ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

การเพิ่มประสิทธิภาพของระบบเครือข่าย โดยการทำเรพลิเคชั่นเครื่องไดเร็คทอรี่เซิฟเวอร์

Increasing Network Performance by Using Replication on Directory Server

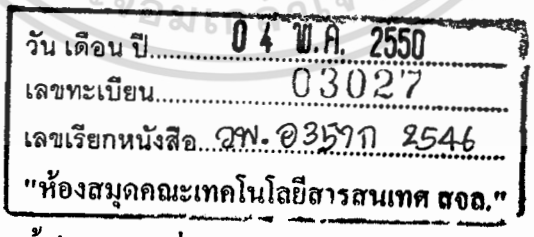
โดย

นายอรรถพล มุกดาประวัติ

รหัส 44067641

อาจารย์ที่ปรึกษา

ดร. ธนารัตน์ ชลิดาพงศ์



รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ

หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 1 ปีการศึกษา 2546

คณะเทคโนโลยีสารสนเทศ

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ชื่อหัวข้อเรื่อง	การเพิ่มประสิทธิภาพของระบบเครือข่ายโดยการทำเรพลิเคชั่นเครื่องไดเร็คทอรี่เซิฟเวอร์
นักศึกษา	นายอรรถพล มุกดาประวัติ
อาจารย์ที่ปรึกษา	ดร. ธนารัตน์ ชลิดาพงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2546

บทคัดย่อ

โครงการศึกษากรณีพิเศษนี้ เป็นการศึกษาถึงกระบวนการเรพลิเคชั่นของไดเร็คทอรี่เซอร์วิส เพื่อเพิ่มประสิทธิภาพให้กับระบบเครือข่าย และลดความเสี่ยงซึ่งอาจเกิดจากไดเร็คทอรี่เซิฟเวอร์หลักไม่สามารถให้บริการได้ตามปกติ ทำให้ผู้ใช้ระบบเครือข่ายไม่สามารถขอใช้บริการหรือทรัพยากรในระบบเครือข่ายได้ นอกจากนี้ในการเลือกใช้ไดเร็คทอรี่เซอร์วิสนั้น ควรจะมีการพิจารณาถึงประสิทธิภาพการทำงานของไดเร็คทอรี่เซอร์วิส และองค์ประกอบต่าง ๆ เช่น รูปแบบการทำงานของไดเร็คทอรี่เซอร์เวอร์, รูปแบบการเรพลิเคชั่น, เครื่องมือในการพัฒนาแอพพลิเคชั่นสำหรับไดเร็คทอรี่เซอร์วิส เป็นต้น เพื่อให้ได้ไดเร็คทอรี่เซอร์วิสที่ดีเหมาะสมกับองค์กรมากที่สุด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Title	Increasing Network Performance by Using Replication on Directory Server
Student	Mr. Attapon Mukdaprawat
Advisor	Dr. Thanarat Chalidabhongse
Level Of Study	Master of Science in Information Technology
Major	Information Technology Management
Academic Year	2003

ABSTRACT

This special study project is a study on methodologies of replication for directory service. We found the replication can increase network efficiency and decrease the risk that failing master directory server cannot serve the users. In addition, this report also illustrates the comparison results of various directory services and replications models. This could be useful for choosing directory service vendor for organization. Network administrator usually consider performance and other components such as directory server architecture, replication model, and tools used in developing applications using directory services.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

กิตติกรรมประกาศ

ความสำเร็จของโครงการศึกษาฉบับนี้มีผู้เกี่ยวข้อง และสนับสนุนจากหลายท่าน ได้แก่ คุณศักดิ์ชัย ลัดนทิน ซึ่งให้การสนับสนุนอุปกรณ์เครื่องคอมพิวเตอร์ในการทดสอบ คุณธิดารัตน์ ลิ้มโยธิน ให้การสนับสนุนทางด้านอุปกรณ์เครือข่าย (Network Card) อีกทั้งเพื่อน ๆ ITM 10 ที่ให้ความสนับสนุนในแนวความคิดต่าง ๆ นอกจากนั้นพี่ ๆ ที่ธนาคารออมสินทุกท่าน ซึ่งมีหน้าที่ดูแลและจัดการการบริหารระบบเครือข่ายให้กับธนาคารก็ได้ให้คำแนะนำต่าง ๆที่เป็นประโยชน์อย่างยิ่ง

นอกจากนี้แล้ว บุคคลที่มีส่วนสำคัญที่ช่วยให้โครงการศึกษาฉบับนี้สามารถเป็นไป ก็คือ อาจารย์ ดร. ธนารัตน์ ชลิดาพงศ์ ซึ่งเป็นอาจารย์ที่ปรึกษาโครงการศึกษากรณีพิเศษ ซึ่งท่านได้ให้ความแนะนำ ปรึกษาและเสนอข้อคิดเห็นต่าง ๆ เป็นแนวทางในการศึกษา และดำเนินการให้เป็นไปอย่างต่อเนื่อง และสำเร็จลุล่วงไปด้วยดี และสุดท้ายขอขอบคุณ คุณแม่ และพี่น้องทางบ้านที่ให้การสนับสนุนให้ข้าพเจ้าได้มีโอกาสศึกษาต่อในระดับนี้

อรรถพล มุกดาประวัติ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ

หน้า

บทคัดย่อภาษาไทย I
บทคัดย่อภาษาอังกฤษ II
กิตติกรรมประกาศ III
สารบัญ IV
สารบัญตาราง VII
สารบัญภาพ VIII
บทที่ 1 1
บทนำ 1
1.1 หลักการและเหตุผล 1
1.2 วัตถุประสงค์ 1
1.3 ขอบเขตการดำเนินงาน 2
1.4 ขั้นตอนการดำเนินงาน 2
1.5 ประโยชน์ที่จะได้รับ 3
บทที่ 2 4
การเรพลิเคชั่น (REPLICATION) 4
2.1 ลักษณะทั่วไป 4
2.2 Replication Approach 6
2.2.1 Gossip Approach 6
2.2.2 Process Group Approach 7
2.3. ความสอดคล้องของข้อมูล และการจัดลำดับการประมวล 9
2.3.1 Request Ordering 9
2.3.2 Implementing request ordering 10
2.3.3 Implementing total ordering 10
บทที่ 3 12
ไดเร็คทอรี่เซอร์วิส (DIRECTORY SERVICE) 12
3.1 ไดเร็คทอรี่เซอร์วิส 12

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

3.1.1 ลักษณะโดยทั่วไป 12
3.1.2 พื้นฐานของไดเร็คทอรี่เซอร์วิส 13
3.1.3 บทบาท และหน้าที่ของไดเร็คทอรี่เซอร์วิส 13
3.2 โพรโตคอล LDAP (Light weight Directory Access Protocol) 16
3.2.1 ลักษณะโดยทั่วไป 16
3.2.2 ลักษณะการทำงานของโพรโตคอล LDAP 17
3.2.3 Operation ใน LDAP protocol 18
3.2.4 โครงสร้าง และสถาปัตยกรรม LDAP 19
3.2.5 LDIF (Light weight Data Interchange Format) 24
3.2.6 LDAP APIs (LDAP Application Programming Interface) 24
3.3 สกีมา (Schema) 25
3.3.1 ความหมายของสกีมา 25
3.3.2 องค์ประกอบของสกีมา 25
3.3.3 รูปแบบสกีมา ที่เป็นที่นิยมจะมีอยู่ 3 รูปแบบ คือ 25
3.3.4 กระบวนการตรวจสอบสกีมา (Schema Checking Process) 26
3.3.5 มาตรฐานสกีมา 26
3.4 รูปแบบของการ Replication ไดเร็คทอรี่เซอร์วิส 26
3.4.1 ความหมาย 26
3.4.2 แนวความคิดของการเรพลิเคชั่น 26
3.4.3 รูปแบบของการเรพลิเคชั่น ในแบบต่าง ๆ (Replication model) 27
บทที่ 4 30
การวิเคราะห์ประสิทธิภาพของไดเร็คทอรี่เซิฟเวอร์ 30
4.1. การวิเคราะห์รูปแบบการเรพลิเคชั่น (Analysis and Compare Replica Model) 30
4.1.1 eDirectory 30
4.1.2 Active Directory 34
4.1.3 Netscape 37
4.2. การเปรียบเทียบประสิทธิภาพของ Directory Service 38
4.2.1 การทดสอบ 38

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญ (ต่อ)

4.2.2 สรุปผลการทดสอบ 40
4.3 การทดสอบถึงประสิทธิภาพของระบบเครือข่าย จากการใช้เทคนิค Replication 40
บทที่ 5 45
สรุปผลการศึกษาและข้อเสนอแนะ 45
5.1 สรุปผลการดำเนินงาน 45
5.2 ข้อเสนอแนะ.....45
บรรณานุกรรม.....46
ภาคผนวก 47
ประวัติผู้เขียน 55

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญตาราง

หน้า

ตารางที่

4.1 คุณสมบัติ และลักษณะของเครื่อง Server และ Client ที่ใช้ในการทดสอบ 38
4.2 การ Loading – Initial Directory 38
4.3 ผลจากการทดสองการส่ง Messaging 39
4.4 ผลจากการทดสอบการทำ Address look-up 39
4.5 ผลจากการทดสอบการ Authentication 39

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ

หน้า

ภาพที่

2.1 Gossip Approach (Master Replica 7
2.2 Multi – user editor 7
2.3 Process Group ลักษณะของ client- 8
2.4 Hierarchical group 8
2.5 Ordering the requests arriving 10
3.1 Central Directory Server 14
3.2 Distribute Directory Server 14
3.3 Supplier and Consumer replica 15
3.4 Directory Information Tree (DIT) 15
3.5 LDAP client retrieves a single entry from LDAP server 17
3.6 ลักษณะโครงสร้างข้อมูลใน Directory 19
3.7 DIT และ Entry Structure 20
3.8 Directory Tree Structure 21
3.9 ตัวอย่างของ Namespace 21
3.10 แสดงรูปแบบของ Single-Master Replication 27
3.11 แสดงขั้นตอนในการทำงาน Floating-Master Replication 28
3.12 แสดงขั้นตอนในการทำงาน Multi-Master Replication 28
3.13 แสดงขั้นตอนในการทำงาน Hub-Master Replication 29
4.1 Master Replica 31
4.2 Read/Write Replica 32
4.3 Subordinate Replica 33
4.4 แสดงความสัมพันธ์ภายใน Domain และการเชื่อมต่อที่เรียกว่า forest 34
4.5 Domain Tree 35
4.6 การเชื่อมหลาย ๆ Domain และ Global Catalog Server 35
4.7 กระบวนการ replication ใน Active Directory 36
4.8 กราฟแสดงผลจากการทดสอบประสิทธิภาพของ Directory Server 40
4.9 แสดงรูปแบบของการเชื่อมต่อคอมพิวเตอร์ที่ใช้ในการทดสอบแบบที่ 1 40

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สารบัญภาพ (ต่อ)

4.10 แสดงรูปแบบของการเชื่อมต่อคอมพิวเตอร์ที่ใช้ในการทดสอบแบบที่ 2 41
4.11 แสดงรูปแบบของการเชื่อมต่อคอมพิวเตอร์ที่ใช้ในการทดสอบแบบที่ 3 42
4.12 ผลสรุปการทดลองทั้ง 3 กรณี 43

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 1
บทนำ

1.1 หลักการและเหตุผล

ปัจจุบันเทคโนโลยีได้มีการเปลี่ยนแปลงไปอย่างรวดเร็ว การค้นหาข้อมูลสารสนเทศสามารถทำได้หลายวิธี ไม่ว่าจะเป็นการค้นหาในอินเตอร์เน็ต รวมถึงการค้นหาข้อมูลภายในองค์กร เช่น การค้นหา ชื่อพนักงาน, ที่อยู่ หรืออีเมล์แอดเดส ถ้ามีการจัดเก็บข้อมูลไว้หลายที่ ก็จะทำให้ยากต่อการค้นหา และบำรุงรักษาข้อมูลนั้น รวมถึงการปรับปรุงข้อมูลให้มีความทันสมัยอยู่ตลอดเวลา และสิ่งที่สำคัญ คือ การถูกต้อง และความสอดคล้องกันของข้อมูล หากมีการเปลี่ยนแปลงข้อมูล ข้อมูลดังกล่าวไม่ว่าจะเป็นที่ใดก็ตาม ควรที่จะต้องมีการเปลี่ยนแปลงให้ถูกต้อง เพราะอาจทำให้ผู้ใช้ข้อมูลเกิดความเข้าใจผิด

การจัดเก็บข้อมูลรวมทั้งสารสนเทศไว้ในที่ ๆ เดียวกันทำให้ง่ายต้องการปรับปรุงแก้ไข ช่วยให้ผู้ใช้ได้รับข้อมูลที่ถูกต้องตรงกับความเป็นจริง ลักษณะการจัดเก็บข้อมูลดังกล่าวคือการเก็บข้อมูลแบบฐานข้อมูล การจัดเก็บดังกล่าวช่วยให้ข้อมูลมีความถูกต้อง และสอดคล้องกัน และสะดวกต่อการเรียกใช้งานของผู้ใช้ รวมถึงการบำรุงรักษาและจัดเก็บก็มีประสิทธิภาพ และประโยชน์จากการเชื่อมโยงกันก็นำมาสู่การใช้ข้อมูลร่วมกันได้ ลดปัญหาการจัดเก็บข้อมูลที่ซ้ำซ้อน และลดความผิดพลาดจากข้อมูลไม่สอดคล้องกันอีกด้วย

ไดเร็คทอรี่เซอร์วิสเป็นบริการที่ให้บริการด้านข้อมูลที่เกี่ยวกับบุคคล และทรัพยากรต่าง ๆ สำหรับการร้องขอจากไคล์เอ็นท์ (Client) ซึ่งข้อมูลจะถูกจัดเก็บในรูปแบบของ object ทำให้ผู้บริหารระบบเครือข่าย (System Administrator) มีความสะดวกในการบริหารจัดการ ไม่ว่าจะเป็นการจัดการเกี่ยวกับระบบรักษาความปลอดภัย มีการตรวจสอบสิทธิการใช้งานของผู้ใช้ทรัพยากรของระบบเครือข่ายฯ ก่อนที่จะมีการอนุญาตให้ใช้งานผู้ใช้มีความสะดวกในการใช้งานทรัพยากรต่าง ๆ โดยการล็อคอินเพียงครั้งเดียว ก็สามารถใช้งานระบบต่าง ๆ หรือแอพพลิเคชั่นต่าง ๆ ตามสิทธิที่ระบุไว้ตามที่ได้มีการออกแบบไว้ตั้งแต่แรก

1.2 วัตถุประสงค์

1. เพื่อให้การบริหารจัดการระบบเครือข่ายมีความสะดวก และมีประสิทธิภาพมากขึ้น เช่น การกำหนดสิทธิการใช้งานทรัพยากรต่าง ๆ รวมถึงการกำหนดเวลาการทำงานของผู้ใช้ในระบบเครือข่าย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. เพิ่มความสะดวกในการจัดเก็บบัญชีรายชื่อพนักงานในองค์กร หรือการกำหนดสิทธิการใช้ทรัพยากรอย่างเหมาะสม
3. เพิ่มความสะดวกให้แก่ผู้ใช้งานทรัพยากรต่าง ๆ ในระบบเครือข่าย จากการที่ผู้ใช้สามารถล็อกอินเข้าสู่ระบบเพียงครั้งแรกครั้งเดียว ก็สามารถที่จะใช้งานระบบต่าง ๆ หรือทรัพยากรต่าง ๆ ได้ทั้งหมด (ขึ้นอยู่กับสิทธิการใช้งานที่ได้กำหนดไว้)
4. เพิ่มความสะดวกจัดการระบบรักษาความปลอดภัย เนื่องจากมีการกำหนด และควบคุมจากไดเร็คทอรี่เซอร์วิสเพียงที่เดียว
5. ผู้บริหารระบบฯ (System Administrator) สามารถนำการออกแบบต่าง ๆ ไม่ว่าจะเป็นการออกแบบสกีมา (Schema) การออกแบบการเรพลิเคชั่น (Replication Schema) และการออกแบบโครงสร้างข้อมูล หรือข้อมูลที่จัดเก็บในไดเร็คทอรี่ (Data Schema) ไปปรับใช้ร่วมกับไดเร็คทอรี่อื่นที่มีลักษณะใกล้เคียงกัน โดยผู้บริหารฯ ไม่จำเป็นจะต้องมีการออกแบบใหม่ทั้งหมด ซึ่งทำให้ประหยัดเวลาได้มาก เพราะสกีมาดังกล่าวมีลักษณะการออกแบบที่เป็นมาตรฐาน
6. ลดความซ้ำซ้อนในการจัดเก็บข้อมูล เพื่อประหยัดการใช้ทรัพยากรคอมพิวเตอร์ และลดปัญหาจากการที่ข้อมูลที่จัดเก็บไม่สอดคล้องกัน ซึ่งนำไปสู่การทำงานที่ผิดพลาดอันเนื่องจากข้อมูลมีความล้าสมัย เพราะไม่ได้ทำการปรับปรุงอย่างเหมาะสม
7. ช่วยให้การบริหารจัดการข้อมูล เป็นไปอย่างมีประสิทธิภาพมากขึ้น เนื่องจากมีการเรพพลิเคชั่นของไดเร็คทอรี่เซอร์วิส ซึ่งช่วยให้สามารถบริการได้อย่างต่อเนื่อง พร้อมทั้งลดปริมาณข้อมูลที่จะเข้าใช้บริการไดเร็คทอรี่เซอร์วิสซึ่งมีเพียงแห่งเดียวในระบบเครือข่าย
8. การนำกระบวนการเรพลิเคชั่นมาใช้กับไดเร็คทอรี่เซอร์ สามารถช่วยเพิ่มประสิทธิภาพให้กับระบบเครือข่ายให้มีการทำงานรวดเร็ว และสามารถให้บริการได้อย่างต่อเนื่อง

1.3 ขอบเขตการดำเนินงาน

เอกสารวิชาโครงการศึกษากรณีพิเศษฉบับนี้ ผู้ศึกษาได้ศึกษา และอธิบายถึงหลักการทำงานของไดเร็คทอรี่เซอร์วิส และมาตรฐานที่ใช้ในการรับส่งข้อมูลที่ระหว่าง Directory Server กับ Directory Client ซึ่งเรียกว่า LDAP (Light weight Directory Access Protocol)

นอกจากนั้นทางผู้ศึกษาได้ทำการศึกษาเกี่ยวกับการทำงานของเรพพลิเคชั่น ซึ่งสามารถนำมาใช้ร่วมกับไดเร็คทอรี่เซอร์เวอร์ เพื่อเพิ่มประสิทธิภาพในการทำงานให้ดีขึ้น

1.4 ขั้นตอนการดำเนินงาน

ศึกษาประโยชน์ของการนำไดเร็คทอรี่เซอร์วิสมาใช้ในระบบเครือข่าย หรือองค์กรทางธุรกิจรวมถึงองค์ประกอบของระบบไดเร็คทอรี่เซอร์วิส รวมถึงประเภทของข้อมูล และระบบการ

เอกสารนี้มีลิขสิทธิ์ ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

จัดเก็บข้อมูลเพื่อให้ไดเร็คทอรี่เซิฟเวอร์สามารถค้นหาข้อมูลต่าง ๆ ที่ต้องการได้สะดวก รวมเร็ว และง่ายต่อการดูแลรักษาข้อมูล รวมถึงการศึกษาถึงกระบวนการทำงานของการเรพพลิเคชั่นในรูปแบบต่าง ๆ เพื่อนำมาเสริมการบริการของไดเร็คทอรี่เซิฟเวอร์ให้มีประสิทธิภาพยิ่งขึ้น

นอกจากนั้นได้ทำการศึกษาการกระบวนการเรพลิเคชันในแต่ละผู้ให้บริการ ได้แก่ Active Directory (Microsoft) , eDirectory (Novell) และ Netscape จากผลการศึกษาจะทำให้เห็นถึงขั้นตอน และกระบวนการในการปรับปรุงข้อมูลในการเรพลิเคชัน

การศึกษาได้มีการ Implement Active Directory 2 เครื่อง (โดยใช้ผลิตภัณฑ์ของทาง Microsoft) ซึ่งตั้งให้อยู่ใน Domain เดียวกับ และแต่ละเครื่องนั้นทำหน้าที่เป็น Domain Controller ซึ่งมีการทำงานที่เท่าเทียมกัน (read – write) หรือที่เรียกว่า Multi-Master และได้มีการใช้เครื่องมือ (Performance Evaluated tool)ในการวัดประสิทธิภาพการทำงานของไดเร็คทอรี่เซอร์วิส ไม่ว่าจะเป็นการสอบถาม หรือใช้บริการค้นหาข้อมูล , การแก้ไขข้อมูล รวมถึงการเพิ่ม - ลบข้อมูลภายในไดเร็คทอรี่เซอร์วิส

1.5 ประโยชน์ที่จะได้รับ

1. ผู้บริหารเครือข่าย (System Administrator) สามารถที่จะควบคุม และจัดการทรัพยากรต่าง ๆ ที่มีอยู่ในระบบ ไม่ว่าจะเป็น ข้อมูลเกี่ยวกับบุคคลในองค์กร , ข้อมูลเกี่ยวกับอุปกรณ์ในระบบเครือข่าย เช่น Printer , Server ในระบบต่าง ๆ รวมไปถึงการกำหนดสิทธิการใช้งานกับทรัพยากรดังกล่าว โดยผ่านทางไดเร็คทอรี่เซิฟเวอร์ (Directory Server)
2. ผู้ใช้มีความสะดวกในการเข้าใช้งานทรัพยากรฯ เนื่องจากสามารถที่จะทำการล็อกอินเข้าสู่ระบบเพียงครั้งเดียว ก็สามารถที่จะใช้ระบบต่าง ๆ ได้ (ตามสิทธิที่เหมาะสม)
3. มาตรฐานสกีมาต่าง ๆ ไม่ว่าจะเป็น Data Schema , Replication Schema รวมถึงการออกแบบชื่อของข้อมูล (Naming Space Design) ให้เป็นไปในแนวทางเดียวกัน ทำให้สามารถใช้งานไดเร็คทอรี่เซอร์วิสซึ่งทำงานต่างแพลตฟอร์มได้ (Global Directory Service) โดยผ่าน LDAP APIs (LDAP Application Programming Interface) ซึ่งเพิ่มความสะดวกให้กับผู้พัฒนาแอพพลิเคชั่น สามารถที่จะใช้งานไดเร็คทอรี่เซอร์วิสนั้นได้อย่างมีประสิทธิภาพ
4. ผู้บริหารระบบฯ สามารถที่จะทำการแก้ไข หรือตอบโต้ผู้บุกรุกใช้ทรัพยากรในระบบเครือข่ายได้อย่างรวดเร็ว เนื่องจากข้อมูลทั้งหมดถูกจัดเก็บไว้ในไดเร็คทอรี่เซิฟเวอร์เท่านั้น
5. การทำงานของไดเร็คทอรี่เซอร์วิส สามารถให้บริการได้อย่างต่อเนื่อง จากการทำสำเนา กับเครื่องไดเร็คทอรี่เซิฟเวอร์อื่น(Directory Server Replication) ที่มีอยู่ในระบบ ช่วยให้ผู้บริหา รเครือข่ายสามารถแก้ไขปัญหาที่เกิดขึ้นกับเครื่อง Master Directory Server ซึ่งจะให้ผู้ใช้บริการสามารถทำงานได้อย่างต่อเนื่อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 2
การเรพลิเคชั่น (Replication)

2.1 ลักษณะทั่วไป

การให้บริการของเครื่องให้บริการ (Server) นั้นเมื่อมีผู้ร้องขอใช้บริการ เครื่องให้บริการจะต้องให้บริการกับเครื่องลูกข่าย (Client) ที่ร้องขอใช้บริการ หากเครื่องให้บริการ (Server) ไม่สามารถให้บริการ หรือไม่สามารถตอบสนองความต้องการของเครื่องลูกข่าย อันเนื่องมาจากความผิดปรกติที่เกิดขึ้นกับเครื่องให้บริการ เช่น เครื่องให้บริการหยุดให้บริการเนื่องจากมีการร้องขอมามาก และทรัพยากรของเครื่องให้บริการมีจำกัด จึงไม่สามารถให้บริการต่าง ๆ ได้ จะทำให้ระบบไม่สามารถทำงานได้ตามปรกติได้

การทำเรพลิเคชั่น (Replication) จะมีลักษณะคล้าย ๆ กับการทำ Backup แต่คือการทำ Backup แบบออนไลน์ นั้นก็คือ เครื่องที่เป็น Backup นั้นจะมีข้อมูล หรือ ทรัพยากรใด ๆ ก็ตามเหมือนกับเครื่องต้นแบบ (Original Server) ทุกอย่าง ดังนั้น หากเครื่องที่ใช้งานอยู่เกิดมีปัญหาหรือไม่สามารถทำงานได้ตามปรกติ ก็อาจมีการเสนอ (promote) ให้เครื่องที่เป็น Backup สามารถทำงานแทนได้ โดยมีจุดประสงค์เพื่อให้เครื่อง Server ที่ให้บริการดังกล่าว สามารถให้บริการได้อย่างต่อเนื่อง (Availability) หรือโอกาสที่ระบบจะไม่สามารถที่จะให้บริการได้มีน้อยที่สุด นั่นคือถ้าให้ความเป็นไปได้ที่เครื่องให้บริการ (Server) จะสามารถให้บริการได้เท่ากับ 1- P แล้ว ฉะนั้นถ้ามีเครื่อง Server 1 เครื่อง แล้วความเป็นไปได้ ที่เครื่อง Server นั้นไม่สามารถให้บริการได้เท่ากับ 1 ดังนั้น เป็นไปได้ที่ระบบจะไม่สามารถให้บริการได้ถ้าเครื่อง Server นั้นไม่สามารถใช้งานได้ แต่ถ้ามีเครื่อง Server มากกว่า 1 เครื่องแล้ว ความน่าจะเป็นที่ระบบจะไม่สามารถให้บริการได้ก็จะลดลง คือ $1-P^n$ (เมื่อ n แทนจำนวนเครื่อง Server)

ในปัจจุบันที่มีการเชื่อมต่อกันเป็นเครือข่าย ไม่ว่าจะเป็นภายในเครือข่ายของท้องถิ่นหรือจะมีการเชื่อมต่อกับเครือข่ายภายนอก เช่น Internet สิ่งที่สำคัญที่จะช่วยให้การส่งผ่านข้อมูลนี้มีความรวดเร็ว นั้นก็คือ ช่องทางที่ใช้ในการขนส่งข้อมูล แต่ถ้ามีผู้ใช้บริการจำนวนมาก ต้องการข้อมูลประเภทเดียวกัน กับเครื่องให้บริการเครื่องเดียวกัน ก็จะทำให้การจราจรหนาแน่นและเป็นไปได้ว่าการขนส่งข้อมูลจะเกิดความล่าช้า เนื่องจากต้องมีการรอคิวในการเข้าใช้บริการนั้น ๆ แนวทางในการแก้ปัญหานี้ก็คือการจัดให้มีเครื่องให้บริการมากกว่า 1 เครื่องเพื่อให้บริการ แก่ผู้ใช้เพื่อแบ่งเบาภาระการทำงาน (Load Balancing) ของเครื่องให้บริการ (Server) ที่มีอยู่เดิม

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประโยชน์ที่จะได้รับจากการ Replication ประกอบด้วย

- **Performance enhancement** ในการเรียกใช้บริการกับเครื่อง server นั้น ถ้ามีเครื่องให้บริการเพียง 1 เครื่อง อาจจะทำให้ประสิทธิภาพในการติดต่อ สื่อสารลดลง ซึ่งเนื่องมาก จากปัญหาคอขวดนั่นเอง ดังนั้น ถ้ามีเครื่องให้บริการ มากกว่า 1 เครื่องย่อมมีการแบ่งเบาภาระ หรือมีการกระจายงาน ให้เครื่อง client สามารถเข้ามาใช้บริการแยกแต่ละเครื่องได้ ซึ่งนั่นก็ปัญหาคอขวดก็ลดลง ทำให้ประสิทธิภาพของระบบเพิ่มขึ้น
- **Enhanced availability** การทำ replication นั้นจะช่วยให้ประสิทธิภาพของระบบเพิ่มขึ้น เนื่องจากมีเครื่องให้บริการ มากกว่า 1 เครื่อง ซึ่งทำให้ความเป็นไปได้ที่ระบบจะไม่สามารถให้บริการได้เท่ากับ $1-P^n$ นั้นหมายถึงว่า ถ้ามีเครื่อง server มากขึ้นเท่าใด ยิ่งทำให้โอกาสที่จะทำให้เครื่อง server นั้นไม่สามารถใช้งานได้พร้อมกันลดลงนั่นเอง
- **Consistency** ถ้ามีเครื่องให้บริการ 1 เครื่องก็ไม่จำเป็นที่จะต้องคำนึงถึง ความสอดคล้องของข้อมูล เพราะว่ามีการเก็บข้อมูลเพียงแห่งเดียว แต่ถ้ามีการเก็บข้อมูลหลาย ๆ ที่ จำเป็นที่จะต้องคำนึงถึงความสอดคล้อง และถูกต้องของข้อมูลเป็นสำคัญ เนื่องจากมี client สามารถเข้ามาใช้บริการกับเครื่องให้บริการทุก ๆ เครื่อง ถ้าข้อมูลที่ client ได้รับไม่ตรงกันก็จะทำให้เกิดปัญหาได้ ดังนั้น ในการทำ replication จะต้องมีการติดต่อสื่อสารกันตลอดเวลา นั่นก็คือต้องมีการส่ง message เพื่อปรับปรุงข้อมูลที่ให้กับ RM ตัวอื่น ๆ ทราบถึงการเปลี่ยนแปลงนั้นอันจะทำให้ข้อมูลที่ถูกเก็บไว้ดนละที่นั้นมีความถูกต้องและสอดคล้องกัน
- **Replication transparency** ไม่ว่า Client จะ access จากที่ใด หรือ access data จาก Replica Manager ตัวใดก็ตาม การ access data นั้นเสมือนว่าได้กระทำ ณ ที่เดียวกัน หรือจากแหล่งข้อมูลเดียวกัน ดังนั้นผู้ใช้ข้อมูลไม่จำเป็นต้องทราบถึงสถานที่เก็บข้อมูล

ในการทำงาน หรือการปฏิบัติงานโดยทั่วไปที่เกี่ยวข้องกับข้อมูล ก็จะมีการปฏิบัติต่อข้อมูล 2 อย่างคือ

- การอ่าน (Read Operation)
- การเขียน (Write Operation)

ในการอ่านข้อมูลนั้นข้อมูลไม่มีการเปลี่ยนแปลง ซึ่งจะอ่านจากเครื่องให้บริการเครื่องใดก็ได้ผลรับที่เหมือนกัน แต่สิ่งสำคัญนั่นคือการเขียน (Write Operation) หรือการที่ข้อมูลมีต้องมีการเปลี่ยนแปลงนั้น จะต้องคำนึงถึงความสอดคล้องกันของข้อมูล (Consistency) ของเครื่องที่ให้บริการ นั่นก็คือเมื่อมีการเปลี่ยนแปลงของข้อมูลแล้ว จะต้องมีการแพร่กระจาย (Propagation) ของข้อมูลที่เปลี่ยนแปลงนั้นให้กับเครื่องอื่น ๆ ด้วย เพื่อให้ข้อมูลสอดคล้องกันตลอดเวลา

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Basic Architecture ของการทำ Replication นั้นประกอบไปด้วย 3 ส่วน คือ

- A client application
- A front-end application
- A replica manager

เมื่อ Client (C) ได้มีการขอใช้บริการ (Request) request ดังกล่าวก็จะถูกส่งผ่านไปยังเครื่อง Front-end (FE) จากนั้น FE จึงส่ง request ต่อให้กับ Replica manager (RM) เพื่อประมวลผลและส่ง Reply กับมาให้กับ FE จากนั้น FE จึงส่ง Reply ดังกล่าวให้กับ C ตามลำดับ ซึ่งเมื่อพิจารณาแล้วในรูปแบบก็ไม่ได้มีความยุ่งยากแต่อย่างใด ถ้าเป็นการอ่านข้อมูลเพียงอย่างเดียว (Read-operation only) แต่ถ้ามีการเขียน หรือเปลี่ยนแปลงข้อมูลแล้ว จะมีวิธีการอย่างไรที่จะทำให้ RM แต่ละตัวมีการเปลี่ยนแปลงข้อมูลให้ถูกต้อง และสอดคล้องกัน

ในการที่จะให้เครื่อง RM มีข้อมูลหมือนกันนั้น RM ดังกล่าวก็จะต้องมีการติดต่อสื่อสารกัน วิธีการส่งค่าที่มีการเปลี่ยนแปลงที่เกิดขึ้นมีอยู่หลายวิธี แต่ในที่นี้ขอกล่าวอยู่ 2 วิธี คือ

2.2 Replication Approach

2.2.1 Gossip Approach

รูปแบบของการปรับปรุงข้อมูล แบบ Gossip Approach นั้นจะมีอยู่ 2 ลักษณะใหญ่ ๆ

- **Master replica manager**

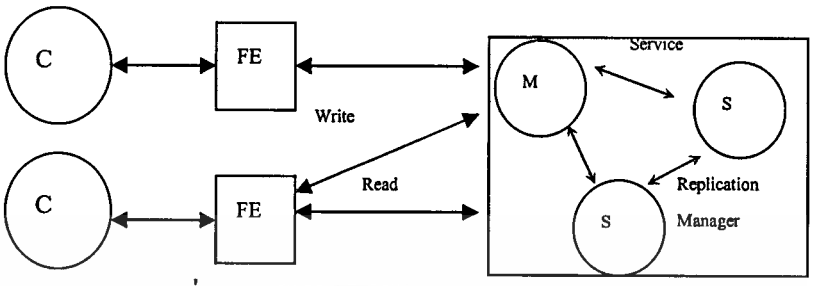
ก็คือจะมีการส่ง Gossip message ให้กับ RM เพื่อเป็นการปรับปรุงข้อมูล ของแต่ละ RM โดยมีการตั้ง RM ตัวหนึ่งเป็น Primary RM เพื่อใช้ควบคุมการเปลี่ยนแปลงของข้อมูล ที่เกิดขึ้นใน Master file

เมื่อ C ส่ง request เพื่อเป็นการอ่านข้อมูล (read – operation) แล้ว FE ก็จะส่งต่อให้กับ RM ตัวใดก็ได้ในระบบ เพื่อประมวลผล หลังจากนั้น RM ก็จะส่ง reply หรือ service ที่ C ร้องขอไปกลับมาให้กับ C นั้น แต่ถ้าขอใช้บริการแล้วจะต้องมีการเปลี่ยนแปลงข้อมูล (Write-operation) แล้ว FE ก็จะส่ง request ดังกล่าวให้กับ Master RM เพื่อทำการประมวลผลและปรับปรุงข้อมูล หลังจากนั้น Master RM ก็จะมีการกระจายการปรับปรุงนั้น (propagation data) ให้กับ RM ตัวอื่นให้มีการปรับปรุงข้อมูลให้สอดคล้องกัน

แต่วิธีนี้ก็มีข้อเสียคือ ถ้า Master RM ไม่สามารถให้บริการได้ตามปกรติ ระบบยังสามารถทำงานได้ ถ้า C ส่ง request เพื่อต้องการอ่านข้อมูลเพียงอย่างเดียว แต่จะไม่สามารถเปลี่ยนแปลงข้อมูลได้ถ้า C ต้องการเปลี่ยนแปลง หรือแก้ไขข้อมูล ดังนั้นจึงมีการแก้ไขโดยเมื่อเครื่อง Master RM ไม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

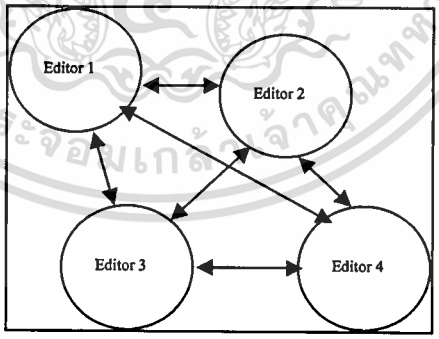
สามารถให้บริการได้ จะต้องมีการ Promote ให้ Slave REPLICA MANAGER ตัวใดตัวหนึ่งขึ้นทำให้ที่เป็น Master RM แทนเพื่อให้ระบบยังสามารถให้บริการได้ตามปกรติ



รูปที่ 2.1 Gossip Approach (Master Replica

- **Multi-user editor or Multi-Master**

ลักษณะการทำงานนั้น คือ FE สามารถที่จะติดต่อได้กับ RM ทุกตัว โดย RM แต่ละตัวจะมีความสามารถเท่ากัน ไม่ว่าจะทำการอ่านข้อมูล หรือเขียนข้อมูล เพราะในวิธีการแบบ Multi-Master เมื่อ RM ใดมีการเปลี่ยนแปลงข้อมูล ก็จะต้องส่งข้อมูลการเปลี่ยนแปลงดังกล่าวให้กับ RM ตัวอื่น ๆ ทราบ โดยการส่ง message เพื่อปรับปรุงข้อมูลที่มีอยู่ วิธีการนี้จะมีอัลกอริทึม ที่ยุ่งยากซับซ้อน แต่จะป้องกันปัญหาที่จะเกิดขึ้นกับ Primary RM นั้นก็คือ ไม่ว่าจะเกิดปัญหาขึ้นที่ RM ตัวไหน ก็ยังสามารถให้บริการอย่างสมบูรณ์กับ client (read – write operation)



รูปที่ 2.2 Multi – user editor

2.2.2 Process Group Approach

- **ลักษณะการทำงาน**

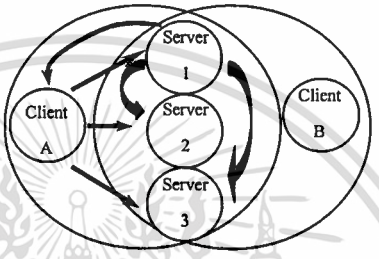
ในลักษณะการทำงานของ Process group นั้น คือจะมีการกระจายข้อมูลต่าง ๆ ให้กับสมาชิกในกลุ่ม โดยการใช้วิธีแบบ multicast communication

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **Group Structure** มีรูปแบบโครงสร้าง ดังนี้

1. Client – Server group

โดยมีการนำมาประยุกต์ใช้กับการทำงานของ replication เช่น ถ้า C มีการส่ง request ให้กับ server ในกลุ่มแล้ว ก็จะมีการกระจาย request ดังกล่าวให้กับเครื่อง server อื่น ๆ ในกลุ่ม (ที่เป็นสมาชิกทั้งหมด) แต่จะมีเครื่อง server เพียงเครื่องเดียวเท่านั้น ที่จะทำการประมวลผล และตอบผล reply ให้กับเครื่อง C นั้นซึ่งกลุ่มแต่ละกลุ่มนั้น จะมีการเชื่อมกัน (พื้นที่ซ้ำกัน) ระหว่างกลุ่มก็ได้ เพื่อที่แต่ละกลุ่มจะสามารถติดต่อ หรือขอใช้บริการร่วมกัน



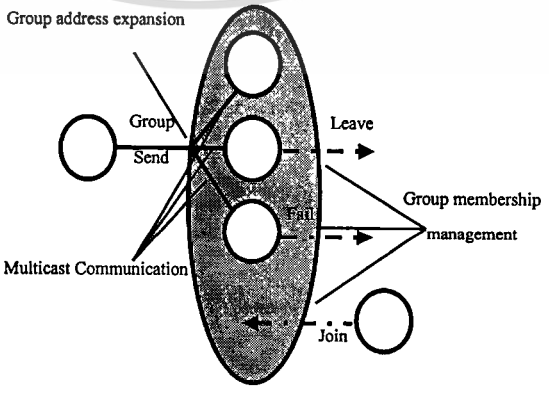
รูปที่ 2.3 Process Group ลักษณะของ client-

2. Subscription group

จะมีลักษณะที่มีการส่งข้อมูลเดี่ยวกัน ให้กับกลุ่มสมาชิก โดยจะไม่มีการ Reply กลับ แต่ในเครื่องของสมาชิกในกลุ่มเอง จะรับ information ดังกล่าวเพื่อนำไปประมวลผลตามที่กำหนดใน application

3. Hierarchical group

เนื่องจากถ้ามีสมาชิกเป็นจำนวนมาก ๆ แล้ว การควบคุมก็จะยาก ดังนั้นจึงมีการจัดแบ่งให้เป็นไปตามรูปแบบของลำดับชั้น (Hierarchical structure) เพื่อให้มีการควบคุมที่ง่ายมากขึ้น



รูปที่ 2.4 Hierarchical group

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- **Group Services**

1. Group membership management

บริการของกลุ่มทางด้านนี้ จะช่วยในการจัดการเกี่ยวกับสมาชิกในกลุ่ม ไม่ว่าจะเป็นทางด้าน การเพิ่มสมาชิก, ลดสมาชิก และปรับปรุงเปลี่ยนแปลงต่าง ๆ ของสมาชิกในกลุ่ม

2. Group address expansion

เป็นบริการของกลุ่ม ที่ช่วยในเรื่องของการอ้างถึงกลุ่ม รวมถึงการขยายตัวของกลุ่ม

3. Multicast Communication

ช่วยในการติดต่อให้มีความสะดวกมากขึ้น เนื่องจากมีการส่งข้อมูลแบบ Multicast

2.3. ความสอดคล้องของข้อมูล และการจัดลำดับการประมวล

สิ่งที่สำคัญนั้น ข้อมูลจะต้องมีความถูกต้องและสอดคล้องกันไม่ว่า Client จะ access เข้า RM ที่ใดก็จะได้ผลลัพธ์เหมือนกัน ดังนั้นถ้าเป็นการอ่านข้อมูลเพียงอย่างเดียวแล้ว ข้อมูลย่อมไม่มีการเปลี่ยนแปลง แต่ถ้ามีการเปลี่ยนแปลงข้อมูลแล้ว ลำดับในการประมวลผลเป็นสิ่งที่สำคัญ ที่จะทำให้ข้อมูลที่ผ่านการประมวลผลแล้วมีความถูกต้อง และครบถ้วนตามรายการที่เกิดขึ้น

2.3.1 Request Ordering

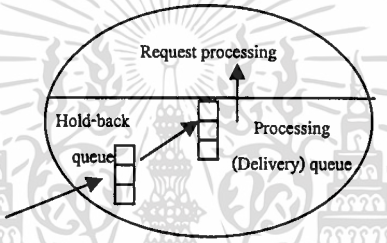
ในการพิจารณาเพื่อจัดลำดับในการประมวลผลนั้นมีวิธีอยู่ 3 วิธี คือ

- **Causal ordered request processing** การควบคุม หรือจัดลำดับการประมวลผล โดยมีการจัดลำดับ ความต้องการในการประมวลผล (request ordering) ตามข้อมูล หรือ request ที่มีความสัมพันธ์กัน โดยจะมีการจัดลำดับก่อนหลัง ที่เรียกว่า "happened-before ordering"
- **Totally ordered request processing** จะมีการจัดลำดับให้กับทุก ๆ request ที่ติดต่อมายัง RM ในทุก ๆ เครื่อง ฉะนั้น request ที่เกิดขึ้นสามารถที่จะระบุลำดับได้โดยทุก ๆ RM จะต้องมีการจัดลำดับที่เหมือนกัน ซึ่งไม่ได้พิจารณาเฉพาะเพียงแต่ request ที่มีความสัมพันธ์กันเท่านั้น แต่พิจารณา request ที่เกิดขึ้นทั้งหมด
- **Sync-ordered request processing** เป็นลักษณะ request ที่เป็นกับการไประบุตำแหน่งในการประมวลผล (request marker) เพื่อสร้างความสัมพันธ์ให้เกิดขึ้นกับ request ที่ไม่สัมพันธ์กัน ซึ่งจะต้องไม่ขัดแย้งกับ request ที่ถูกจัดลำดับไว้ก่อนหน้านี้ หรือทำหน้าที่ในการเชื่อมความสัมพันธ์ของลำดับที่มีอยู่เดิม กับ request ที่จะถูกส่งเข้าไปประมวลผลใหม่

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2.3.2 Implementing request ordering

การส่งข้อมูลผ่านระบบเครือข่าย ซึ่งถ้าในระบบมี Traffic สูงก็จะทำให้ข้อมูลนั้นเดินทางมาถึงปลายทางในเวลาที่ไม่เท่ากัน (คุณสมบัติในการส่งข้อมูลในชั้นของ Network layer จะมีหน้าที่ในการค้นหาเส้นทางที่เหมาะสม แล้วจัดส่งข้อมูลไปตามเส้นทาง ซึ่งจะถูกระบุตาม destination IP address ของข้อมูลนั้น) โดยบางเส้นทางอาจจะมี traffic มากและบางเส้นทางก็มี traffic น้อย ซึ่งอาจทำให้ข้อมูลชุดสุดท้ายอาจจะมาถึงปลายทางก่อนที่ข้อมูลชุดแรกจะเดินทางมาถึง ซึ่งก่อนที่จะมีการประมวลผลให้กับข้อมูลนั้น RM จะต้องแน่นใจก่อนว่า จะได้มีการประมวลผลตามลำดับที่ถูกจัดไว้ และข้อมูลที่ถูกจัดลำดับไว้จะต้องมีความสัมพันธ์กันอย่างถูกต้อง โดยเทคนิคที่นำมาใช้นี้จะมีการทำงาน ดังนี้



รูปที่ 2.5 Ordering the requests arriving

- Hold - back จะทำหน้าที่เก็บ Request ต่าง ๆ ไว้เพื่อรอทำการประมวลผล โดยมี request จาก client ติดต่อมายัง RM เพื่อป้องกันการผิดพลาดจากกระประมวลผลนั้น จะต้องมีลำดับในการประมวลผลของแต่ละ request ดังนั้น RM ก็จะพิจารณาจาก Time stamp ที่มากับ packet ของ request เพื่อดูลำดับก่อน - หลัง โดยมีการจัดลำดับไว้ที่ Hold –back ก่อนที่จะส่งเข้าไปที่ request processing
- Processing queue เมื่อ request ใดเหมาะสมที่จะทำการ process หรือมีลำดับที่ถูกต้องแล้ว ก็จะถูกส่งจากส่วนของ hold - back เพื่อเข้าสู่ Processing queue และเมื่อ request นั้นถึงลำดับที่จะประมวลผลจึงได้นำ request ดังกล่าวไปประมวลผล

2.3.3 Implementing total ordering

เมื่อมีการส่ง Request จาก client ให้กับ FE แล้ว FE ก็จะทำการส่ง request ดังกล่าวให้กับ RM ซึ่งถ้ามี RM เพียง 1 เครื่องก็จะสามารถควบคุม การจัดลำดับให้กับ request เหล่านั้นไม่ยากนัก แต่ถ้ามี RM มากกว่า 1 เครื่องแล้วส่วนนี้จะเป็นการให้ลำดับแก่ request ต่าง ๆ เพื่อให้มีการจัดลำดับเป็นไปอย่างเหมาะสม ซึ่งจะให้ผลลัพธ์ที่เกิดขึ้นนั้นมีความถูกต้อง โดยในลักษณะนี้จะต้องมีการให้ลำดับ กับทุก Request (Assign request ordering) โดยทั่วไปก็มีรูปแบบการทำงานอยู่ 2 วิธี คือ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Sequencer โดยมีหน้าที่ในการ running number หรือ Assign Time Stamp ให้กับทุก request ซึ่งมีลักษณะแบบ Centralization ปัญหาที่เกิดขึ้นเมื่อมี request ติดต่อเข้ามามาก จะทำให้เกิดปัญหาในการติดต่อสื่อสาร หรือ ปัญหาคอขวด เนื่องจากมีผู้ให้ลำดับ หรือ assign time stamp อยู่ที่จุดศูนย์กลางเพียงจุดเดียว แต่วิธีนี้จะควบคุมง่าย
- Distributed Agreement มีหลักการทำงานเสมือนว่าในทุก ๆ RM นั้นมีตัว Logical Sequencer การทำงานจะมีประสิทธิภาพการทำงานดีกว่าแบบแรก เนื่องจากไม่จำเป็นจะต้องรอให้มีการ Assign Queue จากศูนย์กลางที่เดียว แต่จะมีปัญหาในเรื่องของการควบคุม คือ เมื่อมีการให้ลำดับแก่ request แล้วจะต้องมีการแจ้งให้ RM ตัวอื่น ทราบเพื่อที่จะได้ให้ลำดับถัดไป ดังนั้นถ้าการติดต่อสื่อสารไม่มี หรือมีปัญหาการสื่อสารระหว่างกันแล้วจะทำให้การจัดลำดับไม่มีประสิทธิภาพ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 3

ไดเร็คทอรี่เซอร์วิส (Directory Service)

3.1 ไดเร็คทอรี่เซอร์วิส

3.1.1 ลักษณะโดยทั่วไป

ในการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ถ้าในระบบเครือข่ายมีเครื่อง Server ที่ให้บริการอยู่เป็นจำนวนมาก การที่จะควบคุมการใช้งานต่าง ๆ รวมถึงสิทธิการเข้าถึงข้อมูลก็จำเป็นจำต้องมีฐานข้อมูลผู้ใช้ (User) ขึ้นไว้แต่ละเครื่อง Server เพื่อเป็นการกำหนดสิทธิการใช้งานและเป็นการรักษาความปลอดภัยให้กับข้อมูล ซึ่งให้ผู้ที่มีสิทธิการใช้งานเท่านั้น ที่สามารถทำงานกับโปรแกรมนั้น ๆ ได้ ไม่ว่าจะเป็นการอ่าน เขียน หรือทำการเปลี่ยนแปลงข้อมูล ดังนั้น ถ้ามีเครื่อง Server จำนวนมาก ก็จะเป็นต้องมีฐานข้อมูลผู้ใช้ระบบต่าง ๆ มากขึ้นด้วย ซึ่งเป็นการยากในการบริหารจัดการ (การเพิ่ม - ลด จำนวนผู้ใช้ หรือรวมถึงการปรับปรุงสิทธิการใช้งานให้กับผู้ใช้ "Directory Service จะช่วยให้การบริหารทรัพยากรคอมพิวเตอร์รวมถึงทรัพยากรในระบบเครือข่ายเป็นไปได้อย่างมีประสิทธิภาพ โดยการควบคุมการใช้งานเข้าสู่ระบบการใช้งานแอพพลิเคชั่นต่าง ๆ สามารถที่จะทำการล็อกอินการใช้งานเพียงครั้งเดียว ก็สามารถที่จะทำการใช้งานแอพพลิเคชั่นที่มีอยู่ได้ และยังช่วยให้ผู้บริหารระบบ (System Admin) ทำการบริหารจัดการระบบรายชื่อผู้ใช้งานเพียงที่เดียว ซึ่งง่ายและสะดวกต่อการออกแบบระบบการรักษาความปลอดภัย"

Directory Service เป็นบริการหนึ่ง ซึ่งจะช่วยให้การบริหารจัดการระบบเครื่องข่ายมีความง่าย และสะดวกมากขึ้น รวมถึงมีความสามารถในการยืดหยุ่น (Flexibility) และ ความคล่องตัวในการขยายระบบเครือข่าย (Scalability) ที่จะเกิดขึ้นในอนาคต ข้อมูลที่จัดเก็บใน Directory Server นั้นมีหลายประเภท เช่น ข้อมูลของลูกจ้าง หรือพนักงานในองค์กร ข้อมูลเกี่ยวกับอุปกรณ์ต่าง ๆ ที่มีในระบบเครือข่าย รวมถึงข้อมูลของสมาชิก หรือลูกค้า ก็สามารถเก็บได้ ส่วนประกอบในการทำงานของ Directory Service นั้นอย่างน้อยจะต้องประกอบด้วย Directory Server และ Directory Client Program ซึ่งใช้ในการเข้าถึงข้อมูลใน Directory Service ได้ DNS (Domain Name Server) ก็เป็น Directory Service ประเภทหนึ่งซึ่งข้อมูลที่เก็บใน DNS นั้นประกอบด้วย ชื่อของเครื่องคอมพิวเตอร์ ซึ่งจับคู่กับ IP Address ซึ่งช่วยให้การติดต่อในระบบอินเทอร์เน็ตมีความง่ายขึ้น ผู้ใช้ไม่จำเป็นต้องจำ IP Address ซึ่งเป็นสิ่งที่คอมพิวเตอร์ใช้ในการติดต่อระหว่างกัน การจัดเก็บข้อมูลของ Directory Server นั้นจะมีการจัดเก็บข้อมูลต่าง ๆ ไว้ใน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ฐานข้อมูลแห่งเดียว ซึ่งสามารถที่จะมีการเข้าใช้บริการได้จากเครื่องลูกข่าย เครื่องใดก็ได้ ซึ่งอยู่ในระบบเครือข่ายฯ ข้อมูลที่จัดเก็บใน Directory Service เช่น

- อุปกรณ์ (Physical device information) ในระบบฯ เช่น ข้อมูล(Data) ,พรินเตอร์ (Printer) เครื่องแม่ข่ายที่ให้บริการ (Server) เป็นต้น
- ข้อมูลของพนักงานในองค์กรซึ่งเป็นข้อมูลสาธารณะ (Public employee information) เช่น email address, ชื่อ (name) รวมถึง แผนก (department) เป็นต้น
- ข้อมูลในการติดต่อกับลูกค้า หรือข้อมูลอื่น (Contract or account information) เช่น ชื่อลูกค้า วันที่ส่งมอบสินค้า, หมายเลขของสัญญา หรือเอกสารที่ติดต่อ เป็นต้น

ในการติดต่อสื่อสารระหว่าง Client กับ server นั้นจะต้องมีรูปแบบที่สามารถติดต่อกันได้ เช่น web browser ซึ่งเป็น web client จะสามารถติดต่อกับ web server ได้โดยผ่าน Protocol HTTP ซึ่งเป็นมาตรฐานที่ใช้ในการติดต่อสื่อสารกันทั่วไป แต่การติดต่อสื่อสารจาก client ทำการค้นหาข้อมูล email address จาก Directory server อื่น ซึ่งระบบการจัดเก็บข้อมูลของ email system มีความแตกต่างกัน ก็ไม่สามารถค้นข้อมูล หรือร้องขอข้อมูลดังกล่าวได้ ดังนั้นจึงต้องมีมาตรฐานที่ใช้ในการติดต่อระหว่าง Directory client กับ Directory Server นั้นก็คือ LDAP (Lightweight Directory Access Protocol)

3.1.2 พื้นฐานของไดเร็คทอรี่เซอร์วิส

สมุดโทรศัพท์ เป็นไดเร็คทอรี่ประเภทหนึ่ง ที่ทำหน้าที่ใช้ข้อมูลเกี่ยวกับ ชื่อ นามสกุล ที่อยู่ และเบอร์โทรศัพท์ข้อมูลที่เก็บในสมุดโทรศัพท์นั้นจะมีการเก็บข้อมูลต่าง ๆ แบ่งออกเป็นหมวดหมู่ เพื่อให้ง่ายต่อการใช้งาน และสะดวกรวดเร็ว เช่นเดียวกับการทำงานของไดเรคทอรี่เซอร์วิส ประเภทของข้อมูลที่มีการจัดเก็บในไดเร็คทอรี่เซอร์วิสนั้น แบ่งออกเป็น 3 ประเภทดังนี้

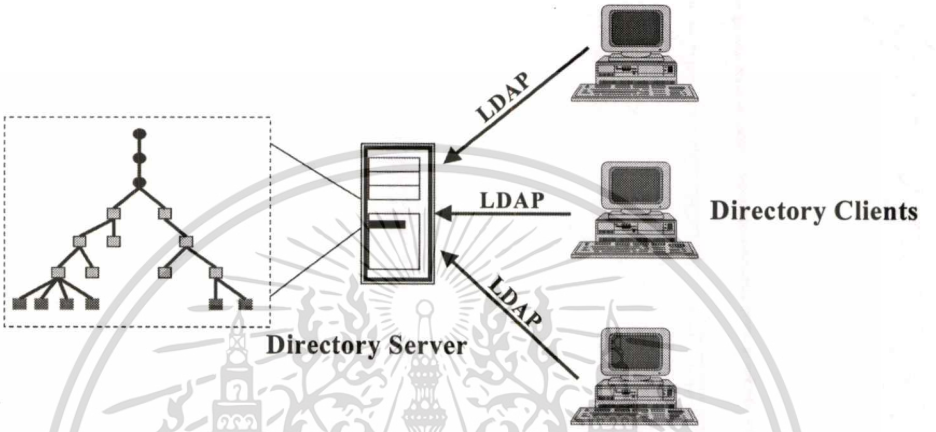
1. ข้อมูลเกี่ยวกับบุคคล เช่น ชื่อ นามสกุล รูปภาพ เลขที่บัตรประจำตัว เป็นต้น
2. ข้อมูลเกี่ยวกับสถานที่ เช่น เลขที่บ้าน อาคาร จังหวัด ประเทศ หรือ email address เป็นต้น
3. ข้อมูลเกี่ยวกับอุปกรณ์ต่าง ๆ ในระบบเครือข่าย เช่น พรินเตอร์,เราท์เตอร์, เซิฟเวอร์ เป็นต้น ซึ่งเมื่อผู้ใช้ทำการล๊อกอินเพื่อเข้าสู่ระบบฯ ระบบฯ ก็จะมีการตรวจสอบการใช้งานกับไดเร็คทอรี่เซิฟเวอร์ ว่ามีสิทธิการใช้งานอะไรบ้างในระบบเครือข่าย

3.1.3 บทบาท และหน้าที่ของไดเร็คทอรี่เซอร์วิส

1. สามารถทำการกระจายฐานข้อมูล หรือบริหารงานจากศูนย์กลางได้ ไดเร็คทอรี่ได้ถูกออกแบบให้สามารถที่จะรองรับการบริการชนิดต่าง ๆ ที่มีความหลากหลาย และสามารถที่จะทำการดูแลระบบจากที่ต่าง ๆ ลักษณะของการเก็บข้อมูลของไดเร็คทอรี่จะทำการเก็บข้อมูลได้ 2 แบบ คือ การเก็บข้อมูลอยู่ที่ศูนย์กลาง (Centralize) และการเก็บข้อมูลแบบกระจาย (Distributed) การเก็บ

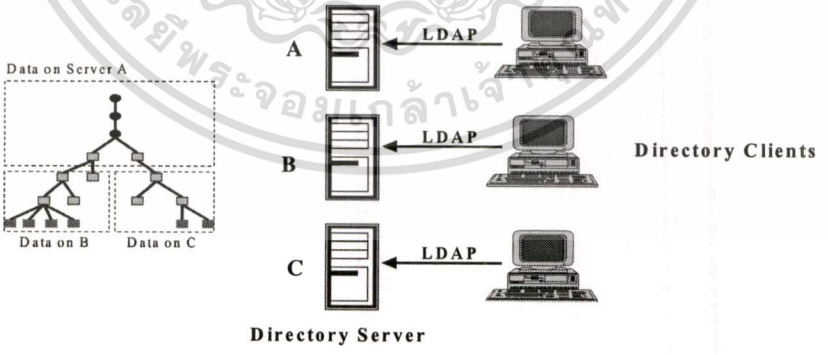
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ข้อมูลอยู่ที่ศูนย์กลางนั้น ข้อมูลทั้งหมดจะเก็บไว้ในไดเร็คทอรี่กลาง การเรียกใช้งานจากไคลเอนต์ จะทำการร้องขอมาที่ไดเร็คทอรี่ศูนย์กลาง ถ้าเราต้องการทำสำรองข้อมูลเพื่อป้องกันข้อมูลจากศูนย์กลางเสียหาย การทำสำรองข้อมูลระหว่างไดเร็คทอรี่เรียกว่า การทำ เรพลิเคชั่น (Replication) การทำ เรพลิเคชั่นนั้นเครื่องที่ทำเรพลิเคชั่นกับเครื่องจากศูนย์กลางจะมีข้อมูลที่เหมือนกัน



รูปที่ 3.1 Central Directory Server

2. การเก็บข้อมูลในไดเร็คทอรี่แบบการกระจายนั้น ข้อมูลที่เก็บในไดเร็คทอรี่ศูนย์กลางสามารถทำการแบ่งเป็น Partition ข้อมูลในไดเร็คทอรี่เฉพาะบางส่วนออกมายังไดเร็คทอรี่เครื่องอื่น ๆ ได้ เพื่อช่วยลดภาระการทำงานที่ไดเร็คทอรี่หลักได้ และยังช่วยให้ประสิทธิภาพการทำงานของระบบมีความเร็วยิ่งขึ้น

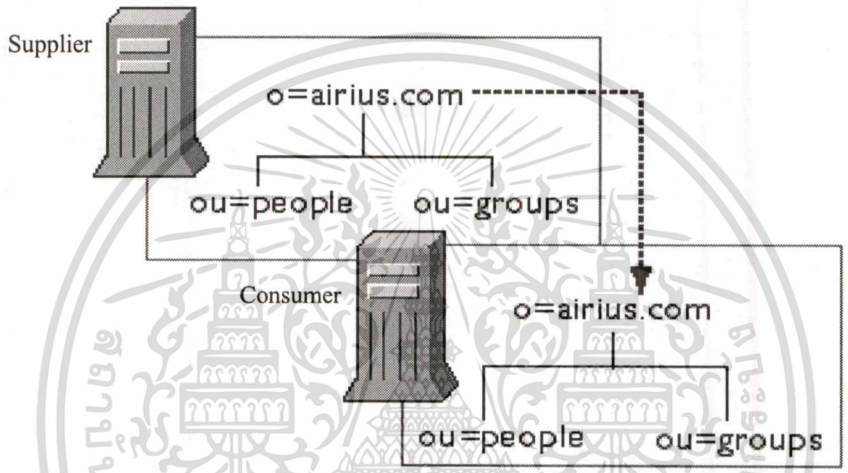


รูปที่ 3.2 Distribute Directory Server

3. สามารถที่จะทำการ Replicaton ข้อมูลได้โดยง่าย กระบวนการ Replication หมายถึง กระบวนการทำสำเนาข้อมูลจากไดเร็คทอรี่เซิฟเวอร์หลักไปยังไดเรคทอรี่เซิฟเวอร์อื่นๆ ที่อยู่ในระบบฯ รูปแบบของการเรพลิเคชั่นจะมีการกำหนดทิศทาง และรูปแบบของเรพลิเคชั่นไว้ สมมติว่าบริษัท ก. มีโรงงานอยู่ 2 สาขา สาขาแรกตั้งอยู่ที่กรุงเทพฯ และสาขาที่2 ตั้งอยู่ที่จังหวัดเชียงใหม่ โรงงานทั้ง 2 แห่งมีการติดตั้งไดเร็คทอรี่เซิฟเวอร์เพื่อให้มีการบริหารจัดการ

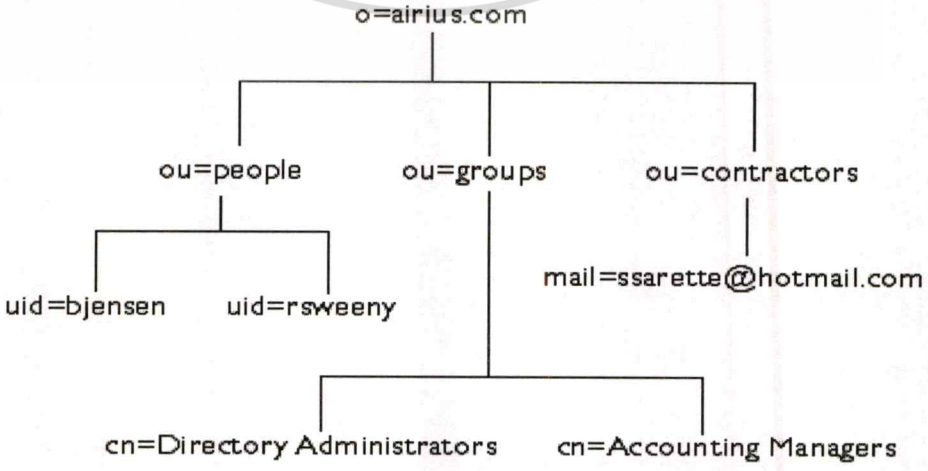
เอกสารนี้เป็นลิขสิทธิ์ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ได้จากส่วนกลาง และเพิ่มความสะดวกในการทำงาน ในกรณีที่ไดเร็คทอรี่เซิฟเวอร์ที่ตั้งอยู่ที่เชียงใหม่ไม่สามารถให้บริการได้ที่จะเขียน หรือเปลี่ยนแปลงข้อมูลต่าง ๆ ของไดเร็คทอรี่เซิฟเวอร์จะทำการ replicate ข้อมูลใหม่ไปยังโรงงานที่สาขาเชียงใหม่ทันที จะทำให้ข้อมูลที่อยู่ในไดเร็คทอรี่เซิฟเวอร์ที่สาขาเชียงใหม่ มีข้อมูลเหมือนกับโรงงานที่สาขากรุงเทพการทำงานของเรพลิเคชั่นนี้จะเรียก ไดเร็คทอรี่เซิฟเวอร์ ที่สาขากรุงเทพว่า "Supplier" และไดเร็คทอรี่เซิฟเวอร์ที่สาขาเชียงใหม่ว่า "Consumer"



รูปที่ 3.3 Supplier and Consumer replica

4. รองรับการขยายตัว และการเปลี่ยนแปลงของระบบเครือข่าย ได้อย่างมีประสิทธิภาพ กล่าวคือ ถ้าอนาคตมีการขยายขนาดของเครือข่าย หรือจำนวนผู้ใช้งานระบบฯ มีมากขึ้น การปรับปรุงไดเร็คทอรี่เซอร์วิส สามารถยืดหยุ่น และปรับตัวทำให้การทำงานมีประสิทธิภาพ
5. เป็นระบบที่มีลักษณะโครงสร้างของข้อมูลเป็น Hierarchical Relational



รูปที่ 3.4 Directory Information Tree (DIT)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6. ข้อมูลที่จัดเก็บในไดเร็คทอรี่เซอร์วิสนั้น จะเน้นการทำงานในลักษณะการใช้อ่านข้อมูลมากกว่าที่จะมีการเปลี่ยนแปลงของข้อมูลบ่อย ๆ ดังนั้น ไดเร็คทอรี่เซอร์วิส จึงมีความรวดเร็วในการค้นหาข้อมูล
7. สามารถกำหนดมาตรฐานของสกีมา ให้เหมาะสมกับองค์กรหรือข้อมูลที่มีการจัดเก็บได้ โดยมีข้อแนะนำในการสร้างสกีมา ดังนี้
   - การตั้งชื่อของ Attribute และ Objectclass การตั้งชื่อนั้นไม่ควรตั้งชื่อที่มีความยากมากและชื่อที่ไม่สื่อความหมาย
   - การกำหนด OID กล่าวคือ การเรียกชื่อของ Attribute และ Objectclass จะมีการเรียกอยู่ 2 ประเภท ได้แก่ การเรียกเป็นชื่อ เช่น cn1 และการเรียกเป็น OID
   - การสร้างคลาสย่อยในสกีมา เพื่อสามารถดึงคุณสมบัติของ Objectclass หลักมาใช้งาน เช่น ถ้าต้องการสร้างคลาสย่อยของพรินเตอร์ที่ชื่อว่า hpPrinter ใน ObjectClass hpPrinter จะดึงเอาคุณสมบัติของคลาสหลักที่ชื่อ Printer มาใช้งาน ทำให้ ObjectClass hpPrinter มีคุณสมบัติต่าง ๆ ตามที่ ObjectClass Printer กำหนดไว้ และสามารถมีคุณสมบัติใหม่ที่ทำการกำหนดเพิ่มเติมเฉพาะ ObjectClass hpPrinter

3.2 โพรโตคอล LDAP (Light weight Directory Access Protocol)

3.2.1 ลักษณะโดยทั่วไป

โพรโตคอล LDAP จะใช้เป็นภาษากลางสำหรับการติดต่อสื่อสารระหว่าง Directory Client และ Directory Server ทำให้สามารถที่จะทำการติดต่อสื่อสารข้ามแพลทฟอร์มกันได้ โดยการใช้ภาษากลางนี้เป็นการลดการออกแบบระบบการทำงานที่มีหลายแพลทฟอร์ม และช่วยในการนำมาใช้งานมีความสะดวก และรวดเร็ว ประโยชน์ของการใช้มาตรฐานของภาษาในการติดต่อ เช่น web server ใช้โพรโตคอล HTTP เป็นภาษากลางในการติดต่อสื่อสาร ทำให้ web browser สามารถที่จะติดต่อกับทุก web server ได้ โดยผ่าน โพรโตคอล HTTP ถึงแม้ว่า web server จะทำงานในแพลทฟอร์มที่ต่างกัน หรือมีระบบปฏิบัติการที่ต่าง ๆ กันก็ตาม

โพรโตคอล LDAP เป็นโพรโตคอลชนิด "Light Weight" หมายถึงเป็นโพรโตคอลที่ออกแบบมาให้ง่ายต่อการใช้งาน มีประสิทธิภาพในการทำงานสูง มีฟังก์ชั่นในการทำงานที่ครบครัน แตกต่างจากโพรโตคอลที่เป็นชนิด "Heavy Weight" เช่น X.500 Directory Access Protocol

โพรโตคอล X.500 DAP จะมีความสามารถในการทำงานที่ต้องการความซับซ้อนในการเข้ารหัส และต้องใช้ OSI network protocol ในกาติดต่อสื่อสาร แต่การทำงานของระบบเครือข่ายส่วนใหญ่ จะทำงานอยู่บนโพรโตคอล TCP/IP ซึ่งทำให้ไม่สามารถใช้งาน X.500 ไดเร็คทอรี่ได้ โพรโตคอล LDAP ถูกออกแบบมาให้ใช้เทคนิคการเข้ารหัสข้อมูลที่ใช้งานได้ง่าย และมี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

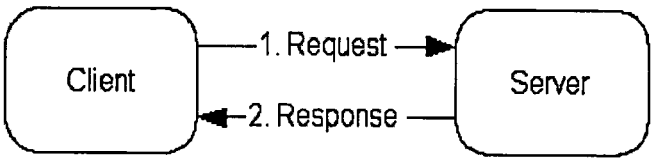
ห้องสมุดคณะเทคโนโลยีสารสนเทศ สจล.

ความปลอดภัยสูง และทำงานอยู่บนโพรโตคอล TCP/IP ปัจจุบันนี้ระบบเครือข่ายที่ทำงานในระบบอินเทอร์เน็ตจะใช้โพรโตคอล TCP/IP เป็นพื้นฐานในการทำงาน ด้วยเหตุนี้ทำให้การเชื่อมต่อต่าง ๆ เป็นไปโดยง่าย เพราะการนำไดเร็คทอรี่ไปใช้งานในโพรโตคอล TCP/IP มีความสะดวกกว่าการนำไปใช้งานในโพรโตคอล OSI เนื่องจากระบบเครือข่ายที่ใช้ OSI ไม่เป็นที่นิยมในการใช้งาน โพรโตคอล LDAP มีการใช้งานอย่างแพร่หลายนั้นเริ่มที่ LSAPv2 หรือ RFC 1777 และ 1778 ในปัจจุบัน โพรโตคอล LDAP มีการพัฒนามาถึง version 3 หรือในมาตรฐาน RFC 2251 ถึง 2256

โพรโตคอล LDAP ได้มีการกำหนดมาตรฐานของฟังก์ชั่นการทำงานออกเป็น 4 ส่วน โดยได้มีการนำข้อดีของโพรโตคอล X.500 มาเป็นโครงสร้างของโพรโตคอล LDAP ฟังก์ชั่นการทำงานของ LDAP ที่กำหนดขึ้นมา เพื่อให้เป็นมาตรฐานเดียวในการติดต่อสื่อสารระหว่าง LDAP client และ Directory Server และเป็นการป้องกันปัญหาในการทำงานร่วมกันระหว่าง Directory จากผู้ผลิตค่ายต่าง ๆ

3.2.2 ลักษณะการทำงานของโพรโตคอล LDAP

LDAP protocol มีลักษณะของการทำงานแบบ Client/Server ทางฝั่งของ client จะมีโปรแกรมของ LDAP client ติดตั้งไว้ เมื่อ LDAP client ต้องการข้อมูลจาก LDAP server จะทำการส่ง request ไปยังเซิฟเวอร์ โดยผ่านโพรโตคอล TCP/IP เมื่อ server ได้รับ request จากทาง client และจะทำการประมวลผลใน LDAP server ตาม request นั้น จากนั้น LDAP server ก็จะทำการส่ง result กลับมายัง client นอกจากลักษณะการทำงานที่เป็น client/server แล้ว โพรโตคอล LDAP ยังทำงานในลักษณะเป็น Messages-Oriented หมายถึง ในขั้นตอนการติดต่อกันระหว่าง LDAP client กับ LDAPserver จะมีการสร้าง messages เป็น request operation ไปยังเซิฟเวอร์ เมื่อ LDAP server ได้รับก็จะทำการส่งผล (result) ที่อยู่ในรูปของ messages เช่นเดียวกัน ส่งไปยัง client ในการรับและส่ง messages ระหว่าง LDAP client/ LDAP server จะมีการรับ-ส่งแบบ "Series LDAP Messages"



รูปที่ 3.5 LDAP client retrieves a single entry from LDAP server

การทำงานของโพรโตคอล LDAP นั้นรองรับการทำงานทั้งที่เป็นแบบ single message และแบบ multi messages โดยมีขั้นตอนการทำงาน โดย LDAP server เมื่อได้รับ operation search 2 คำสั่งก็จะทำการ returned entry messages ID2 ก่อนที่จะทำการส่ง return code,msgid1 เพื่อเป็นการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ป้องกันไม่ให้ LDAP client ทำการส่งคำสั่งอื่น ๆ มายัง LDAP server การทำงานแบบนี้เรียกว่า "Lock-step" เช่นดังตัวอย่างใน HTTP protocol เครื่อง client จะทำการร้องขอบริการ หรือข้อมูลกับ web server โดยจะทำการเปิด connection เท่ากับจำนวนต้องการติดต่อกับ web server ซึ่งลักษณะของการทำงานใน LDAP client ก็จะคล้าย ๆ กัน จำนวนการรองรับการทำงาน พร้อม ๆ กันของ LDAP server จะมีการกำหนดไว้ที่ LDAP server

3.2.3 Operation ใน LDAP protocol

โพรโตคอล LDAP นั้นมีรูปแบบ หรือคำสั่งในการดำเนินการ หรือ Operation ทั้งหมด 9 operation โดยสามารถแบ่งออกได้เป็น 3 กลุ่มใหญ่ ๆ ดังต่อไปนี้

1. Interrogation Operation เป็น operation ที่ใช้สำหรับสอบถามข้อมูล ประกอบด้วย :
   - search operation
   - compare operation
2. Update Operations เป็น operation ที่ใช้ดำเนินการกับข้อมูลใน Directory ประกอบด้วย :
   - add operation
   - delete operation
   - modify operation
   - modify DN (rename) operation
3. Authentication and control operation เป็น operation ที่ใช้สำหรับการแสดงตัวตนของ client ที่เข้ามาใช้งาน ประกอบด้วย :
   - bind operation ในการแสดงตัวตัวเพื่อขอเข้าใช้บริการ LDAP server และ
   - unbind operation เพื่อเป็นการยุติการเข้าขอใช้งานกับ LDAP server
   - abandon ใช้สำหรับ client โดยยกเลิกผลลัพธ์ ที่ LDAP Server ส่งมาจากคำสั่งก่อนหน้านี้

ตัวอย่าง ขั้นตอนการทำงานระหว่าง LDAP Client กับ LDAP Server มีดังนี้

1) LDAP client ทำกาสร้าง connection กับ LDAP server ผ่าน TCP connection และทำการส่ง bind operation (การส่ง bind operation คือการส่ง username และ password ไปยัง LDAP Server
2) LDAP Server ได้ทำการตรวจสอบชื่อ login ผู้ใช้และ passwordว่าถูกต้องหรือไม่ถ้าถูกต้องทั้ง Username และ Password ถูกต้อง LDAP Serverจะทำการส่งผลการ bind operation กลับมายัง LDAP Client
3) LDAP Client ทำการส่ง operation search request ไปยัง LDAP server

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4) และ 5) LDAP server จะทำการส่ง result entry กลับมายัง LDAP client ตาม search request

6) LDAP server ส่งผลการใช้คำสั่ง search operation มาให้ยัง LDAP client

7) LDAP client ส่งคำสั่ง unbind เพื่อทำการยกเลิกการทำงาน และยกเลิก TCP connection

8) LDAP server ทำการตัดการทำงานระหว่าง LDAP client กับ LDAP server

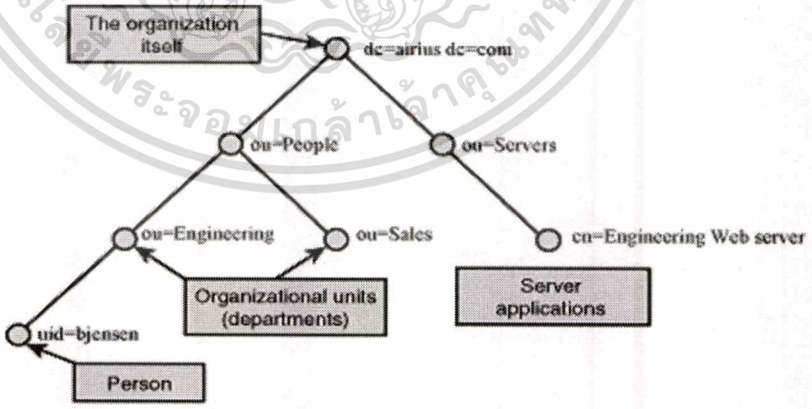
3.2.4 โครงสร้าง และสถาปัตยกรรม LDAP

โครงสร้างของโพรโตคอล LDAP ได้ถูกกำหนดการทำงานออกเป็น 4 หมวด โครงสร้างของ LDAP ทั้ง 4 หมวดโดยจะกล่าวถึงโครงสร้างของ LDAP Model รวมถึงชนิดของข้อมูลที่เก็บและการนำข้อมูลไปใช้งาน

1) LDAP Information Model

หมายถึง ข้อกำหนดชนิดของข้อมูลและกลุ่มของข้อมูลที่เก็บใน ไดเร็คทอรี่หรือการกำหนดชนิดของข้อมูลที่จะทำการเก็บลงในไดเร็คทอรี่เซิฟเวอร์

กลุ่มของข้อมูลที่จะทำการเก็บในไดเร็คทอรี่ เราจะเรียกว่า "Entry" ใน 1 Entry จะประกอบไปด้วยกลุ่มของข้อมูลที่จะอธิบายเกี่ยวกับวัตถุนั้น ตัวอย่างเช่น กลุ่มของข้อมูลที่ทำการอธิบายลักษณะของบุคคล เช่น ชื่อ, นามสกุล, ที่อยู่ เป็นต้น แต่การกำหนด Entry ในไดเร็คทอรี่ยังรวมถึงอุปกรณ์ต่าง ๆ ในระบบเครือข่าย เช่น Server, Printer, Application ต่าง ๆ หรือชื่อของวัตถุที่ต้องการเก็บลงในไดเร็คทอรี่



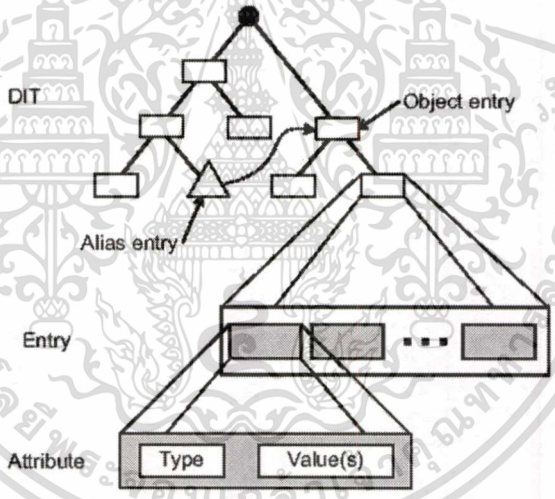
รูปที่ 3.6 ลักษณะโครงสร้างข้อมูลใน Directory

กลุ่มของข้อมูลที่เก็บในไดเร็คทอรี่เรียกว่า Entry ซึ่งเป็นกลุ่มของ Attribute ที่ทำหน้าที่อธิบายความหมายของวัตถุ (object) โดยที่ Attribute จะประกอบด้วย 2 ส่วนคือ ชนิดของ Attribute (Attribute Type) และ ค่าที่เก็บลงใน Attribute (Attribute Values)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ชนิดของ Attribute หมายถึงการอธิบายถึงคุณสมบัติของ Attribute ที่มีความสัมพันธ์กับค่าที่เก็บอยู่ใน Attribute (Attribute Value) การกำหนดชนิดของ Attribute นั้นจะต้องคำนึงถึงชนิดของข้อมูลที่จะทำการจัดเก็บด้วย เช่น ข้อมูลประเภทข้อความ การกำหนดชนิดของ Attribute จะกำหนดเป็น CaseIgnoreString หรือ CaseExacString การกำหนดชนิดของ Attribute นั้นสามารถกำหนดได้ดังนี้

- CaseIgoreString
- CaseExacString
- Directory String
- Integer
- Binary
- Octet String



รูปที่ 3.7 DIT และ Entry Structure

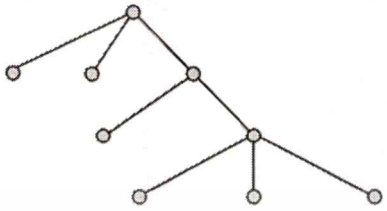
ในการกำหนดชนิดของ Attribute นั้น เพื่อให้มีความเหมาะสมสำหรับการออกแบบสกีมา และ DIT (Directory Information Tree) ของไดเร็คทอรี่ เพื่อให้ไดเร็คทอรี่มีความเร็วในการทำงาน และการ Matching ตามเงื่อนไขในการค้นหาข้อมูลมีความถูกต้อง รวดเร็ว และลดความผิดพลาดในการทำงาน

2) LDAP Naming Model

หมายถึง วิธีการออกแบบโครงสร้างของไดเร็คทอรี่ การกำหนด Naming ใน DIT (Directory Information Tree) การออกแบบโครงสร้างเสมือนขององค์กร หน่วยงาน บริษัท และการอ้างถึงตำแหน่งของ entry เพื่อการนำมาใช้งาน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

โครงสร้างของการกำหนด Naming model ในโครงสร้างของ DIT จะมีการกำหนดเป็นโครงสร้างแบบ Tree structure โครงสร้างของ Tree structure นี้ได้มีการนำมาใช้งานในระบบไฟล์ของยูนิกซ์ และ DNS server โดยมีรูปแบบดังนี้

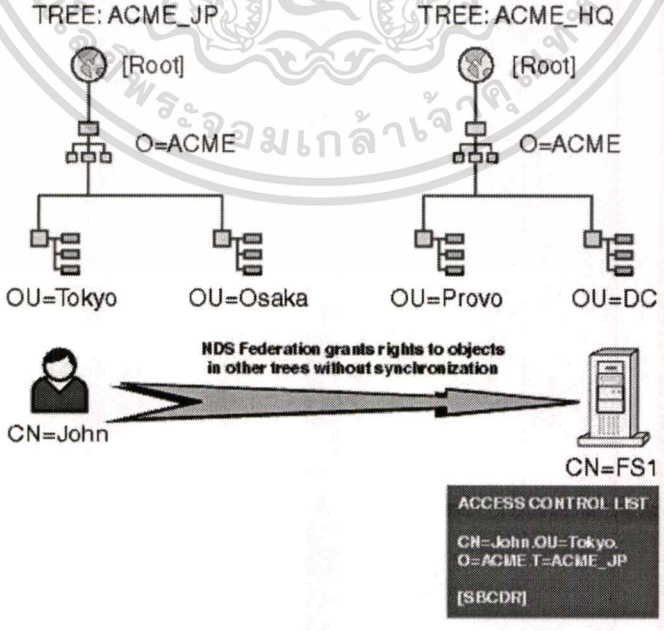


รูปที่ 3.8 Directory Tree Structure

Naming Model ถูกกำหนดเพื่อแสดงการเรียกใช้ชื่อที่มีรูปแบบเป็นมาตรฐาน สามารถเข้าใจได้ง่าย โดยการอ้างอิงตำแหน่งข้อมูลหรือ Entry ในไดเร็คทอรี่ จะเรียกว่า Distinguished Names (DN) เป็นการอ้างตำแหน่งของข้อมูลแบบล่างขึ้นสู่บน การอ้างชื่อใน DN เป็นลักษณะที่เรียกว่า “Uniqueness” ซึ่งแต่ละ DN จะไม่มีชื่อที่ซ้ำกัน ในกรณีที่มีชื่อที่ซ้ำกัน ไดเร็คทอรี่จะทำการยกเลิกชื่อที่เพิ่มเข้ามาที่หลัง ในบางครั้งเราจะพบว่ามีการเรียกการอ้างชื่อของ DN ว่า Relative Distinguished Name (RDN) ซึ่งก็คือ การอ้างชื่อแบบล่างขึ้นสู่บน หรือเรียกว่าเป็น Naming Attribute เช่น “cn=Sam Carter” เป็นต้น

3) LDAP Function Model

หมายถึง ข้อกำหนดการเข้าถึงข้อมูล,การเพิ่ม,แก้ไข และการลบข้อมูลในไดเร็คทอรี่



รูปที่ 3.9 ตัวอย่างของ Namespace

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

LDAP Function Model สามารถแบ่งการทำงานออกเป็น 3 กลุ่ม ดังนี้

I. Interrogation Operation

Operation ที่ใช้ในการสอบถามข้อมูลระหว่าง LDAP Client และ LDAP Server คือการค้นหาข้อมูลหรือ Search และข้อมูลมาให้กับ LDAP Client หรือ retrieve การทำงานของไดเร็คทอรี่จะไม่มี Operation read1 การอ่านข้อมูลในไดเร็คทอรี่จะต้องใน Operation search เพื่อทำการค้นหาข้อมูลและใช้ Operation retrieve สำหรับนำข้อมูลออกมาใช้งาน ในการใช้ Operation search จะประกอบไปด้วยพารามิเตอร์ 8 พารามิเตอร์ที่ใช้ในการระบบตำแหน่งเริ่มต้นของการค้นหาข้อมูล พารามิเตอร์ต่าง ๆ ได้แก่

1) **Base object** บอกตำแหน่งของ DIT ที่จะเริ่มค้นหา เช่น dc=abc,dc=com เป็นการระบุตำแหน่งในการค้นหาที่ตำแหน่งบนสุดของ DIT หรือ ou=people,dc=com เป็นการระบุตำแหน่งการค้นหาที่ ou=people ของ DIT
2) **Scope** ขอบเขตของการค้นหาข้อมูลใน Operation search แบ่งออกเป็น 3 แบบคือ
3) **DerefAliases** เป็นการบอก LDAP server ไม่ใช้การอ้าง Aliases ในการค้นหาข้อมูล เมื่อใช้ Operation search รูปแบบการใช้งานพารามิเตอร์ DereferAliases แบ่งออกเป็น 4 พารามิเตอร์ ได้แก่
4) **Size limit** เป็นการจำกัดจำนวนของ Entry ที่จะมีการส่งไปให้กับไคลเอนท์ เมื่อใช้การ search เพื่อหาข้อมูลทั้งไดเร็คทอรี่ ถ้าไม่มีการกำหนดขนาดของการ search แล้วจะทำให้ server ทำงานหนักมาก โดยปรกติแล้วจะกำหนดค่า Sizeของ Client ไว้ที่ 100 และ Size limit ของ Server จะกำหนดให้ที่ 500 ถ้ากำหนดค่าของ Size limit เท่ากับ 0 หมายถึงการที่ยอมให้ Client สามารถที่จะ search ข้อมูลทั้งหมดของไดเร็คทอรี่ ในกรณีที่ Servcr ทำงานจนถึง Size limit ดังนั้น Directory Server จะทำการหยุดการทำงานของ Operation search และจะส่งค่า LDAP_SIZELIMIT_EXCEEDED กลับไปยัง Client ที่ใช้บริการ search นั้น
5) **Time limit** การกำหนดค่าเวลามากที่สุดที่ใช้ในการทำงานของ Operation search โดยมีการกำหนดเป็นวินาที ถ้าถึงเวลาที่กำหนด Directory Server จะทำการหยุดการทำงานของ Operation search สำหรับการ request และจะทำการส่งค่า LDAP_TIMELIMIT_EXCEEDED ไปยัง Client ถ้ากำหนด Time limit = 0 หมายถึงการไม่กำหนดเวลาในการค้นหา (อาจเกิดปัญหาเช่นเดียวกับ Size limit)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

6) **AttrsOnly** การกำหนดค่าพารามิเตอร์เป็นแบบ Boolean คือ True หรือ Falseถ้าเป็นการกำหนด True แล้ว Server จะทำการส่ง Attribute type ไปยัง LDAP Client แต่จะไม่ส่ง attribute value ไปด้วย ใช้ในกรณีที่ LDAP Client ต้องการที่จะทำการหาชนิดของ attribute ที่อยู่ใน Entry และถ้ากำหนดเป็น False แล้ว Server จะทำการส่งทั้ง attribute type และ attribute value ไปยัง LDAP Client

7) **Filter** การกำหนดเงื่อนไขของการ filter จากการ search ข้อมูลใน ไดเร็คทอรี่เซิฟเวอร์

นอกจาก Search Operation แล้วใน Interrogation Operation จะมี Compare operation หรือการเปรียบเทียบใช้ทำการตรวจสอบค่าของ entry และค่า attributeที่ทาง LDAP client ได้ทำการของใช้สิทธิการใช้งาน LDAP Client ถ้า entry DN ที่ส่งไปนั้นไม่ครบ หรือมีบาง attribute มีค่าเป็นศูนย์ "0" LDAP server จะทำการส่ง Negative Response มายัง LDP Client

II. Update Operation

Operation สำหรับ ปรับปรุง หรือเปลี่ยนแปลงข้อมูลใน Directory Server จะประกอบด้วย .

Operation	**ลักษณะของ Update Operation**
Add	ใช้สำหรับการสร้าง entry ลงในไดเร็คทอรี่เซิฟเวอร์ประกอบด้วย DN และ attribute
Delete	ใช้สำหรับลบ entry ออกจากไดเร็คทอรี่เซิฟเวอร์
Rename	ใช้สำหรับทำการเปลี่ยนชื่อ DN
Modify	ใช้ทำการแก้ไขข้อมูลใน entry รวมทั้ง object class name,object class value, attribute name, attribute value

III. Authentication and Control

การใช้งาน Operation ต่าง ๆ ไม่ว่าจะเป็น Add, Delete, Search หรือ Operation ที่มีการกระทำกับ Directory Server นั้นจะต้องมีการขอ Authentication โดยการใช้ Operation bind และเมื่อยกเลิกการใช้งาน Directory Server จะต้องใช้ Operation unbind เพื่อยกเลิกการติดต่อกับ Directory Server

4) LDAP Security Model

ข้อกำหนดการป้องกัน และระบบการรักษาความปลอดภัยของข้อมูลในไดเร็คทอรี่ใช้ในการกำหนดสิทธิในการใช้งาน และการเข้าถึงข้อมูล โดยที่ LDAP server และ LDAP client จะทำงานในรูปแบบของ Connection-oriented protocol กล่าวคือ LDAP client จะทำ bind operation เพื่อขอสิทธิการเข้าใช้งาน และทาง LDAP server จะทำการตรวจสอบสิทธิดังกล่าว ในการ

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ตรวจสอบสิทธิซึ่งจะยอมให้ LDAP client ทำงานได้ในระดับใดนั้นขึ้นอยู่กับรูปแบบของการควบคุมซึ่งเรียกว่า "Access control"

3.2.5 LDIF (Light weight Data Interchange Format)

LDIF (Lightweight Directory Interchange Format) รูปแบบของไฟล์ที่มีลักษณะเป็น ASCII ไฟล์ ใช้สำหรับการแลกเปลี่ยนข้อมูลกันระหว่างไดเร็คทอรี่เซิฟเวอร์ ซึ่งในการติดต่อ หรือแลกเปลี่ยนข้อมูล จะต้องส่งผ่านข้อมูลในไดเร็คทอรี่ในรูปแบบนี้ เป็นมาตรฐานที่กำหนดไว้ ดังนั้นจึงทำให้ไดเร็คทอรี่ ซึ่งทำงานอยู่บนแพลตฟอร์มหนึ่ง สามารถติดต่อ (Synchronize) กับไดเร็คทอรี่อีกแพลตฟอร์มหนึ่งได้ เช่น ไดเร็คทอรี่ที่ทำงานบน Unix ก็สามารถติดต่อ หรือส่งผ่านข้อมูลกับไดเร็คทอรี่ที่ทำงานบน Windows ได้

ตัวอย่างรูปแบบของ ldif ไฟล์

```
dn: cn=Bernette Peckel, ou=Product Development, o=DirMark Inc.
cn: Bernette Peckel
sn: Peckel
givenName: Bernette
objectClass: top
objectClass: person
objectClass: organizationalPerson
description: This is Bernette Peckel's description
facsimileTelephoneNumber: +1 804 568-7596
ou: Product Development
mail: Bernette_Peckel@DirMark.com
postalAddress: DirMark Inc., Product Development Dept #641, Room#439
telephoneNumber: +1 415 518-1154
title: Elite Product Development Janitor
userPassword: lekcePette
```

3.2.6 LDAP APIs (LDAP Application Programming Interface)

การติดต่อระหว่าง LDAP client กับ LDAP server จะใช้โพรโตคอล LDAP ในการติดต่อสื่อสารกัน แต่ Application อื่นซึ่งทำงานอยู่บน LDAP client จะติดต่อกับ LDAP client ได้จะต้องมีคนกลางในการแปลงข้อมูลให้เป็นรูปแบบเดียวกับซึ่งเรียกว่า Application Programming Interface (API) โดยปัจจุบันก็มีผู้พัฒนาหลายบริษัท ยกตัวอย่าง ดังนี้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- Novell ก็จะมี Novell SDK เป็น API สำหรับการติดต่อกับไดเร็คทอรี่เซิฟเวอร์ค่ายของ Novell
- Microsoft ก็จะมี ADSI โดย ADSI นั้นมีทั้งภาษา C, C++ และ Visual Basic เป็นต้น
- ทางกลุ่ม Open Source ก็มี เช่น PerlLDAP ซึ่งพัฒนาโดย www.mozilla.org รวมทั้งทาง OpenLDAP ก็ได้มีการพัฒนาเช่นกัน ซึ่งสามารถดาว์นโหลดได้ที่ www.openldap.org เป็นต้น

3.3 สกีมา (Schema)

3.3.1 ความหมายของสกีมา

คือ ข้อกำหนดต่าง ๆ ที่อธิบายข้อจำกัด และชนิดของข้อมูลที่จะทำการเก็บลงในไดเร็คทอรี่เซอร์วิส หรือฐานข้อมูลของไดเร็คทอรีเซอร์วิส สกีมาจะเกี่ยวเกี่ยวข้องกับเรื่องของ Objectclass และ Attribute ที่มีการสร้างขึ้น และที่เป็นมาตรฐาน นอกจากนั้นแล้วยังมีหน้าที่ในการตรวจสอบความถูกต้องของข้อมูลที่เก็บลงไหไดเร็คทอรี่เซิฟเฟอร์ระหว่างการทำงานของ LDAP server และ LDAP client

การบริหารสกีมาในระดับ ObjectClass และ Attribute ในไดเร็คทอรี่เป็นสิ่งสำคัญต่อการดูแลรักษาระบบไดเร็คทอรี่เซอร์วิส โครงสร้างของสกีมาถ้าเปรียบเทียบกับ Database Server ที่เรารู้จักก็คือ การออกแบบโครงสร้างตารางใน Database จะมีการกำหนดขนาดความกว้างของแถวในตาราง การกำหนดชนิดของ Data ที่จะเก็บลงในตาราง สิ่งเหล่านี้เป็นข้อกำหนดเบื้องต้นสำหรับการออกแบบ Database

3.3.2 องค์ประกอบของสกีมา

1) Attribute จะทำหน้าที่ในการเก็บข้อมูลให้อยู่ใน Directory Server โดยสามารถแบ่งออกเป็นหมวดหมู่ตามชนิดของ Attribute ดังนี้
   - Attribute type ทำหน้าที่ในการเก็บข้อมูลที่อยู่ในไดเร็คทอรี่เซอร์วิส เช่น ชื่อ เบอร์โทรศัพท์ พรินเตอร์ เป็นต้น
   - Attribute value มีหน้าที่ในการเก็บค่า หรือเป็นรายละเอียดของ Attribute type
2) ObjectClass ในไดเร็คทอรี่เป็นที่รวมกลุ่มของ Attribute ที่ทำหน้าที่คล้ายกัน เช่น การกำหนดชื่อของ Object Class ที่อ้างอิงจากสิ่งของ เช่น person, printer, organizational และใน 1 entry จะประกอบด้วย Object Class และ Attribute ที่อธิบายถึงคุณสมบัติของ Entry ที่อ้างถึง

3.3.3 รูปแบบสกีมา ที่เป็นที่นิยมจะมีอยู่ 3 รูปแบบ คือ

1) Slapd.conf
2) ASN.1
3) LDAPv3

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

3.3.4 กระบวนการตรวจสอบสกีมา (Schema Checking Process)

ในกรณีที่มีการสร้างสกีมาที่ไม่ถูกต้อง ไดเร็คทอรี่จะไม่ยอมให้มีการ add, delete, modify ข้อมูลใน Entry ของไดเร็คทอรี่ และจะมีข้อความที่ตอบกลับมายัง LDAP client สิ่งที่จะต้องทำการตรวจสอบการสร้างสกีมา มีดังนี้

1) ตรวจสอบชนิดของ Value และไวยากรณ์ถูกหรือไม่
2) ตรวจสอบว่ามีอย่างน้อย 1 Objectclass Attribute ที่มีค่าอยู่
3) ตรวจสอบค่าใน Attribute ที่เป็น mandatory โดยจะต้องมีค่า
4) ในกรณีที่เรากำหนดชนิดของ Attribute เป็น single-value ค่าใน Attribute มีเพียงค่าเดียว

3.3.5 มาตรฐานสกีมา

ซึ่งเกิดจากผู้ผลิตซอฟแวร์ไดเร็คทอรี่เป็นผู้กำหนด ที่นิยมใช้งาน มีดังนี้

1) มาตรฐานของ LDAP
2) มาตรฐานของ X.500
3) มาตรฐานของ Industry Consortium Standard

3.4 รูปแบบของการ Replication ไดเร็คทอรี่เซอร์วิส

3.4.1 ความหมาย

การเรพลิเคชั่น คือ การทำสำเนาของไดเร็คทอรี ซึ่งจะมีอยู่ 2 รูปแบบ คือ

1) การเรพลิเคชั่นแบบออนไลน์อัพเดต (Online update) จะมีการอัพเดตข้อมูลระหว่างไดเร็คทอรี่ทุกครั้งที่มีการเปลี่ยนแปลง ทำให้ข้อมูลในไดเร็คทอรี่เซิฟเวอร์มีขนาดเท่ากัน แต่ข้อเสียก็คือ ไดเร็คทอรี่เซิฟเวอร์ที่ทำงานจะต้องมีประสิทธิภาพสูง และความเร็วใน Local Area Network อย่างน้อยต้อง 100 Mb/sec แต่ถ้าเป็น Wide Area Network การสื่อสารหรือความเร็วในการส่งข้อมูลควรจะเร็วกว่า 2 Mb/sec
2) การเรพลิเคชั่นแบบแบทช์อัพเดต (Batch update) จะมีการอัพเดตตามช่วงเวลาที่กำหนด มีข้อดีคือ ช่วยลด Traffic ในระบบการสื่อสารข้อมูล และไดเร็คทอรี่เซิฟเวอร์ไม่ทำงานหนักจนเกินไป แต่ข้อเสียคือ ความไม่เท่ากันของข้อมูลระหว่าง ไดเร็คทอรี่เซิฟเวอร์ ที่มีการเรพลิเคชั่นกัน ทำให้ข้อมูลบางอย่างยังล้าสมัย

3.4.2 แนวความคิดของการเรพลิเคชั่น

1) Suppliers Replication Agreements หมายถึง การทำเรพลิเคชั่นระหว่างหรือมากว่าโดยที่ผู้ผู้ให้ (Source replica) เรียกว่า "Suppliers" ซึ่งเป็นผู้กำหนดการอัพเดตข้อมูลไปยังไดเร็คทอรี่เซิฟ-เวอร์เครื่องอื่น (Destination replica)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การกำหนดค่าเริ่มต้นของการเรพลิเคชั่น เรียกกว่า “replication agreement” ซึ่งมีการกำหนดค่างต่าง ๆ ประกอบด้วย

Hostname	ของไดเร็คทอรี่เซิฟเวอร์ที่เป็น consumer
Port	หมายเลขพอร์ทที่รันโพรเซสของไดเร็คทอรี่
Bind	ชื่อของ user และ passwordที่มีสิทธิในการใช้บริการไดเร็คทอรี่
DIT	ตำแหน่งของ Directory Information Tree (DIT) ที่จะมีการเรพลิเคชั่น

2) Consumers Replication Agreements หมายถึง การทำเรพลิเคชั่นระหว่างเซิฟเวอร์ โดยฝั่งผู้รับเป็นผู้กำหนดขั้นตอน และค่าเริ่มต้นในการเรพลิเคชั่นนั้น

3) The Unit of Replication การกำหนดเรพลิเคชั่นนั้นจะกำหนดผ่าน Distinguish Name(DN) ซึ่งเป็นตำแหน่งที่ใช้อ้างอิงในไดเร็คทอรี่

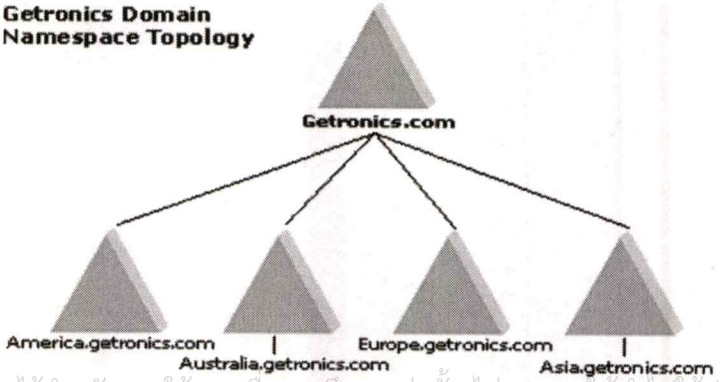
4) Consistency and Convergence หมายถึง ความถูกต้องตรงกันของข้อมูล ในไดเร็คทอรี่เซิฟเวอร์ที่มีการเรพลิเคชั่น

5) Incremental and Total Updates เป็นลักษณะของการอัพเดตของข้อมูลในไดเร็คทอรี่ ซึ่งในการเรพลิเคชั่นครั้งแรกนั้น จะต้องมีการอัพเดตทั้งหมด หรือเรียกว่า total updates หลังจากนั้นก็จะเป็นการอัพเดตแบบ Incremental updates ซึ่งเกิดจากการอัพเดตเพียงบางส่วนเท่านั้น

6) Initial population of a Replica หมายถึง ในการสร้าง Replication Agreement ในการเริ่มต้นการทำงานครั้งแรกนั้น เครื่องที่เป็น Consumer จะยังไม่มีข้อมูลต่าง ๆ ฉะนั้นจะมีการส่งข้อมูลจากเครื่อง supplier มาอัพเดตยังเครื่องของ Consumer เพื่อทำการซิงโครไนซ์ข้อมูลใน DIT และเมื่อเกิดความเสียหายกับเครื่องที่เป็น Supplier ก็สามารถที่จะทำการเรพลิเคชั่นกลับจาก consumer ไปยังเครื่องที่เป็น supplier ได้ เพราะการอัพเดตจะมีการเรพลิเคชั่นจากเครื่องที่มีการอัพเดตครั้งล่าสุดเสมอ

3.4.3 รูปแบบของการเรพลิเคชั่น ในแบบต่าง ๆ (Replication model)

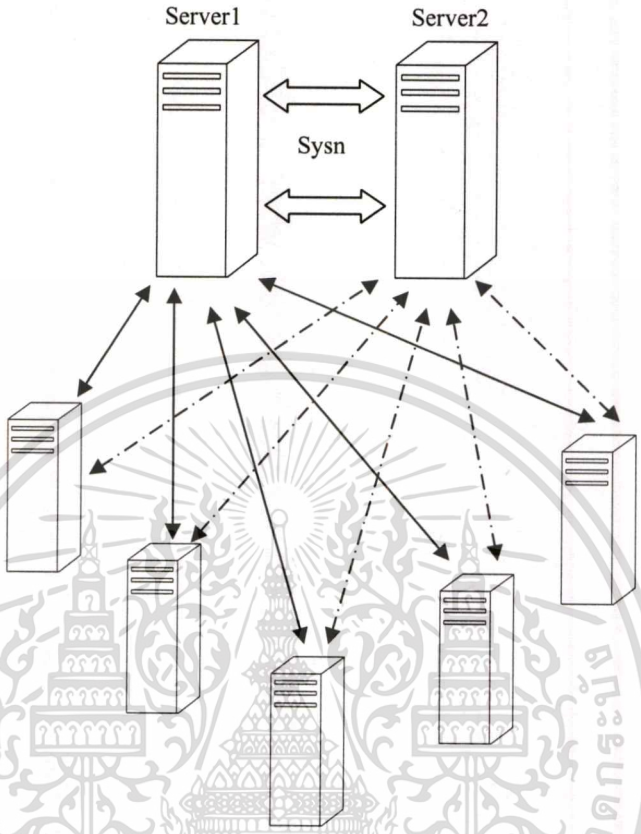
1. Single-Master Replication



รูปที่ 3.10 แสดงรูปแบบของ Single-Master Replication

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

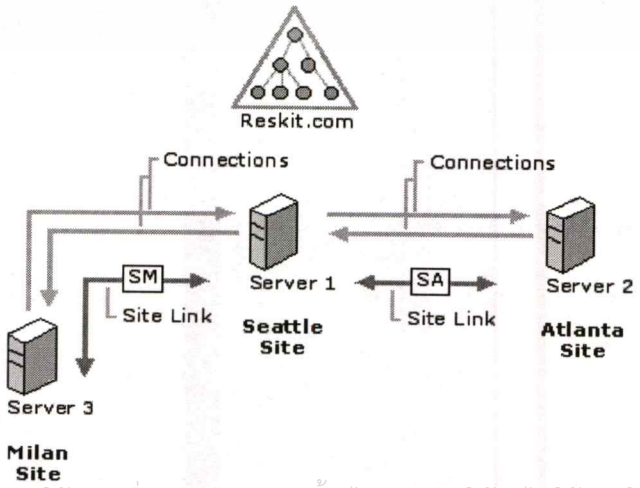
2. Dual-Master Replication



รูปที่ 3.11 แสดงขั้นตอนในการทำงาน Floating-Master Replication

3. Multi-Master Replication

เป็นลักษณะที่เครื่องไดเร็คทอรี่มี Master หลายตัว และสามารถทำการ read-write ได้เหมือนกัน ด้วยรูปแบบนี้จะทำให้ข้อมูลที่ส่งเข้ามาปรับปรุงมีจำนวนมาก และเหมาะกับระบบเครือข่ายที่มีความเร็วสูง



รูปที่ 3.12 แสดงขั้นตอนในการทำงาน Multi-Master Replication

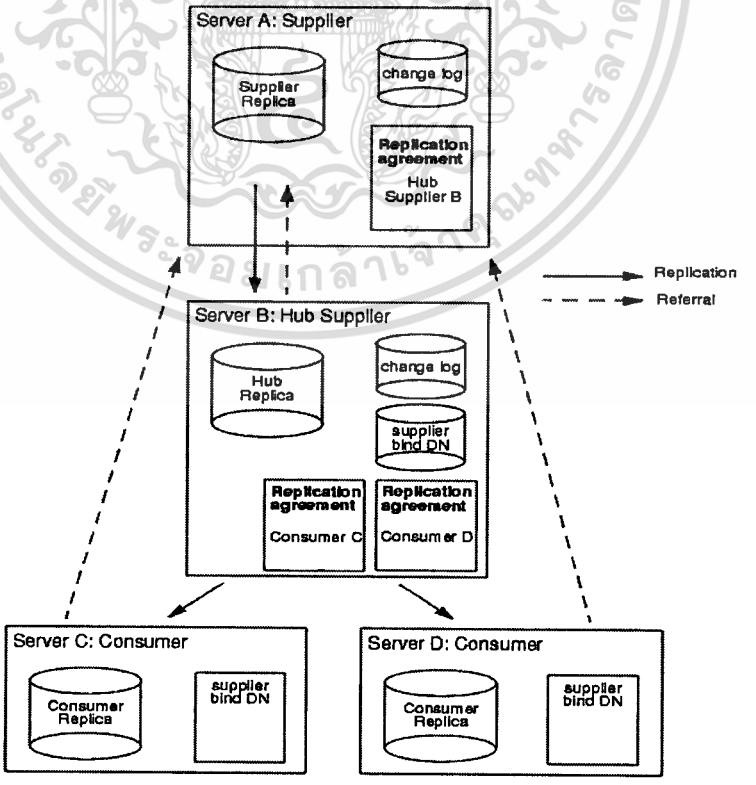
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ในเทคนิคการเรพลิเคชันรูปแบบนี้ จะเหมาะสมในกรณีที่มีเครือข่าย อยู่หลายแห่ง และเชื่อมโยงกันผ่าน WAN link ด้วยประโยชน์ของ multi master replication โดย client สามารถที่จะ access เข้าใช้บริการของระบบเครือข่าย โดยผ่านการตรวจสอบของไดเร็คทอรี่เซอร์ของแต่ละไซต์ (Site)นั้น หรือเรียกว่า Local Directory Server โดยแต่ละ Local Directory Server ก็จะมีการเรพลิเคชันกันโดยผ่าน WAN link

4. Hub Replication หรือเรียกว่า "Cascading Replication"

จะมีลักษณะการส่งผ่านข้องมูลจาก Supplier ให้กับ Consumer โดย Hub replication ที่ทำหน้าที่ส่งผ่านข้อมูลนี้จะทำหน้าที่ forward ข้อมูลจาก Supplier ให้กับ Consumer

ไดเร็คทอรี Supplier ทำการส่งข้อมูลผ่านให้กับไดเร็คทอรที่ทำหน้าที่เป็น Hub ซึ่งทำ Hub replica ก็จะทำการส่งข้อมูลให้กับ ไดเร็คทอรี Consumer ซึ่งในรูปแบบนี้สามารถทำได้โดยใช้ประโยชน์จากช่องทางที่มีการจราจรของข้อมูลไม่หนาแน่น ทำให้สามารถส่งผ่านข้อมูลได้รวดเร็วกว่าเส้นทางตามปกติ จากรูปจะเห็นว่า Server C และ Server D ยังคง referral ไปที่ Server A แม้ว่าข้อมูลจะถูกส่งจาก Server B ก็ตาม ซึ่งนั่นก็หมายถึงว่า ในกรณีที่เส้นทางจาก Supplier นั้นสามารถส่งข้อมูลได้ตามปกติ และมีข้อมูลที่วิ่งอยู่บนเส้นทางไม่มาก Supplier ก็สามารถใช้เส้นทางเดิมในการ Replication ก็ได้



รูปที่ 3.13 แสดงขั้นตอนในการทำงาน Hub-Master Replication

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 4

การวิเคราะห์ประสิทธิภาพของไดเร็คทอรี่เซิฟเวอร์

4.1. การวิเคราะห์รูปแบบการเรพลิเคชั่น (Analysis and Compare Replica Model)

4.1.1 eDirectory

ในการทำงานของ Novell Directory Service (NDS) โครงสร้างของ NDS นั้นสามารถรองรับการขยายตัวของระบบเครือข่ายในอนาคตได้เป็นอย่างดี ซึ่งเทคนิคที่ใช้จะมีการแบ่งเป็น Partition ในแต่ละเครือข่ายย่อย ๆ นั้น เช่น บริษัท ABC จำกัด มีโครงสร้างในการบริหาร หรือ Organization แบ่งเป็น 3 แผนก ซึ่งได้แก่ บัญชี การตลาด และผู้บริหาร ซึ่งในรูปแบบนี้สามารถแบ่งออกเป็น Partition ได้ตามความเหมาะสม เช่น อาจไม่มีการแบ่ง Partition เลยก็ได้ หากบุคลากรในองค์กรมีจำนวนไม่มาก แต่ถ้าในอนาคต แผนกบัญชี แบ่งแยกออกเป็น แผนกการเงิน และแผนกเจ้าหนี้ ลูกหนี้ ก็อาจมีการแบ่งออกเป็น Partition ของแผนกการเงิน และ Partition ของแผนกเจ้าหนี้ลูกหนี้ ซึ่งเป็นการแบ่งเบาภาระในการจัดการกับผู้ใช้ที่จะมีต่อ Network Admin เพียงผู้เดียว ให้กระจายไปตามส่วนงานให้มีส่วนช่วยในการรับผิดชอบ และถ้าในอนาคตมีการยุบรวมแผนก ทาง NDS ก็สามารถนำ Partition ต่าง ๆ นั้นมาทำการรวมกันได้เช่นกัน

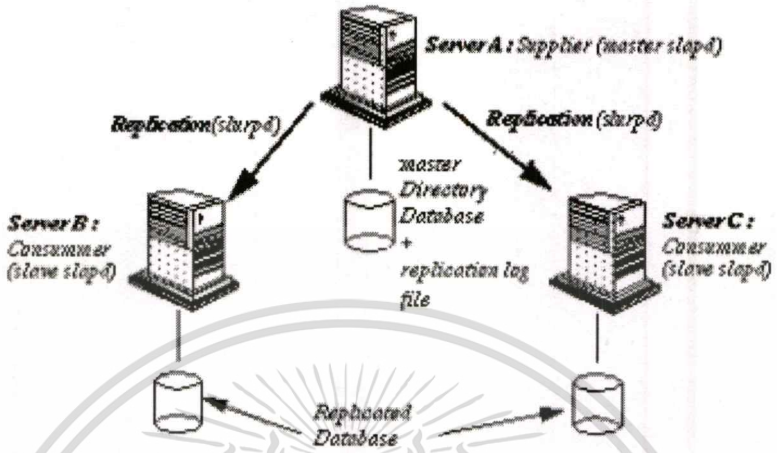
จุดประสงค์ของการทำ Replication ประกอบด้วย

- **Fault Tolerance** ความทนทานของระบบที่สามารถให้บริการได้อย่างต่อเนื่อง ไม่ว่า Primary Directory Server จะไม่สามารถให้บริการได้ก็ตาม
- **Performance** เมื่อมี Local replica ในระบบ การตรวจสอบสิทธิ (Authentication) ผู้ใช้งานระบบก็สามารถทำงานเร็วขึ้น เนื่องจากผู้ใช้ไม่จำเป็นต้อง access ที่เครื่องศูนย์กลาง หรือ Primary Directory Server จึงเป็นการลดปริมาณ Traffic ในระบบเครือข่าย ทำให้มีประสิทธิภาพมากขึ้น
- **Name resolution** ในกระบวนการส่ง request ของผู้ใช้ ซึ่งติดต่อกับ Directory นั้น Directory Server ดังกล่าวจะต้องทำการตรวจสอบข้อมูลที่ Client ต้องการว่าเก็บอยู่ที่ใด กระบวนการดังกล่าวเรียกว่า name resolution หรือ tree walking

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

รูปแบบของ Replica ที่ใช้อยู่ใน eDirectory (Novell Directory Service) มี 4 รูปแบบดังนี้

1. Master Replica



รูปที่ 4.1 Master Replica

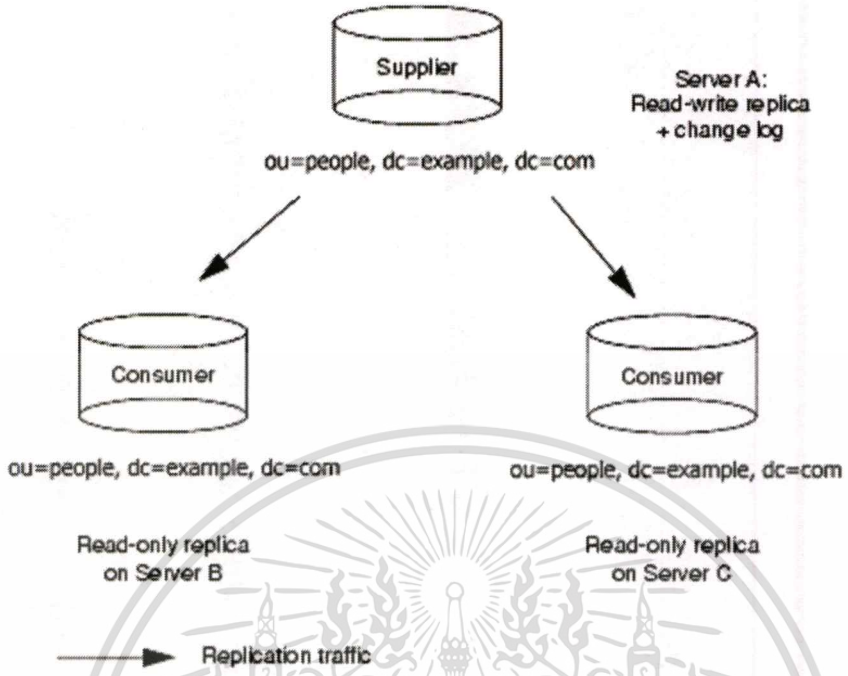
Master Replica นั้นจะถึงสร้างขึ้นเป็น first replica และในแต่ละ partition นั้นก็สามารถมีได้เพียง 1 Master Replica เท่านั้น และมีลักษณะดังนี้

- หน้าที่สำคัญ คือ การเพิ่มจำนวนของ Replica ตัวอื่น ๆ ไม่ว่าจะเป็น Replica read/write , replica read only ,filtered read/write หรือ read only replica และสุดท้าย Subordinate replica
- มีหน้าที่ยอมรับ และปรับปรุงเปลี่ยนแปลงข้อมูลเมื่อมีการเปลี่ยนแปลงของ object หรือ entry ใน Directory นั้น เช่น Client ส่ง request ใน Operation ต่าง ๆ เช่น Add, Delete, Modify เป็นต้น
- มีหน้าที่ควบคุมการจัดการในทุก ๆ partition ซึ่ง Client สามารถที่จะใช้ Master Replica ในการแยก หรือ รวม partition รวมทั้งการย้าย object และ Subtrees
- รองรับมาตรฐานของ X.500 เพื่อให้ Replica นั้นสามารถติดต่อกับ Directory Server ได้เมื่อ Client ส่งRequest Operation เช่น การสอบถามข้อมูล, การเพิ่มข้อมูล เป็นต้น

2. Read/Write หรือ Read only Replica

เป็นลักษณะของ Secondary Replica มีเพื่อให้ NDS นั้นสามารถให้บริการได้อย่างต่อเนื่อง ซึ่ง Client สามารถร้องขอใช้บริการได้ตลอดเวลา แต่มีข้อจำกัดว่า ถ้าเป็น Replica แบบ Read Only แล้ว Client ไม่สามารถที่จะทำการเปลี่ยนแปลข้อมูลกับ Replica นั้นได้ Client ต้องติดต่อกับ Replica ที่เป็น Read/Write จึงจะสามารถเปลี่ยนแปลงข้อมูลในไดเร็คทอรี่เซิฟเวอร์ได้

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.2 Read/Write Replica

ลักษณะของ replica read only มีดังนี้

- Client ไม่สามารถที่จะเปลี่ยนแปลงข้อมูลใน Directory Server ได้ เนื่องจาก Replica ชนิดนี้ Read - only
- เพื่อให้ partition นั้นสามารถให้บริการได้อย่างต่อเนื่อง ในกรณีที่ Master Replica ไม่สามารถให้บริการได้ Secondary Replica ก็สามารถให้บริการแทนได้
- เพื่อเพิ่มประสิทธิภาพให้กับ NDS เนื่องด้วย Client สามารถที่จะ Read/Write ใน Local Replica ได้

3. Filtered Read/Write and Filtered Read Only Replica

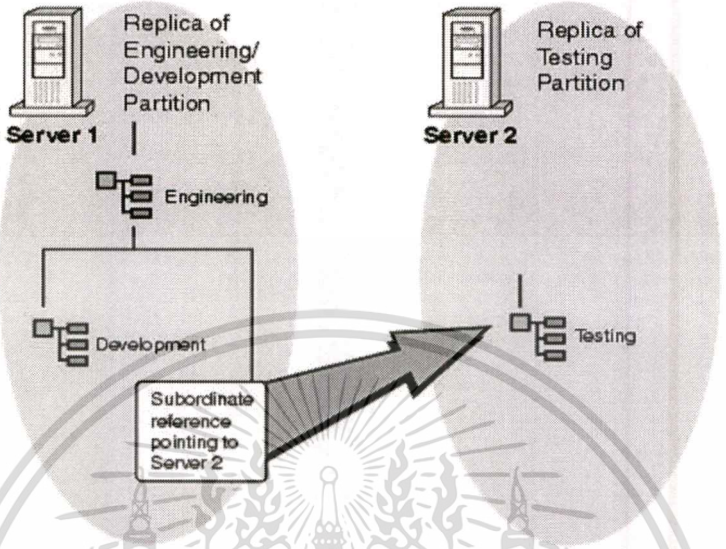
จะเป็น Sub ย่อยของ replica ใน tree นั้น มีไว้เพื่อให้ระบบสามารถทำงานได้ดีขึ้น เนื่องจาก เมื่อมีจำนวนผู้ใช้เพิ่มมากขึ้นใน partition นั้น ผู้บริหารไม่จำเป็นต้องแบ่ง partition ใหม่ ก็อาจใช้วิธีของ Filtered Read/Write หรือ Filtered Read Only Replica เพื่อให้บริการแก่ผู้ใช้ใน Sub นั้นก็ได้

4. Subordinate Replica

ใน Subordinate Replica นั้นก็จะเก็บข้อมูลที่เป็น “Partition Root Object” ซึ่ง Partition root object ก็คือ object ที่อยู่ top level โดย NDS ใช้ Subordinate Replica เพื่อเชื่อมโยงกับ Partition อื่น

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ดังในรูป ก็จะพบว่า ใน Root ของแผนก Engineering นั้นก็จะมี Subordinate Replica เพื่อเชื่อมโยงไปยัง Root ของ Partition “Testing” ใน Server 2 เป็นต้น



รูปที่ 4.3 Subordinate Replica

สรุป

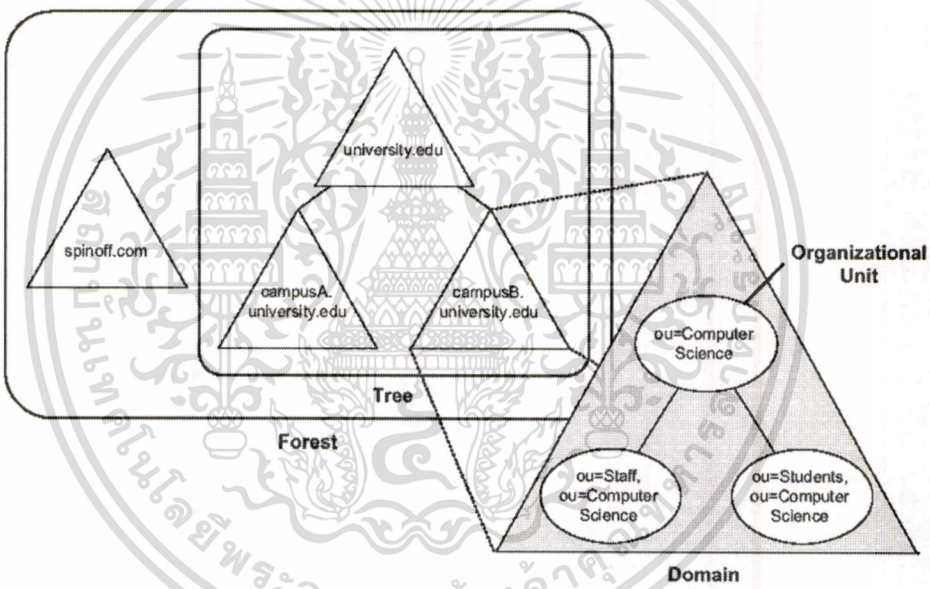
NDS หรือ eDirectory ของ Novell สามารถรอบรับการเปลี่ยนแปลงต่อระบบเครือข่ายในอนาคตได้ดี ซึ่งแบ่งโครงสร้างของ eDirectory ออกเป็น Partition และแต่ละ Partition ก็จะมี Replica ซึ่งอาจเป็น replica ประเภทใด ๆ ก็ได้ ล้วนแต่ส่งผลให้ระบบเครือข่ายสามารถทำงานได้ดีขึ้น นั้นก็คือลดปัญหาจากการใช้ Directory Server ที่เดียว โดย Client สามารถที่จะเข้าใช้บริการกับเครื่อง Replica ใด ๆ ก็ได้ในระบบฯ (ตามสิทธิที่ได้กำหนดไว้ ณ ตอนออกแบบระบบฯ) โดยที่ถ้าในแผนก หรือ partition นั้นมีผู้ใช้จำนวนมากแล้วก็สามารถที่จะแบ่งออกเป็น Filtered Replica (read /write or read only) ก็ได้เพื่อช่วยลดปริมาณข้อมูล หรือความต้องการที่จะใช้ Directory Service เพียงที่เดียว และสุดท้ายก็คือ Subordinate Replica จุดประสงค์โดยที่ทาง NDS นั้นได้มี Subordinate Replica ก็เพื่อให้สามารถเชื่อมโยงกับ Root Partition อื่น ๆ ของ Novell Directory Server เครื่องอื่นได้ นอกจากนั้นแล้ว NDS สามารถที่จะมี replica ได้สูงถึง 250 replica ใน 1 partition ซึ่งเมื่อพิจารณาแล้วจะพบว่ามีความยืดหยุ่นต่อการขนาดเครือข่ายอย่างมาก รวมถึงการ up-to-date ให้กับ replica เครื่องอื่นนั้น สามารถที่จะ filter เฉพาะ Attribute ที่มีการเปลี่ยนแปลงได้ ซึ่งเป็นข้อได้เปรียบของ NDS (ผลจากการศึกษามีอยู่เพียงรายเดียวที่สามารถทำการ Filter Attribute ได้) ทำให้ปริมาณข้อมูลที่ส่งกับเพื่อ up-to-date ระหว่าง replica มีจำนวนน้อย และไม่กระทบต่อ bandwidth ของระบบเครือข่ายแต่อย่างใด

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.2 Active Directory

Active Directory (AD)ซึ่งเป็นผลิตภัณฑ์ของทาง Microsoft นั้นประกอบด้วยองค์ประกอบรวมกัน 2 ส่วน คือ ส่วนที่เป็นเซอร์วิส เรียกว่า Active Directory Service และส่วนที่เป็นฐานข้อมูล เรียกว่า Active Directory Database ข้อมูลที่ถูกจัดเก็บนั้นจะมีลักษณะเป็น Object ซึ่งหลาย ๆ Object นั้นจะถูกรวมกันเป็นอยู่ใน Container หรือที่เรียกว่า Organization Unit (OU)

ในการเชื่อมโยงภายใน Domain นั้นก็จะมีลักษณะเป็น Tree เพื่อเก็บ Object ต่าง ๆ ภายในเครือข่ายนั้น เช่น เครื่อง Server, ชื่อ User Name ของผู้ใช้ระบบเครือข่าย และเมื่อเชื่อมโยงแต่ละ Domain เข้าด้วยกันแล้วก็จะเรียกว่าเป็น “Forest” ใน Domain นั้นเครื่องที่ run window 2000 server Active Directory จะเรียกว่าเป็น “Domain Controller”

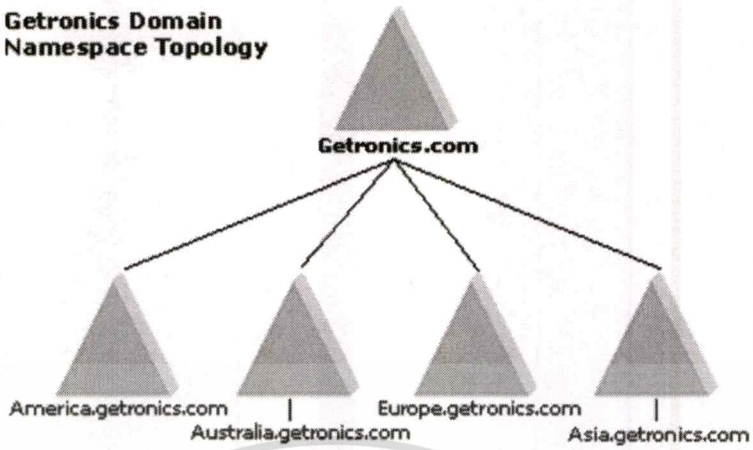


รูปที่ 4.4 แสดงความสัมพันธ์ภายใน Domain และการเชื่อมต่อที่เรียกว่า forest

ใน WindowNT นั้นจะ Implement แบบที่เป็น PDC และ BDC ซึ่ง PDC นั้นทำหน้าที่เป็น Domain Controller มีหน้าที่ในการรับ request จาก client ทั้งการอ่าน และเขียน หรือปรับปรุงข้อมูลใน Directory Server ซึ่งเมื่อ PDC ไม่สามารถให้บริการได้ก็จะต้องมีการ Promote ให้ BDC ทำหน้าที่แทน โดยกระบวนการดังกล่าวผู้บริหารเครือข่ายจะต้องเป็นผู้ดูแล และจัดการในลักษณะที่เป็น Manual Processing เท่านั้น

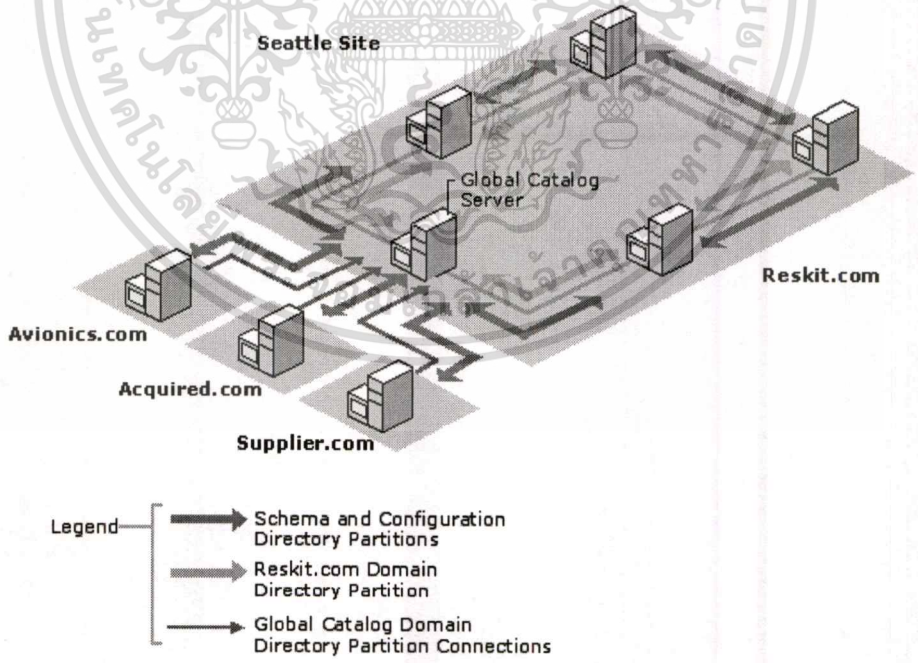
แต่ใน Window 2000 นั้น หรือเรียกว่า Active Directory นั้นจะเป็นลักษณะรูปแบบการเรพลิเคชั่นเป็นแบบที่เรียกว่า Multi-Master Replication หมายถึงว่า ในระบบเครือข่ายนั้น หรือใน Domain นั้นๆ จะสามารถมี Domain Controller ได้มากว่า 1 เครื่อง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้



รูปที่ 4.5 Domain Tree

โดย Client สามารถที่ จะอ่าน หรือเขียนข้อมูลจากเครื่อง Domain Controller ใดก็ได้ ทั้งนี้เพื่อเพื่อประสิทธิภาพให้กับระบบเครือข่าย, ช่วยลดภาระการให้บริการของเครื่อง Domain Controller หลัก เนื่องจาก Client สามารถเข้าใช้บริการจากเครื่อง Local Domain Controller จากรูปข้างต้นใน Domain ของ Getronics.com นั้นมี Domain ย่อย ๆ อยู่ 4 Domain ซึ่งใน Domain ของ Getronics.com และถ้าเชื่อมต่อหลาย ๆ Domain ก็จะเรียกว่า forest



รูปที่ 4.6 การเชื่อมหลาย ๆ Domain และ Global Catalog Server

จากรูปข้างต้นใน 1 forest นั้นจะมีเพียง 1 เครื่องที่ทำหน้าที่เป็น Global Catalog Server (Default นั้ก็จะเป็นเครื่องที่ถูกสร้างในครั้งแรกเมื่อตอนสร้าง Domain นี้ แต่ AD ก็สามารถที่จะ

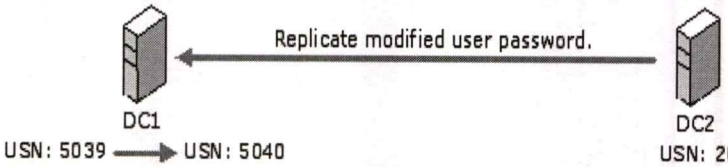
เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

สร้าง Domain ย่อย ๆ เพื่อช่วยให้การบริหาร จัดการเครือข่ายมีความง่าย และสะดวกมากขึ้น) Global Catalog เป็นแหล่งรวมค่าของ Attribute ที่สำคัญและใช้งานบ่อย ๆ ของแต่ละ Object โดย Attribute นี้มักถูกสอบถาม และเรียกค้นบ่อย ๆ จากผู้ใช้ หรือผู้บริหารระบบ

สรุป

ลักษณะการ replication กันนั้นจะเพิ่มความสามารถของ Global Catalog Server เพื่อช่วยลดปริมาณการรับส่งข้อมูลผ่าน WAN site เนื่องจากเส้นทาง หรือความเร็วในการส่งผ่าน WAN นั้นทำได้ช้า ซึ่งทำให้ประสิทธิภาพของ Active Directory ลดลง ดังนั้นทาง Microsoft จึงหาทางแก้ไขโดยให้เครื่องที่เป็นโดเมนคอนโทนเอร์ (Domain Controller) ที่ถูกสร้างขึ้นเป็นเครื่องแรกของ Domain ทำหน้าที่เป็น Global Catalog Server และเก็บ object ต่าง ๆ ที่มีการเรียกใช้งานบ่อย ๆ มาเก็บไว้ โดยเครื่องอื่นสามารถเข้ามา Access ได้(ตามสิทธิที่กำหนดไว้) แต่ Active Directory ก็มีข้อเสียที่ว่า เมื่อมีการ up-to-date ในแต่ละเครื่อง AD แล้ว จะต้องมีการ replication กันระหว่างเครื่องที่เป็น Domain Controller ซึ่งข้อมูลที่ up-to-date กันนี้ไม่สามารถที่จะ filter attribute เฉพาะที่เปลี่ยนแปลงได้ ต้องจังส่งข้อมูลทั้งหมดทั้ง Entry ซึ่งทำให้ปริมาณข้อมูลที่วิ่งอยู่บนระบบเครือข่ายมีจำนวนมาก กอปรการที่รูปแบบของ AD นั้นเป็นแบบ multi master จึงทำให้ผู้ใช้ระบบสามารถที่จะ up-to-date ข้อมูลใน AD ได้ทุ ก ๆ เครื่อง ดังนั้นอาจทำให้ปริมาณข้อมูลในระบบมีมาก และอาจส่งผลถึงประสิทธิภาพโดยรวมของระบบเครือข่ายต่ำลงก็เป็นได้

Object: usnCreated: 1746				Object: usnChanged: 2002		
Property	Value	Local USN	Version	Originating Time	Originating DSA	Originating USN
cn	James Smith	1746	1	1999-09-10 10:49.03	<DC1_GUID>	4711
userPassword	Secaucus2	2002	2	1999-09-10 11:53.29	<DC2_GUID>	2002
sAMAccountName	JSmith	1746	1	1999-09-10 10:49.03	<DC1_GUID>	4711
userPrincipalName	JSmith@reskit.com	1746	1	1999-09-10 10:49.03	<DC1_GUID>	4711



Object: usnCreated: 4711				Object: usnChanged: 5040		
Property	Value	Local USN	Version	Originating Time	Originating DSA	Originating USN
cn	James Smith	4711	1	1999-09-10 10:49.03	<DC1_GUID>	4711
userPassword	Secaucus2	5040	2	1999-09-10 11:53.29	<DC2_GUID>	2002
sAMAccountName	JSmith	4711	1	1999-09-10 10:49.03	<DC1_GUID>	4711
userPrincipalName	JSmith@reskit.com	4711	1	1999-09-10 10:49.03	<DC1_GUID>	4711

รูปที่ 4.7 กระบวนการ replication ใน Active Directory

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.1.3 Netscape

ลักษณะของ Netscape Directory Server จะเน้นสำหรับองค์กรที่ทำ e-commerce เนื่องจากได้มีการออกแบบให้สามารถ Interface กับ Database ของ Oracle ได้เป็นอย่างดี แต่ลักษณะของการ Replication นั้นมีรูปแบบ หรือโมเดล ที่เรียกว่า Multi Master Replica แต่อย่างไรก็ตาม ทาง Netscape ได้กำหนดจำนวนของ Replica ได้เพียง 2 ตัว นั่นก็คือ ในระบบเครือข่ายที่ใช้ Directory Service นั้นสามารถที่จะมี Directory Server ได้เพียง 2 เครื่อง โดยที่เครื่องแรกนั้นจะทำหน้าที่เป็น Master-Replica ซึ่ง Client สามารถที่จะทำ Operation ในการอ่าน-เขียน หรือปรับปรุงข้อมูลก็สามารถทำได้ในตัวนี้ และอีก 1 เครื่องจะทำหน้าที่เป็น Secondary-Replica โดยที่ Client ทำได้เพียงแต่การอ่านข้อมูล ไม่สามารถที่จะเขียน หรือ up-to-date ข้อมูล ใด ๆ ได้ ในลักษณะของการ Replication ดังกล่าวจะเรียกว่า Dual Master Replication

ปัญหาจากการที่เครื่องทั้ง 2 เครื่องจะไม่ Synchronized หรือกรณีที่ข้อมูลจะไม่สอดคล้องตรงกันนั้นมีโอกาสเป็นไปได้น้อย เมื่อเปรียบเทียบกับทางเทคนิคของ Multi-Master ที่สามารถอ่าน-เขียน ข้อมูลได้ที่ Replica ตัวใดก็ได้ แต่ทาง Netscape Directory นั้นมี Master Replica เครื่องเดียวเท่านั้นที่สามารถเปรียบแปลงข้อมูลในฐานข้อมูลของ Directory Database ในเฉพาะเครื่องที่เป็น Master Replica ได้เท่านั้น นอกจากนั้นยังมีลักษณะการทำงานที่แตกต่างจาก Active Directory คือสามารถแบ่งเป็น Partition ตามความต้องการ ซึ่งได้เพิ่มความยืดหยุ่นในการเพิ่ม หรือลดขนาดของระบบเครือข่ายได้ตามความเหมาะสมคล้ายกับลักษณะของทางของ NDS (Novell Directory Service) รวมทั้ง eDirectory และยังรองรับการทำ Virtually Unlimited นั้นก็คือรองรับการเพิ่มขึ้นของ Object ต่าง ๆ หรือข้อมูลที่จะเก็บใน Directory Database อย่างไม่จำกัด และในกรณีที่เป็น Master Replica ไม่สามารถให้บริการได้ เครื่องที่เป็น Secondary Replica ก็จะถูก Promote ให้ต้องทำหน้าที่แทน Master Replica ทันทีรวมถึงรองรับกับมาตรฐานของ LDAP v3 และ XML development tool

Netscape Directory Server นั้นไม่เหมาะสมกับ Enterprise เนื่องจากปัญหาในเรื่องของการรองรับ object ที่สามารถจัดเก็บใน Directory Database รวมถึงความยืดหยุ่นในการขยายหรือรวม partition ยังไม่มีเสถียรภาพมากนั้น แต่อย่างไรก็ตาม Netscape Directory สามารถที่จะ access ผ่านทาง web browser (Netscape browser) ซึ่งเป็น feature หนึ่งของทาง Netscape เพื่อเพิ่มความสะดวกให้แก่ผู้ที่ต้องการจะ Access Netscape Directory Server โดยตรง

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2. การเปรียบเทียบประสิทธิภาพของ Directory Service

ในการเปรียบเทียบประสิทธิภาพทางผู้ศึกษา ได้มีการกำหนดความสามารถของเครื่อง Server และ Clientที่จะทำการทดสอบไว้ดังนี้

ตารางที่ 4.1 คุณสมบัติ และลักษณะของเครื่อง Server และ Client ที่ใช้ในการทดสอบ

Server Machine	Client Machine
AMD Athion 750 Mhz	Intel PIII 500
RAM 256 MB	128 MB with OS window2000
SuSE Linux 7.0 (Kernel 2.2.16)	DirectoryMark 1.2 software
Windows 2000 Server SP1 Build 5.00.2195 (Active Directory Testing)	

4.2.1 การทดสอบ

มีการใช้ Script ดังต่อไปนี้เพื่อ simulate ข้อมูล

- dbgen.pl ใช้ในการ Generate Data เพื่อ Load เข้าสู่ฐานข้อมูลของ Directory Server
- scriptgen.pl ใช้ในการ Generate Transaction โดย scriptgen.pl นี้สามารถที่จะปรับเปลี่ยน parameter ตามที่ต้องการได้ เช่น จำนวนของ threads และจำนวนของ operation per threads เป็นต้น
- ใช้ Tool ของทาง DirectoryMark.exe เพื่อ simulate จำนวนของ Client

ขั้นตอนในการทดสอบ

1. การ Load มูลเข้า Directory Database โดยการใช้ Tool ดังในตารางนี้

ตารางที่ 4.2 การ Loading – Initial Directory

Directory Service	Tool	Time [m:ss]
Active Directory	Ldapmodify	33:43
edirectory (v. 8.5)	Ice	255:53
Netscape Directory Server	Ldif2db	2:23
Open LDAP	Slapadd	4:22
SecureWay Directory (IBM)	Ladpmodify	66:55

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

2. Messaging

ตารางที่ 4.3 ผลจากการทดสองการส่ง Messaging

Directory Service	Operations/s	Average Time(ms)	Max Time (ms)
Active Directory	637	1	24
eDirectory	204	4	76
Netscape Directory Server	606	1	269
Open LDAP	270	3	208
SecureWay Directory (IBM)	48	20	148

3. Address Look-up

ตารางที่ 4.4 ผลจากการทดสอบการทำ Address look-up

Directory Service	Operations/s	Average Time(ms)	Max Time (ms)
Active Directory	582	4	254
eDirectory	142	27	2826
Netscape Directory Server	356	8	2883
Open LDAP	128	25	10203
SecureWay Directory(IBM)	26	150	29695

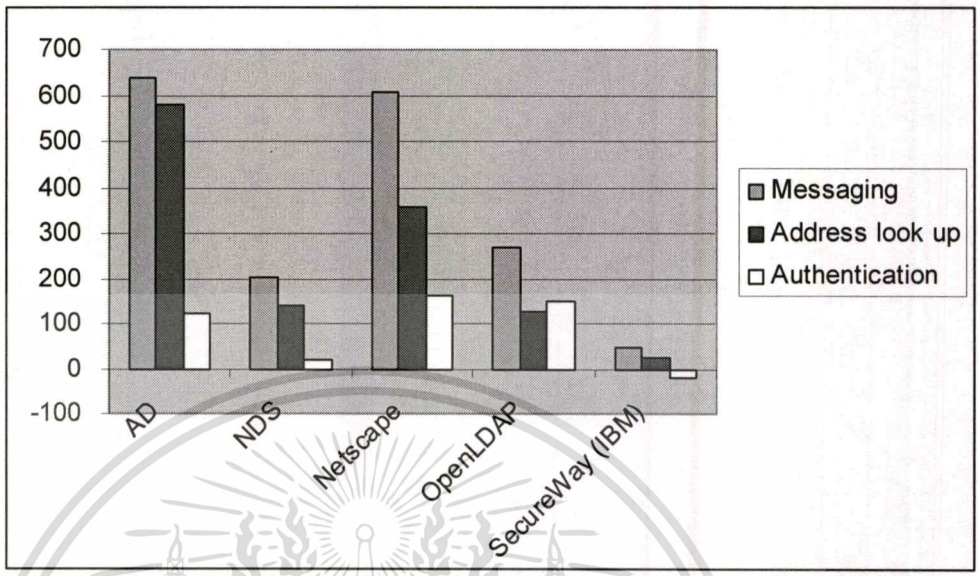
4. Authentication

ตารางที่ 4.5 ผลจากการทดสอบการ Authentication

Directory Service	Operations/s	Average Time(ms)	Max Time (ms)
Active Directory	123	2	136
eDirectory	20	90	449
Netscape Directory Server	162	5	372
Open LDAP	151	4	258
SecureWay Directory(IBM)	(20)	(61)	(1107)

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

4.2.2 สรุปผลการทดสอบ

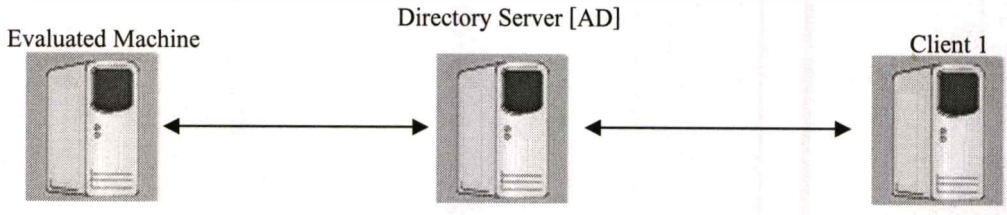


รูปที่ 4.8 กราฟแสดงผลจากการทดสอบประสิทธิภาพของ Directory Server

ผลการทดสอบ ดังกล่าวมีการ Simulate รายการ 10,000 entry จำนวน 3 ครั้ง แล้วนำมาหาค่าเฉลี่ย เมื่อวิเคราะห์จะพบว่า Active Directory และ Netscape Directory Server จะให้ประสิทธิภาพดีว่า แต่เมื่อพิจารณาทางด้านการ Authentication แล้วจะเห็นว่าทาง Openldap ก็มีประสิทธิภาพไม่ด้อยไปกว่าทาง Netscape Directory Server แต่จะมีประสิทธิภาพดีกว่าทาง Active Directory ด้วย

4.3 การทดสอบถึงประสิทธิภาพของระบบเครือข่าย จากการใช้เทคนิค Replication

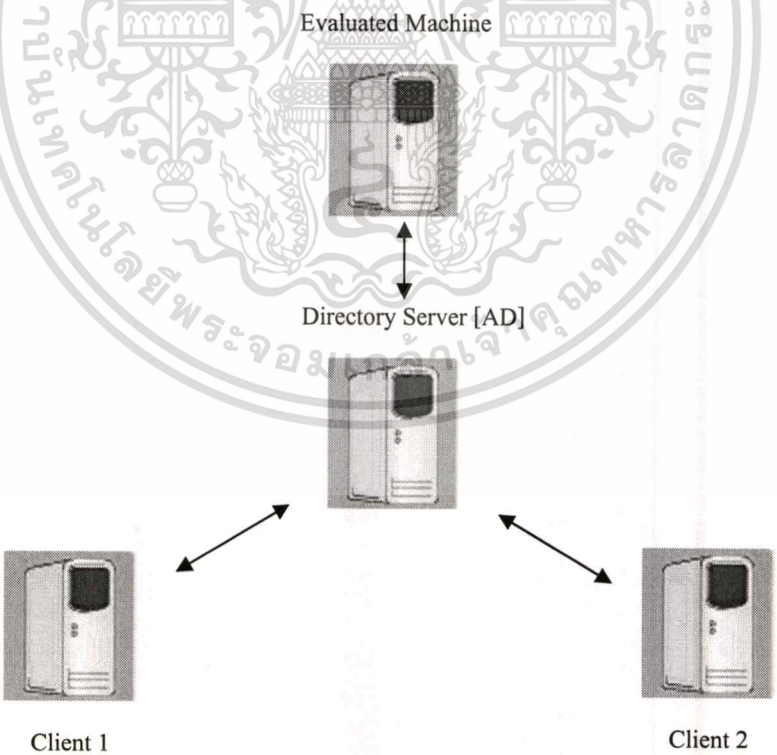
ในการทดสอบนี้ ได้มีการใช้ Tool ของทาง บริษัท Microsoft เพื่อทดสอบ โดยได้มีการจัดรูปแบบของการทดสอบดังนี้



รูปที่ 4.9 แสดงรูปแบบของการเชื่อมต่อคอมพิวเตอร์ที่ใช้ในการทดสอบแบบที่ 1

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

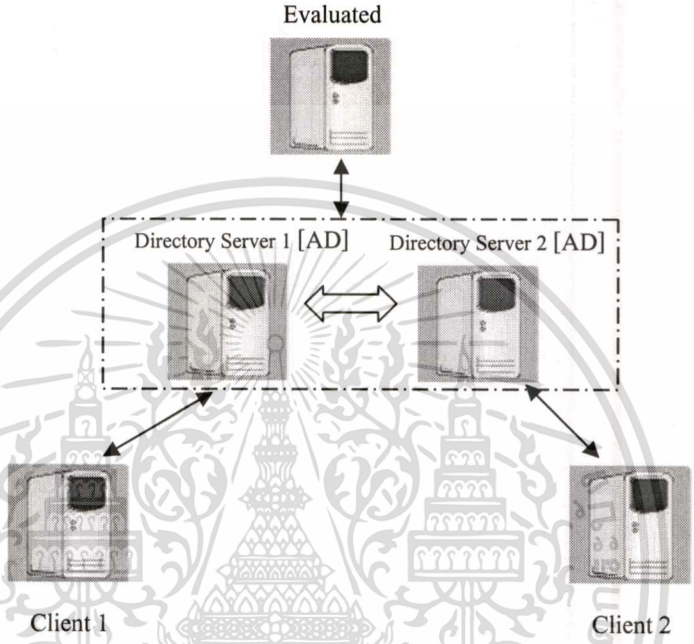
1. การทดสอบในกรณีที่มี Client 1 เครื่อง Server 1 เครื่อง และ Evaluated Client 1 เครื่อง ประกอบด้วย :
   - Client จำนวน 2 เครื่อง ทำหน้าที่ในการส่งค่าการ Operation ต่าง ๆ 1 เครื่อง และ Evaluated Client 1 เครื่อง นำมาจัดทำเป็นรายงานแสดงผล ซอฟแวร์ ที่ใช้คือ Windows 2000 workstation (SP2) และ Microsoft excel และ ActivePerl เพื่อใช้ในการ run Perl script สำหรับ Evaluated Client
   - Server ซึ่งใช้ในการทดสอบจำนวน 1 เครื่อง ซอฟแวร์ที่ใช้คือ ระบบปฏิบัติการ Windows 2000 Server ซึ่งได้ติดต่อเป็น Active Directory ทำหน้าที่เป็น Directory Server และ ActivePerl เพื่อใช้ในการ run Perl script
2. การทดสอบในกรณีที่มี Client 2 เครื่อง Server 1 เครื่อง และ Evaluated Client 1 เครื่อง โดยที่ Server จะส่งสัญญานให้ Client ทำการส่งค่า operation ต่าง ๆ ที่ได้กำหนดใน Script แล้วจะมีการเก็บค่าที่ได้จากการทดลองในแต่ละกรณีไว้ใน Evaluated Client โดยมีรูปแบบการเชื่อมต่อดังนี้



รูปที่ 4.10 แสดงรูปแบบของการเชื่อมต่อคอมพิวเตอร์ที่ใช้ในการทดสอบแบบที่ 2

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

การทดสอบในกรณีที่มี Client 2 เครื่อง Server 2 เครื่อง และ Evaluated Client 1 เครื่อง โดยที่ Server จะส่งสัญญานให้ Client ทำการส่งค่า และจำนวนขนาดในการทำ operation ต่าง ๆ ที่ได้กำหนดใน Script แล้วจะมีการเก็บค่าที่ได้จากการทดลองในแต่ละกรณีไว้ใน Evaluated Client โดยมีรูปแบบการเชื่อมต่อดังนี้



รูปที่ 4.11 แสดงรูปแบบของการเชื่อมต่อคอมพิวเตอร์ที่ใช้ในการทดสอบแบบที่ 3

ในการทดสอบนั้น เพื่อทำการเก็บค่าจากการ access ของ client โดยได้มีการ Modifies Script ของ Adtest.ats และ Stresstest.vbs ซึ่งเป็น VB script รวมถึงไฟล์ Runall.bat เป็นการกำหนดค่า parameter ให้กับ Stresstest.vbsโดยที่ Adtest.ads นั้นมีสิ่งที่สามารถ modifies ได้ดังนี้

- DN <mask>
- FILTER <filter>
- RATE <operations/second>
- SCOPE <scope>
- OP <option value>
- LOOP <loop type>
- TEST <function> or <class>
- RUN <function> or <class> (starts an independent thread)
- ATTR <mask>[:value]
- PWD <password>
- SID <sid cache mask>

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

- RANGE <mask>

และไฟล์ Stresstest.vbs ซึ่งมี parameter ดังนี้

- Runtime
- Testname
- Variation
- NumberOfWorkstations
- ThreadCount
- Debug

สรุปผลการทดลอง

จากการทดลองนั้นสามารถแบ่งได้เป็น 3 กรณี คือ กรณีแรกนั้น มี Client 1 เครื่อง ต่อเชื่อมกับ Directory Server 1 เครื่อง กรณีที่สอง นั้น นั้น มี Client 2 เครื่อง ต่อเชื่อมกับ Directory Server 1 และในกรณีที่สามนั้นมี Client 2 เครื่อง ต่อเชื่อมกับ Directory Server 2 โดยทั้ง 3 กรณี จะต้องต่อกับ เครื่อง Eval Client เพื่อเก็บ collection ต่าง ๆ นั้น จะได้ผลการ Base Search เป็นค่าของ Op/sec นั้น ใช้เวลา 5.35 และค่าของ cost เป็น 16.96 ซึ่งเท่ากันทั้ง 3 กรณี (ในเงื่อนไขของ Addition Attributes เป็น 10 และ 20 Attributes) แต่ค่าที่มีความแตกต่างอย่างเห็นได้ชัดคือค่าของการ Addition Attribute จำนวน 30 Attributes โดยมีค่า op/sec เป็น 5.31 , 5.88 , 5.31 ตามลำดับ และค่าของ Cost เป็น 13.44 , 19.28 , และ 13.44 ตามลำดับ นอกจากนั้นแล้วเมื่อพิจารณาเกี่ยวกับค่า Additional record returned มีค่า Cost เป็น 6.42 , 6.37 , 6.42 ในกรณีของ 10 , 100 user filter แต่ถ้าเป็น 1000 user filter มีค่าเป็น 10.83 , 40.09, 10.83 ตามลำดับ

	1 Client 1 Server				2 Client 1 Server				2 Client 2 Server			
	Op/sec	**%CPU**	**CxSw/sec**	**Cost**	**Op/sec**	**%CPU**	**CxSw/sec**	**Cost**	**Op/sec**	**%CPU**	**CxSw/sec**	**Cost**
Base Search	5.35	9.07	1037.37	16.96	5.35	9.07	1037.37	16.96	5.35	9.07	1037.37	16.96
Additional Attribute												
10 Attributes	5.32	4.09	529.78	7.68	5.32	4.09	529.78	7.68	5.32	4.09	529.78	7.68
20 Attributes	5.96	5.34	609.89	8.96	5.96	5.34	609.89	8.96	5.96	5.34	609.89	8.96
30 Attributes	5.31	7.14	731.57	13.44	5.88	11.33	891.63	19.28	5.31	7.14	731.57	13.44
Additional record returned												
10 user filter	6.42	6.36	703.96	9.92	6.37	22.67	1477.42	35.58	6.42	6.36	703.96	9.92
100 user filter	6.37	8.95	707.84	14.03	7.67	18.10	1318.19	23.60	6.37	8.95	707.84	14.03
1000 user filter	6.19	6.71	672.63	10.83	6.43	25.77	1560.13	40.09	6.19	6.71	672.63	10.83

รูปที่ 4.12 ผลสรุปการทดลองทั้ง 3 กรณี

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ซึ่งผลการทดลองสรุปได้ว่า เมื่อมีการเพิ่มจำนวน Directory Server เข้าไปในระบบเครือข่าย สามารถช่วยเพื่อให้การบริการที่มีต่อ Client นั้นมีประสิทธิภาพมากขึ้น และการ replication ในแต่ละ Directory Server นั้น ก็ไม่ได้ส่งผลให้ระบบมีประสิทธิภาพลดลงแต่ช่วยให้ Directory Server นั้นสามารถที่จะให้บริการได้อย่างต่อเนื่อง และ Client สามารถที่จะทำ Operation (read or write) กับเครื่อง Directory Server เครื่องใดก็ได้ ซึ่งส่งผลโดยรวมให้ Performance ของระบบดีขึ้น

แต่อย่างไรก็ตามในการทดลองครั้งนี้ก็มีข้อจำกัดไม่ว่าจะเป็น environment ต่าง ๆ เช่น จำนวนของ Client, ปริมาณของข้อมูลที่วิ่งอยู่บนระบบเครือข่าย เพื่อให้ได้ผลตามวัตถุประสงค์ที่ตั้งไว้ ดังนั้นหากผู้ที่สนใจทดสอบจะนำไปใช้ทดสอบกับระบบเครือข่ายจริงนั้น อาจจะต้องศึกษาเพิ่มเติม และกำหนด parameter ต่าง ๆ ให้เหมาะสมกับ environment นั้น ๆ โดยเพื่อให้ได้ผลที่ใกล้เคียง หรือตรงตามสภาพแวดล้อมนั้นด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บทที่ 5
สรุปผลการศึกษาและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

จากการได้ศึกษา การทำงานของไดเร็คทอรี่เซอร์วิสมาช่วยนั้น จะช่วยเพิ่มความสะดวกและรวดเร็วในการัดการมากขึ้น ลดความซ้ำซ้อนในการจัดเก็บข้อมูล รวมถึงความง่ายต่อการค้นหาข้อมูล หรืออุปกรณ์ต่าง ๆ ที่มีให้บริการอยู่ในระบบฯ

ระบบการจัดการบริหารแบบกระจาย Distributed Management System ก็ทำให้ลดภาระหน้าที่ และความรับผิดชอบของผู้บริหารเครือข่ายโดยการโอนอำนาจให้กับส่วนงานต่าง ๆ เพื่อบริหารจัดการเอง รวมถึงการนำกระบวนการเรพลิเคชันมาใช้กับเครื่องไดเร็คทอรี่เซอร์วิสน่าจะส่งผลให้ระบบสามารถที่จะให้บริการได้อย่างต่อเนื่อง เพิ่มความคงทนให้กับระบบฯ

แต่เนื่องจากปัจจุบันมีผู้ให้บริการทางด้าน ไดเร็คทอรี่เซอร์อยู่หลายราย ดังนั้น ได้ในเลือกใช้ก็จำเป็นต้องพิจารณาทั้งทางด้าน ประสิทธิภาพการทำงานของไดเร็คทอรี่เซิฟเวอร์เอง รวมถึงการความสามารถทางด้านอื่น ๆ ของไดเร็คทอรี่เซิฟเวอร์นั้นก่อนที่จะนำมาใช้กับระบบเครือข่าย

ในการเลือกพิจารณาใช้ Directory Server ของทางบริษัทใดจำเป็นที่จะต้องทราบข้อมูลอื่นประกอบในการตัดสินใจ เช่น สนับสนุนกับโปรโตคอล LDAP v3 หรือมีเครื่องมืออะไรบ้างในการพัฒนา Directory Service สิ่งดังกล่าวก็มีความสำคัญเช่นกัน กอปรการที่จะนำไดเร็คทอรี่เซอร์เวอร์มาใช้นั้น ควรจะมีการศึกษาถึงการกำหนด สกีมา รวมถึงการออกแบบ โทโปโลยี ก็มีส่วนสำคัญที่ทำให้สามารถใช้งานไดเร็คทอรี่เซอร์วิส ได้อย่างมีประสิทธิภาพ และคุ้มค่าต่อการลงทุนในอนาคตอีกด้วย

5.2 ข้อเสนอแนะ

ก่อนที่จะมีการนำไดเร็คทอรี่เซอร์วิสมาใช้ภายในองค์กร ควรที่จะมีการวิเคราะห์ ออกแบบโครงสร้างขององค์กร และระบบเครือข่าย โดยมองภาพรวม และโอกาสในการขยายระบบเครือข่าย นอกจากนั้นยังควรพิจารณา Applicationที่จะนำมาใช้งานร่วมกับไดเร็คทอรี่เซอร์วิส และที่สำคัญคือ ประสิทธิภาพ ของไดเร็คทอรี่เซอร์วิส ควรที่จะได้รับการทดสอบประสิทธิภาพเพื่อให้มั่นใจได้ว่า สามารถรองรับกับการขยายตัวของระบบเครือข่าย รวมถึงรองรับกับปริมาณข้อมูลที่จะมีการใช้งานก็เป็นปัจจัยสำคัญในการพิจารณาเลือกชนิด รูปแบบ รวมถึง vender ที่จะให้บริการในด้านนี้ด้วย

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

บรรณานุกรม

ชัยนันท์ กมลวดี. 2546. **เจาะลึก เพิ่มพลังเครือข่ายเต็มพิกัดด้วย Directory Service.** กรุงเทพฯ: เอส.พ.ซี. บุ๊คส์

สุทธา ศรีวิริยาจารย์ 2545. **Microsoft Windows2000 Server ภาคปฏิบัติสำหรับผู้ดูแลเน็ตเวิร์ก** กรุงเทพ: ซีเอ็ดยูเคชั่น.

Active Directory Performance Tool. [Online]. Available: Http://www.microsoft.com

Adamou,M., Anthomelidis,D., Antonis, 2539 K. **Dynamic Load Balancing for Web Clusters.** System Design Research Lab (SDRL), Department of Computer & Information Science. Univertsity. of Pennsylvania.

Coulouris ,George, Dollimore, Sean, Kindberg,Tim. 1994. **Distributed System.** 2nd ed.

"Directory Primer" September 2000. Novell Document AppNotes.

DirectoryMark is a Trademark of Mindcraft, Inc. and Netscape Communications Corporation. , [Online]. Available: Http://www.DirectoryMark1.2.1-Bin-NT\DirectoryMark1.2.1-Bin-NT\Doc\overview.html

Klasen,Norbert 2001. **"Directory Service for Linux in Comparison with Novell and Microsoft Active Directory."** Diploma –infomatiker, Reinisch-westf" Alischete Technische Hochchule Aachen,Germany.

Novell eDirectory Design and Implementation. [Online]. Available: Http://www.novell.com

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ภาคผนวก

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

Runall.bat

```
rem 19 Jan 2001
rem
rem If Jumppoint is specified goto there
rem
if NOT (%1) == () GOTO %1
rem
rem The rem'd lines below mark tests where the function is still missing in the ATS files
rem
:sg0
stresstest.vbs 300 inter inter0 all 20
sleep.vbs 20
stresstest.vbs 300 network network all 20
sleep.vbs 20
stresstest.vbs 300 batch batch all 20
sleep.vbs 20
GOTO PWD
:g5
5ggroups.bat
:sg5
stresstest.vbs 300 inter inter5 all
:g10
5-10ggroups.bat
:sg10
stresstest.vbs 300 inter inter10 all
:g25
11-25ggroups.bat
:sg25
stresstest.vbs 300 inter inter25 all
sleep.vbs 200stresstest.vbs 300 network group25_net all
sleep.vbs 200
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

stresstest.vbs 300 batch group25_bat all

:g50

25-50ggroups.bat

:sg50

stresstest.vbs 300 inter inter50 all

sleep.vbs 200

stresstest.vbs 300 network group50_net all

sleep.vbs 200

stresstest.vbs 300 batch group50_bat all

:g75

50-75ggroups.bat

:sg75

stresstest.vbs 300 inter inter75 all

sleep.vbs 200

stresstest.vbs 300 network group75_net all

sleep.vbs 200

stresstest.vbs 300 batch group75_bat all

:g100

75-100ggroups.bat

:sg100

stresstest.vbs 300 inter inter100 all

sleep.vbs 200

stresstest.vbs 300 network group100_net all

sleep.vbs 200

stresstest.vbs 300 batch group100_bat all

sleep.vbs 200

:pwd

stresstest.vbs 300 pwd pwd all 20sleep.vbs 20

:B2

stresstest.vbs 300 b2 b2 all

sleep.vbs 20

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
:B3
stresstest.vbs 300 b3 b3 all
sleep.vbs 20
:A1_26attr
rem stresstest.vbs 300 a1_26attr a1_26attr all
rem sleep.vbs 20
:A1_52attr
rem stresstest.vbs 300 a1_52attr a1_52attr all
rem sleep.vbs 20
:A1_78attr
rem stresstest.vbs 300 a1_78attr a1_78attr all
rem sleep.vbs 20
:A18
rem 1 client 20 thread for our 20 roots
stresstest.vbs 300 a18 a18 1 20
sleep.vbs 20

:ADDRES
rem stresstest.vbs 300 addres addres all
rem sleep.vbs 200
:ADDUNI
rem stresstest.vbs 300 adduni adduni all
rem sleep.vbs 200
:ADDACC
rem stresstest.vbs 300 addacc addacc all
rem sleep.vbs 200:MEMACC
rem stresstest.vbs 300 memacc memacc all
rem sleep.vbs 200
:D1
rem stresstest.vbs 300 d1 d1 all
rem sleep.vbs 200
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

```
:D2
rem 1 client 20 threads
stresstest.vbs 300 d2 d2 1 20
sleep.vbs 20
:DELACC
rem stresstest.vbs 300 delacc delacc all
rem sleep.vbs 200
:L1
stresstest.vbs 300 l1 l1 all
sleep.vbs 20
:L1_10attr
stresstest.vbs 300 l1_10attr l1_10attr all
sleep.vbs 20
:L1_20attr
stresstest.vbs 300 l1_20attr l1_20attr all
sleep.vbs 20
:L1_30attr
stresstest.vbs 300 l1_30attr l1_30attr all
sleep.vbs 20
:L1_25ace
rem stresstest.vbs 300 l1_25ace l1_25ace all
rem sleep.vbs 200
:L1_50ace
rem stresstest.vbs 300 l1_50ace l1_50ace allrem sleep.vbs 200
:L1_75ace
rem stresstest.vbs 300 l1_75ace l1_75ace all
rem sleep.vbs 200
:L5
stresstest.vbs 300 l5 l5 all
sleep.vbs 20
:L5_25ace
```

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

มาตรฐานเกี่ยวกับโพรโตคอล X.500

- X.500 Overview of concepts, models and services
- X.501 Models
- X.509 Authentication framework
- X.511 Abstract service definition
- X.518 Procedures for distributed operation
- X.519 Protocol specifications
- X.520 Selected attribute types
- X.521 Selected object classes
- X.525 Replication
- X.530 Use of systems management for administration of the Directory

มาตรฐานเกี่ยวกับโพรโตคอล LDAP v3

- RFC 2251: "Lightweight Directory Access Protocol (v3)" includes the directory information model and describes the format of the LDAP PDUs.
- RFC 2252: "Attribute Syntax Definitions" defines how attribute types and object classes are to be constructed.
- RFC 2253: "UTF-8 String Representation of Distinguished Names".
- RFC 2254: "A String Representation of LDAP Search Filters".
- RFC 2255: "The LDAP URL Format" specifies how to represent references to directory data as a Universal Resource Locater (URL).
- RFC 2256: "A Summary of the X.500(96) User Schema for use with LDAPv3" lists which common X.500 schema elements should be supported by LDAP implementations.

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้

ประวัติผู้เขียน

ชื่อ – นามสกุล	นายอรรถพล มุกดาประวัติ
วัน/เดือน/ปีเกิด	1 พฤศจิกายน พ.ศ. 2518
ประวัติการศึกษา	ปริญญาตรี มหาวิทยาลัย ศรีนครินทรวิโรฒ ประสานมิตร
ประวัติการทำงาน	พนักงานปฏิบัติการคอมพิวเตอร์ ธนาคารออมสิน จนถึงปัจจุบัน

เอกสารนี้เป็นเอกสารที่สงวนไว้สำหรับการใช้งานเพื่อการศึกษาเท่านั้น ไม่อนุญาตให้นำไปใช้ประโยชน์ด้านการค้า ไม่ว่ากรณีใดๆทั้งสิ้น อีกทั้งห้ามมิให้ดัดแปลงเนื้อหา และต้องอ้างอิงถึงเจ้าของเอกสารทุกครั้งที่มีการนำไปใช้