข้อมูลจำนวนมาก ระบบปฏิบัติการและซอฟต์แวร์	ควบคุมการเข้าถึงโดยตัวบุคคล
ไฟล์เซอร์เวอร์ของเครือข่าย	ขโมย หรือ ทำลายเครื่อง เข้าใช้งานโดยไม่ได้รับอนุญาต แก้ไขระบบทำให้เกิดความเสียหาย	ควบคุมการเข้าถึงโดยบุคคล
เราเตอร์ บริดจ์ อุปกรณ์เชื่อมโยงอื่นๆ	แก้ไขส่วนประกอบของระบบ ทำให้เกิดความเสียหาย	ใช้รหัสผ่าน

ตารางที่ 4.1 แสดงการรักษาความปลอดภัยขององค์ประกอบในเครือข่าย

9.3 การป้องกันระบบเครือข่ายจากไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์เป็นการจำลองตัวเองให้เป็นรหัสส่วนหนึ่งที่ซ่อนอยู่ในโปรแกรมของเครื่องคอมพิวเตอร์หรืออยู่ในหน่วยความจำ หลังจากนั้นจะเกาะไปยังโปรแกรมอื่นหรือติดไปตามโปรแกรมที่ถูกคัดลอกไปยังแผ่นบันทึกข้อมูลหรือระบบเครือข่าย ซึ่งทำให้ไวรัสกระจายไปทั่วเครือข่ายได้ วิธีที่ใช้ป้องกันได้คือใช้โปแกรมที่ทำหน้าที่ตรวจสอบไวรัสและกำจัดไวรัสถ้าพบว่ามีอยู่ในเครือข่าย บนระบบเครือข่ายส่วนใหญ่ผู้จัดการระบบเครือข่ายจะเป็นผู้ทำหน้าที่ในการติดตั้งโปรแกรมต่างๆเข้าสู่ระบบ ดังนั้นก่อนทำการติดตั้งโปรแกรมใดๆ ควรจะต้องตรวจสอบไวรัสคอมพิวเตอร์เสียก่อน และจะต้องออกข้อกำหนดห้ามผู้ใช้งานระบบเครือข่ายนำโปรแกรมใดๆเข้าสู่ระบบโดยไม่ได้ผ่านผู้จัดการระบบ

จากหลักการดังกล่าวจึงได้ออกแบบให้การรักษาความปลอดภัยในเครือข่ายคอมพิวเตอร์ของกรมตำรวจมีลักษณะดังนี้

1. กำหนดสิทธิการใช้งานเครือข่ายดังต่อไปนี้

ระดับที่ 1 ไม่อนุญาตให้เข้ามาใช้เครือข่าย

ระดับที่ 2 สามารถเข้าถึงข้อมูลที่เปิดเผยต่อตำรวจทั่วไปได้ เช่น หมายจับ เป็นต้น และสามารถใช้จดหมายอิเล็คโทรนิคเพื่อการสื่อสารได้

ระดับที่ 3 รวมสิทธิในระดับที่ 2 และสามารถใช้บริการต่างๆที่จัดไว้ให้และสามารถเข้าถึงข้อมูลบริหารระดับปฏิบัติการ

ระดับที่ 4 รวมสิทธิในระดับที่ 3 และ สามารถเข้าถึงข้อมูลสำหรับผู้บริหารระดับสูงได้

ระดับที่ 5 มีสิทธิตามระดับที่ 3 และ มีสิทธิในการจัดการเครือข่ายและทรัพยากรของระบบ

ระดับที่ 6 มีสิทธิตามระดับที่ 4 และ มีสิทธิในการจัดการเครือข่ายและทรัพยากรของระบบ

ระดับที่ 7 มีสิทธิตามระดับที่ 4 และ มีสิทธิในการจัดการเครือข่ายและทรัพยากรของระบบได้สูงสุด

2. สำหรับผู้ที่สามารถเข้าใช้ระบบเครือข่ายได้นั้นสามารถแบ่งออกเป็นระดับต่างๆได้ดังนี้

ระดับที่ 1 อธิบดีกรมตำรวจ

ระดับที่ 2 ผู้ช่วยอธิบดีกรมตำรวจ หัวหน้าภาค ผู้บัญชาการ ผู้บังคับการ

ระดับที่ 3 ผู้กำกับหรือรองผู้กำกับ หัวหน้าสถานีตำรวจ (สน. และ สภ.อ.)
ระดับที่ 4 ผู้ปฏิบัติการเครือข่าย (เป็นเจ้าหน้าที่ที่หัวหน้าหน่วยงานเป็นผู้แต่งตั้ง)
ระดับที่ 5 ผู้บริหารเครือข่าย (อธิบดีกรมตำรวจเป็นผู้แต่งตั้ง)
ระดับที่ 6 เจ้าหน้าที่ตำรวจทั่วไป

3. กำหนดสิทธิให้กับเจ้าหน้าที่ตำรวจระดับต่างๆดังนี้

ระดับของเจ้าหน้าที่ตำรวจ	สิทธิที่ได้รับ
1	3 และ 4
2	3 และ 4
3	3 และ 4
4	4 และ 5
5	6 หรือ 7
6	2 เท่านั้น

ตารางที่ 4.2 แสดงการกำหนดสิทธิให้กับเจ้าหน้าที่ระดับต่างๆ

ในปีพ.ศ. 2528 รัฐบาลสหรัฐอเมริกาได้จัดพิมพ์หนังสื่อที่เรียกว่า Trusted Computer Security Evaluation Criteria (หรือรู้จักกันในชื่อว่าหนังสือปกสีส้ม) ในหนังสือนี้กล่าวถึงขอบข่ายของระบบที่ปลอดภัยและการจัดระดับความปลอดภัยของระบบ ซึ่งต้องใช้วิธีการเฉพาะในการตรวจสอบระบบที่จะนำมาจัดระดับของการรักษาความปลอดภัย และได้กำหนดระดับของการรักษาความปลอดภัยไว้ตั้งแต่ระดับ D คือระบบที่ไม่มีการรักษาความปลอดภัยเลย จนถึงระดับ A1 ที่เป็นระบบที่มีระเบียบวิธีสำหรับการตรวจสอบความปลอดภัย ต่อมาจึงได้มีการวิจัยและพัฒนาระบบที่มีความยืดหยุ่นมากขึ้น ซึ่งกลไกรักษาความปลอดภัยที่พัฒนาขึ้นนี้เรียกว่า Type Enforcement Security Model

โมเดลรักษาความปลอดภัยนี้เป็นกลไกในการรักษาความปลอดภัยที่กำหนดให้ทุกโปรแกรมในระบบ ทำงานเฉพาะสิ่งที่โปรแกรมนั้นๆถูกกำหนดให้ทำเท่านั้นเรียกว่า สิทธิขั้นต่ำ

(Least privilege) การกำหนดเช่นนี้จะใช้กับโปรแกรมประยุกต์ แฟ้มข้อมูล และระบบปฏิบัติการด้วยโดย Type Enforcement มีหลักการทำงานโดยการจัดกระบวนการ (process) หลายๆกระบวนการเข้าด้วยกันเป็นหมวด โดยแต่ละหมวดจะเรียกว่า โดเมน (Domain) และในลักษณะเดียวกันแฟ้มข้อมูลต่างๆในระบบก็จะถูกจัดเป็นหมวดโดยแต่ละหมวด จะเรียกว่า ไทพ์ (Type) ซึ่งทั้งโดเมนและไทพ์จะทำงานตามที่ถูกกำหนดไว้ในตารางกำหนดลักษณะของโดเมน ซึ่งเป็นตารางที่กำหนดสิทธิของโดเมน (Domain Definition table) ในการติดต่อเข้าถึงไทพ์ โดยที่ตารางนี้จะไม่สามารถเปลี่ยนแปลงในขณะที่ระบบกำลังทำงานอยู่ได้ ตัวอย่างการทำงานโดยการกำหนดสิทธิในตารางนี้ เช่น ระบบฐานข้อมูลสามารถที่จะติดต่อได้เฉพาะกับ แฟ้มฐานข้อมูลเท่านั้น โปรแกรมประยุกต์ทางด้านบรรณาธิกร ก็จะติดต่อได้เฉพาะกับแฟ้มของผู้ใช้เท่านั้น สำหรับงานที่เป็นเครือข่ายอินเตอร์เน็ตนั้น สามารถทำการอ่านแฟ้มข้อมูลของผู้ใช้ได้แต่ไม่สามารถแก้ไขได้ และยังเป็นโดเมนเดียวที่สามารถติดต่อเข้าสู่ระบบเครือข่ายได้ นอกจากตารางกำหนดสิทธิแล้วยังมีตารางที่ทำหน้าที่ควบคุมการติดต่อระหว่างโดเมนกับโดเมนอีกด้วย แฟ้มที่เป็นเอ็กซิคิวเทเบิล (executable) หรือโปรแกรมต่างๆนั้น จะถูกควบคุมการใช้งานอย่างเข้มงวด มีการกำหนดว่า โปรแกรมใดสามารถทำงานได้ในโดเมนใดบ้าง ต้องเป็นผู้ที่สามารถแก้ไขโปรแกรมนั้นได้ ดังนั้นโปรแกรมไวรัสหรือม้าโทรจันจึงไม่สามารถทำงานได้ นอกจากนี้ดาต้าโฟลหรือการไหลของข้อมูลไปมาในระบบจะถูกกำหนดเส้นทางโดยโมเดลนี้เพื่อจัดระเบียบการไหลเวียนของข้อมูลระหว่างโปรแกรม

เนื่องจากการแยกโปรแกรมประยุกต์อาจจะไม่เพียงพอต่อการรับประกันความปลอดภัยของระบบ ดังนั้นต้องมีการควบคุมว่าข่าวสารผ่านไปมาในระบบได้อย่างไร โมเดลนี้ได้มีการสร้างไปพ์ไลน์ (pipeline) เพื่อจัดรูปแบบการไหลเวียนของข้อมูลในระบบ เพื่อรับประกันได้ว่าข้อมูลที่ไหลเวียนในระบบมีความปลอดภัย โมเดล ไทพ์เอ็นฟอร์ซเมนต์ (Type Enforcement) จะควบคุมข้อมูลที่โปรแกรมต่างๆจะทำการอ่านหรือบันทึก นอกจากนี้ยังมีการแบ่งโปรแกรมออกเป็นส่วนย่อยๆเพื่อเป็นการง่ายต่อการวิเคราะห์และมั่นใจได้ว่าแต่ละส่วนย่อยนั้นทำงานได้ถูกต้องตามปกติ ซึ่งเป็นการเพิ่มความปลอดภัยและความมั่นคงให้กับระบบอีกด้วย

ในปัจจุบัน โมเดล ไทพ์เอ็นฟอร์ซเมนต์ ได้พัฒนาเข้ากับ ไฟร์วอลล์ เพื่อสร้างความยืดหยุ่นระหว่างเครือข่ายที่เป็นอิสระต่อกัน การเป็นอิสระต่อกันระหว่างอินเตอร์เน็ตและเครือข่ายภายในของหน่วยงานเป็นสิ่งสำคัญอย่างยิ่งโดยเฉพาะกับเครือข่ายของกรมตำรวจ และเนื่องจากไฟร์วอลล์เป็นระบบป้องกันการเข้าถึงอินเตอร์เน็ตเวอร์คอาจมีการนำโมเดลไทพ์เอ็นฟอร์ซเมนต์เข้ามาทำงานร่วมกันกับไฟร์วอลล์ซึ่งเป็นไปได้เนื่องจากโมเดลนี้มีความยืดหยุ่นเพียงพอ สำหรับไฟร์วอลล์นั้น จะแยกเครือข่ายภายในกับภายนอกโดยอยู่บนเครื่องเดียวกันนั่นคือ ไฟร์วอลล์เก็บข้อมูลข่าวสารแยกออกมาจนกว่าจะผ่านการตรวจสอบว่าข้อมูลนั้นได้รับอนุญาตผ่านออกไปหรือ

ไม่ โมเดลไทพ์เอ็นฟอร์ซเมนต์ทำงานร่วมกับไฟร์วอลล์ด้วยเน็ตเวอร์คการ์ดสองตัว ซึ่งสามารถบอกได้ว่าข้อมูลเหล่านั้นมาจากที่ใด เครือข่ายสองระบบจะเชื่อมต่อเข้ากับโปแกรมแยกโดเมนของเครือข่าย ดังนั้นจึงเป็นการป้องกันการถูกหลอกโดยโปรโตคอลของเครือข่ายได้ด้วย

การใช้โมเดลไทพ์เอ็นฟอร์ซเมนต์และการแยกข้อมูลตามความสำคัญนั้นนอกจากจะมีผลโดยตรงกับข้อมูลแล้วยังช่วยในการควบคุมการเข้าไปใช้ทรัพยากรทางการสื่อสารอย่างมีประสิทธิภาพด้วยและยังรับประกันซอฟต์แวร์ที่มีหน้าที่ในการจัดสรรทรัพยากรให้ทำงานอย่างถูกต้องอีกด้วย ตัวอย่างระบบรักษาความปลอดภัยสำหรับระบบเครือข่ายที่น่าสนใจคือระบบไฟร์วอลล์-1

Firewall-1 หรือ ไฟร์วอลล์-1 เป็นระบบที่ทำหน้าที่เป็นทั้งเกตเวย์และตัวกรองแพกเก็ตสำหรับใช้งานในด้านการรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ ซึ่งไฟร์วอลล์-1นั้นเป็นระบบรักษาความปลอดภัยที่รู้จักกันอย่างแพร่หลายและยังสามารถกำหนดวัตุประสงค์ในการป้องกันเครือข่ายได้สะดวกและไม่ยากนัก ไม่ว่าจะเป็นเครือข่ายของผู้ให้บริการระบบเครือข่ายเอง เครือข่ายเฉพาะหน่วยงาน เครือข่ายที่มีเครื่องที่เป็นโฮสต์และเครื่องที่เป็นตัวให้บริการตัวเดียวกลุ่มของโฮสต์ ที่ต้องการปกป้องระบบเครือข่ายจากผู้ที่ไม่ได้รับอนุญาตให้เข้ามาใช้งานเครือข่ายทั้งจากภายนอกและภายในระบบ เนื่องจากไฟร์วอลล์ทำงานอยู่ที่ระหว่างระดับชั้นดาต้าลิ้งกับระดับชั้นเน็ตเวอร์ค จึงรองรับอินเตอร์เน็ตแพกเก็ตที่รูปแบบต่างๆของโปรแกรมประยุกต์เกือบทุกชนิดได้ และยังอนุญาตให้ผู้ใช้งานกำหนดหรือเพิ่มเติมบริการต่างๆได้อย่างง่ายๆ ข้อแตกต่างที่เด่นชัดของไฟร์วอลล์จากเทคโนโลยีการกรองแพกเก็ตทั่วไปคือกระบวนการตัดสินใจที่อยู่บนพื้นฐานของเนื้อหาของสารสนเทศและเนื้อหาของแพกเก็ต ด้วยคุณสมบัติเฉพาะตัวที่ฉลาดเหล่านี้จึงทำให้ไฟร์วอลล์เป็นระบบที่มีประสิทธิภาพและดูแลความปลอดภัยให้กับระบบเครือข่ายได้เป็นอย่างดี

10. การพัฒนาบุคลากรของกรมตำรวจ

แนวทางการพัฒนาบุคลากรของกรมตำรวจมีดังนี้

บุคลากรในกรมตำรวจที่เกี่ยวข้องกับการใช้งานเครือข่ายควรแบ่งตามหน้าที่ได้ดังต่อไปนี้

10.1 ผู้ใช้ระบบทั่วไป ได้แก่

10.1.1 เจ้าหน้าที่ระดับบริหารในกรมตำรวจ ได้แก่ อธิบดีกรมตำรวจ รองอธิบดีกรมตำรวจ ผู้ช่วยอธิบดีกรมตำรวจ และ นายเวรทุกนาย

10.1.2 เจ้าหน้าที่ระดับบริหารในตำรวจภูธรภาค ได้แก่ ผู้ช่วยอธิบดีกรมตำรวจ หัวหน้าภาค ผู้บัญชาการ (ระดับรองหัวหน้าภาค) รองผู้บัญชาการ (ระดับรองหัวหน้าภาค) ผู้

ช่วยผู้บัญชาการ (ระดับผู้ช่วยหัวหน้าภาค) และนายเวรทุกนาย ผู้บังคับการอำนวยการและนายเวรทุกนาย ผู้กำกับการข่าว รวมทั้งสารวัตรสถิติ

10.1.3 เจ้าหน้าที่ระดับบริหารในกองบัญชาการ ได้แก่ ผู้บัญชาการ รองผู้บัญชาการ ผู้ช่วยผู้บัญชาการ ผู้บังคับการในกองบัญชาการทุกนาย ผู้กำกับการข่าว และสารวัตรสถิติ

10.1.4 เจ้าหน้าที่ระดับบริหารในกองบังคับการ ได้แก่ ผู้บังคับการศูนย์ข้อมูลข้อสนเทศ ผู้บังคับการกองทะเบียน ผู้บังคับการกองทะเบียนประวัติอาชญากร ผู้บังคับการกองบังคับการตำรวจจราจร ผู้บังคับการกองพิสูจน์หลักฐาน รวมทั้งรองผู้บังคับการและนายเวรทุกนายด้วย

10.1.5 เจ้าหน้าที่ระดับบริหารในสถานีตำรวจทุกนาย

โดยเจ้าหน้าที่ระดับบริหารเหล่านี้ ควรได้รับการฝึกอบรมการใช้งานคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ในระดับที่จะทำให้สามารถใช้งานระบบได้โดยไม่เกิดความรู้สึกว่าระบบคอมพิวเตอร์เป็นเรื่องยากเกินไป และสิ่งสำคัญสำหรับการอบรมเจ้าหน้าที่ระดับบริหารระดับสูงของกรมตำรวจก็คือจะต้องสามารถทำให้เจ้าหน้าที่เหล่านี้เข้าใจการทำงานและประโยชน์ของระบบคอมพิวเตอร์ซึ่งจะช่วยงานอะไรได้บ้าง

10.2 เจ้าหน้าที่ปฏิบัติงานระบบ

เจ้าหน้าที่หรือบุคคลที่ได้รับมอบหมายให้ทำการใช้งานเครือข่าย หรือ โอเปอร์เรเตอร์ ทำหน้าที่ป้อนข้อมูล บันทึกข้อมูล หรือถ่ายโอนข้อมูล ซึ่งจะต้องประจำอยู่ที่สถานีตำรวจทุกแห่งหรือเป็นเจ้าหน้าที่ตำรวจในสถานีตำรวจนั้นๆ ควรจะได้รับการฝึกอบรมการใช้งานระบบเครือข่ายและระบบคอมพิวเตอร์ให้อยู่ในขั้นที่สามารถใช้งานได้อย่างคล่องแคล่ว และสามารถแก้ปัญหาเฉพาะหน้าได้บ้างหรืออย่างน้อยที่สุดสามารถที่จะทราบว่าจะต้องติดต่อประสานงานกับใครเมื่อระบบมีปัญหาเกิดขึ้น

10.3 ผู้จัดการระบบ

เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่ในการจัดการระบบเครือข่ายและระบบคอมพิวเตอร์ บุคคลเหล่านี้จะต้องได้รับการฝึกอบรมให้สามารถจัดการเกี่ยวกับทรัพยากรต่างๆในระบบเครือข่ายได้เป็นอย่างดี เช่นการดูแลและบริหารระบบเครือข่าย งาน

บริหารระบบฐานข้อมูล งานติดตั้งซอฟต์แวร์ งานสำรองข้อมูล เป็นต้น ดังนั้นเจ้าหน้าที่เหล่านี้จะต้องได้รับการฝึกอบรมเกี่ยวกับการจัดการเรื่องดังกล่าวอย่างดี

10.4 เจ้าหน้าที่สนับสนุนระบบงาน

เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่คอยให้การสนับสนุนทางด้านเทคนิคแก่ผู้ใช้ทั่วไป รวมทั้งให้ความรู้ความเข้าใจและให้คำปรึกษาแก่ผู้ใช้ทุกคน ดังนั้นเจ้าหน้าที่ในส่วนนี้จึงควรที่จะได้รับการฝึกอบรมเกี่ยวกับเทคโนโลยีที่เกี่ยวข้องเป็นอย่างดี เนื่องจากจะต้องใช้บุคลากรค่อนข้างมากในส่วนนี้จึงควรจัดตั้งเป็นหน่วยงานเฉพาะหรือทีมงานสำหรับดูแลรับผิดชอบและแบ่งหน้าที่อย่างชัดเจนว่ากลุ่มใดดูแลสนับสนุนงานด้านใด จะทำให้การสนับสนุนทางด้านเทคนิคเป็นไปอย่างมีประสิทธิภาพ