

L2VPN และเครือข่ายนิยามบนซอฟต์แวร์สำหรับเครือข่ายเพื่อการศึกษา

นางสาวแพรวา มณีศรี

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

ปีการศึกษา 2557


L2 VPN and SDN UniNet Express Lane

Ms. Praewa Maneesri

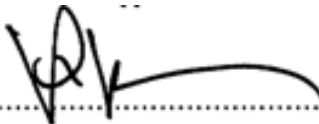
A PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR THE DEGREE OF BACHELOR OF COMPUTER ENGINEERING  
DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING  
FACULTY OF ENGINEERING  
KING MONGKUT'S UNIVERSITY OF TECHNOLOGY NORTH BANGKOK  
ACADEMIC YEAR 2014

ปริญญานิพนธ์เรื่อง : L2VPN และเครือข่ายนิยามบนซอฟต์แวร์สำหรับเครือข่ายเพื่อ  
การศึกษา  
ชื่อ : นางสาวแพรวา มณีศรี  
สาขาวิชา : วิศวกรรมคอมพิวเตอร์  
ภาควิชา : วิศวกรรมไฟฟ้าและคอมพิวเตอร์  
คณะ : วิศวกรรมศาสตร์  
อาจารย์ที่ปรึกษา : รองศาสตราจารย์ ดร.วรา วราวิทย์  
ปีการศึกษา : 2557

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ อนุมัติให้  
ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต  
สาขาวิชาวิศวกรรมคอมพิวเตอร์

  
.....  
(ผู้ช่วยศาสตราจารย์ ดร. นกคณ วิวัชรโกเศศ)

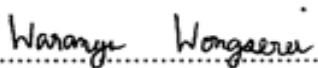
หัวหน้าภาควิชาวิศวกรรมไฟฟ้า  
และคอมพิวเตอร์

  
.....  
(รองศาสตราจารย์ ดร.วรา วราวิทย์ )

ประธานกรรมการ

  
.....  
(รองศาสตราจารย์ ดร.นุช ไชยรัตน์)

กรรมการ

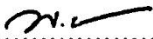
  
.....  
(ผู้ช่วยศาสตราจารย์ ดร.วรัญญู วงษ์เสรี)

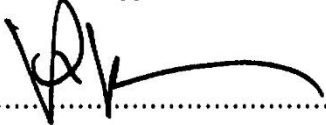
กรรมการ


ลิขสิทธิ์ของภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์ คณะวิศวกรรมศาสตร์  
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

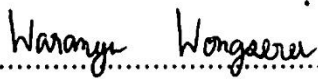
Project Report Title : L2 VPN and SDN UniNet Express Lane  
Name : Ms. Praewa Maneesri  
Major Field : Computer Engineering  
Department : Electrical and Computer Engineering  
Faculty : Engineering  
Project Advisor(s) : Assoc. Prof. Dr. Vara Varavithya  
Academic Year : 2014

Accepted by the Faculty of Engineering, King Mongkut's University of Technology  
North Bangkok in Partial Fulfillment of the Requirements for the Degree of Bachelor of  
Computer Engineering

  
.....  
(Asst. Prof. Dr. Noppadol Wiwatcharagoses)      Chairperson of Department of Electrical  
and Computer Engineering

  
.....  
(Assoc. Prof. Dr. Vara Varavithya)      Chairperson

  
.....  
(Assoc. Prof. Dr. Nachol Chaiyaratana)      Member

  
.....  
(Asst. Prof. Dr. Waranyu Wongseree)      Member

Copyright of the Department of Electrical and Computer Engineering, Faculty of Engineering  
King Mongkut's Institute of Technology North Bangkok

## บทคัดย่อ

ปัจจุบันนี้การติดต่อสื่อสารผ่านช่องทางอินเทอร์เน็ตเป็นสิ่งจำเป็นมากขึ้นในชีวิตประจำวัน แต่อินเทอร์เน็ตที่เราใช้กันอยู่ทุกวันนี้มี Traffic หลากหลายบนเครือข่าย เมื่อต้องการใช้งานอินเทอร์เน็ตทางด้านการศึกษาพบว่าทำให้เกิดความล่าช้าและมีประสิทธิภาพต่ำ จึงมีเครือข่ายเพื่อการศึกษาวิจัย UniNet เกิดขึ้นเพื่อสนับสนุนกิจกรรมทางศึกษา โดยไม่ต้องแย่งช่องทางกับอินเทอร์เน็ตทั่วไปและเชื่อมกับเครือข่าย REN (Research & Education Network) ทั่วโลก โดยปริญาณิพนธ์นี้ได้จัดทำแบบจำลอง VPN (Virtual Private Network) โดยใช้เราเตอร์ Cisco 3600 ทำงานในลักษณะเซฟเวอร์และไคลเอนต์ และใช้โปรโตคอล PPTP (Point-to-Point) สร้างอุโมงค์ข้อมูล (Tunnel) ศึกษาการใช้กระบวนการ Federation service เพื่อใช้ยืนยันตัวตนของผู้ใช้งานให้เข้าถึงแหล่งข้อมูลข้ามระบบเครือข่าย เช่น การใช้งานเครือข่าย eduraom และศึกษาสถาปัตยกรรม Science DMZ เป็นสถาปัตยกรรมที่ถูกพัฒนาขึ้นใหม่สนับสนุนงานด้านวิทยาศาสตร์โดยเฉพาะเนื่องจากการทดลองทางวิทยาศาสตร์มีข้อมูลขนาดใหญ่ และต้องการการถ่ายโอนข้อมูลที่รวดเร็วและปลอดภัยสูง ซึ่งช่วยลดปัญหาการสูญหายของข้อมูล และเชื่อมต่อเข้ากับ REN backbone เพื่อสามารถนำข้อมูลไปต่อยอดได้ในอนาคต พบว่า L2VPN ทำให้ข้อมูลรับ-ส่งกันผ่าน Tunnel ที่มีความปลอดภัยและมีความยืดหยุ่นสูง Federation Service ช่วยให้ผู้ใช้และผู้ใช้งานและรหัสผ่านเพียงชุดเดียวใช้งานข้ามเครือข่ายได้ และ Science DMZ ช่วยเรื่องถ่ายโอนข้อมูลด้านวิทยาศาสตร์ขนาดใหญ่ และมีเครื่องมือตรวจสอบเครือข่ายที่ดีสามารถแก้ไขปัญหาได้ง่าย

## **Abstract**

At present, the communication via the internet is more important in everyday life but there are a lot of traffics on the internet and its poor performance when using the same network for research and education. Thailand's Research and Education Network, the UniNet supports all activities of Research and Education without using the same traffic as general-purpose network and it connects to other REN (Research and Education Network) around the world. This project is making model of VPN by Cisco 3600 router for server and client and using PPTP protocol for a tunnel. Federation service is the technology for using the same username and password to identity, authentication and authorization to access the resources in a different system like using eduroam. Science DMZ, a scalable network design model for high-performance science data transfers. It's reducing the packet loss and connecting to REN backbone for the development in the future. This project found that L2VPN lets every campus transfer a big data with high security and capable bandwidth by a special tunnel. Federation Service let everyone can use the same username and password to access the resource in different system. And Science DMZ is a network model for big data transfer with the best measurement tool and simply troubleshooting.

## กิตติกรรมประกาศ

โครงการนี้สำเร็จได้ด้วยดีเนื่องจากได้รับความกรุณาจากบุคคลหลายท่าน ในที่นี้ขอขอบพระคุณ รองศาสตราจารย์ ดร. วรา วราวิทย์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผู้ซึ่งสละเวลาให้ความรู้และคำแนะนำและข้อคิดเห็นต่าง ๆ ทั้งด้านการศึกษาและวิจัยมาโดยตลอดการทำวิทยานิพนธ์ ขอขอบคุณห้องบริการคอมพิวเตอร์ ห้องเน็ตเวิร์ค ห้องซอฟต์แวร์และเจ้าหน้าที่ภาควิชาวิศวกรรมไฟฟ้าและคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ที่ได้เอื้อเฟื้อวัสดุอุปกรณ์และสถานที่สำหรับทำวิทยานิพนธ์นี้ และขอบคุณเพื่อน ๆ ที่ได้ให้ความช่วยเหลือในการทำวิทยานิพนธ์

ขอกราบขอบพระคุณบิดามารดาและครอบครัว ผู้ที่คอยสนับสนุน ให้กำลังใจ และให้การศึกษามีค่า ขอขอบคุณครูบาอาจารย์ทุกท่านที่เคยได้อบรมสั่งสอนประสิทธิ์ประสาทความรู้ทั้งทางด้านวิชาการและการดำเนินชีวิต ขอขอบพระคุณเป็นอย่างสูง

สุดท้ายนี้ผู้จัดทำหวังเป็นอย่างยิ่งว่าวิทยานิพนธ์ฉบับนี้จะเป็นประโยชน์สูงสุดต่อผู้ที่สนใจไม่มากนักน้อย

แพรวา มณีสรี

## สารบัญ

	หน้า
บทคัดย่อภาษาไทย	จ
บทคัดย่อภาษาอังกฤษ	ฉ
กิตติกรรมประกาศ	ช
สารบัญตาราง	ฌ
สารบัญภาพ	ญ
บทที่ 1. บทนำ	1
บทที่ 2. L2VPN และ SDN ทางด่วนข้อมูล UniNet	3
2.1 การส่งข้อมูล	3
2.2 เทคโนโลยี VPN	7
2.3 เทคโนโลยี MPLS	11
2.4 DMZ	14
บทที่ 3. สถาปัตยกรรมของระบบบริการข้อมูล	17
3.1 การทำงานของ Federation Service	17
3.2 เครือข่ายเพื่อการศึกษาวิจัยและบริการบนเลเยอร์ 2	25
3.3 สถาปัตยกรรม Science DMZ	32
บทที่ 4. การทดลองแบบจำลองระบบและการทดสอบ	41
4.1 ผลการทดลองและผลการศึกษา	41
บทที่ 5. สรุปผลการทดลองแบบจำลองระบบและการทดสอบ	45
เอกสารอ้างอิง	48
ประวัติผู้แต่ง	50



## สารบัญตาราง

ตารางที่	หน้า
3-1 ความแตกต่างระหว่าง L2VPN และ L3VPN	29
3-2 ประโยชน์ L2VPN และ L3VPN	30

## สารบัญภาพ

ภาพที่	หน้า
2-1 แบบจำลอง OSI 7 เลเยอร์	4
2-2 ตัวอย่าง MAC Address Table	7
2-3 การรับส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ตผ่านอุโมงค์ข้อมูล (Tunnel)	8
2-4 ตัวอย่างการเชื่อมโยงเครือข่ายส่วนตัวเสมือน VPN	9
2-5 Label Edge Router และ Label Switching Router ในเครือข่าย MPLS	12
2-6 Label Switched Path (LSP) ใน MPLS	12
2-7 ตัวอย่างเครือข่าย MPLS	13
2-8 Zoning ในระบบเครือข่าย	15
2-9 การแบ่ง Zoning	16
3-1 ลักษณะการทำงานของ Federation Service	21
3-2 การใช้งานเครือข่ายของผู้ใช้สถาบันอื่นมาใช้งานที่มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ	23
3-3 การใช้งานเครือข่ายของผู้ใช้มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือไปใช้งานที่สถาบันอื่น	24
3-4 แผนภาพที่การบริการเครือข่ายเพื่อการศึกษาวิจัยที่ครอบคลุมทั้งประเทศ	26
3-5 การเชื่อมต่อเครือข่ายของ UniNet กับเครือข่าย REN อื่น ๆ	27
3-6 Topology VPN เบื้องต้นโดยใช้โปรโตคอล PPTP	28
3-7 simple science DMZ diagram	37
3-8 supercomputer center network	38
3-9 big data site	39
4-1 แสดง traceroute ของการเชื่อมต่อ VPN จาก remote client มายัง server	41
4-2 แสดง traceroute ของการเชื่อมต่อ VPN จาก server มายัง remote client	42

## สารบัญภาพ (ต่อ)

ภาพที่	หน้า
4-2 แสดงการ Ping จาก PPTP server ไปหา Client	42
4-3 แสดง trace route ของอุโมงค์ข้อมูลจาก Server ไปหา Client	43

## บทที่ 1

### บทนำ

ในปัจจุบันนี้ปฏิเสธไม่ได้เลยว่าการติดต่อสื่อสารผ่านทางอินเทอร์เน็ต ได้เข้ามามีบทบาทในชีวิตประจำวันของทุกคนมากขึ้นเรื่อย ๆ ไม่เพียงแต่ใช้สำหรับการติดต่อสื่อสารเท่านั้นแต่ยังใช้งานอินเทอร์เน็ต เพื่อความบันเทิง ฟังเพลง ดูภาพยนตร์ การสืบค้นข้อมูลความรู้ หรือการดาวน์โหลดต่าง ๆ ซึ่งเห็นได้ว่าการใช้งานอินเทอร์เน็ตนั้นมี traffic ที่หลากหลายใช้งานอยู่บนเครือข่าย ในส่วนของภาคการศึกษาได้มีการใช้งานอินเทอร์เน็ตมากขึ้น แต่ถ้าใช้งานร่วมกันกับการใช้งานอินเทอร์เน็ตทั่วไปพบว่าจะต้องแย่งช่องทางกันทำให้เกิดความล่าช้าและคุณภาพไม่ดี จึงมีการจัดตั้งเครือข่ายเพื่อการศึกษาวิจัยขึ้นโดยเฉพาะคือ UniNet เพื่อสนับสนุนในส่วนของการศึกษาวิจัย หรือการจัดกิจกรรมการเรียนการสอนที่ต้องการใช้แบนด์วิดสูง เช่น การใช้งานฐานข้อมูลเพื่อการค้นคว้าและการใช้ทรัพยากรทางการศึกษาร่วมกัน ระบบการประชุมและจัดการเรียนการสอนทางไกล ซึ่งจะเป็ช่องทางสำคัญที่จะช่วยให้คณาจารย์ นักวิจัย นักศึกษา สามารถใช้เครือข่าย UniNet เพื่อดำเนินกิจกรรมทางการศึกษาได้โดยไม่มี Traffic แบบอื่นเข้ามาเจือปนจึงทำให้เครือข่ายมีประสิทธิภาพและมีความปลอดภัยระหว่างเน็ตเวิร์คสูง

เครือข่ายที่มีการสร้างและจัดตั้งขึ้นมาเพื่อการศึกษาและวิจัยนั้น จะถูกเรียกกันในนามของ Research and Education Network (REN) โดยปัจจุบันหลากหลายประเทศต่าง ๆ ทั่วโลกได้มีการสร้างและจัดตั้งขึ้นมาโดยเฉพาะในทุก ๆ ประเทศและในส่วนของประเทศไทยนั้น UniNet ได้สร้างและจัดตั้งกลุ่มถูกเรียกกันในนามของ ThaiREN เพื่อที่จะสนับสนุนและประสานความร่วมมือระหว่างหน่วยงานทางการศึกษาวิจัยทั้งในประเทศและต่างประเทศ รวมถึงการเชื่อมต่อเข้ากับเครือข่ายเพื่อการศึกษาวิจัยอื่น ๆ รวมกลุ่มกันจนเกิดเป็น Community ทางด้านการศึกษาและวิจัย เช่น Internet2 จะเชื่อมโยงมหาวิทยาลัยชั้นนำของสหรัฐอเมริกา, TEIN4 จะเชื่อมโยงสถาบันการศึกษาและวิจัยในทวีปเอเชียและยุโรป, APAN จะเชื่อมโยงสถาบันการศึกษาวิจัยในทวีปเอเชียแปซิฟิก เป็นต้น

ในปฏิญานีพนธ์นี้จะใช้การบริการ Layer2 VPN ของ UniNet ที่ให้การสนับสนุนการบริการเครือข่ายด้านการศึกษาและวิจัยของสถาบันการศึกษาและมหาวิทยาลัยต่าง ๆ โดยการรับส่งข้อมูลต่าง ๆ ต้องมีความปลอดภัยและความยืดหยุ่นสูง ซึ่งการเข้าใช้งานทรัพยากรทางการศึกษาร่วมกันหรือข้ามสถาบัน โดยมีชื่อผู้ใช้งานและรหัสผ่านเดียวกันทำได้โดยกระบวนการ Federation Service มีการศึกษาวิจัยถึงรูปแบบการทำงานสถาปัตยกรรม Science DMZ เป็นสถาปัตยกรรมที่ได้ยอมรับและใช้กันอย่างแพร่หลายในประเทศสหรัฐอเมริกาสนับสนุนกิจกรรมทางด้านวิทยาศาสตร์ ซึ่งสามารถเคลื่อนย้ายถ่ายโอนข้อมูลที่มีขนาดใหญ่ระหว่างอาคาร สถานที่ หรือสถาบันการศึกษาต่าง ๆ เพื่อให้มั่นใจได้ว่าข้อมูลจะถูกถ่ายโอนอย่างปลอดภัย ไม่เกิดการสูญหายของข้อมูล เพื่อเพิ่มประสิทธิภาพของการทำงานของเครือข่ายการศึกษาและวิจัย และพบว่า Layer2 VPN ช่วยในส่วนของการส่งข้อมูลที่รวดเร็วและมีแบนด์วิธที่ยืดหยุ่นสูง สามารถใช้งานเครือข่ายข้ามสถาบันเพียงแค่มีชื่อผู้ใช้และรหัสผ่านเพียงชุดเดียวโดยใช้กระบวนการ Federation Server และสถาปัตยกรรม Science DMZ ช่วยให้การถ่ายโอนข้อมูลจากงานวิจัยที่มีขนาดใหญ่มหาศาลได้อย่างรวดเร็วและปลอดภัย

## บทที่ 2

### L2VPN และ SDN ทางด่วนข้อมูล UniNet

ในการจัดทำโครงการนี้จำเป็นต้องใช้ความรู้ในด้านเน็ตเวิร์ก (Network) เข้ามาช่วยในส่วนของการทำแบบจำลองระบบเครือข่ายได้ใช้องค์ความรู้ในเรื่องของข้อมูลบน Layer 2 (Data link Layer) และการส่งข้อมูลที่ปลอดภัยด้วย VPN (Virtual Private Network) ที่ใช้โปรโตคอล PPTP (point-to-point) ในการสร้างอุโมงค์ข้อมูล (Tunnel) เนื่องจากการใช้งานอินเทอร์เน็ตที่มากขึ้นทำให้การใช้งานอินเทอร์เน็ตเพื่อการศึกษาต้องแข่งเส้นทางการกับเครือข่ายสาธารณะ จึงมีเครือข่ายเพื่อการศึกษาวิจัย UniNet ให้บริการกิจกรรมทางการศึกษา ใช้ Federation service ในการเข้าใช้งานระบบข้ามสถาบันได้เพื่อแลกเปลี่ยนข้อมูล และสถาปัตยกรรม Science DMZ เป็นเทคโนโลยีที่เกิดขึ้นใหม่ซึ่งเชื่อมต่อกับเครือข่ายเพื่อการศึกษาวิจัย REN และสามารถถ่ายโอนข้อมูลขนาดใหญ่ได้อย่างรวดเร็วและปลอดภัย มีดังต่อไปนี้

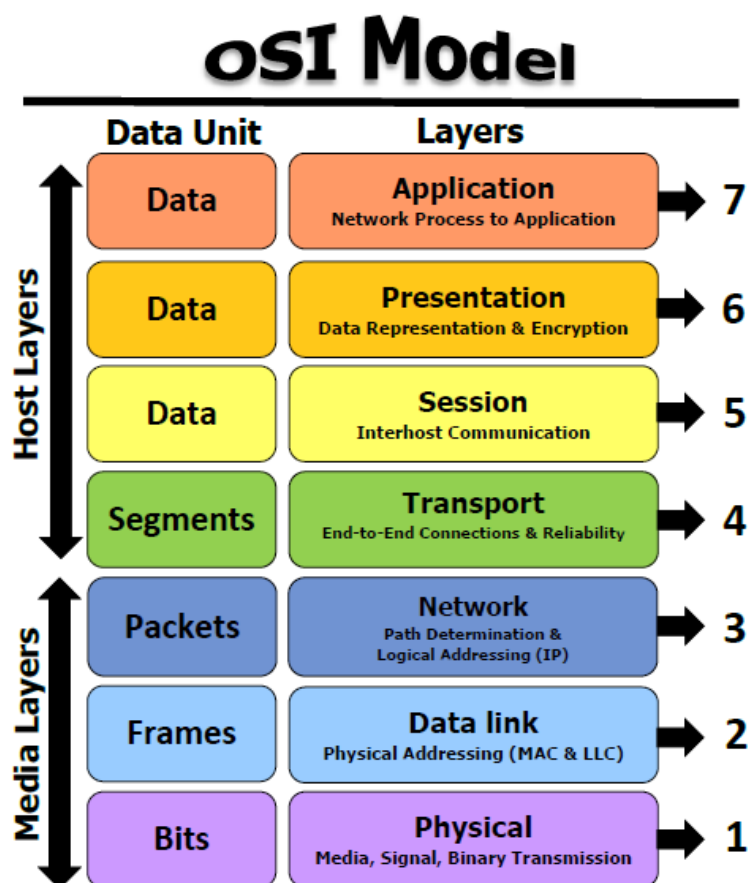
#### 2.1 การส่งข้อมูล

##### 2.1.1 การส่งข้อมูลในแบบจำลอง OSI

แบบจำลอง OSI (Open Systems Interconnection) ถูกใช้เป็นมาตรฐาน ข้อตกลงหรือข้อกำหนด สำหรับการติดต่อสื่อสารกันในระบบเครือข่าย ระหว่างอุปกรณ์เครื่องคอมพิวเตอร์ต่าง ๆ ให้ส่งข้อมูลหรือโต้ตอบกันได้ ทำให้อุปกรณ์เครื่องคอมพิวเตอร์แต่ละระบบสามารถติดต่อสื่อสารกันได้อย่างอิสระ ไม่ว่าจะเป็นระบบเดียวกันหรือในระบบที่แตกต่างกัน

โดยทั่วไปไม่มีผู้ผลิตซอฟต์แวร์หรือฮาร์ดแวร์ทั้งหมดด้วยตัวเอง จะใช้โครงสร้างการส่งข้อมูลโดยอ้างอิงแบบจำลอง OSI สำหรับผลิตอุปกรณ์เครื่องคอมพิวเตอร์ต่าง ๆ ซึ่งผู้ผลิตซอฟต์แวร์หรือฮาร์ดแวร์สามารถผลิตแยกส่วนกันได้ตามความถนัดเพื่อให้ทำงานร่วมกันและติดต่อสื่อสารถึงกันได้ทั้งหมด ทั้งในส่วนของการส่งและด้านรับให้สามารถทำงานร่วมกันได้อย่างมีประสิทธิภาพ

แบบจำลอง OSI แบ่งออกเป็น 7 เลเยอร์ได้แก่



ภาพที่ 2-1 แบบจำลอง OSI 7 เลเยอร์

ในการทำปริญญานิพนธ์เล่มนี้ได้ทำการศึกษาการส่งข้อมูลที่ Layer 2 หรือ Data Link Layer ซึ่งหน้าที่ความรับผิดชอบหลักของ Layer 2 นี้จะเป็นการส่งข้อมูลบน Network ดูแลเรื่องการห่อหุ้มข้อมูลจาก Layer บน ไว้ภายใน Frame และส่งจากต้นทางไปยังอุปกรณ์ปลายทางใน Layer2 นี้จะมีการระบุหมายเลข MAC Address ต้นทางและปลายทางของเครื่องหรืออุปกรณ์ เป็น Address ที่ไม่สามารถเปลี่ยนเองได้ ซึ่งรายละเอียดมีดังต่อไปนี้

### 2.1.2 การส่งข้อมูลใน Layer 2

หน้าที่รับผิดชอบหลักของ Layer2 นี้คือรับผิดชอบในเรื่องการส่งข้อมูลบน Network แต่ละประเภท เช่น Ethernet, Token ring, FDDI, หรือบน WAN ต่าง ๆ และคอยจัดการดูแลเรื่องการห่อหุ้มข้อมูลจากเลเยอร์บน เช่น Packet IP ไว้ภายใน Frame (การรับส่งข้อมูลใน Layer นี้ มีหน่วยเป็น Frame) รวมถึงการจัดส่งข้อมูลจากต้นทางไปยังอุปกรณ์ตัวถัดไปหรือปลายทาง ในเน็ตเวิร์กแบบ Ethernet Layer นี้จะมีการระบุหมายเลข MAC Address (เป็น Address ของเครื่องหรืออุปกรณ์ต้นทางกับเครื่องหรืออุปกรณ์ปลายทางด้วย Hardware Address) ซึ่ง MAC Address เป็น Address ที่ไม่สามารถเปลี่ยนได้เพราะถูกกำหนดมากับเครื่องอุปกรณ์นั้นแล้ว ตัวอย่างเช่น ผู้ที่ใช้งาน Ethernet จะพบว่าต้องมีหมายเลข MAC Address ของ Network Card ที่เสียบอยู่ในเครื่องคอมพิวเตอร์ระบุกำกับไว้เสมอ ซึ่ง MAC Address เป็นตัวเลขขนาด 6 byte โดยที่ 3 byte แรกจะได้รับการจัดสรรโดยองค์กรกลาง IEEE ให้แก่ผู้ผลิตแต่ละราย ส่วนตัวเลข 3 byte หลังทางผู้ผลิตสามารถกำหนดเองได้ ตัวอย่างของโปรโตคอล ในชั้นนี้ คือ Ethernet, Token Ring, IEEE 802.3/202.2, Frame Relay, FDDI, HDLC, ATM เป็นต้น

ใน Layer2 จะทำหน้าที่ป้องกันไม่ให้เครื่องส่งทำการส่งข้อมูลรวดเร็วจนเกินไปหรือเกินขีดความสามารถของเครื่องผู้รับจะสามารถรับข้อมูลได้ และอีกหน้าที่หนึ่งก็จะเป็นจะเสมือนเป็นผู้ควบคุมหรือผู้ตรวจสอบความผิดพลาดในข้อมูลแต่ละครั้งที่ส่งออกไปเป็น Packet หรือ Frame กรณีที่ผู้รับได้รับข้อมูลถูกต้องแล้วก็จะส่งสัญญาณ ACK (acknowledgment) ให้กับผู้ส่งเพื่อยืนยันตอบกลับมาว่าได้รับข้อมูลแล้ว แต่ถ้าผู้ส่งไม่ได้รับสัญญาณ ACK หรือได้รับสัญญาณ NAK (Negative Acknowledge) กลับมา ผู้ส่งก็อาจจะทำการส่งข้อมูลไปให้ใหม่

Layer2 แบ่งออกเป็น LAN และ WAN ซึ่งปัจจุบันบน Layer2 LAN จะนิยมใช้เทคโนโลยีแบบ Ethernet ในบริษัท องค์กร สถาบันการศึกษา หน่วยงานต่าง ๆ ส่วนของ WAN จะติดต่อสื่อสารระยะทางที่ห่างไกล WAN จะมีหลายแบบแตกต่างกันไป เช่น Lease Line เป็นต้นซึ่ง LAN แบ่งย่อยออกเป็น 2 sublayers ได้แก่

#### 1) Logical Link Control (LLC)

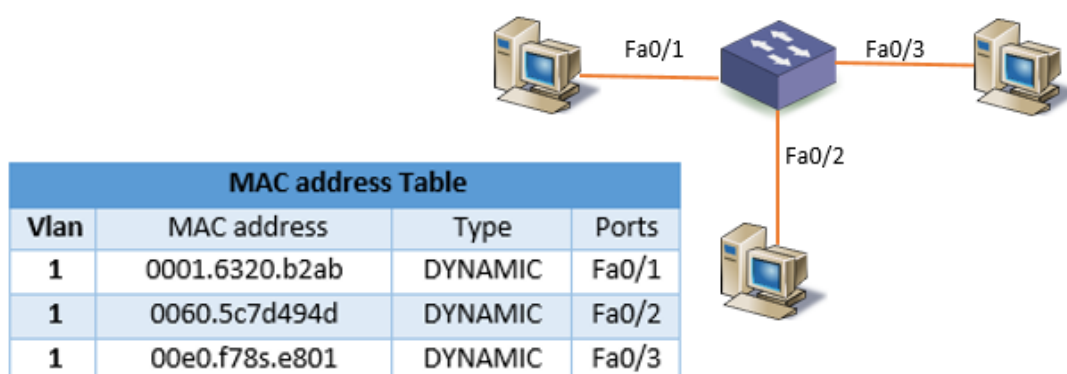
ให้บริการกับ Layer ที่อยู่ด้านบน สำหรับการเข้าใช้สัญญาณเพื่อการรับหรือส่งข้อมูล จะอนุญาตให้ LAN ที่ต่างกันสามารถทำงานร่วมกันได้ หมายความว่า Layer ด้านบนไม่จำเป็นต้องทราบว่าการรับ-ส่งข้อมูลใน Physical Layer จะใช้สายสัญญาณประเภทใดในการรับ-ส่งข้อมูล เพราะ LLC มีหน้าที่คอยปรับ Frame ของข้อมูล ให้สามารถส่งไปได้ในสายสัญญาณทุก



ประเภทได้ ไม่จำเป็นต้องรู้ว่าการส่งผ่านข้อมูลใน Physical Layer ข้อมูลนั้นจะใช้การรับส่งแบบใด และไม่จำเป็นว่าข้อมูลจะส่งผ่านรูปแบบเครือข่ายแบบใด เช่น Ethernet, Token Ring เพราะ LLC จัดการเรื่องเหล่านี้ทั้งหมด

## 2) Media Access Control (MAC)

MAC จะมีหน้าที่ควบคุมการติดต่อสื่อสารกับ Layer 1 และรับผิดชอบในการรับส่งข้อมูลให้สำเร็จลุล่วง การอ้างอิงระบุ MAC Address ของอุปกรณ์เครือข่าย สำหรับการส่งข้อมูลจากต้นทางไปยังอุปกรณ์เครือข่ายถัดไปหรือปลายทาง เช่น จากอุปกรณ์เครือข่ายต้นทางส่ง MAC Address หมายเลข XX-XX-XX-XX-XX-XX ไปสู่ปลายทางหมายเลข YY-YY-YY-YY-YY-YY ซึ่งจะรู้ว่าใครส่งมา เมื่อปลายทางได้รับข้อมูลแล้ว จะได้ตอบกลับไปยังบน Ethernet ให้ถูกต้อง MAC Address มีหน้าที่ในการรับผิดชอบในการรับ-ส่งข้อมูลให้สำเร็จโดยที่ Frame Check Sequence (FCS) ก็คือการตรวจสอบข้อผิดพลาดในการส่งข้อมูล และยังตรวจสอบด้วยว่าช่องสัญญาณพร้อมสำหรับส่งข้อมูลกับ Physical Layer หรือไม่ ถ้าว่างก็ส่ง ถ้าไม่ว่างก็ต้องรอ กลไก CSMA/CD ใช้ตรวจสอบการชนกันของข้อมูล บน Ethernet โดยจะส่งสัญญาณ (jam signal) ถ้ามีการชนกันเกิดเพื่อให้หยุดส่งข้อมูลแล้วสุ่มรอเวลา (back off) เพื่อส่งใหม่อีกครั้ง



ภาพที่ 2-2 ตัวอย่าง MAC Address Table

## 2.2 เทคโนโลยี VPN

### 2.2.1 ความหมายของ VPN

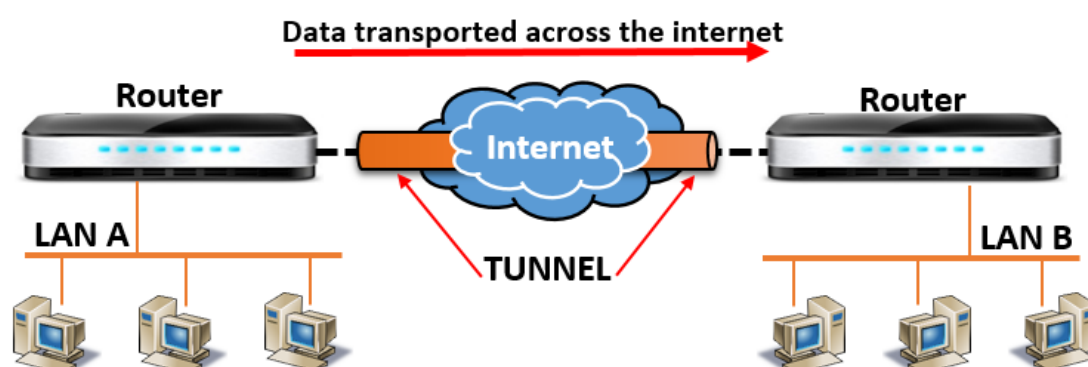
เครือข่ายส่วนตัว (Private Network) เป็นระบบเครือข่ายที่จัดตั้งขึ้นไว้เฉพาะสำหรับ บริษัท องค์กร สถานบันการศึกษา หน่วยงานต่าง ๆ ที่มีความต้องการการใช้ข้อมูลหรือทรัพยากรร่วมกัน ซึ่งข้อมูลทรัพยากรหรือการสื่อสารที่มีอยู่ในเครือข่ายส่วนตัว จะมีไว้เฉพาะบุคคลในองค์กร หรือบุคคลที่มีสิทธิ์เข้ามาใช้งานเท่านั้น บุคคลภายนอกไม่มีสิทธิ์และไม่สามารถเข้าร่วมใช้งาน ข้อมูลทรัพยากรบนเครือข่ายขององค์กรได้ ระบบเครือข่ายส่วนตัวมีการรักษาความปลอดภัยและความปลอดภัยเป็นจุดเด่น ถึงแม้ว่าจะมีการเชื่อมโยงกันระหว่างเครือข่ายสาธารณะและสาขาขององค์กรก็ตาม การรับ-ส่งข้อมูลในเครือข่ายส่วนตัวจะสร้างความปลอดภัยให้กับข้อมูลโดยจะมีการเข้ารหัส แพ็กเกจก่อนการส่งข้อมูลไปตามเส้นทางที่สร้างขึ้นเปรียบเสมือนกับอุโมงค์ (Tunnel) ที่อยู่ภายในเครือข่ายสาธารณะ (Public Network) หรือเครือข่ายอินเทอร์เน็ตนั่นเอง

เครือข่ายส่วนตัวเสมือน Virtual Private Network (VPN) ช่วยให้สามารถส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่งได้ โดยผ่านระบบอินเทอร์เน็ต ทำให้ได้รับความปลอดภัยสะดวกและรวดเร็วในการส่งข้อมูลในแต่ละครั้ง เทคโนโลยี VPN ใช้ อินเทอร์เน็ตเป็นสื่อกลางเข้ามาสร้างระบบเน็ตเวิร์คจำลอง เสมือนว่าระบบนั้นเป็นระบบเน็ตเวิร์คเดียวกัน แต่มีการสร้างอุโมงค์ข้อมูล (Tunnel) ที่ใช้สำหรับรับ-ส่งข้อมูลต่าง ๆ โดยเฉพาะ ซึ่งอุโมงค์ข้อมูลนั้นจะเชื่อมต่อกันระหว่างต้นทางกับปลายทาง ข้อมูลที่ถูกส่งผ่านไปสู่อุโมงค์ข้อมูลจะมีความปลอดภัยสูง ใกล้เคียงกับการเช่าสายสัญญาณ leased line แต่ค่าใช้จ่ายในการทำ VPN นั้นต่ำกว่าการเช่าสายสัญญาณมาก

VPN จะถูกนำมาใช้กับองค์กรขนาดใหญ่ที่มีสาขาอยู่ตามที่ต่าง ๆ มากมายและต้องการที่จะต่อเชื่อมแต่ละสาขาเข้าหากัน โดยที่เครือข่ายยังคงสามารถใช้ได้เฉพาะคนภายในองค์กรหรือคนที่เกี่ยวข้องด้วยเท่านั้น นอกจากนี้แล้วกลไกในการสร้างเครือข่าย VPN อีกประเภทหนึ่งคือ MPLS (Multiprotocol Label Switch) เป็นวิธีในการส่งแพ็กเกจโดยการแปะ Label ที่ส่วนหัวของข้อความ และค่อยเข้ารหัสข้อมูลจากนั้นจึงส่งไปยังจุดปลายทาง เมื่อถึงปลายทางก็จะถอดรหัสที่ส่วนหัวออก ซึ่งจะเพิ่มความปลอดภัยให้มากยิ่งขึ้น

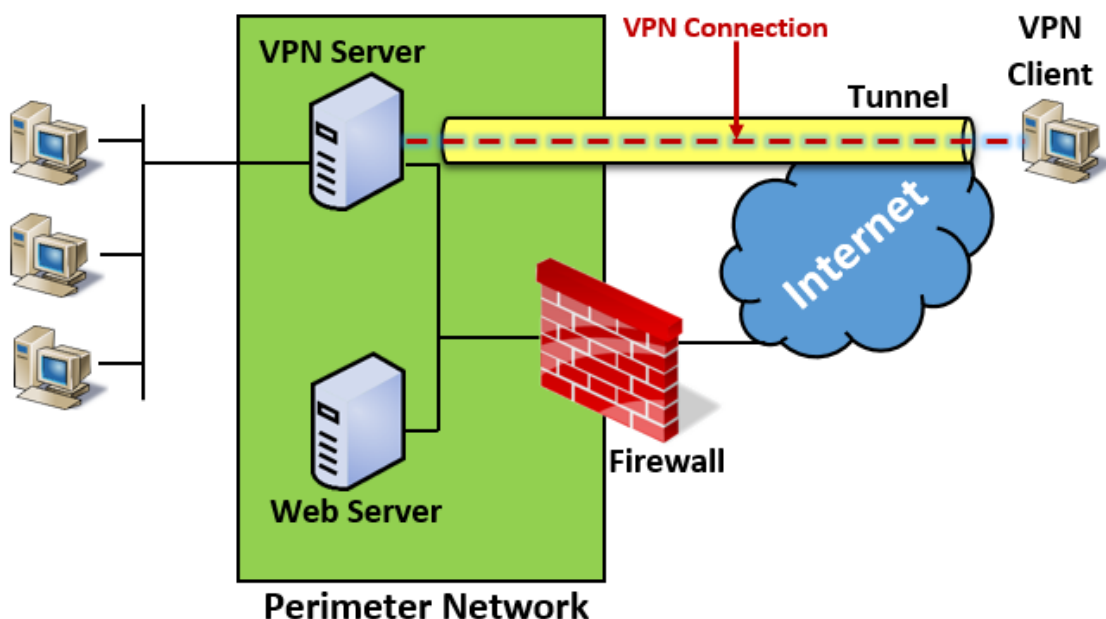
### 2.2.2 ลักษณะการทำงานของ VPN

VPN เป็นเครือข่ายที่อาศัยเส้นทางการทำงานภายใต้เครือข่ายสาธารณะ ซึ่งการส่งข้อมูลในเครือข่ายส่วนตัวเสมือนนั้นจะมีการส่งข้อมูลในรูปแบบแพ็กเกจ ออกมาที่เครือข่ายอินเทอร์เน็ต โดยก่อนการส่งข้อมูลจะต้องมีการเข้ารหัสข้อมูล (Data Encryption) เพื่อเพิ่มความปลอดภัยให้กับข้อมูลก่อนแล้วจึงส่งข้อมูลนั้นผ่านทางอุโมงค์ข้อมูล (Tunnel) ซึ่งจะถูกสร้างขึ้นระหว่างผู้ให้บริการ VPN กับผู้ใช้บริการ VPN จากจุดต้นทางไปยังจุดปลายทาง การเข้ารหัสข้อมูลถือเป็นการไม่อนุญาตให้บุคคลอื่นหรือผู้ที่ไม่เกี่ยวข้องกับข้อมูลเข้ามาอ่านข้อมูลได้จนสามารถส่งข้อมูลไปถึงปลายทางได้อย่างปลอดภัย และมีเพียงผู้รับปลายทางเท่านั้นที่สามารถถอดรหัสข้อมูลและนำข้อมูลไปใช้ได้



ภาพที่ 2-3 การรับส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ตผ่านอุโมงค์ข้อมูล (Tunnel)

จากภาพที่ 2-3 คือตัวอย่างการรับ-ส่งข้อมูลโดยใช้งานเครือข่ายอินเทอร์เน็ตผ่านอุโมงค์ข้อมูล (Tunnel) เป็นจำนวนทั้งสิ้น 2 สาขา โดยที่ทั้ง 2 สาขานี้ต้องการความปลอดภัยการสร้างอุโมงค์ข้อมูล (Tunnel) สำหรับการรับ-ส่งข้อมูลถึงกันระหว่างเราเตอร์ทั้งสองฝั่ง เพื่อที่จะรับ-ส่งข้อมูลไปบนเครือข่ายอินเทอร์เน็ต เพื่อไม่ให้ผู้อื่นหรือผู้ที่ไม่เกี่ยวข้องเข้ามาล่วงรู้ข้อมูลที่รับ-ส่งกันได้



ภาพที่ 2-4 ตัวอย่างการเชื่อมโยงเครือข่ายส่วนตัวเสมือน VPN

## 2.2.3 ประเภทของ VPN

### 2.2.3.1 Intranet VPN

จะใช้งานในรูปแบบงานเฉพาะภายในองค์กรเท่านั้น ตัวอย่างเช่น การเชื่อมต่อกันระหว่างสาขาของสำนักงานใหญ่และสำนักงานสาขาย่อย ซึ่งหมายถึงการเชื่อมต่อกันระหว่างจังหวัด เช่น สำนักงานใหญ่ในจังหวัดกรุงเทพมหานครและสาขาย่อยต่างจังหวัด โดยเชื่อมต่ออินเทอร์เน็ตผ่านผู้ให้บริการท้องถิ่นแล้วจึงเชื่อมต่อเข้ากับเครือข่ายส่วนตัวเสมือนขององค์กร ซึ่งก่อนหน้านี้มักจะนิยมการเชื่อมต่อโดยใช้การเช่าสายสัญญาณ Leased Line หรือ Frame Relay แต่ราคาค่อนข้างสูง

### 2.2.3.2 Extranet VPN

รูปแบบการใช้งานจะเป็นแบบ Intranet VPN แต่มีการขยายให้กว้างออกไปยังกลุ่มต่าง ๆ ภายนอกองค์กร เช่น ซัพพลายเออร์ ลูกค้า เป็นต้น คล้ายกับการเชื่อมต่อแลนค์ต่าง

แลนค์เข้าด้วยกันนั่นเอง ประสิทธิภาพการรักษาความปลอดภัยของข้อมูลทั้งหมดนั้นจะขึ้นอยู่กับ  
เครือข่ายของผู้ให้บริการ ที่สามารถรักษาความปลอดภัยของข้อมูลของผู้ใช้บริการ

### 2.2.3.3 Remote Access VPN

รูปแบบใช้งานนี้เป็นการใช้งานที่ต้องเข้าถึงเครือข่ายระยะทางไกลจากอุปกรณ์  
เคลื่อนที่ต่าง ๆ ซึ่งสามารถเข้าถึงเครือข่ายได้ถึง 2 ลักษณะ คือ

1) เข้าถึงจากไคลเอนต์ทั่วไป ซึ่งไคลเอนต์ต้องอาศัยผู้ให้บริการอินเทอร์เน็ตเป็น  
ตัวกลางในการติดต่อเชื่อมต่อ และเข้ารหัสในการส่งสัญญาณจากไคลเอนต์ไปยังผู้ให้บริการ  
เครือข่าย ISP (Internet Service Provider)

2) เข้าถึงจากเครื่องแอคเซสเซิร์ฟเวอร์ (Network Access Server - NAS) ผู้ใช้ต้อง  
หมุนโมเด็มเชื่อมต่อมายัง ISP หรือผู้ให้บริการ จากนั้นจะเข้ารหัสข้อมูลเพื่อจะส่งต่อไปยังปลายทาง  
ได้

### 2.2.4 Tunneling

หลักการทำงานของ VPN คือการส่งข้อมูลผ่านอุโมงค์ข้อมูล (Tunnel) เข้าไปสู่ระบบ  
เครือข่ายจากต้นทางไปปลายทางด้วยความปลอดภัย เนื่องจากอุโมงค์ข้อมูลที่สร้างขึ้นนั้นสร้างผ่าน  
ระบบอินเทอร์เน็ตและการส่งต้องมีการจัดการ Packet ต่าง ๆ ให้ผ่านไปตามอุโมงค์ข้อมูลให้ถูกต้อง

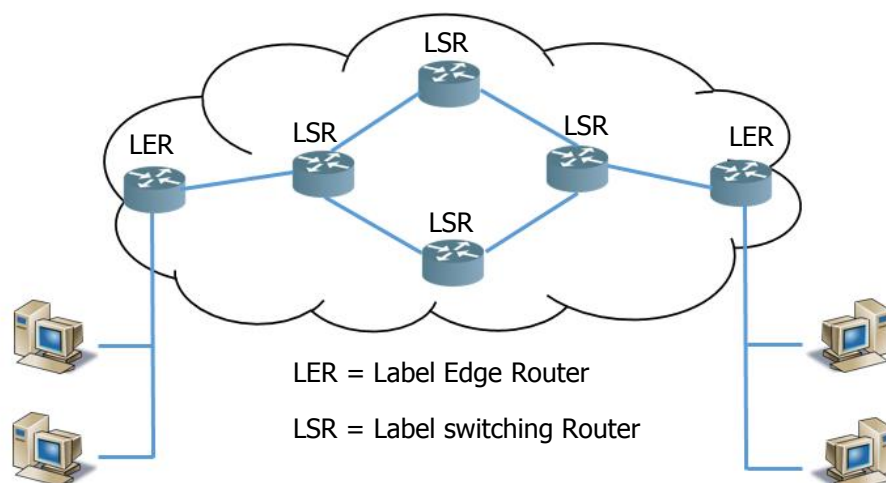
PPTP (Point-to-Point Tunneling Protocol) เป็นโปรโตคอลที่กล่าวถึงมาตรฐานการ  
Encryption และ Authentication ซึ่งพัฒนาจากบริษัทต่าง ๆ โดยมีบริษัท Microsoft และ 3Com  
ร่วมมือกันด้วย ดังนั้นจึงเป็นโปรโตคอลที่เป็น Default ของ Windows ที่จะใช้งาน VPN ซึ่ง  
โปรโตคอลนี้ มีพื้นฐานอยู่บน PPP ทำให้โปรแกรมที่ใช้โปรโตคอลนี้ เป็นการเชื่อมต่อในลักษณะ  
คอมพิวเตอร์เครื่องเดียวทำการเชื่อมต่อ VPN ไปยังระบบเน็ตเวิร์คที่รองรับการใช้งาน PPTP ซึ่งมี  
ข้อดีคือความสะดวกในการนำมาใช้งาน ที่ไม่ต้องมีการลงทุนทั้งในด้าน Software และ Hardware  
มากนัก

## 2.3 เทคโนโลยี MPLS

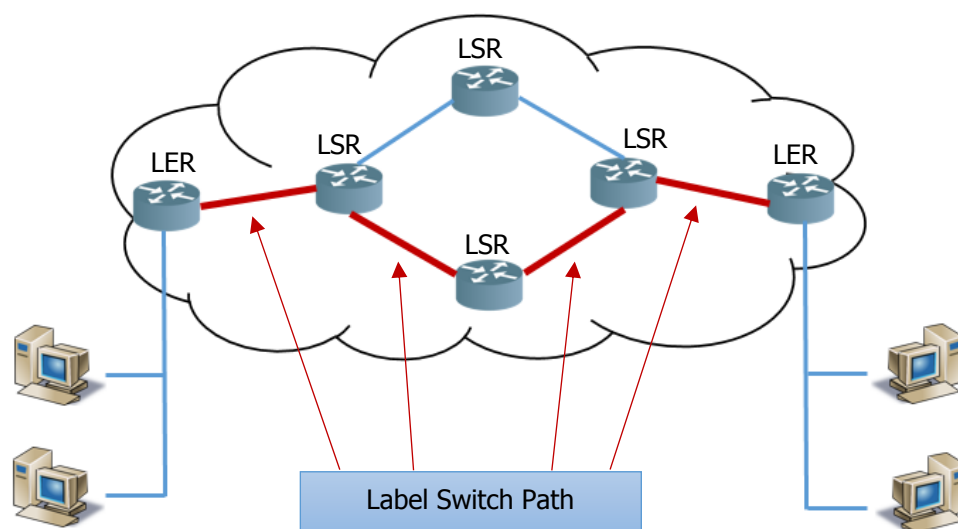
MPLS (Multiprotocol Label Switch) เป็นโพรโทคอลที่กำหนดขึ้นโดย The Internet Engineering Task Force (IETF) หลักการทำงานของเทคโนโลยี MPLS คือการติดป้ายใส่ Label เพื่อที่พิจารณาการส่งต่อ IP packet แทนที่จะใช้ IP address สำหรับใช้กำหนดเส้นทางในอุปกรณ์ Router และส่งต่อ IP packet โดย Label ที่ใช้ในการส่งต่อ IP packet นั้นจะเหมือนกันกับการส่งข้อมูลโดยใช้อุปกรณ์ Switch ซึ่งจะติด Label ให้กับ IP packet จะส่งผลทำให้ IP packet สวิตช์ไปยังเส้นทางที่กำหนดโดยไม่จำเป็นต้องจัดการเกี่ยวกับเรื่องการค้นหาเส้นทาง ทำให้สามารถส่งต่อ IP packet ไปยังปลายทางได้รวดเร็วมากขึ้น โดยไม่ต้องจัดการกับกระบวนการการค้นหาเส้นทางที่ดีที่สุดในเวลา เพราะกระบวนการดังกล่าวนี้ต้องใช้เวลาในการประมวลผลขณะหนึ่ง MPLS ถูกคิดค้นขึ้นมาเพื่อการส่งต่อข้อมูลโดย IP packet และลดกระบวนการส่งข้อมูลต่าง ๆ ลงให้เหมือนกับการส่งข้อมูลด้วยสวิตช์ ข้อดีที่เกิดขึ้นก็คือทำให้หน่วยประมวลผลหรือ CPU ของอุปกรณ์ทำงานน้อยลงตามไปด้วย ซึ่งทำให้การส่งข้อมูลจากจุดหนึ่งไปอีกจุดหนึ่ง ทำได้รวดเร็วและไม่เกิดความล่าช้า

### 2.3.1 องค์ประกอบของ MPLS

ในเครือข่าย MPLS จะประกอบด้วยอุปกรณ์ที่ขอบของเครือข่ายที่เรียกว่า Label Edge Router (LER) หรือ Provider Edge Router (PE) และอุปกรณ์ที่อยู่ภายในของเครือข่ายที่เรียกว่า Label Switching Router (LSR) หรือ Provider Router (P) แสดงในภาพที่ 2-5 และภาพที่ 2-6



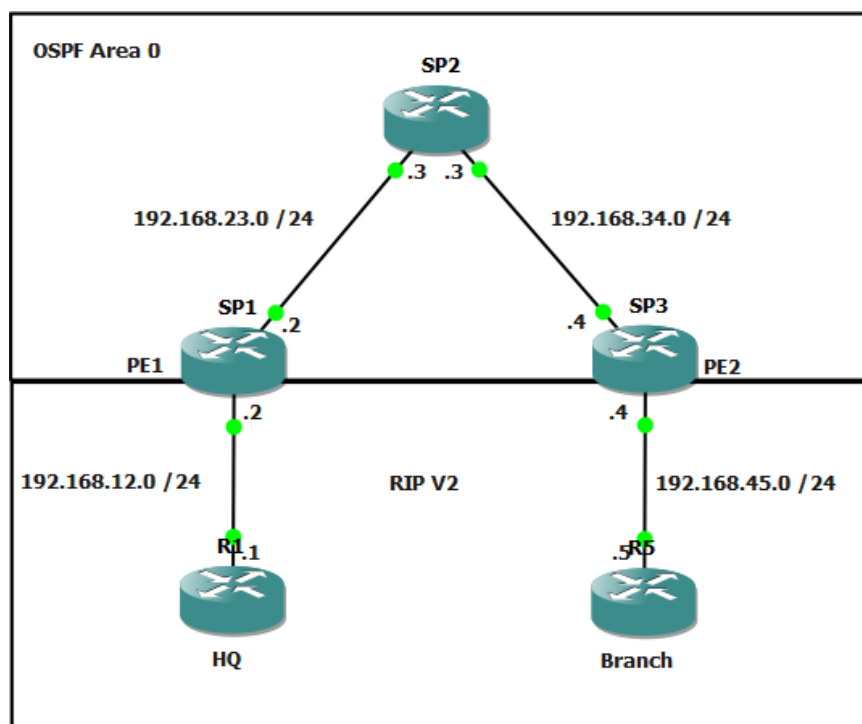
ภาพที่ 2-5 แสดง Label Edge Router และ Label switching Router ในเครือข่าย MPLS



ภาพที่ 2-6 แสดง Label Switched Path (LSP) ใน MPLS

เครือข่าย MPLS จะจัดการกำหนดเส้นทางเชื่อมต่อจาก LER ในส่วนขาเข้าของเครือข่ายไปยัง LER ในส่วนขาออกของเครือข่าย โดยผ่าน LSR ต่าง ๆ ภายในระบบเครือข่ายผ่านอุโมงค์ข้อมูลทิศทางเดียว (Unidirectional Tunnel) โดยเรียกเส้นทางนี้ว่า Label Switched Path (LSP) ทั้งนี้เพื่อให้ Packet ที่ LER ในส่วนขาเข้าถูกส่งไปยัง LER ขาออกผ่านเส้นทาง LSP

### 2.3.2 กลไกการทำงานของ MPLS



ภาพที่ 2-7 ตัวอย่างเครือข่าย MPLS

กระบวนการของ MPLS มีหลักการทำงานโดยสังเขปคือการกระบวนการสร้างการจัดการเส้นทางของ packet หรือการ Routing ขึ้นมาใหม่ ภายใต้บริเวณของเครือข่ายที่ต้องการ ซึ่งจะเรียกเส้นทางนี้ว่า LSP (Label Switched Path) โดยภายในบริเวณขอบเขตเครือข่ายนี้ packet ที่เข้ามาจะถูกกำหนด Label ขึ้นมาใหม่ และไม่สนใจ Header เดิม (อาจจะเป็นของ TCP/IP ก็ได้) แล้ว packet จะวิ่งไปตามเส้นทางที่ถูกกำหนดไว้ใน LSP ซึ่งเส้นทางนี้สามารถกำหนดไว้ล่วงหน้าตายตัว หรือจะเปลี่ยนแปลงการกำหนดตามความเหมาะสม ซึ่งจะมีความซับซ้อนมากกว่าโปรโตคอลที่ใช้กำหนดเส้นทางของข้อมูลที่ใช้อยู่เดิมในระบบเครือข่าย TCP/IP เช่น การคำนวณจำนวน hop โดยพิจารณาจากเวลาที่ใช้ส่งน้อยที่สุด หรือพยายามส่งให้ได้ตามเวลาจริง (Real Time) สำหรับการส่งข้อมูลต่าง ๆ

การทำงานลักษณะนี้จะรวดเร็วกว่า Routing เพราะการคำนวณจะเป็นการกำหนดและจัดเส้นทางไว้ล่วงหน้า การรับส่งข้อมูลแต่ละ packet เป็นอิสระต่อกัน คือมีหน้าที่จัดเส้นทางใหม่ก็จัด



ไปซึ่งเมื่อเสร็จก็เก็บไว้ใช้งาน ส่วนหน้าที่รับส่งข้อมูลก็ทำไปด้วยเช่นกันและไม่ยุ่งเกี่ยวกับ เมื่อมีข้อมูลเข้ามาถึงจะนำเส้นทางที่ได้เตรียมไว้มาใช้รับส่งข้อมูล เมื่อข้อมูลวิ่งถึงปลายทางของ LSP ก็ให้นำ Label ออกจาก packet และปล่อยให้เป็นหน้าที่ของ Header เดิมของ Packet ทำหน้าที่นำข้อมูลส่งถึงปลายทางอย่างแท้จริง

## 2.4 DMZ

### 2.4.1 ความหมายของ DMZ

Demilitarized Zone (DMZ) เป็น Network Segment ที่แยกตัวออกจากเครือข่ายอื่น ซึ่งหลาย ๆ องค์กรจะใช้ DMZ เพื่อแยกเครือข่าย Local Area Network (LAN) ของแต่ละองค์กรออกจากอินเทอร์เน็ตทั่วไป โดยมีการเพิ่มเงื่อนไขความปลอดภัย กำหนดรูปแบบ Security ระหว่างเครือข่ายขององค์กรและอินเทอร์เน็ตจากภายนอก โดยสามารถเรียก DMZ ว่าเป็นโซนปลอดภัย

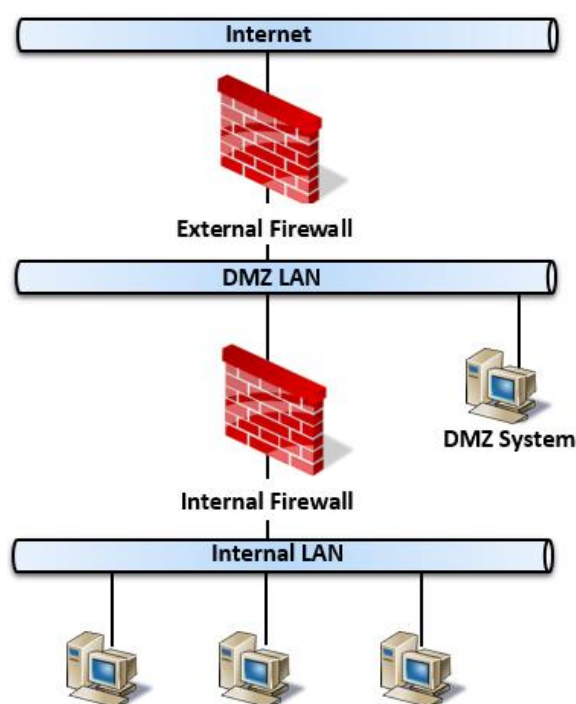
โดยปกติแล้ว DMZ คือ Public Facing Serve เช่น ถ้าองค์กรตั้ง website ขององค์กรบน server ซึ่ง Web Server นั้นถือว่าเป็น DMZ ถ้าเกิดการบุกรุกในส่วนนี้ ระบบเครือข่ายส่วนที่เหลือขององค์กรก็ไม่ตกอยู่ในอันตราย โดยจะใช้ DMZ สำหรับระบบ Server ต่าง ๆ ที่สามารถเข้าถึงจากอินเทอร์เน็ตภายนอก ไม่ว่าจะเป็น Web Server, Web Email หรือระบบอื่น ๆ ที่สามารถรักษาระบบเครือข่ายขององค์กรให้ปลอดภัยจากผู้บุกรุกหรือจากข้อมูลที่เป็นอันตรายประสงคร้ายต่อระบบของเครือข่ายองค์กร

ในทุก ๆ องค์กรไม่ว่าจะเป็นองค์กรที่มีขนาดเล็ก ขนาดกลาง หรือขนาดใหญ่ ถ้ามีการเชื่อมต่อระบบอินเทอร์เน็ต อินทราเน็ต ทั้งภายในหรือภายนอกองค์กร ผลกระทบที่ได้รับส่วนใหญ่อาจจะเป็นปัญหาในเรื่องของการบุกรุกข้อมูลหรือไวรัสและสิ่งที่ไม่ต้องการให้เกิดขึ้น การถูกเจาะระบบจากผู้ประสงคร้าย แต่ทุก ๆ องค์กรมีความจำเป็นที่ต้องติดต่อสื่อสารกันอย่างหลีกเลี่ยงไม่ได้ ดังนั้นสิ่งที่จำเป็นที่สุดคือ จะต้องจัดการป้องกันและมีการจัดแบ่งระบบเครือข่ายของแต่ละองค์กรออกเป็นโซน เพื่อให้เกิดความปลอดภัยในการจัดการและความคุม โดยเฉพาะในส่วนการติดตั้งระบบ Firewall ทั้งนี้เพื่อให้เกิดความปลอดภัยของข้อมูลหรือในระบบเครือข่ายขององค์กรจะจัดแบ่งโซนออกเป็นทั้งหมด 3 ประเภทหลักได้แก่

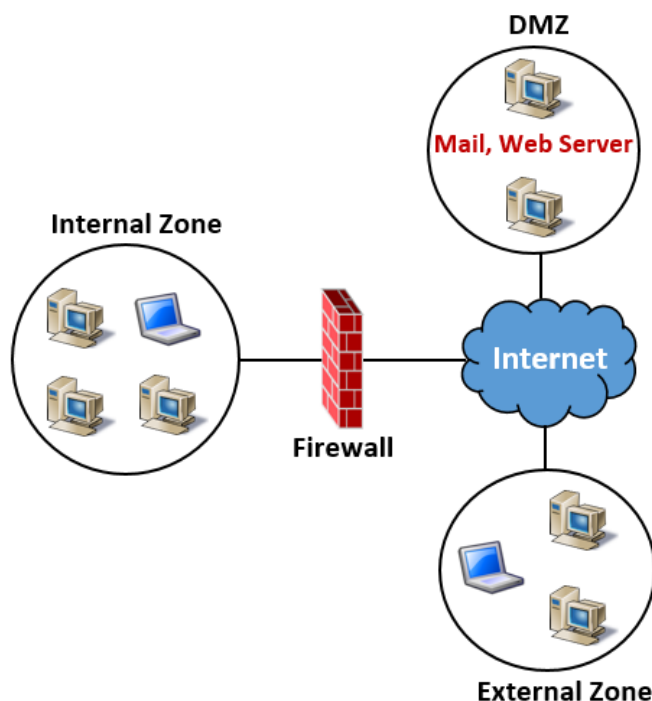
1) Internal Zone หมายถึง ระบบเครือข่ายภายในองค์กรขององค์กรเอง นับว่าเป็นโซนที่มีความปลอดภัยมากที่สุดและน่าเชื่อถือสูงสุด

2) External Zone หมายถึง ระบบเครือข่ายภายนอก จัดว่าเป็นโซนที่มีความปลอดภัยต่ำมาก (แต่ไม่ได้หมายความว่าเครือข่ายนอกองค์กรจะเป็นเครือข่ายที่ไม่ปลอดภัยหรือไม่น่าเชื่อถือ) เนื่องจากปฏิกิริยาไม่ได้ที่แต่ละองค์กรจำเป็นต้องมีการติดต่อสื่อสารกับเครือข่ายภายนอก จึงมีความจำเป็นอย่างมากที่จะต้องมีการควบคุมในเรื่องของการติดต่อสื่อสาร ตัวอย่าง External Zone ได้แก่ คอมพิวเตอร์ต่าง ๆ ภายนอกองค์กร รวมทั้งระบบเครือข่ายอินเทอร์เน็ต ที่ใช้สำหรับติดต่อสื่อสารกัน เป็นต้น

3) Demilitarized Zone (DMZ) จัดเป็นโซนพิเศษเฉพาะ ซึ่งไม่ได้หมายถึงทั้ง Internal Zone และ External Zone การทำงานของโซน DMZ นั้น จะติดต่อโดยตรงทั้ง Internal Zone และ External Zone ตัวอย่างของ DMZ เช่น Mail server, Web server เป็นต้น



ภาพที่ 2-8 Zoning ในระบบเครือข่าย



ภาพที่ 2-9 การแบ่ง Zoning

ภาพที่ 2-8 และ ภาพที่ 2-9 แสดง Zoning ในระบบเครือข่าย และการแบ่ง Zoning ซึ่ง DMZ เป็นส่วนหนึ่งที่ใช้ร่วมกับ Firewall โดยเป็นโซนที่สามารถกำหนดให้คอมพิวเตอร์เครื่องใดก็ได้ในวงแลนไปอยู่ในโซนนี้ ซึ่งอาจจะถูกยกเว้นโดย Firewall หรืออาจกล่าวได้ว่า คอมพิวเตอร์ที่อยู่ใน DMZ Zone เป็นคอมพิวเตอร์ที่ไม่ใช้ Firewall ในการป้องกันนั่นเอง สำหรับ Zone นี้จะไม่มีเรื่อง Security มาเกี่ยวข้อง ดังนั้นอุปกรณ์ใดก็ตามที่อยู่ใน Zone นี้ หรือ Port ที่เป็น DMZ นี้ ก็จะไม่มีการ Policy ของ Firewall มาปกป้องหรือป้องกันนั่นเอง ถ้าเปรียบเทียบเห็นภาพที่ชัดเจนขึ้นกับบริเวณของบ้าน ซึ่งมักจะมียุคคลภายนอกเข้ามาในบ้านตลอดเวลา แน่นอนว่าแขกที่แวะมาหานั่นจะไม่ถูกเชิญเข้าไปนั่งคุยในห้องนอนของบ้าน แต่มักจะบริเวณรับแขกสำหรับแขกที่แวะเวียนมานั่งพูดคุยธุระ แยกตัวออกจากบริเวณบ้านหรือห้องนอน ซึ่งการมีห้องรับแขกก็เปรียบเสมือน DMZ Zone

## บทที่ 3

### สถาปัตยกรรมของระบบบริการข้อมูล

ในโครงการนี้ใช้ Federation Service เพื่อการรวมตัวและสนับสนุนการใช้ทรัพยากรร่วมกัน ในองค์กรภายใต้เงื่อนไขเดียวกันข้ามระบบเครือข่ายได้ และในส่วนของการทำแบบจำลองเครือข่าย ส่วนตัวเสมือน VPN สามารถนำมาปรับใช้กับบริการ Layer2 UniNet เพื่อการส่งข้อมูลที่รวดเร็วและปลอดภัยสูงภายใต้ L2VPN ซึ่งมีเทคโนโลยีใหม่ ๆ คือ Science DMZ คอยมีส่วนช่วยในการส่งข้อมูลที่มีขนาดใหญ่มหาศาลได้อย่างมีประสิทธิภาพสูงสุด

#### 3.1 การทำงานของ Federation Service

Federated Identity Management (FIM), Identity Federation, Identity Access Federation และ Web Single-sign-on/SAML Federations นั้นหมายถึงสิ่งเดียวกัน ในทางของธุรกิจ Federation Service จะหมายถึงการรวมกลุ่มของข้อตกลงทางธุรกิจ ข้อตกลงทางเทคโนโลยี หรือนโยบายที่จะอนุญาตให้ทุก ๆ บริษัทพัฒนาให้ดำเนินการก้าวสู่เป้าหมายสูงสุดได้อย่างสมบูรณ์และดีที่สุด โดยดำเนินการให้สอดคล้องกับรูปแบบโครงสร้างทางธุรกิจของบริษัทกับนโยบายทางด้านเทคโนโลยีสารสนเทศต่าง ๆ เช่น ความปลอดภัย ความเป็นส่วนตัว ระบบการควบคุม การบริหารจัดการ และความต้องการที่เป็นอันหนึ่งอันเดียวกัน

ส่วนในทางด้านของเทคโนโลยีนั้น จะหมายถึงการรวมตัวกันหรือการกลายเป็นโครงสร้างพื้นฐานบนความไว้วางใจเมื่อเกิดการรวมตัวของธุรกิจต่าง ๆ ขึ้น เทคโนโลยีนี้จะอนุญาตให้แต่ละบริษัทนั้นสามารถที่จะเข้าร่วมกลุ่มใช้งานข้อมูลทรัพยากรต่าง ๆ ร่วมกันหรือเชื่อมโยงติดต่อกันได้บนโครงสร้างทางเทคโนโลยีสารสนเทศของพวกเขาเหล่านั้นภายใต้เครือข่ายที่เรียบง่ายและมีความปลอดภัยสูง โดยที่สมาชิกไม่จำเป็นต้องสร้างข้อมูลหลักฐานการมีตัวตน (Identity) ซ้ำซ้อนหลายครั้ง

### 3.1.1 ความหมายของ Federation Service

การบริหารจัดการโดยการใช้นโยบาย กระบวนการต่าง ๆ หรือเทคโนโลยีเพื่อใช้ในการพิสูจน์ยืนยันตัวตนของผู้ใช้งานระบบรวมถึงกฎต่าง ๆ เกี่ยวกับการเข้าถึงแหล่งข้อมูลดิจิทัล หรืออีกนัยหนึ่งคือ การที่ต้องมีข้อมูลหลักฐานการมีตัวตน (Identity) หรือข้อมูลประจำตัว (Credential) ที่แยกกันในแต่ละระบบ Federated identity Management จะอนุญาตให้ผู้ใช้งานระบบสามารถใช้ข้อมูลหลักฐานการมีตัวตน (Identity) หรือข้อมูลประจำตัว (Credential) เพียงอันเดียว ในการใช้งานระบบต่าง ๆ ซึ่งที่นิยมใช้กันมากก็คือชื่อผู้ใช้งาน (Username) ร่วมกับรหัสผ่าน (Password) ในการเข้าถึงข้อมูลทรัพยากรต่าง ๆ ของระบบทั้งหมดที่ผู้ใช้งานระบบมีสิทธิ์ในการใช้ได้

Identification หมายถึง การยืนยันตัวตน การระบุตัวตนที่ชัดเจนของทุก ๆ สิ่งในระบบ เรียกได้ว่าเป็นกระบวนการที่ผู้ใช้งานระบบนั้นต้องแสดงหลักฐานการมีตัวตน (Identity) ของตนเอง ต่อกระบวนการ Identification ซึ่งผู้ใช้งานระบบอาจจะใช้ชื่อผู้ใช้หรือรหัสผ่านเป็นต้น ให้การยืนยันตัวตน โดยหลักการของ Identification จะต้องเป็นเจ้าของของสิ่งนั้น ๆ อย่างแท้จริง และคุณสมบัติของ Identity ที่ดีนั้นไม่ควรปลอมแปลงง่ายและเก็บรักษาเฉพาะบุคคลเท่านั้น

Authentication หมายถึง กระบวนการที่ใช้เพื่อพิสูจน์ตัวตนว่าเป็นบุคคลคน ๆ นั้นที่ใช้งานระบบอยู่หรือไม่ เนื่องจากการพิสูจน์ตัวตนการใช้งานระบบต่าง ๆ มักจะใช้งานจากระยะไกล จึงไม่สามารถพิสูจน์ตัวตนที่แท้จริงได้เพราะไม่สามารถเห็นหน้า ไม่ทราบลักษณะที่ชัดเจน แต่จะเห็นแค่ข้อมูลที่วิ่งผ่านกันเท่านั้น นั่นหมายความว่าการทำงานระบบต่าง ๆ เป็นแบบ Logical ที่แทนตัวบุคคลนั้น ๆ จึงใช้กระบวนการ Authentication สำหรับตรวจสอบแทนตัวบุคคลหรือระบบต่าง ๆ ว่าใช่ตัวแทนของบุคคลหรือระบบนั้น ๆ หรือไม่ ตัวอย่าง กระบวนการการทำ Authentication ได้แก่ การพิสูจน์หลักฐานเพื่อบ่งบอกว่าบุคคลนั้น ๆ เป็นคน ๆ นั้นจริงหรือไม่ เช่น Username และ Password

Authorization หมายถึง การพิสูจน์ว่าบุคคลที่ผ่านมาจากกระบวนการ Authentication ซึ่งเกี่ยวข้องกับการการตั้งค่าของสิทธิ์ต่าง ๆ ของผู้ใช้งานในระบบ ตรวจสอบสิทธิ์ของผู้ใช้งานระบบว่ามีสิทธิ์ใช้งานทรัพยากรหรือระบบใดได้บ้างและสามารถดำเนินการกิจกรรมต่าง ๆ ได้อย่างถูกต้องตามกฎหมายของระบบที่ได้กำหนดไว้ล่วงหน้า

กระบวนการ Identification Authentication และ Authorization ทั้งหมดนี้มีส่วนเกี่ยวข้องในการควบคุมการเข้าถึงทรัพยากร โดยในการใช้งานระบบผู้ใช้งานจะแสดง Identity ของ

ตนเองเพื่อ Authentication และระบบจะทำการ Authorization เมื่อมีการใช้งานทรัพยากรใด ๆ ในระบบนั้นเองสำหรับข้อมูลต่าง ๆ ของผู้ใช้งานนี้ระบบจำเป็นต้องมีการจัดเก็บเพื่อใช้ในระบบ Authentication โดยกระบวนการ Authentication คือการที่ผู้ใช้งานระบบพิสูจน์ Identity ของตัวเองโดยใช้ Credential ภายหลังจากผ่านกระบวนการ Authentication แล้วระบบนั้น ๆ จะทำการ Authorization โดยดึงข้อมูล Identity และข้อมูลอื่น ๆ ที่เกี่ยวข้องกันเพื่อตัดสินใจว่าผู้ใช้งานระบบหรือโปรแกรมนั้น ๆ จะสามารถใช้งานได้จริงหรือไม่ ซึ่งกระบวนการ Authorization นี้สามารถดำเนินการได้โดยใช้ข้อมูล Group, Membership, Organization และ Application Right

องค์ประกอบของ Federation Service มีทั้งหมด 3 ส่วนได้แก่

#### 1. User

ผู้ใช้งานในระบบแต่ละรายจะมีลักษณะโดยเฉพาะของแต่ละบุคคลที่แตกต่างกันไป เพื่อที่จะแสดงความเป็นตัวตนของผู้ใช้งานระบบซึ่งมักจะประกอบด้วยคุณลักษณะและรายละเอียดต่าง ๆ เช่น

- ชื่อผู้ใช้งานระบบและรหัสผ่าน
- ลักษณะส่วนบุคคล
- ข้อมูลติดต่อ/สถานที่
- ข้อมูลการศึกษา
- ข้อมูลการทำงาน
- ข้อมูลชี้เฉพาะบุคคล
- การเข้าถึงข้อมูล/ข้อมูลการบริหาร
- รูปแบบลักษณะการรักษาความปลอดภัย
- การรักษาความลับ
- การอนุญาตและการให้สิทธิ์
- คุณลักษณะกลุ่มที่เกี่ยวข้อง
- คุณลักษณะอื่น ๆ

## 2. Identity Provider (IdP)

Federated Identity Management จะช่วยเพิ่มในส่วนการรักษาความปลอดภัยและความสะดวกสบาย โดยผู้ให้บริการเครือข่ายเฉพาะที่ได้รับความน่าเชื่อถือในการใช้งาน ปฏิบัติงาน การจัดการและการพิสูจน์ตัวตนของผู้ใช้จะได้รับมอบหมายให้เป็นหน้าที่ของ Identity Provider ซึ่ง ผู้ดูแลระบบจะสามารถควบคุมคุณสมบัติของผู้ใช้งานระบบและกลไกในการยืนยันตรวจสอบ ตัวตนของผู้ใช้งานระบบ

Identity Provider จะรับผิดชอบในส่วนของการตรวจสอบการยืนยันตัวตน ในการเข้าใช้งานระบบ ตรวจสอบข้อมูลพิสูจน์ตัวตนจากฐานข้อมูลบัญชีสมาชิก ตรวจสอบการมีตัวตนของผู้ใช้งานในระบบว่ามีตัวตนอยู่จริงเพื่อเข้าใช้งานระบบได้หรือไม่ อยู่ภายใต้ความน่าเชื่อถือต่อลูกค้าของสถาบันผู้ให้บริการเครือข่ายรวมถึงการสร้างการปรับปรุงแก้ไข การเพิ่มการควบคุมสมบัติ ลักษณะเฉพาะของผู้ใช้งานระบบและกำหนดข้อบังคับต่าง ๆ สำหรับผู้ใช้งานระบบปฏิบัติตามกฎ ความเป็นส่วนตัวของ Identity Provider

## 3. Service Provider (SP)

Service Provider จะมีหน้าที่อนุญาตให้ผู้ใช้งานระบบสามารถใช้งานทรัพยากรต่าง ๆ ได้ผ่านการตรวจสอบยืนยันหรือพิสูจน์ตัวตนหรืออนุญาตให้ทำการยืนยันสิทธิ์การใช้งาน ซึ่ง การตัดสินใจและการอนุญาตนั้นขึ้นอยู่กับคุณลักษณะของผู้ใช้งานระบบบริการต่าง ๆ ว่าถูกต้อง สามารถเชื่อมต่อได้จริงหรือไม่ โดยจะตรวจสอบการพิสูจน์ตัวตนจาก Identity Provider

ในบรรดาข้อมูลของผู้ให้บริการการเชื่อมต่อจะไม่ทำหน้าที่เหมือน Identity Service ที่คอยทำหน้าที่ในส่วนของการยืนยันหรือพิสูจน์การมีตัวตนของผู้ใช้งานระบบแต่ Service Provider จะอาศัยข้อมูลการยืนยันสิทธิ์เกี่ยวกับผู้ใช้งานระบบจาก Identity Service แทน

### 3.1.2 ลักษณะการทำงานของ Federation Service



ภาพที่ 3-1 ลักษณะการทำงานของ Federation Service

การใช้งานระบบต่าง ๆ ที่มีมากกว่า 1 ระบบ ผู้ใช้งานระบบจะต้องมีชื่อผู้ใช้งาน (User) และรหัสผ่าน (Password) ของระบบต่าง ๆ เพื่อยืนยันสิทธิ์การเข้าใช้งานระบบนั้น ๆ ซึ่งอาจจะเกิดความสับสนยุ่งยากสำหรับการจดจำชื่อผู้ใช้งานและรหัสผ่านที่มีมากกว่า 1 ระบบ และอาจเกิดปัญหาการลืมรหัสผ่านได้ ผู้ดูแลระบบจึงควรตั้งค่าให้ผู้ใช้งานระบบสามารถใช้ชื่อและรหัสผ่านชุดเดียวกันได้ในหลาย ๆ ระบบหรือที่เรียกกันว่า Single Sign-On (SSO)

สำหรับการทำ Single Sign-On นั้นสามารถทำได้โดยใช้กระบวนการของ Federated Identity Management ซึ่งกระบวนการ Single Sign-On สามารถทำ Authentication และ Authentication ข้ามระบบในอีกองค์กรหรือสถาบันหนึ่งได้และจำเป็นต้องมี Federation Service ในแต่ละระบบและสร้างระบบความน่าเชื่อถือขึ้นระหว่างระบบ และใช้ Security Assertion Markup Language (SAML) เป็นโปรโตคอลที่เชื่อมต่อเครือข่ายเพื่อทำงานร่วมกับระบบหลาย ๆ ระบบ โดยจะมีรับรองการทำงานของ Identity Provider และ Service Provider มีจุดประสงค์เป็นการแลกเปลี่ยนข้อมูลเพื่อการแสดงตัวตน Authentication และการอนุญาต Authorization ในการเข้าใช้งานระบบ



### 3.1.3 การทำงานร่วมกันระหว่าง Federation Service และ eduroam

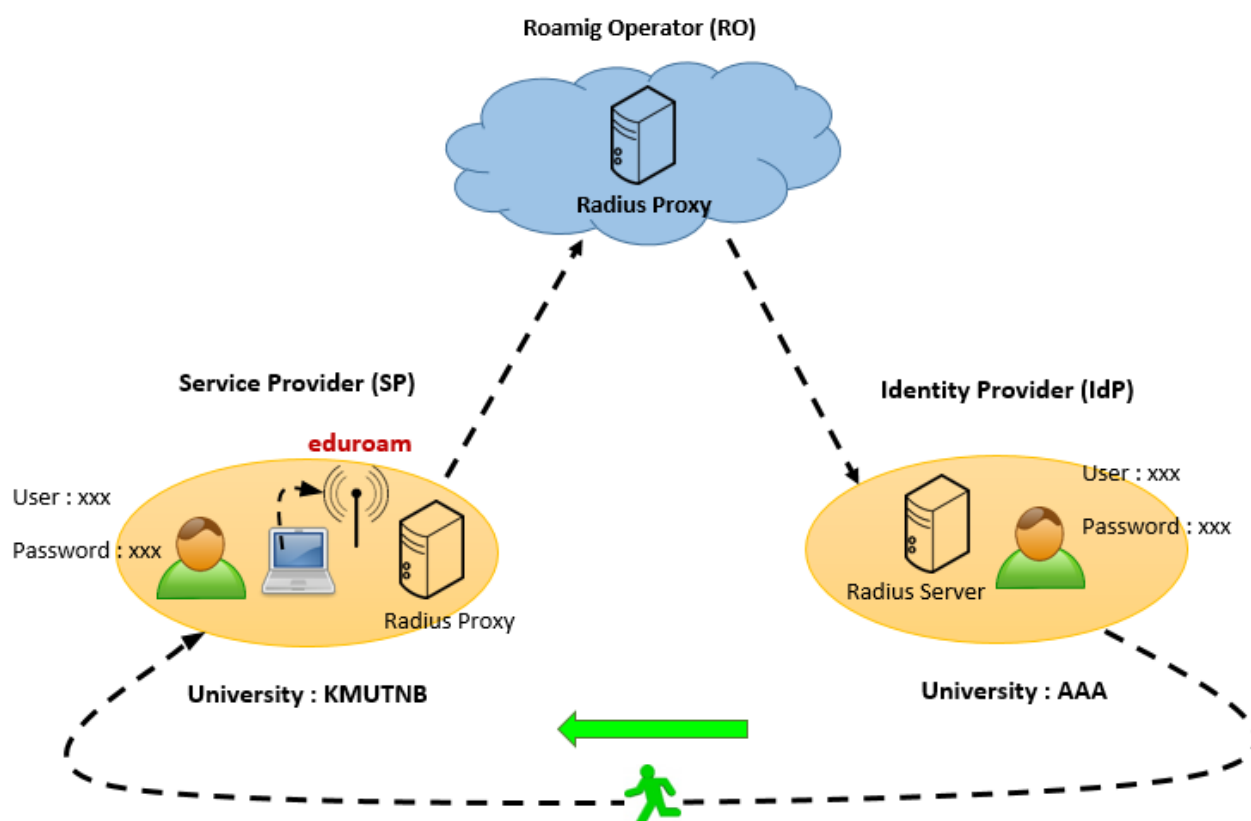
จุดมุ่งหมายหลักของการรวมตัวกันของแต่ละองค์กรสถาบันการศึกษา ใช้กระบวนการ Federation Service เพื่อต้องการสนับสนุนและใช้ทรัพยากรในด้านการศึกษาวិชาลัยร่วมกัน เพื่อพัฒนานวัตกรรมใหม่ที่จะเกิดขึ้นในอนาคตได้อย่างกว้างไกล โดยสมาชิกของแต่ละหรือสถาบันการศึกษาสามารถเข้าใช้งาน eduroam ได้

eduroam ย่อมาจาก educational roaming เป็นบริการเครือข่ายโรมมิ่งข้ามเครือข่าย เพื่อการศึกษาและวิจัยสำหรับ อาจารย์ นักศึกษา และนักวิจัยของแต่ละสถาบันการศึกษาที่เป็นสมาชิกของเครือข่าย eduroam ซึ่งจะคอยอำนวยความสะดวกในการเข้าใช้งานเครือข่ายอินเทอร์เน็ต เพื่อการใช้งานข้ามเครือข่ายที่ปลอดภัย และสามารถรองรับการขยายตัวของผู้ใช้งานที่เพิ่มจำนวนมากขึ้นให้อยู่ภายใต้เงื่อนไขการใช้งานของสถาบันผู้ให้บริการเครือข่าย (Service Provider) โดยบริการเครือข่ายโรมมิ่งข้ามเครือข่ายนี้จะใช้มาตรฐาน 802.1x ทำงานร่วมกับ Radius Server ของแต่ละสถาบัน คอยให้บริการกับอาจารย์ นักศึกษา และนักวิจัยจากสถาบันสมาชิก สำหรับในประเทศไทย UniNet จะทำหน้าที่เป็นผู้ดำเนินการหลักเป็นผู้รับผิดชอบการให้บริการ eduroam และเป็นผู้กำหนดนโยบายการใช้งานระดับประเทศ โดย eduroam

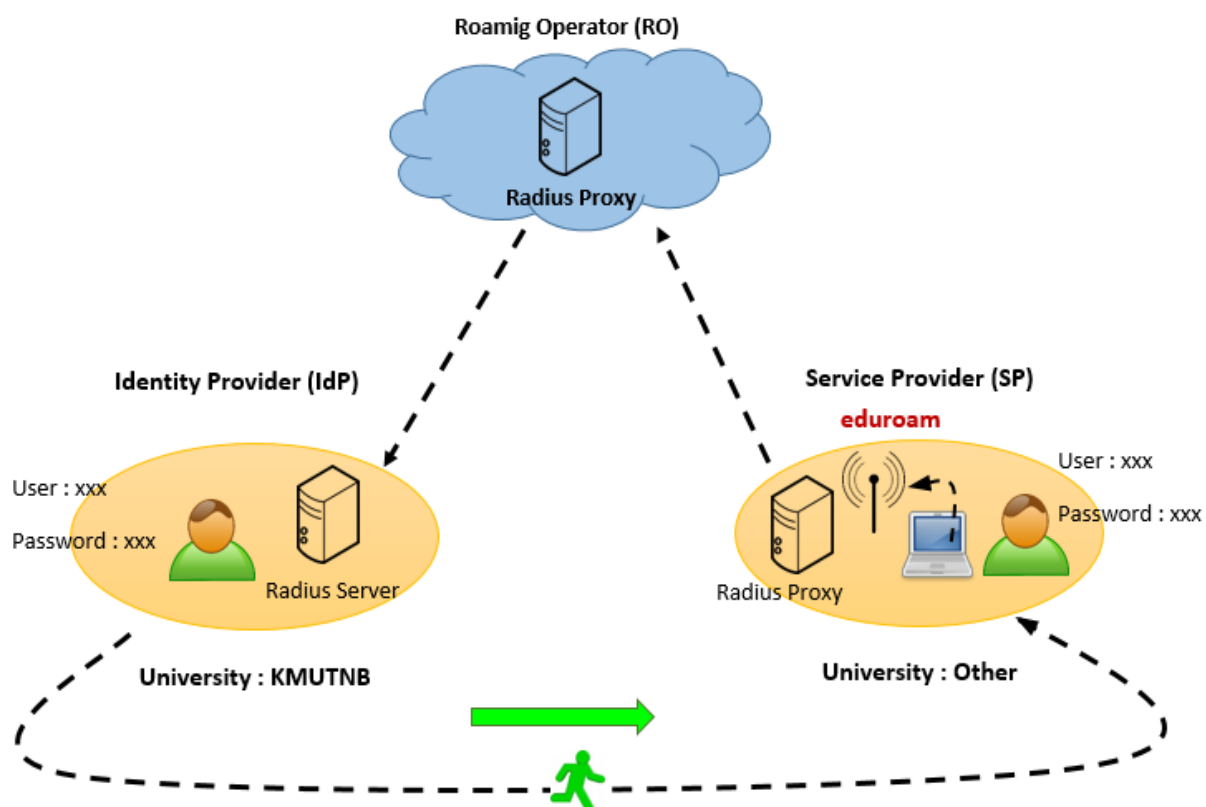
#### 3.1.3.1 การทำงานของ eduroam

นักศึกษา อาจารย์ นักวิจัยหรือนุคลากรต่าง ๆ ของสถาบันการศึกษาที่เป็นสมาชิกเครือข่ายของ eduroam จะได้รับความสะดวกในการเข้าใช้งานเครือข่ายอินเทอร์เน็ตข้ามสถาบันการศึกษา เช่น ผู้ใช้งานที่มีบัญชีผู้ใช้ของสถาบัน ก. แต่ปัจจุบันไปศึกษาดูงานหรือทำงานวิจัยหรือเชื่อมต่ออินเทอร์เน็ตของสถาบัน ข. ซึ่งทั้ง 2 สถาบันเป็นสมาชิกเครือข่าย eduroam ฉะนั้นผู้ใช้งานสามารถเข้าใช้อินเทอร์เน็ตด้วยบัญชีผู้ใช้ของสถาบัน ก. ในพื้นที่ใช้งานสถาบัน ข. ได้ โดยไม่ต้องสร้างบัญชีผู้ใช้ใหม่แต่อย่างใด

ในส่วนของกระบวนการ Federation Service นั้น User จะเป็นบัญชีผู้ใช้งานระบบและ Password คือรหัสผ่านของแต่ละสถาบันการศึกษา Identity Provider (IdP) จะเป็นส่วนของสถาบันต้นสังกัดหรือสถาบันการศึกษา ที่ทำหน้าที่เป็นผู้กำหนดและตรวจสอบการยืนยันตัวตนพิสูจน์ตัวตน เพื่อเข้าใช้งานระบบของ อาจารย์ นักศึกษา นักวิจัย บุคลากรต่าง ๆ ของสถาบันของตน สุดท้ายคือ Service Provider (SP) คือ สถาบันหรือสถาบันการศึกษาที่ให้บริการการเชื่อมต่อเครือข่ายแก่ผู้มาเยือน ให้เชื่อมต่อเข้าเครือข่าย eduroam ได้โดยจะอนุญาตการเข้าใช้งานเมื่อสถาบันต้นสังกัดของผู้ใช้ที่มาเยือน ตอบยืนยันตัวตนนั่นเอง



ภาพที่ 3-2 การใช้งานเครือข่ายของผู้ใช้สถาบันอื่นมาใช้งานที่มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ



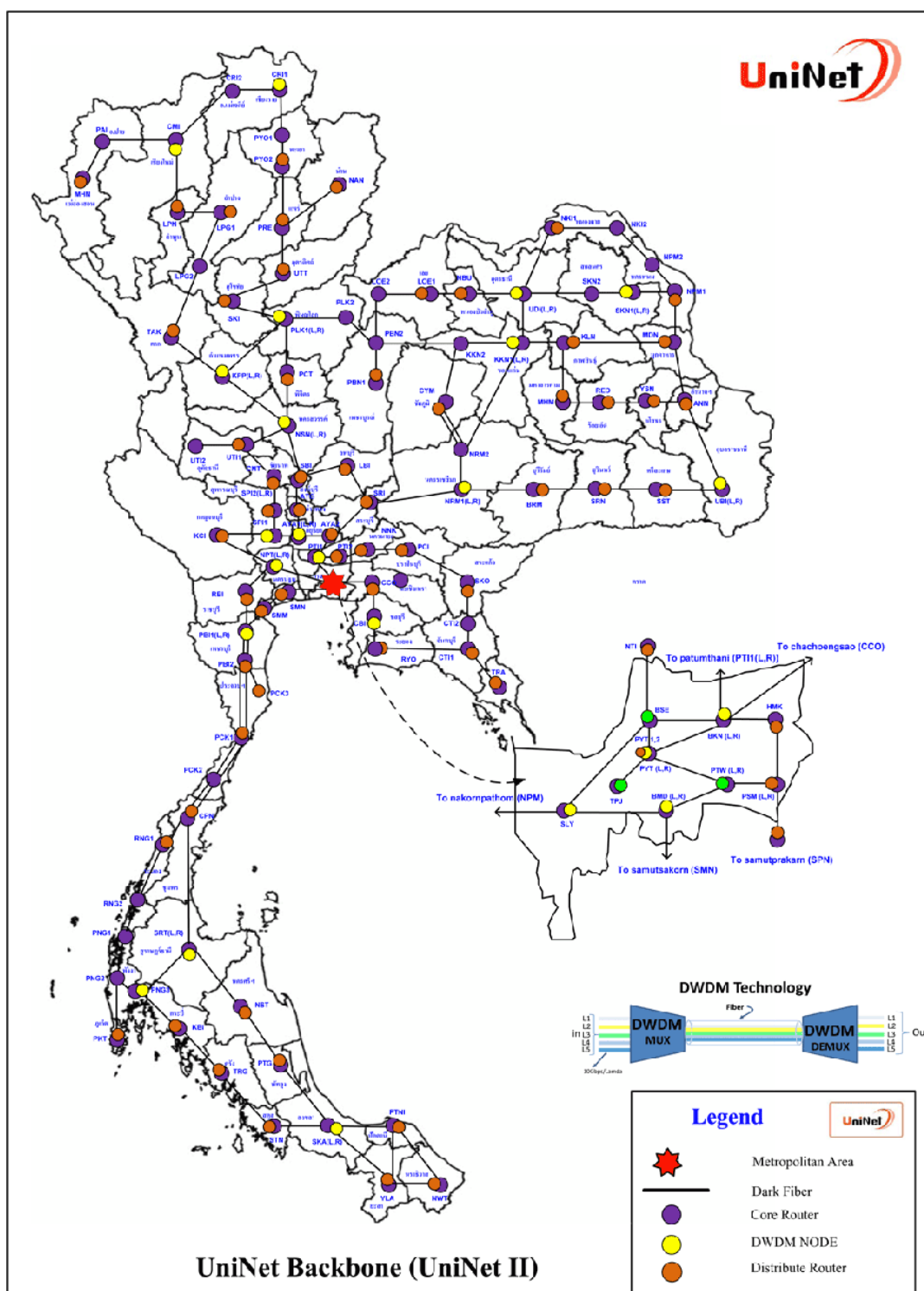
ภาพที่ 3-3 การใช้งานเครือข่ายของผู้ใช้มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือไป  
ใช้งานที่สถาบันอื่น

### 3.2 เครือข่ายเพื่อการศึกษาและการบริการบนเลเยอร์ 2

“UniNet” เครือข่ายเพื่อการศึกษาวิจัยโดยเฉพาะ ซึ่งเป็นเครือข่ายหลักระดับประเทศและเป็นระบบเครือข่ายแบบกระจาย โดยที่เครือข่ายนี้จะมีสายเคเบิลใยแก้วนำแสงที่สามารถเชื่อมไปยังสถาบันการศึกษาที่ครอบคลุมทุกจังหวัดทั่วประเทศไทย ซึ่งสนับสนุนสถาบันการศึกษาต่าง ๆ ในประเทศไทย ให้มีการดำเนินกิจกรรมการเรียนการสอนและการวิจัยต่าง ๆ เพื่อเพิ่มประสิทธิภาพในการเข้าถึงและนำเอาเทคโนโลยีสารสนเทศและการสื่อสารมาประยุกต์ใช้ให้เกิดประโยชน์สูงสุดซึ่ง UniNet มีโหนดที่เชื่อมต่อกันครอบคลุมทั่วประเทศไทย ดังภาพที่ 3-4

บริการบนเลเยอร์ 2 จะจัดทำให้สมาชิกในสถาบันการศึกษาต่าง ๆ มีความสามารถเพื่อที่จะได้รวมกลุ่มแลกเปลี่ยนและสนับสนุนทรัพยากรต่าง ๆ ทางด้านการศึกษาวิจัย ปัจจุบันเครือข่ายเปิดรองรับการใช้งานของการส่งต่อหรือแลกเปลี่ยนข้อมูลที่มีความแตกต่างทางการศึกษาวิจัยทางด้านเทคโนโลยีวิทยาศาสตร์ มีการแลกเปลี่ยนข้อมูลขนาดใหญ่ระหว่างในประเทศและทั่วโลก อาจารย์ นักศึกษา นักวิจัย จะได้รับประกันความปลอดภัยในการใช้งานในการถ่ายโอนข้อมูลที่เกี่ยวข้องกับการศึกษาวิจัย และได้รับการสนับสนุนการจัดการระบบเครือข่ายที่มีประสิทธิภาพและขนาดของแบนด์วิธที่เลือกใช้ได้เหมาะสมตามความต้องการ ซึ่งจะไม่ยุ่งเกี่ยวกับเครือข่ายสาธารณะอื่น ๆ ที่ใช้ทั่วไป ขณะนี้การบริการของ UniNet Layer 2 ได้จัดหาเครือข่ายระดับชาติที่มีขนาดและมีความยืดหยุ่นตามความเหมาะสมและความต้องการของสมาชิกที่สร้างวงจรส่วนตัวเสมือน VPN บนเลเยอร์ 2 ระหว่างจุดปลายทาง (Endpoint) บนเครือข่าย UniNet Layer 2 เพื่อตอบสนองทุกความต้องการของผู้ใช้เครือข่ายอินเทอร์เน็ตที่สนับสนุนในส่วนของการศึกษาและวิจัยหรือการจัดกิจกรรมการเรียนการสอน โดยไม่ต้องไปแย่งช่องทางกับผู้อื่นในเครือข่ายสาธารณะ

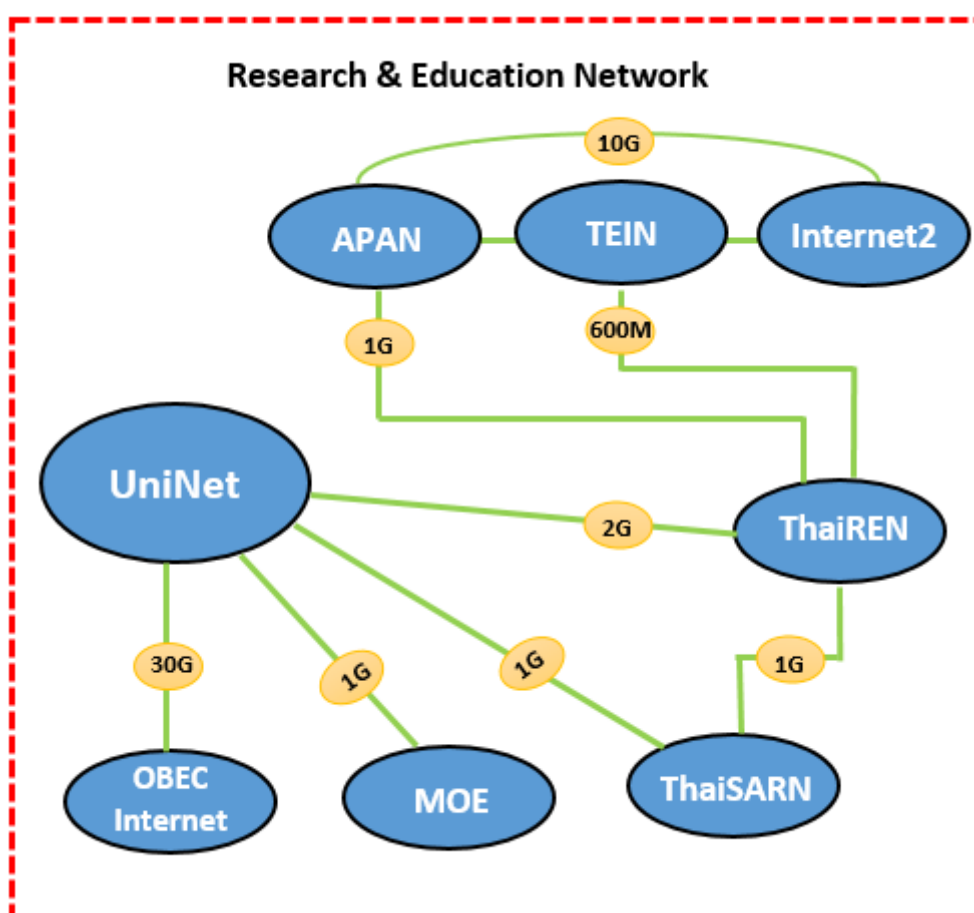
การบริการของ UniNet เป็นองค์การไม่แสวงหากำไร ไม่มีค่าใช้จ่ายในการขอใช้บริการ มีความน่าเชื่อถือสูง มีระบบเครือข่ายขั้นสูงซึ่งถูกออกแบบมาเพื่อการศึกษาวิจัยต่าง ๆ เมื่อต้องการใช้งานเครือข่ายสามารถติดต่อโดยทำหนังสือขอใช้งานบริการโดยตรงที่ UniNet เพราะเป็นเครือข่ายที่สนับสนุนทางด้านการศึกษาวิจัยโดยเฉพาะ



ภาพที่ 3-4 แสดงแผนที่การบริการเครือข่ายเพื่อการศึกษาวิจัยที่ครอบคลุมทั้งประเทศ

ที่มา: [http://www.uni.net.th/UniNet/uninet\\_network\\_map.php](http://www.uni.net.th/UniNet/uninet_network_map.php)

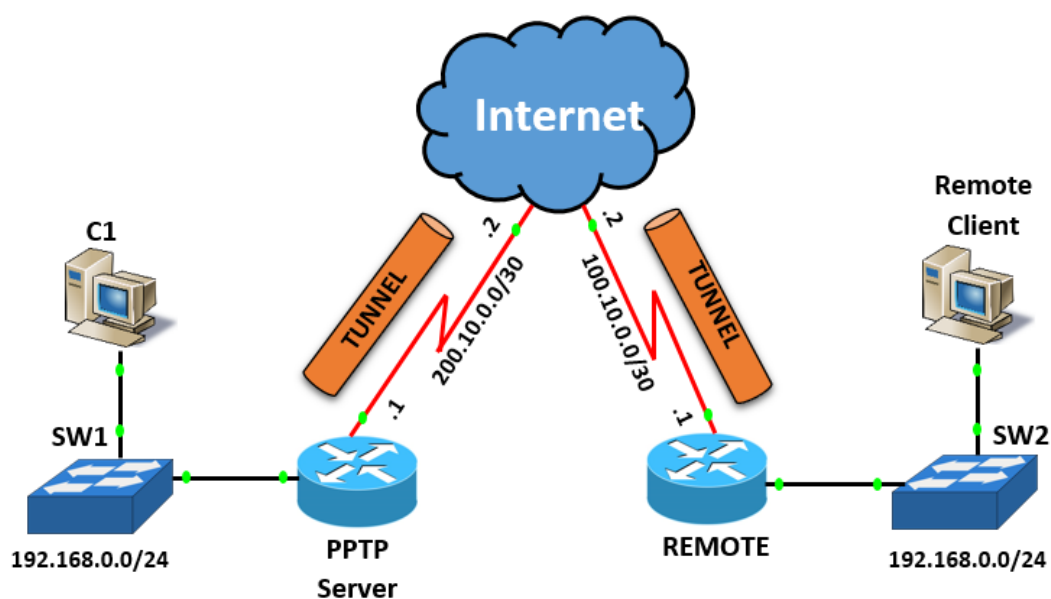
เครือข่ายประเภทที่มีการจัดตั้งและสร้างขึ้นมาเพื่อการศึกษาและวิจัย จะเรียกกันในนามของ REN (Research and Education Network) โดยปัจจุบันหลากหลายประเทศต่าง ๆ ทั่วโลกนั้นมีการจัดตั้งและสร้างขึ้นมาโดยเฉพาะในทุกประเทศ ในส่วนของประเทศไทยนั้น UniNet ได้จัดตั้งกลุ่มในนามของ ThaiREN เพื่อประสานงานความร่วมมือระหว่างหน่วยงานทางการศึกษาและวิจัยทั้งในประเทศและต่างประเทศ รวมถึงการเชื่อมต่อเข้ากับเครือข่ายศึกษาวิจัยอื่น ๆ และรวมกลุ่มกันจนเกิดเป็นชุมชน Community ทางด้านการศึกษาและวิจัย เช่น Internet2 ซึ่งเชื่อมโยงมหาวิทยาลัยชั้นนำในสหรัฐอเมริกา, APAN ซึ่งเชื่อมโยงสถาบันการศึกษาวิจัยในทวีปเอเชียแปซิฟิก, TEIN4 ซึ่งเชื่อมโยงสถาบันการศึกษาและวิจัยในทวีปเอเชียและยุโรป



ภาพที่ 3-5 การเชื่อมต่อเครือข่ายของ UniNet กับเครือข่าย REN อื่น ๆ

### 3.2.1 บริการเลเยอร์ 2 บนเครือข่ายการศึกษาวิจัย

ปัจจุบันได้มีการพัฒนาเทคโนโลยีของการเชื่อมต่อแบบ L2VPN (Layer 2 Virtual Private Network) ซึ่งเป็นเทคโนโลยีที่มีการพัฒนาเพื่อใช้งานบนเครือข่าย MPLS (Multi-Protocol Label Switching) จะคล้าย ๆ กับเป็นการสร้างอุโมงค์บนช่องทางอินเทอร์เน็ต โดยมีระดับความปลอดภัยของข้อมูลเทียบเท่าระบบ Switching Network เพราะ L2VPN มอง provider เป็น switch ตอบโจทย์ในเรื่อง ความเร็วและความปลอดภัยสูง อีกทั้งยังมีความคล่องตัวในการกำหนดขนาดช่อง ความเร็วแบนด์วิธได้ตามความต้องการเพื่อให้เหมาะสมกับความจำเป็นและยังสามารถกำหนดจุดปลายทางได้



ภาพที่ 3-6 Topology VPN เบื้องต้นโดยใช้โปรโตคอล PPTP

จากภาพที่ 3-6 แสดง Topology การทำ VPN เบื้องต้นโดยเราเตอร์ Cisco 3600 และใช้โปรโตคอล PPTP (Point-to-point) โดยการทำงานในลักษณะของไคลเอนต์และเซิร์ฟเวอร์ จะทำงานโดยใช้ซอฟต์แวร์ทำหน้าที่สร้างอุโมงค์ข้อมูล และมีหน้าที่ในการเข้ารหัสและการถอดรหัสข้อมูลบนคอมพิวเตอร์ ซึ่งมีการติดตั้งซอฟต์แวร์เข้าไปในเครื่องไคลเอนต์เพื่อเชื่อมต่อกับเซิร์ฟเวอร์ที่ติดตั้งซอฟต์แวร์ VPN แล้วสร้างอุโมงค์ข้อมูลเชื่อมต่อกันขึ้น ในครั้งนี้เครื่องไคลเอนต์จะทำ VPN Connection จากระบบปฏิบัติการ Windows ไปยังเซิร์ฟเวอร์

ตารางที่ 3-1 ความแตกต่างระหว่าง L2VPN และ L3VPN

L2VPN	L3VPN
<ul style="list-style-type: none"> <li>• Service Provider จะไม่มีการแลกเปลี่ยน routing information ไม่ยุ่งเกี่ยวกับ routing กับผู้ใช้บริการ</li> <li>• ส่งข้อมูลเป็น Frame จาก router ของผู้ใช้บริการฝั่งหนึ่งไปยัง อีกฝั่งหนึ่งผ่านทางอุโมงค์ Tunnel หรือ Virtual Circuit (VC)</li> <li>• ผู้ใช้บริการมอง router ฝั่ง Service Provider เสมือนเป็นสาย LAN ระยะไกลหรือ Switch ตัวหนึ่ง ที่จะเชื่อมต่อไปยังจุดต่อจุดหรือหลายจุดเข้าหากันก็ได้ นิยมใช้แบบจุดต่อจุด</li> <li>• Provider Edge Router (PE) เป็นทางผ่าน โดย PE ทั้ง 2 ฝั่งจะต้องสร้าง Tunnel ระหว่างกัน โดยเรียกกันว่า Virtual Circuit (VC) หรือ Pseudo Wire (PW) หรือ Virtual Link ถูกมองเป็น Link เท่านั้น</li> <li>• configure IP Address อินเทอร์เน็ตของ Customer Edge router (CE) ทั้งสองฝั่งให้อยู่ใน subnet เดียวกัน</li> <li>• PE router จะส่ง routing update ผ่านไปที่ CE เท่านั้น โดยจะไม่เข้าแลกเปลี่ยน routing update กับ CE และจะไม่ run routing protocol กับ CE ด้วย</li> </ul>	<ul style="list-style-type: none"> <li>• Service Provider จะมีบริการเกี่ยวกับการ routing ให้แก่ผู้ใช้บริการ โดยที่ routing information ของผู้ใช้บริการแต่ละรายจะไม่เกี่ยวข้องกัน</li> <li>• router ฝั่งผู้ใช้บริการมองทั้งเครือข่ายของ Service Provider เสมือนเป็น router ตัวใหญ่ๆ ตัวหนึ่ง นิยมใช้การเชื่อมแบบหลายจุดเข้าหากัน</li> <li>• PE กับ CE ใน L3VPN เชื่อมต่อกันด้วย IP และอินเทอร์เน็ตเฟสของทั้ง PE และ CE ต้องอยู่ใน subnet เดียวกัน</li> <li>• ผู้ใช้บริการมอง PE เสมือนเป็น router ตัวหนึ่ง ในเครือข่ายของผู้ใช้บริการเพราะ CE กับ PE จำเป็นต้อง run routing protocol เพื่อแลกเปลี่ยน routing information ซึ่งกันและกัน</li> </ul>



ตารางที่ 3-2 ประโยชน์ L2VPN และ L3VPN

L2VPN	L3VPN
<ul style="list-style-type: none"> <li>• มีความยืดหยุ่นสูงโดยเฉพาะการทำ Remote Access ให้ผู้ใช้ติดต่อเข้ามาใช้งานเครือข่ายจากภายนอกสถานที่และสามารถรองรับการเพิ่มการขยายของแบนด์วิธตามความต้องการของผู้ใช้บริการ</li> <li>• สามารถใช้งานได้จากทุกที่ทั่วโลก</li> <li>• สามารถเพิ่มไซต์หรือสาขาของ VPN ใหม่ได้ง่าย โดยที่ไม่มีการเปลี่ยนแปลงที่ระบบเครือข่าย</li> <li>• สามารถใช้งานได้กับพอร์ตของเราเตอร์ได้จากทุกหนทุกแห่ง</li> <li>• องค์กรหรือผู้ให้บริการดูแลรักษาระบบเครือข่ายเองได้ง่าย</li> <li>• สามารถใช้ MPLS ได้</li> <li>• แอปพลิเคชันจะเขียนบน Non-IP Protocols ได้แก่ SNA, IP.X และอื่น ๆ เป็นต้น</li> </ul>	<ul style="list-style-type: none"> <li>• สามารถใช้งานได้จากทุกที่ทั่วโลก</li> <li>• Service Provider บริหารจัดการและดูแลรักษา กำหนดเส้นทางทั้งหมด รวมถึงข้อมูลการ routing และการเปลี่ยนแปลงต่าง ๆ ของระบบเครือข่าย</li> <li>• จัดจ้างแผนกไอทีจากภายนอกเพื่อคอยดูแลรักษา กำหนด ควบคุมการตัดสินใจในระบบ routing ของเครือข่ายทั้งหมด</li> <li>• ส่วนมากแอปพลิเคชันจะเป็น IP-based applications</li> </ul>

## การเปรียบเทียบ L2VPN และ L3VPN

ในโครงการนี้สนใจในส่วนของ L2VPN และการเปรียบเทียบ มีดังต่อไปนี้

1. มีความยืดหยุ่นสูง L2VPN โดยมีการเชื่อมต่อเฉพาะที่เลเยอร์ 2 ซึ่งไม่ได้เข้าไปเกี่ยวข้องกับ การแลกเปลี่ยน routing information กับผู้ใช้บริการ สามารถลดภาระ (Load) ของ PE หรือแม้กระทั่ง ภาระ (Load) ของระบบเครือข่ายของ Service Provider ทั้งหมด และรองรับการใช้งาน VPN ที่ เพิ่มขึ้นด้วย

2. มีความเชื่อถือ ความปลอดภัยความเป็นส่วนตัวของ routing information สูง เพราะไม่ได้เข้าไป เกี่ยวข้องกับการแลกเปลี่ยน routing information กับผู้ใช้บริการ ซึ่ง L2VPN จะไม่รับเอา routing information ของผู้ใช้บริการมาและรับประกันความปลอดภัย routing information ของผู้ใช้บริการ VPN

3. สนับสนุนโปรโตคอลที่ทำงานในหลาย ๆ เลเยอร์ (multiple network layer protocols) เช่น IP, IPX, and SNA เป็นต้น

เครือข่ายเพื่อการศึกษาวิจัยเป็นเครือข่ายที่ให้การสนับสนุนการบริการเครือข่ายเกี่ยวกับด้าน การศึกษาและการวิจัยของสถาบันการศึกษาและมหาวิทยาลัยต่าง ๆ โดยบริการที่สนใจศึกษาใน โครงการนี้คือบริการ L2VPN (Layer2 Virtual Private Network) ซึ่งรายละเอียดของการบริการ บริการ L2VPN จะใช้ MPLS (Multiprotocol Label Switch) ในการส่งข้อมูลและผู้สนใจใช้บริการจะ ได้ VLAN แบบ PTP (Point-to-Point) ไปใช้นั่นเอง

ตัวอย่างของโครงการที่ใช้ L2VPN ได้แก่ ศูนย์วิทยพัฒนามหาวิทยาลัยสุโขทัยธรรมาราช ซึ่งเป็นหน่วยงานหนึ่งของมหาวิทยาลัยที่มีสาขที่ตั้งอยู่ในส่วนภูมิภาคต่าง ๆ ได้ใช้บริการ L2VPN ในการเชื่อมต่อศูนย์วิทยพัฒนาทั้งหมด 10 ศูนย์กระจายไปตามจังหวัดต่าง ๆ ทั่วทุกภาคของประเทศไทยไว้ด้วยกันและสามารถติดต่อกันได้อย่างทั่วถึงเพื่อทำหน้าที่สนับสนุนระบบการจัดการเรียน การสอนทางไกลของแต่ละมหาวิทยาลัย ศูนย์วิทยพัฒนาทั้งสิ้น 10 ศูนย์มีดังต่อไปนี้

1. ศูนย์วิทยพัฒนามสธ. จังหวัดจันทบุรี
2. ศูนย์วิทยพัฒนามสธ. จังหวัดเพชรบุรี
3. ศูนย์วิทยพัฒนามสธ. จังหวัดนครนายก
4. ศูนย์วิทยพัฒนามสธ. จังหวัดนครศรีธรรมราช
5. ศูนย์วิทยพัฒนามสธ. จังหวัดนครสวรรค์
6. ศูนย์วิทยพัฒนามสธ. จังหวัดลำปาง

7. ศูนย์วิทยพัฒนามสธ. จังหวัดยะลา
8. ศูนย์วิทยพัฒนามสธ. จังหวัดสุโขทัย
9. ศูนย์วิทยพัฒนามสธ. จังหวัดอุบลราชธานี
10. ศูนย์วิทยพัฒนามสธ. จังหวัดอุดรธานี

นอกจากการรวมกลุ่มกันของแต่ละสถาบันการศึกษาเพื่อสนับสนุนการจัดการระบบการศึกษาทางไกลแล้ว ในการบริการ Layer 2 นั้นสามารถทำการ VDO conference เพื่อทำการประชุมจากต่างสถานที่ได้ และสามารถถ่ายทอดกิจกรรมทางการแพทย์อย่างเช่น การผ่าตัดเพื่อเป็นกรณีศึกษาเป็นต้น

### 3.3 สถาปัตยกรรม Science DMZ

ในโครงการได้ศึกษาสถาปัตยกรรม Science DMZ เป็นกรณีศึกษาเพื่อนำมาปรับใช้ได้ในได้อินาคตซึ่งถูกออกแบบโดยวิศวกรของ Esnet รูปแบบของ Science DMZ เป็นรูปแบบการใช้งานเครือข่ายร่วมกันของสถาบันการศึกษาซึ่งปรับปรุงแก้ไขปัญหาที่พบมากในสถาบันวิจัยต่าง ๆ เพื่อปฏิบัติการทำงานร่วมกันที่ดีที่สุด องค์ประกอบที่สำคัญของ Science DMZ คือ มีความยืดหยุ่น (scalable) ซึ่งเป็นรูปแบบการทำงานที่สนับสนุนการทำงานทางด้านวิทยาศาสตร์ในสถาบันการวิจัยต่าง ๆ รวมไปถึงการส่งการถ่ายโอนข้อมูลขนาดใหญ่มาก การควบคุมการทดลองในระยะไกล และการวิเคราะห์นำเสนอข้อมูลขนาดใหญ่ (Data Visualization) สามารถปรับและขยายแบบดัดวิธีให้มีความยืดหยุ่นได้ มีประสิทธิภาพสูงขึ้นและง่ายต่อการประยุกต์ใช้เพื่อรวบรวมเทคโนโลยีที่เกิดขึ้นใหม่ไว้ด้วยกัน เช่น 100 Gigabit Ethernet services, virtual circuits, และ SDN (software-defined networking)

รูปแบบการทำงาน Science DMZ ได้ถูกใช้งานอย่างแพร่หลายและเป็นสถาปัตยกรรมที่ได้การ ซึ่งจะอนุญาตให้มีการเคลื่อนย้ายถ่ายโอนหรือแชร์ข้อมูลที่มีขนาดใหญ่มาก ระหว่าง อาคาร สถานที่ หรือสถาบันการศึกษาต่าง ๆ เพื่อให้มั่นใจว่าข้อมูลนั้นถูกเคลื่อนย้ายอย่างปลอดภัยและเป็นส่วนหนึ่งของเครือข่าย ซึ่งถูกสร้างขึ้นเพื่อใช้กับสถาบันการศึกษาหรือ local perimeter network ของห้องปฏิบัติการ ซึ่งถูกออกแบบมาในลักษณะของอุปกรณ์ การ configuration หรือนโยบายการรักษาความปลอดภัยที่เหมาะสมสำหรับเพิ่มประสิทธิภาพการใช้งานของอินเทอร์เน็ตทางด้านวิทยาศาสตร์มากกว่าวัตถุประสงค์ทางธุรกิจ

สถาปัตยกรรม Science DMZ ประสบความสำเร็จอย่างมากมาในด้านวิทยาศาสตร์ เช่น เครื่อง Supercomputer center ของ NERSC ที่อำนวยความสะดวกในการร่วมมือกันของเครื่องยิงอนุภาคแฮดรอน (Large Hadron Collider collaboration) ซึ่งรูปแบบของ Science DMZ ถูกพัฒนาจากห้องปฏิบัติการและมหาวิทยาลัยต่าง ๆ โดยการร่วมมือกันกับ Internet2 และ Science DMZ มีบทบาทมากในส่วนของการพัฒนารูปแบบนวัตกรรมใหม่ ๆ บนบริการเลเยอร์ 1, 2, 3 ในการทำงานร่วมกันจะมีการเชื่อมต่อห้องปฏิบัติการของสมาชิกของแต่ละสถาบันวิจัยต่าง ๆ เชื่อมต่อกันโดย internet2 มีจุดประสงค์เพื่อที่จะช่วยให้สมาชิกไม่ว่าจะเป็น นักศึกษาหรือคณาจารย์ของสถาบันการศึกษาหรือมหาวิทยาลัยต่าง ๆ นั้นสามารถใช้ประโยชน์จากความสามารถของระบบเครือข่ายขั้นสูง (Advanced Network) เพื่อช่วยเร่งให้เกิดการค้นพบการวิจัยใหม่ ๆ ในแต่ละสถาบันการศึกษา ซึ่งกุญแจสำคัญของ Science DMZ ก็คือ

- ลดและจัดการปัญหาการสูญหายข้อมูล (Packet loss) ที่เกิดจากประสิทธิภาพของ TCP ที่ต่ำ
- เข้าถึงทรัพยากรจากการศึกษาวิจัยจากต่างประเทศต่าง ๆ ได้โดยใช้ Virtual Circuit, Software Defined Networking (SDN) และ 100 Gigabit infrastructures ได้
- การทดสอบเครือข่าย (network testing) การตรวจวัดเครือข่าย (network measurement) และการวิเคราะห์สมรรถนะ (performance analysis) โดยใช้งาน perfSONAR แก้ไขได้โดยง่าย

ทำไมต้องเป็น Science DMZ

ห้องปฏิบัติการห้องแลปโดยปกติมักจะสนับสนุนการทำงานหรือภารกิจของแต่ละองค์กร โดยที่เริ่มแรกจะต้องมีการจัดหาโครงสร้างพื้นฐานสำหรับการจราจรของเครือข่าย (Network traffic) เกี่ยวข้องกับการปฏิบัติการหรือการดำเนินธุรกิจทั่วไปขององค์กรหรือไม่ รวมทั้ง อีเมลล์ ระบบจัดซื้อ web browsing และอื่น ๆ ระบบเครือข่ายจึงจำเป็นต้องมีคุณลักษณะการรักษาความปลอดภัยที่คอยป้องกันข้อมูลทางการเงินหรือข้อมูลบุคลากรขององค์กรที่ดี และในเวลาเดียวกันนั้นเครือข่ายเหล่านี้ยังใช้เป็นเครือข่ายพื้นฐานของกระบวนการการวิจัยทางด้านวิทยาศาสตร์ของ นักวิจัย หรือนักวิทยาศาสตร์ขึ้นอยู่กับโครงสร้างพื้นฐานเพื่อจะแชร์แบ่งปัน และใช้จัดเก็บหรือวิเคราะห์ข้อมูลการวิจัยจากแหล่งข้อมูลภายนอกที่แตกต่างกัน

อย่างไรก็ตามในกรณีส่วนใหญ่ เครือข่ายจะใช้ทำให้การใช้งานที่ดีที่สุดหรือมีประสิทธิภาพมากที่สุดสำหรับการดำเนินกิจการทางธุรกิจหรือการใช้งานขององค์กรต่าง ๆ เรียกการใช้งานเครือข่ายเหล่านี้ว่าเครือข่าย “General-purpose Network” ซึ่งไม่ได้รับการออกแบบมาเพื่อสนับสนุนหรือรองรับความต้องการการใช้งานทางด้านการศึกษาวิจัยหรือด้านวิทยาศาสตร์มากนัก ซึ่งเมื่อนักวิทยาศาสตร์ใช้งานเครือข่ายที่หนาแน่นกับข้อมูลที่มีขนาดใหญ่มากก็มักจะพบปัญหาประสิทธิภาพต่ำและ

เกิดความล่าช้า ในหลายกรณีแล้วแต่ส่งผลกระทบต่อกิจกรรมหรือภารกิจทางด้านวิทยาศาสตร์อย่างมีนัยสำคัญ

รูปแบบของ Science DMZ สำเร็จเห็นผลได้ชัดเจนโดยสร้างส่วนหนึ่งของเครือข่าย ซึ่งถูกวางแผนออกแบบมาโดยเฉพาะสำหรับการใช้งานด้านการศึกษาวิจัยด้านวิทยาศาสตร์ ไม่สนับสนุนจุดประสงค์การใช้งานทั่วไป (general-purpose use) โดยจะแยกระบบเครือข่ายทางวิทยาศาสตร์ที่มีประสิทธิภาพสูง (Science DMZ) ออกจากระบบเครือข่ายที่ใช้งานทั่วไป ซึ่งแต่ละเครือข่ายก็สามารถทำงานได้อย่างมีประสิทธิภาพโดยปราศจากการรบกวนซึ่งกันและกัน

#### การพัฒนาของ Science DMZ

ในขณะที่ภารกิจหลักของ Science DMZ สนับสนุนการใช้งานทางด้านการศึกษาวิจัยการทดลองด้านวิทยาศาสตร์ที่มีประสิทธิภาพสูงและจะไม่สามารถเกิดขึ้นได้ถ้าขาดการร่วมมือทางด้านวิทยาศาสตร์ โดยความพยายามเชื่อมต่อเครือข่ายแบบปลายทางสู่ปลายทาง (end-to-end) ซึ่งมีรูปแบบการบริการการสนับสนุนการรวมตัวทางด้านการศึกษาวิจัยวิทยาศาสตร์อย่างกว้างขวาง รวมไปถึง virtual circuits และ SDN (software defined networking) และเทคโนโลยีใหม่ เช่น 100 gigabit Ethernet ในขณะที่เครือข่ายทั่วไป (General-purpose network) อาจต้องพยายามอย่างมากที่จะทำให้การใช้งานเทคโนโลยีที่มีประสิทธิภาพสูงเหมือนกับรูปแบบการบริการนี้ Science DMZ จะอนุญาตให้ทรัพยากรทางด้านวิทยาศาสตร์ท้องถิ่นเชื่อมต่อกันกับบริการของเครือข่ายที่ต้องการจะดำเนินการทางด้านวิทยาศาสตร์ โดยปราศจากการรบกวนกับโครงสร้างพื้นฐานของเครือข่ายที่มีจุดประสงค์ใช้งานทั่วไปนั่นเอง

สถาปัตยกรรม Science DMZ เป็นรากฐานพื้นฐานของการออกแบบเครือข่าย การดำเนินการหรือการรักษาความปลอดภัย ซึ่ง Science DMZ มาจาก DMZ network ซึ่งเป็นองค์ประกอบทั่วไปในสถาปัตยกรรมความปลอดภัยของเครือข่าย จุดประสงค์พิเศษของ Science DMZ คือ

- บริเวณใกล้เคียง network perimeter เพิ่มเข้ามาเพื่อความปลอดภัยการออกแบบคือ host ส่วนของ site service ที่เชื่อมต่อกับเน็ตเวิร์กภายนอก เช่น external web, incoming email, และ authoritative DNS servers
- นโยบายความปลอดภัยต่าง ๆ
- Network device configuration
- Tailored for the DMZ ซึ่งไม่ได้รวมกับนโยบายการรักษาความปลอดภัยและโครงสร้างการ configuration ของเน็ตเวิร์กภายใน internal local area (LAN)

Science DMZ คือแนวคิดเพื่อสนับสนุนการดำเนินการทางด้านการศึกษาวิจัยวิทยาศาสตร์ รวมถึงการเคลื่อนย้ายข้อมูลขนาดใหญ่ หรือตัวอย่างข้อมูลการทดลองอย่างละเอียดโดย Science DMZ ที่ส่วนของ campus จะอยู่ติดกับ perimeter network ถูกออกแบบและคอนฟิก เพื่อสนับสนุนการดำเนินการทางด้านการศึกษาวิจัยวิทยาศาสตร์ และเมื่อมีเหตุขัดข้องยังสามารถจะแสดงลักษณะขัดข้องและแก้ไขปัญหาได้ ดังนั้นปัญหาจึงสามารถได้รับการแก้ไขอย่างรวดเร็วโดยใช้ perfSONAR ซึ่งสามารถจะทดสอบในบริเวณกว้างได้ หรือบริเวณที่ทำงานร่วมกันกับห้องทดลองของมหาวิทยาลัยต่าง ๆ

perfSONAR คือ Toolkit สำหรับตรวจสอบหรือวัดประสิทธิภาพของเครือข่าย ซึ่งรวมถึงชุดเครื่องมือวินิจฉัยเครือข่ายให้ง่ายในการแก้ปัญหาประสิทธิภาพการทำงานแบบ end-to-end สามารถตรวจสอบการแลกเปลี่ยนข้อมูลระหว่างเครือข่าย เพื่อลดความซับซ้อนของปัญหาประสิทธิภาพระบบเครือข่าย การแก้ไขปัญหาที่เกิดขึ้นระหว่างโหนดที่เชื่อมต่อผ่านเครือข่ายหลายเครือข่าย เช่น ศูนย์วิจัยแห่งชาติและเครือข่ายการศึกษาและอื่น ๆ ตัวอย่างเช่น trace route perfSONAR สามารถแสดงแบนด์วิดท์ที่ใช้ในการเชื่อมโยงทั้งหมดของเส้นทางที่กำหนด แบนด์วิดท์จะถูกดึงมาจากคลังเก็บบริการของชุด perfSONAR ว่าการแลกเปลี่ยนการใช้การเชื่อมโยงในส่วนหนึ่งของเส้นทางทั้งหมด ในลักษณะที่เป็นมาตรฐานหรือไม่ เครื่องมือนี้จะทำให้ง่ายต่อการค้นหาที่มาของ congestions ซึ่งส่งผลให้เกิดปัญหาประสิทธิภาพของระบบเครือข่าย

Science DMZ ช่วยเรื่องของประสิทธิภาพของใน TCP

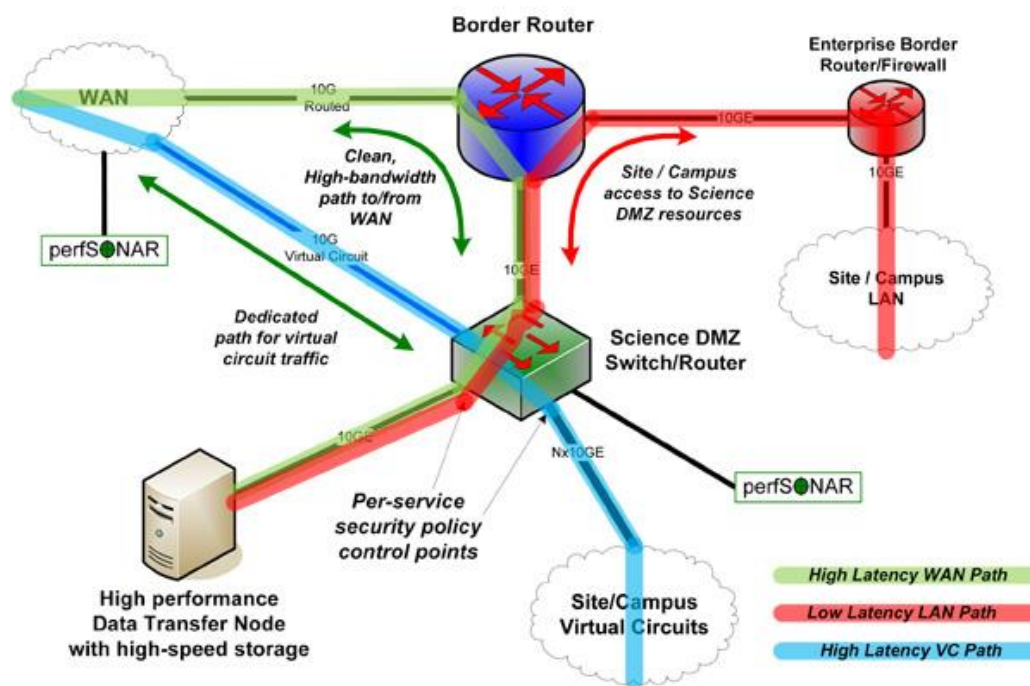
สำหรับการเคลื่อนไหวของข้อมูล (data movement) และการเกิดการสูญหายของข้อมูล (packet loss) สามารถทำให้เกิดปัญหาในประสิทธิภาพ TCP packet loss ถือเป็นความแออัดของเครือข่าย (network congestion) และเมื่อการสูญหายเกิดขึ้นใน TCP แล้วจะทำให้อัตราการส่งข้อมูลลดลง ถ้าเกิดการสูญหายเรื่อย ๆ ต่อไปก็จะเกิดอัตราการส่งลดลงอย่างต่อเนื่อง จะกลายเป็นปัญหาใหญ่ของการติดต่อสื่อสารแม้กระทั่งปัญหาการสูญหายเล็ก ๆ น้อยกว่า 1% ก็เพียงพอที่จะทำให้ประสิทธิภาพของ TCP ลดลงได้ มันจะง่ายถ้าปรับการจัดการ TCP มากกว่าปรับปรุง TCP เพื่อลดการอดทน (loss tolerate) นั่นหมายถึง โครงสร้างเครือข่ายที่สนับสนุนการดำเนินการทางด้านการศึกษาวิจัยวิทยาศาสตร์ควรจัดหา loss-free IP service to TCP สำหรับกรณีปกติ รูปแบบ science DMZ จะอนุญาตให้ห้องปฏิบัติการสถาบันการศึกษาต่าง ๆ สร้างโครงสร้างจุดประสงค์พิเศษ ซึ่งมีบริการที่อนุญาตให้การดำเนินการทางด้านการศึกษาวิจัยวิทยาศาสตร์ให้ทำงานได้อย่างมีประสิทธิภาพ

Science DMZ Architecture

สถาปัตยกรรม Science DMZ ตรงกับความต้องการเครือข่ายที่ยืดหยุ่น (scalable network) ซึ่งอำนวยความสะดวกอย่างชัดเจน กับการดำเนินกิจกรรมทางด้านการศึกษาวิจัยวิทยาศาสตร์ให้มีประสิทธิภาพสูง ในขณะที่ไม่ต้องแย่งเครือข่ายกับการใช้งานอินเทอร์เน็ตทั่วไป

Science DMZ เชื่อมต่อโดยตรงไปที่ border router เพื่อที่จะลดจำนวนของอุปกรณ์ที่ต้องกำหนดค่า Configure เพื่อสนับสนุน การส่งหรือถ่ายโอนข้อมูลขนาดใหญ่ที่มีประสิทธิภาพสูงและการประยุกต์ใช้งานในด้านการดำเนินกิจกรรมทางด้านการศึกษาวิจัยวิทยาศาสตร์อื่น ๆ การทำให้เครือข่ายมีประสิทธิภาพเป็นเรื่องที่ยากที่จะทำต่อระบบทั้งหมด โดยกำหนดค่าเริ่มต้นของอุปกรณ์เครือข่ายแต่ละตัวในสถานที่ต่าง ๆ Science DMZ ที่ site perimeter ช่วยลดความยุ่งยากของระบบและกระบวนการการปรับแต่งเครือข่าย นอกจากนี้ถ้ามีปัญหาประสิทธิภาพการทำงานจะเป็นเรื่องง่ายที่จะแก้ไขปัญหของอุปกรณ์ มากกว่าแก้ไขวัตถุประสงค์โครงสร้างพื้นฐานระบบ LAN ขนาดใหญ่

Simple Science DMZ มีองค์ประกอบที่สำคัญ เช่น ประสิทธิภาพของ WAN และโครงสร้างการบริการอุปกรณ์เครือข่ายที่มีประสิทธิภาพสูงและทรัพยากรด้านวิทยาศาสตร์ เช่น Data Transfer Node (DTN) โดยทั่วไปแล้วระบบคอมพิวเตอร์ที่ใช้การถ่ายโอนข้อมูลบนพื้นที่บริเวณกว้างและอยู่ห่างไกลกันมากต้องใช้ DTN ซึ่งเป็น PC-based Linux servers ที่มีประสิทธิภาพสูงและถูกกำหนดค่าเฉพาะสำหรับการถ่ายโอนข้อมูลพื้นที่บริเวณกว้างอยู่ห่างไกลกันมาก DTN สามารถเข้าถึง local storage หรือเรียกว่า เป็น local high-speed disk subsystem เชื่อมต่อกับโครงสร้างของ Local storage เช่น Storage Area network (SAN) จะเชื่อมต่อเข้ากับ High-speed parallel system file เช่น GPFS หรือเชื่อมต่อโดยตรงเข้าด้วยกันทั้งหมด ซึ่ง DTN จะมี software tool ที่ออกแบบมาเพื่อการถ่ายโอนข้อมูลที่รวดเร็วของระบบที่อยู่ห่างไกลกันคือ GridFTP (Grid File Transfer Protocol) ช่วยในการถ่ายโอนไฟล์ที่ดีที่สุดและมีความน่าเชื่อถือสำหรับประสิทธิภาพไฟล์ขนาดใหญ่ สำหรับการเชื่อมโยงแต่ละโหนดที่ติดต่อกันหรือทำงานร่วมกันภายใต้ Globus Online เป็นเทคโนโลยีของเว็บเซอร์วิสที่ทำให้กริดโหนดสามารถติดต่อสื่อสารกันได้ ซึ่ง DTN จะมี high-speed network interfaces ถึง 10Gbps และสามารถมีได้มากถึง 40Gbps



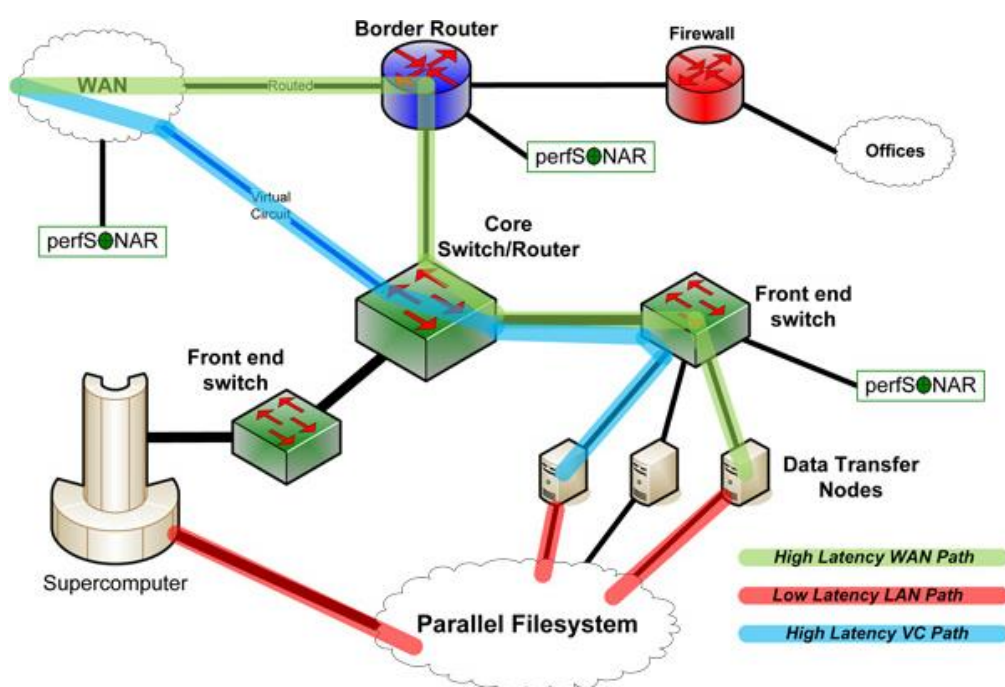
ภาพที่ 3-7 simple science DMZ diagram

ที่มา : <http://fasterdata.es.net/assets/dmz-simple-vc.jpg>

จากภาพที่ 3-7 แสดงองค์ประกอบที่สำคัญและ data path ของสถาปัตยกรรม Science DMZ อย่างง่าย จะเห็นได้ว่า DTN จะเชื่อมต่อโดยตรงกับสวิตช์หรือเราเตอร์ Science DMZ ที่มีประสิทธิภาพสูง ซึ่งเชื่อมต่อโดยตรงกับ Border Router หน้าที่ของ DTN คือการเคลื่อนย้ายข้อมูลทางวิทยาศาสตร์ขนาดใหญ่อย่างมีประสิทธิภาพของแต่ละ remote site เช่น สถาบันการศึกษาต่าง ๆ วัตถุประสงค์เพื่อการบังคับใช้นโยบายการรักษาความปลอดภัยสำหรับ DTN ทำได้โดยใช้ access control lists บน Science DMZ switch หรือ router ซึ่งไม่อยู่กับ firewall แยกออกจากหาก การเก็บข้อมูลจากขนาดใหญ่ในงานวิจัยด้านวิทยาศาสตร์หรือจากอุปกรณ์จัดเก็บข้อมูล เช่น ข้อมูลจากกล้องจุลทรรศน์ กล้องโทรทรรศน์ โดยมีฮาร์ดแวร์ที่ออกแบบมาเพื่อเป็นส่วนสำคัญในเป็นระบบบริหารจัดการจัดเก็บและดูแลกลุ่มของอุปกรณ์การจัดเก็บข้อมูลที่มีประสิทธิภาพสูง กลุ่มของอุปกรณ์การจัดเก็บข้อมูลเหล่านี้ มีการเชื่อมต่อกันทางด้านเครือข่ายกับระบบเครือข่ายภายในให้เป็นอันหนึ่งอันเดียวกัน เพื่อสะดวกในการถ่ายโอนหรือส่งข้อมูลไปสู่พื้นที่จัดเก็บหรือนำไปต่อยอดอย่างยืดหยุ่น อุปกรณ์จัดเก็บข้อมูลเหล่านี้มักจะไม่ได้เตรียมไว้สำหรับการเปิดเผยในเครือข่ายสาธารณะและควรที่จะได้รับการปกป้องคุ้มครอง ถ้า Firewall ต้องการมีนโยบาย local access ระหว่างอุปกรณ์จัดเก็บ



ข้อมูลระหว่างเครือข่ายภายนอก DTN จะมีเวลาหน่วงสั้น ๆ (short latency) คือเวลาที่ใช้ในการนำ 1 packet ของข้อมูล จากจุดหนึ่งไปอีกจุดหนึ่งเพื่อจะเอาชนะ overcome และมีผลกระทบต่อ protocol เช่น TCP ควรจะไม่ได้รับผลกระทบ ไม่ควรเกิดการ loss packet เส้นทางสีแดงในแผนผังด้านบนอธิบายได้ว่าเมื่อ latency น้อยจะสามารถส่งข้อมูลเร็วขึ้น

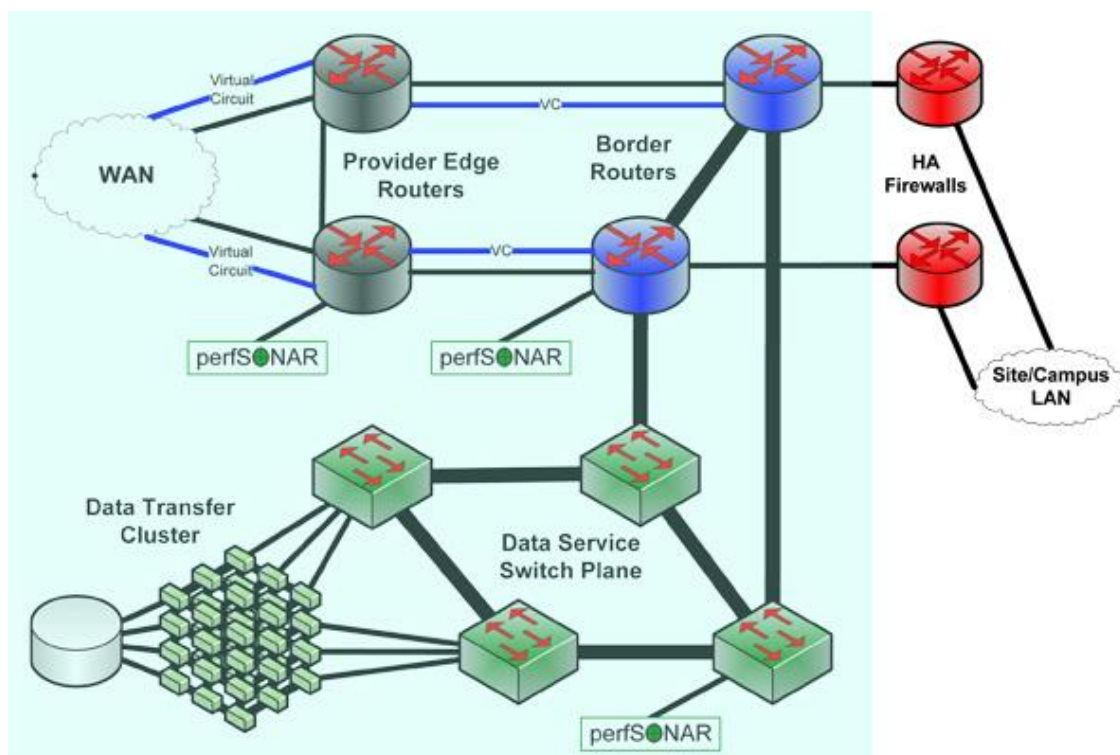


ภาพที่ 3-8 supercomputer center network

ที่มา: <http://fasterdata.es.net/assets/dmz-supercomputer.jpg>

ภาพที่ 3-8 แสดงเครือข่ายศูนย์ซูเปอร์คอมพิวเตอร์ Supercomputer แบบง่ายในกรณีที่อาจจะไม่เหมือนภาพที่ 3-8 ข้างต้น แต่มีหลักการเดียวกันถูกนำมาใช้ในการออกแบบ ในกรณีเครือข่ายศูนย์ซูเปอร์คอมพิวเตอร์ ซึ่งส่วนมากนั้นเป็นโครงสร้างพื้นฐานของเครือข่าย อาจจะเรียกได้ว่า Science DMZ ถูกสร้างขึ้นมาเพื่อจัดการกับอัตราการไหลข้อมูลอย่างสูงของข้อมูลโดยไม่เกิด packet loss และถูกออกแบบมาให้ง่ายต่อการแก้ไขปัญหาประสิทธิภาพของระบบเครือข่าย มีการทำงานการตรวจสอบ และการวัดเครื่องมือที่ใช้ perfSONAR ที่ช่วยวิเคราะห์ตรวจสอบข้อมูลการแลกเปลี่ยนระหว่างเครือข่าย ระบุตำแหน่งความผิดพลาด และแก้ไขปัญหาได้อย่างราบรื่นและรวดเร็ว มีการเข้าถึง access ไปที่ parallel file system ของการถ่ายโอนข้อมูลระหว่างพื้นที่บริเวณ

กว้างผ่าน Data Transfer Nodes (DTN) ซึ่ง DTN เมื่อต้องการจะจัดเก็บข้อมูลจะถูกถ่ายโอนไปที่ DTN และเขียนไปที่ parallel file system ซึ่งข้อมูลจะมีพร้อมอยู่ในทรัพยากรของ Supercomputer ทันทีโดยไม่จำเป็นต้องคัดลอกข้อมูลซ้ำ (double-copy)



ภาพที่ 3-9 big data site

ที่มา: <http://fasterdata.es.net/assets/dmz-bigdata.jpg>

ภาพที่ 3-9 แสดง Big Data Site สำหรับไซต์ (Site) ที่ต้องรับมือกับปริมาณข้อมูลขนาดใหญ่ เช่น การทดลองเครื่องชนอนุภาคแฮดรอนขนาดใหญ่ LHC ทำให้โหนดการถ่ายโอนข้อมูล DTN ไม่เพียงพอไซต์เหล่านี้ต้องการ Data Transfer Clusters เป็นกลุ่มของเครื่องมือรองรับการใช้งานและเข้าถึงจากหลาย ๆ โหนดและรองรับการจัดเก็บข้อมูลเก็บข้อมูลขนาดใหญ่มาก (multi-petabyte) แต่อย่างไรก็ตามหลักการของ Science DMZ จะปรับใช้กับระบบเพื่อใช้สำหรับการส่ง ถ่ายโอนข้อมูลขนาดใหญ่อย่างรวดเร็วและปลอดภัย ง่ายต่อการแก้ไขปัญหาประสิทธิภาพระบบเครือข่าย มีการทำงานการตรวจสอบการทดสอบ การวัดประสิทธิภาพเครือข่าย multiple location ระบบเครือข่าย

แบบนี้จะคล้ายกับระบบเครือข่ายศูนย์ซูเปอร์คอมพิวเตอร์ Supercomputer ซึ่งในส่วน of เส้นทางบริเวณกว้างนั้นจะครอบคลุมเครือข่ายทั้งหมด (front – end)

ระบบเครือข่ายนี้มีการเชื่อมต่อแบบ Redundant กับโครงข่ายเพื่อการศึกษาวิจัย Research Network Backbone ซึ่งมีความสามารถของการเร้าต IP และบริการวงจรเสมือน virtual circuit services ซึ่งระบบเครือข่ายนี้มี high-capacity redundant infrastructure นำมาใช้งานกับข้อมูลทางด้านวิทยาศาสตร์ที่มีข้อมูลขนาดใหญ่ และนำ redundant firewalls มาใช้งานและมีการควบคุมความปลอดภัยของข้อมูลบน routing และ switching plane เพื่อป้องกัน firewall จากการสร้างปัญหาเกี่ยวกับประสิทธิภาพการทำงานเพราะอัตราการส่งข้อมูลสูงมากเช่น 10 Gbit/s หรือ 100 Gbit/s มักอยู่นอกเหนือความสามารถของฮาร์ดแวร์ไฟร์วอลล์

## บทที่ 4

### การทดลองแบบจำลองระบบและการทดสอบ

จากการจำลองระบบ VPN โดยฝั่งไคลเอนต์สามารถเชื่อมต่อ VPN ไปหา Server ได้ทำให้ข้อมูลเดินทางผ่านอุโมงค์ การสนับสนุนกิจกรรมต่าง ๆ ทางด้านการศึกษาและใช้ทรัพยากรร่วมกัน โดยใช้ Federation Service ยืนยันตัวตนเข้าใช้งานทรัพยากรข้ามเครือข่าย เพื่อใช้งาน eduroam โครงสร้างสถาปัตยกรรม Science DMZ เป็นสิ่งที่ช่วยอำนวยความสะดวกทางด้านวิทยาศาสตร์ เพราะข้อมูลปริมาณมหาศาลนั้นต้องการความเร็วในการถ่ายโอนข้อมูล ความทนทาน ความยืดหยุ่น และมีความปลอดภัยที่สุด ถือเป็นนวัตกรรมใหม่ที่สามารถนำมาใช้ในอนาคตได้เพื่อประโยชน์สูงสุด โดยมีผลการทดลองและผลการศึกษาดังต่อไปนี้

#### 4.1 ผลการทดลองและผลการศึกษา

##### 4.1.1 ผลการทดสอบแบบจำลอง VPN

ในการทดลองวงจรมี VPN ได้มีการทดลองบนอุปกรณ์เราเตอร์ Cisco 3600 ซึ่งเป็นการจำลองการทำงานของเซิร์ฟเวอร์และไคลเอนต์โดยมีการสร้างท่ออุโมงค์ข้อมูล (Tunnel) เพื่อให้ข้อมูลเดินทางผ่านซึ่งเป็นช่องทางเฉพาะ มีดังผลการทดลองต่อไปนี้

```
C:\Users\VPN>tracert 192.168.0.100

Tracing route to 192.168.0.100 over a maximum of 30 hops
  0  <1 ms    <1 ms    <1 ms    192.168.10.1
  1  1 ms      1 ms      1 ms     100.10.0.2
  2  2 ms      2 ms      2 ms     200.10.0.1
  3  2 ms      2 ms      2 ms     192.168.0.100
Trace complete.

C:\Users\VPN>tracert 192.168.0.100

Tracing route to 192.168.0.100 over a maximum of 30 hops
  0  4 ms      4 ms      4 ms     200.10.0.1
  1  4 ms      5 ms      4 ms     192.168.0.100
Trace complete.
```

ภาพที่ 4-1 แสดง traceroute ของการเชื่อมต่อ VPN จาก remote client มายัง server

จากภาพที่ 4-1 แสดง traceroute โดยที่เมื่อมีการ connect VPN (เครือข่ายส่วนตัวเสมือน) จากฝั่ง remote client มายัง server จะพบว่าข้อมูลเดินทางผ่านท่อ Tunnel ที่เราสร้างไว้จริง

```

guest-oc6F0v@OFController:~$ tracepath 192.168.10.3
 1:  OFController.local                                0.
088ms pmtu 1500
 1:  192.168.0.1                                        1.
097ms
 1:  192.168.0.1                                        1.162ms
 2:  200.10.0.2                                         8.628ms
 3:  100.10.0.1                                        14.164ms
 4:  192.168.10.3                                     18.378ms reached
Resume: pmtu 1500 hops 4 back 125
guest-oc6F0v@OFController:~$ tracepath 192.168.0.103
 1:  OFController.local                                0.096ms pmtu 1500
 1:  192.168.0.1                                        1.831ms
 1:  192.168.0.1                                        1.070ms
 2:  192.168.0.103                                    21.509ms reached
Resume: pmtu 1500 hops 2 back 127
guest-oc6F0v@OFController:~$

```

ภาพที่ 4-2 แสดง trace route ของการเชื่อมต่อ VPN จาก server มายัง remote client

จากภาพที่ 4-2 แสดง trace route โดยที่เมื่อมีการ connect VPN (เครือข่ายส่วนตัวเสมือน) จากฝั่ง server มายัง remote client จะพบว่าข้อมูลเดินทางผ่านท่อ Tunnel ที่เราสร้างไว้จริง

```

C:\Windows\system32\cmd.exe

PPP adapter UPNConnection:

Connection-specific DNS Suffix . : 
IPv4 Address. . . . . : 192.168.0.104
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 0.0.0.0

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : fe80::9c3d:606:a73f:e5bb%11
IPv4 Address. . . . . : 192.168.0.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1

Tunnel adapter isatap.{D49C0D91-1BC0-4343-A579-DD1C1BB532F3}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 

C:\Users\UPN>
C:\Users\UPN>
C:\Users\UPN>ping 192.168.103

Pinging 192.168.0.103 with 32 bytes of data:
Reply from 192.168.0.103: bytes=32 time=4ms TTL=127
Reply from 192.168.0.103: bytes=32 time=2ms TTL=127
Reply from 192.168.0.103: bytes=32 time=2ms TTL=127
Reply from 192.168.0.103: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.0.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms

```

ภาพที่ 4-3 แสดงการ Ping จาก PPTP server ไปหา Client

```

C:\Users\UPN>tracert 100.10.0.1

Tracing route to 100.10.0.1 over a maximum of 30 hops

  1      4 ms      4 ms      4 ms    200.10.0.1
  2      6 ms      5 ms      5 ms    200.10.0.2
  3      7 ms      7 ms      7 ms    100.10.0.1

Trace complete.

```

ภาพที่ 4-4 แสดง trace route ของอุโมงค์ข้อมูลจาก Server ไปหา Client

#### 4.1.2 ผลการศึกษา Federation Service

การใช้งานระบบต่าง ๆ มากกว่า 1 ระบบ เช่น มหาวิทยาลัย สถาบันเทคโนโลยี สถาบันการวิจัย หรือหน่วยงานราชการต่าง ๆ ผู้ใช้งานจะต้องมีชื่อผู้งานและรหัสผ่านเพื่อยืนยันสิทธิ์เข้าใช้งานระบบนั้น ๆ มักเกิดความสับสนในการจดจำชื่อผู้งานและรหัสผ่านมากกว่า 1 ระบบ แต่เมื่อใช้ Single Sign-on (SSO) ภายใต้ Federated identity Management ทำการ Authentication ข้ามระบบในอีกองค์กรหรือสถาบันหนึ่งได้ ทำให้สามารถแลกเปลี่ยนข้อมูลเพื่อการแสดงตัวตน Authentication และ Authorization เพื่อใช้งานข้ามเครือข่ายได้

- ง่ายต่อการปฏิบัติตามข้อกำหนดกฎนโยบายรักษาความปลอดภัยต่าง ๆ ร่วมกัน
- สอดคล้องกับมาตรฐานการ Authentication เดียวกัน
- มีความสะดวกในการเข้าใช้งานทรัพยากรในหลาย ๆ ระบบ สำหรับผู้ใช้งาน
- สามารถทำงานร่วมกับระบบการจัดการการเข้าถึงทรัพยากรต่าง ๆ ที่มีอยู่แล้ว
- ไม่จำเป็นต้องสร้างบัญชี ฐานข้อมูลผู้ใช้ ในหลาย ๆ databases
  - ✓ จะถูกตรวจสอบ Authentication โดย Identity Provider
  - ✓ สามารถอนุมัติ Authorize ในแต่ละสถาบัน บทบาท หรือตามแต่สิทธิของผู้ใช้บริการ
- ลดข้อกำหนดต่าง ๆ ที่ผู้ใช้งานระบบ User ต้องระบุ
- ใช้เวลาน้อยในการอนุมัติของผู้ใช้งานระบบ
- สามารถปรับแต่งรูปแบบการบริการตามการใช้งานและการตั้งค่าตามความเหมาะสม
- อำนวยความสะดวกในใช้ทรัพยากรร่วมกันและความร่วมมือในทุกภาคส่วน

#### 4.1.3 ผลการศึกษา Science DMZ

การใช้งานเครือข่าย General purpose Network พบว่ามี traffic การใช้งานที่หลากหลาย ถ้าใช้งานเครือข่ายประเภทนี้เพื่อการดำเนินการกิจกรรมทางการศึกษาวิจัย จะพบว่าเกิดการล่าช้าในการส่งข้อมูลขนาดใหญ่มหาศาลและมีประสิทธิภาพต่ำ สถาบันฯ กรม Science DMZ พัฒนา ขึ้นเพื่อให้ใช้งานด้านวิทยาศาสตร์ที่มีขนาดข้อมูลมหาศาลและต้องการการถ่ายโอนข้อมูลมหาศาลที่รวดเร็วและปลอดภัยสูง องค์ประกอบที่สำคัญคือ Data Transfer Node (DTN) เชื่อมต่อเข้ากับ high-speed network interfaces ที่ใช้ในการถ่ายโอนข้อมูลที่ดียิ่งที่สุดและมีความน่าเชื่อถือบนพื้นที่บริเวณกว้างอยู่ห่างไกลกันมากต้องใช้ DTN สำหรับการถ่ายโอนข้อมูลโดยเข้าถึง local storage ที่เชื่อมต่อกับ Storage Area network (SAN) และเชื่อมต่อเข้ากับ High-speed parallel system file เช่น GPFS และเครือข่ายจะเชื่อมต่อกับโครงข่ายเพื่อการศึกษาวิจัย Research network Backbone

- ช่วยลดและจัดการปัญหาการ Packet loss ที่เกิดการประสิทธิภาพของ TCP ที่ต่ำ
- เข้าถึงทรัพยากรจากการศึกษาวิจัยจากต่างสถานที่ต่าง ๆ ได้โดยใช้ Virtual Circuit, Software Defined Networking (SDN) และ 100 Gigabit infrastructures
- perfSONAR Toolkot ใช้ในการทดสอบเครือข่าย (network testing) การตรวจวัดเครือข่าย (network measurement) และการวิเคราะห์สมรรถนะ (performance analysis) ง่ายในการแก้ไขปัญหาได้อย่างราบรื่นและรวดเร็ว

## บทที่ 5

### สรุปผลการทดลองแบบจำลองระบบและการทดสอบ

ผลที่ได้จากการทำปริญญานิพนธ์นี้ โดยการประยุกต์ใช้ VPN (Virtual Private Network) ทำการสร้างท่อ Tunnel เพื่อการส่งถ่ายโอนข้อมูลที่มีความปลอดภัยมากที่สุด ซึ่งปัจจุบันมีความต้องการใช้งานอินเทอร์เน็ตที่มากขึ้นจะเห็นว่ามี Traffic หลากหลายอยู่บนเครือข่ายอินเทอร์เน็ต แต่ในส่วนของการด้านการศึกษาวิจัยนั้นต้องการเครือข่ายที่มี ประสิทธิภาพและแบนด์วิธ ที่สูง พบว่าถ้าการใช้งานกับเครือข่ายอินเทอร์เน็ตทั่วไปมักจะเกิดความล่าช้าและคุณภาพไม่ดี ส่งผลกระทบต่อการจัดกิจกรรมการเรียนการสอน จะต้องไปแข่งช่องทางกับผู้อื่นในเครือข่ายอินเทอร์เน็ต เช่น การใช้งานฐานข้อมูลเพื่อการสืบค้นและการใช้ทรัพยากรทางการศึกษาที่ให้บริการ ระบบสำหรับประชุมและจัดการเรียนการสอนทางไกล จึงเกิดเครือข่ายเฉพาะกิจขึ้นมาเพื่อสนับสนุนในส่วนของการศึกษาและวิจัยโดยเฉพาะ ในนามของ REN: Research and Education Network ในส่วนของประเทศไทยนั้น UniNet ได้จัดตั้งกลุ่มในนามของ ThaiREN เพื่อประสานงานความร่วมมือระหว่างหน่วยงานทางการศึกษาและวิจัยทั้งในประเทศและต่างประเทศ รวมถึงการเชื่อมต่อเข้ากับเครือข่ายศึกษาวิจัยอื่น ๆ และรวมกลุ่มกันจนเกิดเป็น Community ทางด้านการศึกษาและวิจัย โดย UniNet มีบริการ Layer 2 ทำการสร้าง L2VPN เพื่อกำหนดจุด End-to-end โดย Node รองรับตามสถาบันการศึกษาทั่วประเทศไทย สามารถทำการประชุมและจัดการเรียนการสอนทางไกลหรือถ่ายทอดสดกิจกรรมทางการแพทย์ได้อย่างมีประสิทธิภาพ เนื่องจากเครือข่ายนั้นไม่เกี่ยวข้องกับเครือข่ายอินเทอร์เน็ตทั่วไปจึงมีความรวดเร็วและปลอดภัยสูง

จุดมุ่งหมายหลักของการรวมตัวกันของแต่ละสถาบันการศึกษาใช้ Federation Service ทำ Single Sign-on (SSO) ในการ ทำ Authentication ข้ามระบบในอีกรองค์หรือสถาบันหนึ่งได้เป็นการแลกเปลี่ยนข้อมูลเพื่อการแสดงตัวตน Authentication เพื่อสนับสนุนให้เข้าใช้ทรัพยากรด้านการศึกษาวิจัยร่วมกัน โดยสมาชิกของแต่ละหรือสถาบันการศึกษาสามารถเข้าใช้งาน eduroam ซึ่งเป็นบริการเครือข่ายโรมมิ่งเพื่อการศึกษาและวิจัยสำหรับนักศึกษาและบุคลากรของ



สถาบันการศึกษาที่เป็นสมาชิกเครือข่าย eduroam เพื่ออำนวยความสะดวกในการใช้งานเครือข่ายอินเทอร์เน็ตได้ข้ามสถาบันโดยอยู่ภายใต้เงื่อนไขการใช้งานของสถาบันผู้ให้บริการเครือข่าย

การศึกษางานวิจัยของสถาบันศรียกรรม Science DMZ ถือเป็นสิ่งใหม่ที่จะนำมาใช้ในอนาคตเนื่องจากในการทดลองทางด้านวิทยาศาสตร์นั้นมักจะมีข้อมูลขนาดใหญ่มหาศาล เช่น การทดลองเครื่องชนอนุภาคแฮดรอนขนาดใหญ่ LHC สร้างขึ้นเพื่อยิงลำอนุภาค 2 ลำ ให้ชนกันด้วยความเร็วเข้าใกล้แสงและต้องการพื้นที่ในการจัดเก็บข้อมูลจำนวนมากและต้องการการถ่ายโอนข้อมูลที่รวดเร็ว ป้องกัน packet loss จุดเด่น Science ได้มี Data Transfer Node (DTN) ที่เชื่อมต่อโดยตรงกับสวิตช์หรือเราเตอร์ของ Science DMZ ที่มีประสิทธิภาพสูง ซึ่งเชื่อมต่อโดยตรงกับ Border Router หน้าทีของ DTN คือการเคลื่อนย้ายข้อมูลทางวิทยาศาสตร์ขนาดใหญ่อย่างมีประสิทธิภาพของแต่ละ remote site และสามารถเข้าถึง access ไปที่ parallel file system ของการถ่ายโอนข้อมูลระหว่างพื้นที่บริเวณกว้างผ่าน Data Transfer Nodes (DTN) ซึ่งเชื่อมต่อกับโครงสร้างของ Local storage เช่น Storage Area network (SAN) จะเชื่อมต่อเข้ากับ High-speed parallel system file เช่น GPFS เมื่อต้องการจะจัดเก็บข้อมูลจะถูกถ่ายโอนไปที่ DTN และเขียนไปที่ parallel file system สถาบันศรียกรรม Science DMZ จะเชื่อมต่อแบบ Redundant กับโครงข่ายเพื่อการศึกษาวิจัย Research network Backbone ซึ่งมีความสามารถในการเรดัด IP และใช้งานจรเสมือน virtual circuit services ซึ่งระบบเครือข่ายนี้มี high-capacity redundant infrastructure มีการควบคุมความปลอดภัยของการโอนถ่ายข้อมูลขนาดใหญ่ และถูกออกแบบมาให้ง่ายต่อการแก้ไขปัญหาประสิทธิภาพการทำงาน การตรวจสอบโดยใช้ perfSONAR ที่ช่วยวิเคราะห์ตรวจสอบข้อมูลการแลกเปลี่ยนระหว่างเครือข่ายสามารถระบุตำแหน่งความผิดพลาดและแก้ไขปัญหาได้อย่างราบรื่นและรวดเร็ว

การทำปริญญานิพนธ์นี้เป็นการนำเทคโนโลยีใหม่ ๆ มาช่วยพัฒนาระบบระบบเครือข่ายอินเทอร์เน็ตเพื่อการศึกษาวิจัยให้ประสิทธิภาพมากยิ่งขึ้น แต่ยังเป็นเพียงแค่การศึกษาผลงานวิจัยเท่านั้น ยังไม่สามารถใช้งานได้อย่างสมบูรณ์ในประเทศไทย ต้องมีศึกษาและพัฒนาต่อไปเพื่อให้ใช้งานจริงได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

### ปัญหาที่เกิดขึ้นในการดำเนินการ

ปัญหาในการจัดทำปฏิญานีพนธ์นี้ เนื่องจากเทคโนโลยี VPN เริ่มใช้งานในประเทศไทยได้ สักกระยะหนึ่งและยังไม่เป็นที่นิยมนัก ในส่วนของ Federation Service และสถาปัตยกรรม Science DMZ เทคโนโลยีใหม่ที่เพิ่งคิดค้นขึ้นมาแต่ยังไม่เป็นที่แพร่หลายในประเทศไทยเท่าที่ควร ทำให้การค้นหาข้อมูลเป็นเรื่องที่ค่อนข้างลำบาก จึงจำเป็นต้องใช้เวลาในการค้นหาข้อมูลและความเข้าใจศึกษาซึ่งทำให้เสียเวลาพอสมควร

### แนวทางในการแก้ปัญหา

ในการทำปฏิญานีพนธ์นี้ ปัญหาต่าง ๆ ที่เกิดขึ้น สามารถแก้ไขได้โดย ต้องรู้ก่อนว่าปัญหาเกิดจากอะไร เมื่อเรารู้ปัญหาได้ตรงจุด ก็จะสามารถหาวิธีแก้ปัญหานั้นได้ ควรทำการศึกษาข้อมูลให้ละเอียดและแน่ใจว่าข้อมูลที่ได้นั้นถูกต้องและสามารถนำมาใช้งานได้จริง จึงต้องศึกษาค้นคว้าหาข้อมูลเกี่ยวกับเทคโนโลยี VPN ให้ดีก่อน และค้นหาข้อมูลจากเว็บไซต์ต่างประเทศเกี่ยวกับข้อมูลกระบวนการ Federation Service และสถาปัตยกรรม Science DMZ และใช้เวลาในการทำ ความเข้าใจมากเนื่องจากข้อมูลไม่มีแพร่หลายในประเทศไทย

## เอกสารอ้างอิง

1. APAN Task For Proposal [Online]. Available  
[archive.apan.net/org/IAMTaskForceV1.0.pdf](http://archive.apan.net/org/IAMTaskForceV1.0.pdf)
2. Internet2 Innovation Platform FAQ [Online]. Available  
[www.internet2.edu/media/.../Internet2-Innovation-Platform-FAQ.pdf](http://www.internet2.edu/media/.../Internet2-Innovation-Platform-FAQ.pdf)
3. เทคโนโลยี VPN [Online]. Available  
[cad.go.th/ewtadmin/ewt/netgrp/download/VPN.pdf](http://cad.go.th/ewtadmin/ewt/netgrp/download/VPN.pdf)
4. Layer2 and Layer3 Virtual Private Network: Taxonomy, Technology, and Standardization Efforts [Online]. Available  
[https://www.isoc.org/pubs/guest/ComMag\\_June04\\_Knight.pdf](https://www.isoc.org/pubs/guest/ComMag_June04_Knight.pdf)
5. Network Zoning [Online]. Available  
<http://www.it-guides.com/training-a-tutorial/network-system/network-zoning>
6. Layer 2 Service [Online]. Available  
<http://www.internet2.edu/products-services/advanced-networking/layer-2-services/>
7. Virtual Private Network [Online]. Available  
[https://en.wikipedia.org/wiki/Virtual\\_private\\_network](https://en.wikipedia.org/wiki/Virtual_private_network)
8. VPN Services: Layer2 or Layer3? [Online]. Available  
[http://www3.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG\\_CABINET=Docs\\_and\\_Resource\\_Ctr&LMSG\\_CONTENT\\_FILE=White\\_Papers/vpn\\_services.pdf](http://www3.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=White_Papers/vpn_services.pdf)
9. Layer 2 Service infosheet [Online]. Available  
<http://www.internet2.edu/media/medialibrary/2016/04/29/IS-advanced-layer-2-service-20160429.pdf>
10. Internet2 Advanced Layer2 Service [Online]. Available  
<http://www.internet2.edu/media/medialibrary/2014/12/05/Internet2-AL2S-brochure-2014.pdf>
11. eduroam คืออะไร [Online]. Available  
<http://eduroam.uni.net.th/eduroam-th/index.php?var=about&lang=thai>
12. นโยบายการเข้าร่วม eduroam ประเทศไทย [Online]. Available  
[http://eduroam.uni.net.th/eduroam-th/file\\_Uploads/3\\_2\\_20130613\\_163553.pdf](http://eduroam.uni.net.th/eduroam-th/file_Uploads/3_2_20130613_163553.pdf)

### เอกสารอ้างอิง (ต่อ)

13. Science DMZ [Online]. Available  
<https://fasterdata.es.net/science-dmz/>
14. Science DMZ Architecture [Online]. Available  
<https://fasterdata.es.net/science-dmz/science-dmz-architecture/>
15. Science DMZ: Data Transfer Nodes [Online]. Available  
<https://fasterdata.es.net/science-dmz/DTN/>
16. เทคโนโลยี MPLS [Online]. Available  
<http://product.south.cattelcom.com/knowledge/MPLS/MPLS.pdf>
17. MPLS L2VPN [Online]. Available  
<http://www.bloggang.com/mainblog.php?id=likecisco&month=02-05-2015&group=3&gblog=40>
18. What is perfSONAR [Online]. Available  
<http://www.perfsonar.net/about/what-is-perfsonar/>

### ประวัติผู้แต่ง

ปริญญานิพนธ์เรื่อง : L2VPN และเครือข่ายนิยามบนซอฟต์แวร์สำหรับเครือข่ายเพื่อ  
การศึกษา

สาขาวิชา : วิศวกรรมคอมพิวเตอร์

ภาควิชา : วิศวกรรมไฟฟ้าและคอมพิวเตอร์

คณะ : วิศวกรรมศาสตร์

ชื่อ : นางสาวแพรวา มณีศรี

ประวัติ

เกิดเมื่อวันที่ 22 เดือนตุลาคม พ.ศ. 2535 อยู่บ้านเลขที่ 5/51 ถนนหลักเมือง ตำบลในเมือง อำเภอเมืองสุรินทร์ จังหวัดสุรินทร์ 32000 สำเร็จการศึกษาระดับมัธยมศึกษาตอนปลาย จาก โรงเรียนสิรินธร จังหวัดสุรินทร์ สาขาวิทยาศาสตร์-คณิตศาสตร์ ปีการศึกษา 2553 และสำเร็จ การศึกษาในระดับปริญญาตรี สาขาวิชาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมไฟฟ้าและ คอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ในปี การศึกษา 2557