แผนบริหารการสอนประจำบท
บทที่ 2 แบบจำลองโอเอสไอ (OSI Model)

วัตถุประสงค์

1. บอกถึงกระบวนการทำงานในแต่ละชั้นของโมเดลโอเอสไอได้
2. อธิบายการเชื่อมต่อกันระหว่างอุปกรณ์ประเภทต่าง ๆ ได้
3. อธิบายเกี่ยวกับการแบ่งเครือข่ายออกเป็นย่อย ๆ ได้
4. บอกถึงสิ่งที่ควรคำนึงในการการออกแบบเครือข่ายได้
5. อธิบายแนวทางในการจัดการเครือข่ายได้

เนื้อหา

1. หน้าที่และความสำคัญของ OSI Model
2. การแบ่งเครือข่าย Lan
3. โมเดลการออกแบบเครือข่ายในลักษณะโครงสร้างตามลำดับชั้น
4. ข้อควรคำนึงในการออกแบบเครือข่าย
5. แนวทางการจัดการเครือข่าย

กิจกรรมการเรียนการสอน

1. ผู้สอนอธิบายวัตถุประสงค์ ความคิดรวบยอด ขอบเขตเนื้อหา วิธีการเรียน และกิจกรรมการเรียนการสอนประจำบทเรียน
2. ผู้สอนใช้สไลน์และเอกสารประกอบการสอนในรูปแบบไฟล์อิเล็กทรอนิกส์ประเภท PPT ประกอบการบรรยายเนื้อหาประเด็นสำคัญ
3. ผู้สอนบรรยายสรุปเนื้อหาและประเด็นสำคัญประจำบทเรียน
4. ผู้เรียนทำแบบฝึกหัด เพื่อเป็นการทำทวนความรู้ความเข้าใจเนื้อหาประจำบท และประเมินผลเป็นคะแนนระหว่างเรียน
5. ผู้เรียนทำงานตามที่ได้รับมอบหมายประจำบทเรียน โดยให้ผู้เรียนส่งงานในรูปแบบต่าง ๆ ตามที่ผู้สอนกำหนด

สื่อการเรียนการสอน

1. เอกสารประกอบการสอน รายวิชาความรู้เบื้องต้นเกี่ยวกับเครือข่ายคอมพิวเตอร์ ซึ่งเรียบเรียงโดยอาจารย์สุลัยมาน เภอโส๊ะ สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์เทคโนโลยีและการเกษตร

2. สไลน์ประกอบการสอน รายวิชาความรู้เบื้องต้นเกี่ยวกับเครือข่ายคอมพิวเตอร์ ซึ่งเผยแพร่ไว้บนเว็บไซต์อีเลิร์นนิ่งของมหาวิทยาลัยราชภัฏยะลา โดยมีที่อยู่ของเว็บไซต์ คือ http://elearning.yru.ac.th

การวัดผลและการประเมินผบ

1. วัดและประเมินผลจากคะแนนแบบฝึกหัด และให้คะแนนตามเกณฑ์ที่กำหนดไว้ล่วงหน้า แล้วบันทึกเป็นคะแนนระหว่างเรียนของผู้เรียนแต่ละคน

2. ประเมินผลงานหรือการบ้านที่ผู้สอนมอบหมายให้ผู้เรียนปฏิบัติประจำบทเรียน และให้คะแนนตามเกณฑ์ที่กำหนดไว้ล่วงหน้า แล้วบันทึกเป็นคะแนนระหว่างเรียนของผู้เรียนแต่ละคน

บทที่ 2
แบบจำลองโอเอสไอ (OSI Model)

เนื้อหาในบทนี้จะกล่าวถึงโมเดลการออกแบบเครือข่ายตามแบบจำลองโอเอสไอและมาตรฐานของแบบจำลองโอเอสไอ เพื่อให้ผู้เรียนได้มองเห็นภาพการเชื่อมต่อระหว่างอุปกรณ์เครือข่ายประเภทต่าง ๆ การเชื่อมต่อเครือข่าย LAN และ WAN การออกแบบโครงสร้างเครือข่ายแบบลำดับชั้น สิ่งที่ต้องคำนึงในการออกแบบ รวมไปถึงพื้นฐานในการบริหารจัดการเครือข่าย

2.1 หน้าที่และความสำคัญของ OSI Model

แบบจำลองโอเอสไอ (Open Systems Interconnection model: OSI model) (ISO/IEC 7498-1) เป็นรูปแบบความคิดที่กล่าวถึงคุณสมบัติพิเศษและมาตรฐานการทำงานภายในของระบบการสื่อสารโดยแบ่งเป็นชั้นนามธรรม และโพรโทคอลของระบบคอมพิวเตอร์ พัฒนาขึ้นโดยองค์การระหว่างประเทศว่าด้วยการมาตรฐาน (ISO) แบบจำลองนี้จะทำการจับกลุ่มรูปแบบฟังก์ชันการสื่อสารที่คล้ายกันให้อยู่ในเลเยอร์ใดเลเยอร์หนึ่งจากทั้งหมด 7 เลเยอร์ ดังภาพที่ 2.1

OSI Model			
	Data unit	**Layer**	**Function**
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption and decryption, convert machine dependent data to machine independent data
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	Reliable delivery of segments between points on a network.
Media layers	Packet/Datagram	3. Network	Addressing, routing and (not necessarily reliable) delivery of datagrams between points on a network.
	Bit/Frame	2. Data link	A reliable direct point-to-point data connection.
	Bit	1. Physical	A (not necessarily reliable) direct point-to-point data connection.

ภาพที่ 2.1 OSI Model

ที่มา : IBM (n.d.).

หน้าที่ของแต่ละเลเยอร์

2.1.1 Physical Layer

เลเยอร์นี้จะกำหนดมาตรฐานของสัญญาณทางไฟฟ้าและมาตรฐานของคอนเน็กเตอร์เชื่อมต่อต่าง ๆ รวมถึงมาตรฐานของสายเคเบิลที่จำเป็นต้องใช้ เช่น มาตรฐานสาย CAT ประเภทต่าง ๆ มาตรฐานของหัวต่อเชื่อม V.35 ที่ใช้ใน WAN และมาตรฐาน RS232 เป็นต้น รวมทั้งแรงดันทางไฟฟ้าและรูปแบบการรับส่งบิตข้อมูลที่เกิดขึ้นในสื่อนำสัญญาณ ในระดับ Physical Layer ซึ่งเป็นระดับล่างสุดที่เกี่ยวข้องกับสายเคเบิลและการ Wiring สายโดยตรงจะต้องมีผู้ผลิตสายเคเบิลประเภทต่าง ๆ ขึ้นมา อย่างเช่น สายไฟเบอร์อปติก สาย UTP CAT5, CAT5E และ CAT6 ผู้ผลิตเหล่านี้เช่น AT&T, AMP เป็นต้น นอกจากนั้นเลเยอร์นี้จะกำหนดมาตรฐานในการรับส่งสัญญาณทางไฟฟ้า (electrical signal) บนสายเคเบิลนั้น ๆ ด้วย เช่น ส่งด้วยการหักล้างหรืออาศัยผลต่างของสัญญาณทางไฟฟ้า (ที่ใช้ในสาย UTP) หรือส่งด้วยลำแสง (ที่ใช้ในสายไฟเบอร์) องค์กรที่กำหนดมาตรฐานดังกล่าวนี้คือ IEEE

2.1.2 Datalink Layer

รับผิดชอบในการส่งข้อมูลบนเครือข่ายแต่ละประเภทเช่น Ethernet, Token Ring, FDDI หรือบน WAN ต่าง ๆ และดูแลเรื่องการห่อหุ้มข้อมูลจากเลเยอร์บนเช่น แพ็กเก็ต IP ไว้ภายใน “เฟรม (frame)” และส่งจากต้นทางไปยังอุปกรณ์ตัวถัดไป เลเยอร์นี้จะเข้าใจได้ถึงกลไกและอัลกอริทึม รวมทั้งฟอร์แมตขอเฟรมที่ต้องใช้ในเครือข่ายประเภทต่าง ๆ เป็นอย่างดี ในเครือข่ายแบบอีเทอร์เน็ต การสื่อสารในเลเยอร์นี้จะมีการระบุหมายเลขแอดเดสรของเครื่อง/อุปกรณ์ต้นทางกับเครื่อง/อุปกรณ์ปลายทางด้วยฮาร์แวร์แอดเดรสที่เรียว่า MAC Address ผู้ใช้งานอีเทอร์เน็ตจะพบว่า การ์ดเครือข่ายที่เสียบอยู่ในเครื่องคอมพิวเตอร์ต้องมีหมายเลข MAC Address กำกับอยู่เสมอ MAC Address นี้เป็นแอดเดรสที่ฝังมากับฮาร์ดแวร์ ไม่สามารถเปลี่ยนแปลงโดยผู้ใช้ปลายทางได้ MAC Address เป็นตัวเลขขนาด 6 ไบต์ 3 ไบต์แรกจะได้รับการจัดสรรโดยองค์กรกลาง IEEE ให้กับผู้ผลิตแต่ละราย ส่วนตัวเลข 3 ไบต์หลังนั้น ในระดับ Datalink Layer ซึ่งเป็นระดับที่กำหนดฟอร์แมตของเฟรมว่าต้องมีฟิลด์ใดบ้าง และกำหนดอัลกอริทึมในการส่งข้อมูลไปบนสายเคเบิล ตัวอย่างของโพรโทคอลในระดับนี้ได้แก่ อัลกอริทึมแบบ CSMA/CD ที่ใช้ในเครือข่ายแบบอีเทอร์เน็ต และอัลกอริทึกแบบ Token passing ที่ใช้ในเครือข่ายแบบ Token Ring ซึ่งอาศัยหลักการว่าใครจับโทเค็น (Token) ได้ก็จะมีสิทธิในการส่งข้อมูลผู้รับผิดชอบในเลเยอร์นี้ได้แก่ ผู้ผลิตเครือข่ายการ์ดที่ติดตั้งไว้ที่เครื่องคอมพิวเตอร์ และผู้ผลิตอุปกรณ์เครือข่ายต่าง ๆ

2.1.3 Network Layer

เป็นเลเยอร์ที่มีหน้าที่หลักในการส่งแพ็กเก็ต (packet) จากเครื่องต้นทางให้ไปถึงเครื่องปลายทางด้วยความพยายามที่ดีที่สุด (best effort delivery) เลเยอร์นี้จะกำหนดให้มีการตั้งลอจิคัลแอดเดรสขึ้นมาบนเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเพื่อใช้ระบุตัวตน ตัวอย่างของโพรโทคอลเลเยอร์นี้ได้แก่ โพรโทคอล IP และลอจิคัลแอดเดรสที่ใช้ก็คือหมายเลข IP Address นั่นเองในเลเยอร์นี้จะเกี่ยวข้องกับอุปกรณ์เครือข่ายเช่น Router หรือ Switch L3 เมื่อมันได้รับแพ็กเก็ตมาจากเครื่องคอมพิวเตอร์ มันก็จะพยายามหาให้ได้ว่าจะส่งแพ็กเก็ตออกไปทางอินเตอร์เฟซไหนของมัน เพื่อให้ไปถึงยังเครื่องคอมพิวเตอร์ปลายทางให้ได้ โพรโทคอลที่ทำงานในเลเยอร์นี้จะไม่ทราบว่าแพ็กเก็ตจริง ๆ แล้วไปถึงเครื่องปลายทางหรือไม่ หน้าที่ของการยืนยันว่าข้อมูลได้ไปถึงปลายทางจริง ๆ แล้วก็คือหน้าที่ของ Transport Layer นั่นเอง ในระดับ Network / Transport โดยปกติผู้สร้างและพัฒนาระบบปฏิบัติการเครือข่ายมักจะสร้างไดรเวอร์สำหรับโพรโทคอลในเลเยอร์ Network / Transport มาให้พร้อมกับระบบปฏิบัติการอยู่แล้วอย่างเช่น ใน UNIX และใน Windows NT , 2000, 2003 จะมีไดรเวอร์สำหรับโพรโทคอล TCP/IP บรรจุอยู่ภายใน โพรโทคอล TCP/IP ทำงานอยู่ในเลเยอร์ Network และ Transport โดยโพรโทคอล IP ทำงานในระดับ Network Layer และโพรโทคอล TCP อยู่ในระดับ Transport Layer หรืออีกตัวอย่างหนึ่งทางบริษัทโนเวลผู้ผลิตเน็ตแวร์ก็ได้สร้างไดรเวอร์ของโพรโทคอล IPX/SPX ขึ้นมาทำงานภายในเน็ตแวร์เซิร์ฟเวอร์และเน็ตแวร์ไคลเอนต์ของตน นอกจากนั้นผู้ผลิตอุปกรณ์เครือข่ายอย่างซิสโก้ก็สร้าง “เราเตอร์” ขึ้นมาเพื่อรับผิดชอบในการรับส่งแพ็กเก็ตในเลเยอร์ Network ระหว่างเครือข่ายต่าง ๆ เช่น รับส่งแพ็กเก็ต IP และแพ็กเก็ต IPX

2.1.4 Transport Layer

เป็นเลเยอร์ที่มีหน้าที่หลัก ๆ ในการแบ่งข้อมูลในเลเยอร์บนให้พอเหมาะกับการจัดส่งไปในเลเยอร์ล่าง (segmentation), ทำหน้าที่ประกอบรวมข้อมูลต่าง ๆ ที่ได้รับมาจากเลเยอร์ล่าง (assembly) และให้บริการในการแก้ไขปัญหาเมื่อเกิดข้อผิดพลาดขึ้นในระหว่างทางของการส่ง (error recovery) หน่อยของข้อมูลในเลเยอร์นี้มักถูกรียกว่า Segment ตัวอย่างของโพรโทคอลในเลเยอร์นี้ที่รู้จักกันดีก็คือโพรโทคอล TCP และ UDP

2.1.5 Session Layer

เป็นเลเยอร์ที่ครบคุมการสื่อสารจากต้นทางไปยังปลายทางแบบ End to End และคอยครบคุมช่องทางการสื่อสารในกรณีที่มีหลาย ๆ โปรเซสต้องการรับส่งข้อมูลพร้อม ๆ กันบนเครื่องเดียวกัน และยังให้อินเตอร์เฟซสำหรับแอปพลิเคชันเลเยอร์ด้านบนในการควบคุมขั้นตอนการทำงานงานของโพรโท

คอลในระดับ Transport/Network อย่างเช่น Socket ที่ใช้ในยูนิกซ์ หรือ Windows socket ที่ใช้ในวินโดวส์ ซึ่งได้ให้ Application Programming Interface (API) แก่ผู้พัฒนาซอฟต์แวร์ในระดับบนสำหรับการเขียนโปรแกรมเพื่อควบคุมการทำงานของโพรโทคอล TCP/IP ในระดับล่าง ในระดับ Session / Presentation และ Application ผู้รับผิดชอบในเลเยอร์มักได้แก่ ผู้พัฒนาซอฟต์แวร์แอปพลิเคชันขึ้นมาทำงานบนเครื่องคอมพิวเตอร์โดยอาศัยบริการขั้นพื้นฐานในการรับส่งแพ็กเก็ตข้อมูลจากเลเยอร์ที่ต่ำกว่า

2.1.6 Presentation Layer

จุดประสงค์หลักของเลเยอร์นี้ก็คือ กำหนดฟอร์แมตของการสื่อสาร อย่างเช่น ASCII Text, EBCDIC, ไบนารี (binary) และ JPEG การเข้ารหัสก็รวมอยู่ในเลเยอร์นี้ด้วย ตัวอย่างเช่น โปรแกรม FTP ต้องการรับส่งโอนย้ายไฟล์กับเครื่องเซิร์ฟเวอร์ปลายทางโพรโทคอล FTP จะอนุญาตให้ผู้ใช้ระบุฟอร์แมตของข้อมูลที่โอนย้ายกันได้ว่าเป็นแบบ ASCII Text หรือเป็นแบบไบนารี

2.1.7 Application Layer

เป็นเลเยอร์ที่กำหนดอินเตอร์เฟซระหว่างแอปพลิเคชันที่ทำงานบนเครื่องคอมพิวเตอร์กับซอฟต์แวร์สื่อสารต่าง ๆ ที่ทำงนอยู่บนเครื่องคอมพิวเตอร์ ตัวอย่างเช่น เว็บเบราเซอร์ถือว่าเป็นแอปพลิเคชันที่ทำงานอยู่บนเครื่องคอมพิวเตอร์ เมื่อมันต้องการรับส่งข้อมูลเว็บเพจกับเครื่องเซิร์ฟเวอร์ มันจะอาศัยความสามารถของเลเยอร์ 7 ในการอินเตอร์เฟซกับซอฟต์แวร์สื่อสารในเลเยอร์ต่าง ๆ ระดับล่างเพื่อให้ได้มาซึ่งเว็บเพจที่มันต้องการ

จากคำอธิบายข้างต้นจะเห็นได้ว่า การแบ่งโพรโทคอลออกเป็นหลาย ๆ เลเยอร์ช่วยทำให้ผู้ผลิตแต่ละรายสามารถพัฒนาฮาร์ดแวร์และซอฟต์แวร์สำหรับโพรโทคอลในแต่ละเลเยอร์ได้โดยอิสระ ตามความถนัดและประสบการณ์เฉพาะทางของตนเอง อย่างเช่น AMP ผลิตสื่อนำสัญญณความเร็วสูงขึ้นมาใช้งานระดับฟิสิคัลเลเยอร์ ในขณะที่ Intel และ 3COM เป็นผู้ผลิตเครือข่ายการ์ดขึ้นมาใช้งานในเครือข่ายแบบอีเทอร์เน็ตซึ่งอยู่ในระดับดาต้าลิงก์เลเยอร์ และไมโครซอฟท์เป็นผู้สร้างไดรเวอร์สำหรับโพรโทคอล TCP/IP ขึ้นมาในระบบปฏิบัติการวินโดวส์ พร้อมทั้งได้ให้ API สำหรับนักพัฒนาโปรแกรมที่ต้องการสร้างแอปพลิเคชันให้ทำงานบนโพรโทคอล TCP/IP

แต่ในเมื่อมีการแบ่งแยกออกเป็น 7 เลเยอร์แล้ว การทำให้ทั้ง 7 เลเยอร์ทำงานผสมผสานเป็นหนึ่งเดียวกันนั้นก็ต้องการอาศัยหลักการส่งผ่านข้อมูลจากเลเยอร์บนคือ เลเยอร์ที่ 7 ลงไปจนถึงเลเยอร์สุดท้ายที่ระดับฟิสิคัลเลเยอร์ในฝั่งผู้ส่ง และมีการส่งผ่านย้ายกลับจากระดับฟิสิคัลเลเยอร์ขึ้นไปจนถึงเลเยอร์ที่ 7

อีกครั้งในฝั่งผู้รับโดยในการส่งผ่านข้อมูลระหว่างเลเยอร์ที่สูงกว่ากับเลเยอร์ที่ต่ำกว่านั้นจะผ่านทาง “จุดเชื่อมต่อการให้บริการ (service access point)”

โดยสรุป ข้อดีของการแบ่งออกเป็น 7 เลเยอร์ได้แก่

1) ผู้ผลิตแต่ละรายสามารถทำงานในเลเยอร์ที่ตนถนัดได้อย่างเต็มที่
2) เป็ดช่องทางให้อุปกรณ์และซอฟต์แวร์ของผู้ผลิตต่าง ๆ สามารถทำงานร่วมกันได้
3) ง่ายต่อการพัฒนาโพรโทคอลในแต่ละเลเยอร์และง่ายต่อการเรียนรู้

ตารางที่ 2.1 ตัวอย่างของโพรโทคอลในแต่ละเลเยอร์

เลเยอร์	ตัวอย่างโพรโทคอล
Application Layer	Telnet, HTTP, FTP, WWW, NFS, SMTP, SNMP
Presentation Layer	JPEG, ASCII, EBCDIC, TIFF, GIF, MPEG, Encryption
Session Layer	RPC, SQL, NFS, NetBIOS, Windows socket, DECNet SCP, AppleTalkk ASP
Transport Layer	TCP, UDP, SPX
Network Layer	IP, IPX, AppleTalk
DataLink Layer	Ethernet, Token Ring, IEEE 802.3/202.2, Frame Relay, HDLC, FDDI, ATM
Physical Layer	EIA/TIA-232, V.35, EIA/TIA-449, RJ-45

อุปกรณ์เครือข่ายที่ทำงานในเลเยอร์ที่สองจะส่งผ่านข้อมูลโดยพิจารณาจากแอดเดรสในเลเยอร์ที่สองหรือ Media Access Control (MAC) Address เป็นหลัก ส่วนอุปกรณ์เครือข่ายที่ทำงานในเลเยอร์ที่สามจะส่งผ่านข้อมูลโดยพิจารณาแอดเดรสในเลเยอร์ที่สามเป็นหลัก ต้องพิจารณาว่าเป็นเลเยอร์ที่สามของชุดโพรโทคอลใด สำหรับโพรโทคอล IP แอดเดรสในเลเยอร์ที่สามคือ หมายเลข IP Address สำหรับโพรโทคอล IPX แอดเดรสในเลเยอร์ที่สามคือ IPX Network Address

2.2 การแบ่งเครือข่ายแลน (LAN Segmentation)

LAN Segmentation หมายถึงการแบ่ง LAN ออกเป็นเครือข่ายส่วนย่อย ๆ ซึ่งเรียกว่าแบ่งเป็น “เซกเมนต์ (segment)” โดยใช้อุปกรณ์เครือข่ายต่าง ๆ ได้แก่ บริดจ์/สวิตช์ และเราเตอร์ ซึ่งแต่ละแบบ

นั้นจะมีผลต่อเรื่องของ Collision Domain และ Broadcast Domain ต่างกัน LAN Segment นั้นเป็นคำศัพท์ที่ติดมาจากยุคแรก ๆ ของการมีระบบเครือข่ายที่สมัยนั้นยังมีการใช้สายโคแอกเชียลแบบ 10BASE2 และสายอีเทอร์เน็ตอย่างหนา แบบ10BASE5 โดยเครื่องคอมพิวเตอร์ที่เชื่อมต่อกันบนสายโคแอกเชียลชุดเดียวกันโดยใช้หัวต่อแบบ BNC จะถูกเรียกว่า เชื่อมต่อกันบน “เซกเมนต์” เดียวกันและเมื่อหมดยุคของ 10BASE2 เข้ามาสู่ยุคความรุ่งเรื่องของ 10BASET ซึ่งใช้สาย UTP ต่อจากฮับลากเข้ามายังแต่ละเครื่องคอมพิวเตอร์ คำศัพท์ว่าเซกเมนต์นี้ก็ยังถูกนำมาใช้อยู่ โดยในคราวนี้ เครื่องคอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อกับฮับตัวเดียวกันกจะถูกเรียกว่าอยู่ภายใน “เซกเมนต์” เดียวกัน สาเหตุที่ยังเรียกว่า “เซกเมนต์” อยู่ เพราะภายในฮับมี Backplane หรือบัสหลักภายในที่ทุก ๆ พอร์ตยังต้องคอนเน็กเข้ามาและสื่อสารกันบน Backplane เดียวกัน

LAN Segmentation พอสรุปได้ดังนี้

2.2.1 Collision Domain

2.2.1.1 Hub ทุกพอร์ต เป็น 1 Collision Domain

2.2.1.2 Switch แต่ละพอร์ต คือ 1 Collision Domain

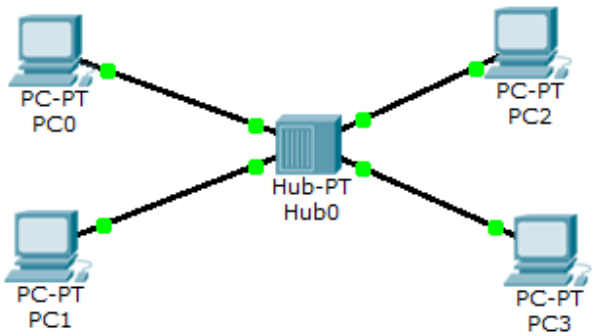
2.2.1.3 Router แต่ละพอร์ต คือ 1 Collision Domain

2.2.2 Broadcast Domain

2.2.2.1 Hub 1 ตัว เป็น 1 Broadcast Domain

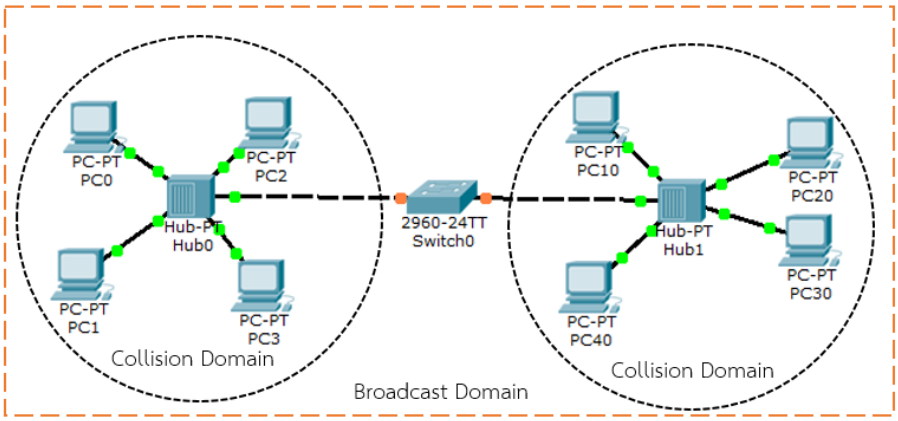
2.2.2.2 Switch 1 ตัว คือ 1 Broadcast Domain

2.2.2.3 Router แต่ละพอร์ตที่ใช้ คือ 1 Broadcast Domain



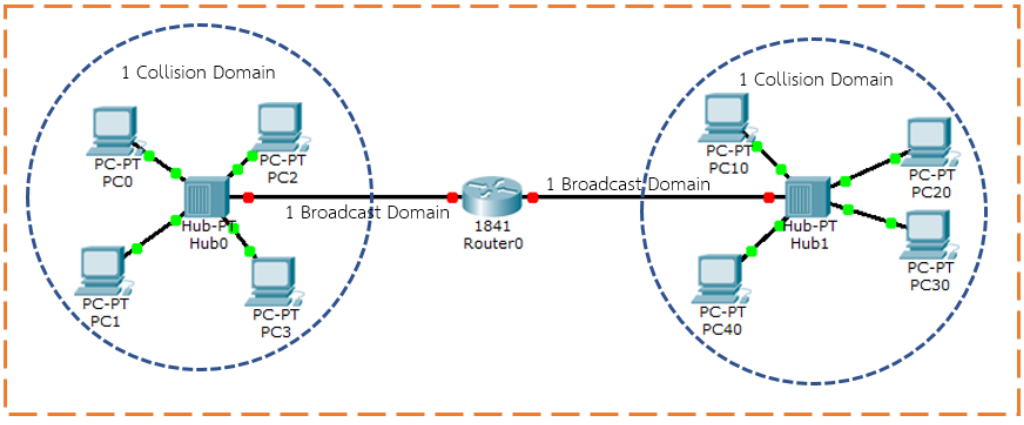
ภาพที่ 2.2 HUB 1 Collision Domain 1 Broadcast Domain

จากภาพที่ 2.2 เครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่บนฮับตัวเดียวจะถือว่าอยู่ภายใต้ Collision Domain เดียวกัน เครื่องที่อยู่ใน Collision Domain เดียวกันมีโอกาสที่จะส่งเฟรมมาชนกันได้หากมีเครื่องอื่นส่งเฟรมมาพร้อม ๆ กัน ตามอัลกอริทึมของ CSMA/CD ที่ใช้ในโลกของเครือข่ายอีเทอร์เน็ต



ภาพที่ 2.3 Bridge/Switch 1 Broadcast Domain

จากภาพที่ 2.3 การเชื่อมต่อผ่านบริดจ์หรือสวิตช์ เครื่องแต่ละเครื่องที่อยู่คนละด้านของบริดจ์หรือสวิตช์จะอยู่ต่าง Collision Domain กัน และจะมีไม่มีโอกาสทส่งเฟรมมาชนกันได้ อย่างไรก็ดี ทุก ๆ พอร์ตของบริดจ์ยังถือว่าอยู่ภายใต้ Broadcast Domain เดียวกัน Broadcast Domain เดียวกันหมายความว่า เมื่อใดก็ตามที่มีเครื่องใดเครื่องหนึ่งส่งบรอดคาสต์เฟรมออกมา บรอดคาสต์เฟรมดังกล่าวจะถูกแพร่กมระจายออกไปที่ทุก ๆ พอร์ตของอุปกรณ์บริดจ์หรือสวิตช์



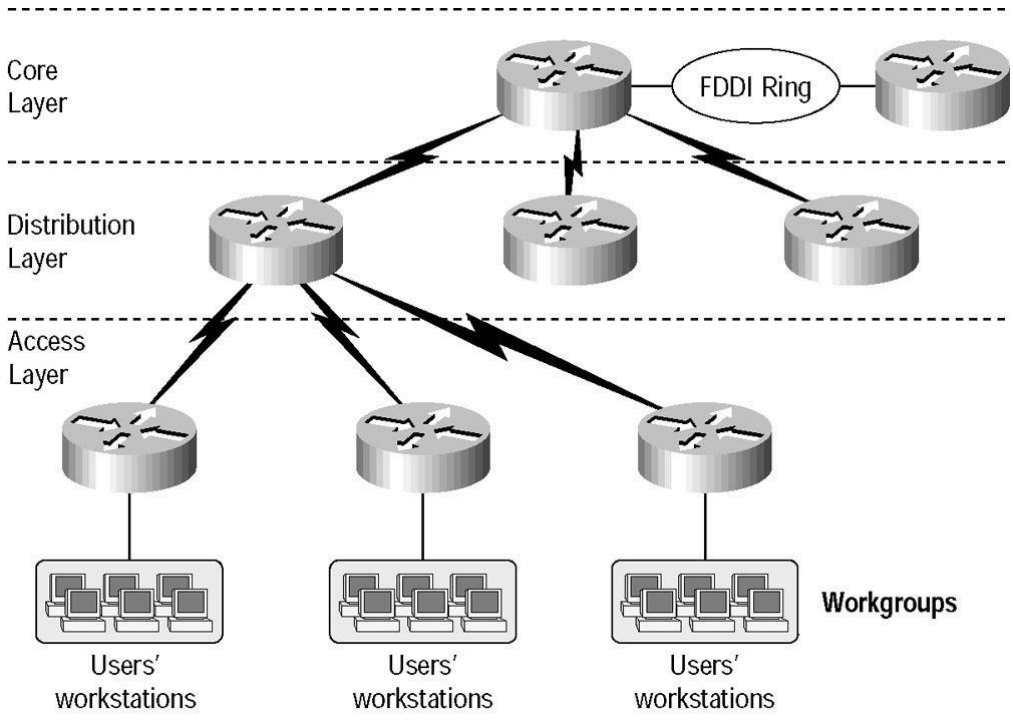
ภาพที่ 2.4 Router : 2 Broadcast Domain

จากภาพที่ 2.4 การเชื่อมต่อผ่านทางเราเตอร์ แต่ละพอร์ตของเราเตอร์ นอกจากจะถือว่าเป็นตัวแบ่งแยก Collision Domain แล้วยังสามารถแบ่งแยก Broadcast Domain ได้อีกด้วย โดยบรอดคาสต์

เฟรมที่ถูกส่งออกจากเครื่องคอมพิวเตอร์ที่อยู่ด้านหนึ่งของเราเตอร์จะถูกส่งข้ามไปยังอีกพอร์ตหนึ่งของเราเตอร์

2.3 โมเดลการออกแบบเครือข่ายในลักษณะโครงสร้างตามลำดับชั้น (Hierarchical Design)

เครือข่ายโดยทั่วไปควรได้รับการออกแบบในลักษณะมีโครงสร้างตามลำดับชั้น ซึ่งประกอบไปด้วยเลเยอร์ที่เรียกว่า Core Layer, Distribution Layer และ Access Layer ตามลำดับ เลเยอร์ที่กล่าวนี้เป็นเลเยอร์ในของการออกแบบเครือข่าย ไม่ได้เกี่ยวข้องกับเลเยอร์ที่กล่าวมาในหัวข้อ OSI Model ข้างต้น การแบ่งเครือข่ายออกเป็นเลเยอร์ต่าง ๆ นี้จะทำให้ง่ายต่อการเลือกใช้อุปกรณ์เครือข่าย การวางแผนเรื่องของการเซตคอนฟิกูเรชัน และการอิมพลีเมนต์ฟีเจอร์ต่าง ๆ ที่เหมาะสม สวิตช์ที่ทำงานอยู่ใน Core Layer เรียกว่า Core Switch สวิตช์ที่ทำงานอยู่ใน Distribution Layer เรียกว่า Distribution Switch และเรียกสวิตช์ที่ทำงานอยู่ใน Access Layer ว่า Access Switch ดังภาพที่ 2.5



ภาพที่ 2.5 โมเดลการออกแบบเครือข่ายแบบมีโครงสร้างตามลำดับชั้น

ที่มา : Tech-faq. (n.d).

2.3.1 Access Layer

เป็นเลเยอร์ที่ใกล้ชิดติดกับผู้ใช้มากที่สุด เป็นจุดที่นำเครื่องคอมพิวเตอร์ของผู้ใช้เข้าสู่ระบบเครือข่าย สำหรับ LAN และ Campus Network อุปกรณ์เครือข่ายที่ทำงานอยู่ในเลเยอร์นี้มักเป็นสวิตช์เลเยอร์ 2 ตัวเล็ก ๆ ที่มีจำนวนพอร์ตที่เพียงพอต่อการรองรับการเชื่อมต่อจากเครื่องคอมพิวเตอร์ของผู้ใช้ผ่านทางสายเคเบิล เช่น UTP สวิตช์ที่ว่านี้จำเป็นต้องมีพอร์ต UPLINK เพื่อเชื่อมโยงขึ้นไปยังสวิตช์ที่อยู่ในระดับ Distribution Layer หรือระดับ Core Layer ความเหมาะสมของอุปกรณ์ที่ทำงานในเลเยอร์นี้ คือ ควรมีต้นทุนของอุปกรณ์ที่ต่ำ ยังไม่จำเป็นต้องมีฟีเจอร์ขั้นสูงมากนัก และควรติดตั้งได้ง่ายใช้เวลาไม่นาน

2.3.2 Distribution Layer

เป็นจุดที่รองรับการเชื่อมต่อจาก Access Layer หลายๆ จุดเข้าด้วยกัน และผ่านต่อไปยัง Core Layer สำหรับ LAN และ Campus Network อุปกรณ์ที่ทำงานอยู่ในเลเยอร์นี้มักเป็นสมวิตช์ที่มีประสิทธิภาพ มีฟีเจอร์ขั้นสูงพอสมควรและมีจำนวนพอร์ตมากพอสำหรับรองรับการเชื่อมโยงไปยังสวิตช์ที่ทำงานอยู่ใน Access Layer สวิตช์ในเลเยอร์นี้ถือได้ว่าเป็นเสมือน “จุดศูนย์รวม” ของสวิตช์ต่าง ๆ ที่อยู่ในเลเยอร์ Access Layer เพื่อให้ผู้ใช้ที่เชื่อมต่อเข้าสวิตช์ใน Access Layer ตัวหนึ่งสามารถพูดคุยและสื่อสารกันกับผู้ใช้ที่เชื่อมต่อเข้ากับสวิตช์ตัวอื่น ๆ ใน Access Layer ได้ ภายในสวิตช์ที่อยู่ใน Distribution Layer นี้ควรการอิมพลีเมนต์ฟีเจอร์อย่างเช่น Inter VLAN Routing, Access Control Lists (ACL) หรือรวมถึง QoS และ Policy ต่าง ๆ ในการใช้งานเครือข่ายด้วย สวิตช์ที่ทำงานในเลเยอร์นี้มักเป็นสวิตช์เลเยอร์ 3

2.3.3 Core Layer

เป็นจุดศูนย์กลางและหัวใจหลักของเครือข่าย ทำหน้าที่เชื่อมต่อ Distribution Layer หลาย ๆ จัดเข้าไว้ด้วยกัน เลเยอร์นี้ควรสามารถรับส่งแพ็กเก็ตได้อย่างรวดเร็วมาก อย่างไรก็ดีในบางเครือข่าย อุปกรณ์ที่ทำงานในเลเยอร์ Core Layer กับ Distribution Layer อาจเป็นตัวเดียวกันก็ได้คือสวิตช์ตัวหลักหนึ่งตัวที่ทำหน้าที่เป็น Core Switch และมีสวิตช์ปลายทางหลาย ๆ ตัวทำหน้าที่เป็น Access Switch

2.5 ข้อควรคำนึงในการออกแบบเครือข่าย

ข้อควรคำนึงต่าง ๆ ต่อไปนี้ควรได้รับการพิจารณาเมื่อกำลังออกแบบเครือข่าย ได้แก่

2.5.1 ความสามารถในการรองรับการเพิ่มขยายได้ในอนาคต (Scalability)

หมายถึง เครือข่ายที่ออกแบบขึ้นมาสามารถรองรับการขยายตัวหรือเติบโตได้มากน้อยเพียงใด องค์กรขนาดใหญ่กำลังเพิ่มปริมาณผู้ใช้ที่ต้องการใช้งานระบบเครือข่าย แอปพลิเคชันบนเครือข่ายที่กำลังเพิ่มขึ้น ไซต์สาขาที่เพิ่มเติม และเครือข่ายคอนเน็ตชันที่เชื่อมต่อไปยังภายนอกที่ขยายตัวขึ้น เหล่าที่ล้วนมีผลต่อการออกแบบให้มี Scalability ถ้าเป็นไปได้ ในฐานะผู้ออกแบบเครือข่ายให้กับลูกค้า ควรถามลูกค้าเพื่อให้เข้าใจถึงสิ่งต่าง ๆ ต่อไปนี้ ตัวอย่างคำถามที่ควรถามเช่น จะมีไซต์เพิ่มขึ้นหรือไม่ในปีถัดไปหรืออีกสองปีถัดไป เครือข่ายที่ไซต์ใหม่จะต้องรองรับปริมาณผู้ใช้มากน้อยแค่ไหน ในอีกหนึ่งหรือสองปีข้างหน้า จะมีผู้ใช้ที่ต้องเข้าถึงเครือข่ายที่ส่วนกลางมากน้อยแค่ไหน และจะมีเครื่องเซิร์ฟเวอร์หรือโฮสต์ถูกเพิ่มเข้าไปในเครือข่ายทั้งหมดมากน้อยแค่ไหนในอีกหนึ่งหรือสองปีข้างหน้า

การทำให้บรรลุเป้าหมายนี้อาจไม่ใช่เรื่องง่ายนักอาจต้องมีกระบวนการอื่น ๆ เข้ามาเกี่ยวข้องด้วย อย่างเช่น การวางแผนโครงสร้างพื้นฐานเครือข่ายให้เหมาะสม การวิเคราะห์ลักษณะของแอปพลิเคชันที่ใช้งานอยู่และกำลังจะใช้ และการเลือกอุปกรณ์เครือข่ายที่สามารถปรับเปลี่ยนเพิ่มเติมโมดูลต่าง ๆ ได้ในภายหลังโดยสะดวก

ตัวอย่างหนึ่งของการวางแผนโครงสร้างพื้นฐานเครือข่ายที่อาจเป็นอุปสรรคต่อ Scalability ได้แก่

1) การไม่ได้แบ่ง VLAN ไว้ตั้งแต่แรกบนสวิตช์ คือยังคงใช้งานแบบ Flat Network อยู่ ซึ่งอาจก่อให้เกิดปัญหาเกี่ยวกับ Scalability ได้ในกรณีที่มีปริมาณผู้ใช้เพิ่มมากขึ้น และโดยเฉพาะอย่างยิ่งถ้าแอปพลิเคชันของผู้ใช้หรือเครือข่ายแอปพลิเคชันมีการส่งบรอดคาสต์เฟรมออกมามาก (เพราะสวิตช์เลเยอร์ 2 จะส่งบรอดคาสต์เฟรมออกไปที่ทุก ๆ พอร์ต ทุก ๆ เซ็กเมนต์ที่เชื่อมต่ออยู่)

2) การใช้งานโพรโทคอลที่มีการส่งบรอดคาสต์เฟรมออกมาค่อนข้างมาก ได้แก่ โพรโทคอลที่ใช้กันในระบบปฏิบัติการของไมโครซอฟท์รุ่นเก่า ๆ ได้แก่ โพรโทคอล NetBEUI เป็นต้น

2.5.2 ความสามารถในการทนทานต่อความผิดพลาด (Fault Tolerance) และสามารถทำงานได้อย่างต่อเนื่องไม่หยุดชะงัก (Availability)

หมายถึง ปริมาณของเวลาที่เครือข่ายพร้อมรองรับการใช้งานผู้ใช้และบ่อยครั้ง ถือได้ว่า Availability เป็นเป้าหมายที่สำคัญที่สุดในการออกแบบเครือข่ายให้กับลูกค้า สามารถกล่าวถึง Availability ได้ในฟอร์แมตของเปอร์เซ็นต์ Uptime เทียบต่อปี ต่อเดือน ต่อวัน หรือต่อชั่วโมงโดยเทียบกับเวลาทั้งหมดในช่วงขณะนั้น ตัวอย่างเช่น ในเครือข่ายที่ใช้บริการ 24 ชั่วโมง 7 วันต่อหนึ่งสัปดาห์ ถ้าเครือข่ายนั้นมี Uptime 165 ชั่วโมงในหนึ่งสัปดาห์ซึ่งมี 168 ชั่วโมง สามารถกล่าวได้ว่าค่าของ Availability เป็น 98.21 เปอร์เซ็นต์

ในปัจจุบัน ลูกค้าหรือผู้คนทั่วไปมักมองว่า Availability มีความหมายมากกว่านั้น Availability อาจใช้สื่อความหมายถึง เวลามากเท่าใดที่เครือข่ายปฏิบัติงานได้อย่างต่อเนื่อง Availability มักถูกนำไปเชื่องโยงกับคำว่า Redundancy หรือ Fault Tolerance แต่ Redundancy ไม่ใช่เป้าหมายของการออกแบบเครือข่ายโดยตรง Redundancy เป็นโซลูชันหนึ่งเพื่อให้บรรลุเป้าหมายของ Availability, Redundancy หมายความถึงการเพิ่มลิงก์ (link) สำรอง หรืออุปกรณ์เครือข่ายสำรองเข้าไปในเครือข่ายเพื่อหลีกเลี่ยงเวลาสูญเสีย (downtime) ด้วยการมีลิงก์หรืออุปกรณ์ที่สามารถทำงานทดแทนได้ Availability ยังถูกนำไปเชื่องโยงความหมายเข้ากับคำว่า Reliability ด้วย แต่ Availability จะมีความหมายที่เจาะจงเฉพาะตัวมากกว่า (คือเปอร์เซ็นต์ Uptime) ส่วน Reliability นั้นหมายความรวมถึงหลาย ๆ ประเด็น เช่น ความถูกต้องของข้อมูล (accuracy) อัตราความผิดพลาด (bit error rates) ความมีเสถียรภาพ (stability) เป็นต้น นักออกแบบบางคนอาจใช้คำว่า Recoverability เข้ามาอ้างถึงความยากง่ายและช่วงเวลาที่ปัญหาของเครือข่ายสามารถถูกแก้ไขได้ว่ารวดเร็วแค่ไหน Recoverability เป็นส่วนผสมหนึ่งของ Availability

Availability ยังเชื่องโยงกับคำว่า Recoverability ด้วย ซึ่งคำนี้เป็นคำที่ได้รับความนิยมเป็นอย่างมากในนิตยสารเครือข่ายปัจจุบัน Resiliency หมายถึง ระดับความหนักหน่วงของโหลดที่เครือข่ายที่สามารถรองรับได้มี Availability ที่ดีด้วย

อีกแง่มุมหนึ่งของ Availability ก็คือ แผนการรองรับความผิดพลาด (disaster recovery) องค์กรส่วนใหญ่มักมีแผนการกรอบกู้ระบบเครือข่ายที่อาจเกิดขึ้นจากความเสียหายด้วยไม่ว่าจะเกิดขึ้นจากภัยธรรมชาติหรือเกิดขึ้นจากน้ำมือของมนุษย์ Disaster Recovery Planning ก็ควรถือเป็นส่วนหนึ่งของ Availability ด้วย

โดยทั่วไป เป้าหมายของลูกค้าในเรื่องของ Availability ก็คือ การทำให้แอปพลิเคชันที่มีความสมำคัญยิ่งยวดทำงานได้อย่างรวบรื่นไม่สะดุด วิธีที่จะช่วยให้เราและลูกค้าของเราเข้าใจถึงความต้องการของ Availability ก็คือ ให้ทดลองคำนวณถึงเวลาและมูลค่าความเสียหายของธุรกิจ อันเนื่องมาจากระบบเครือข่ายไม่สามารถให้บริการแก่แอปพลิเคชันเชิงธุรกิจที่สำคัญมากได้ ให้จัดทำเอกสารประกอบว่าบริษัทจะต้องสูญเสียรายได้ไปเท่าไหร่ถ้าหากแอปพลิเคชันนั้นไม่สามารถทำงานได้เนื่องจากเครือข่ายดาวน์ลงไป

2.5.3 ความสามารถในการส่งผ่านข้อมูลต่าง ๆ อย่างรวดเร็ว (Performance)

การวิคราะห์ประสิทธิภาพการทำงาน (Performance) ของเครือข่าย โดยทั่วไปมักเกี่ยวข้องกับการวิเคราะห์เครือข่ายที่มีอยู่ การวิเคราะห์เครือข่ายที่มีอยู่จะช่วยให้พิจารณาได้ว่าสิ่งใดต้องมีการเปลี่ยนแปลงบ้าง เพื่อทำให้บรรลุเป้าหมายด้าน performance เป้าหมายด้าน performance กับเป้าหมายด้าน scalability มักมีความเกี่ยวข้องกัน ควรเข้าใจแผนการเติบโตของเครือข่ายก่อนที่จะวิเคราะห์เป้าหมายด้าน performance

นิยามเกี่ยวกับ Network performance ควรให้ความสนใจกับข้อกำหนดหรือความต้องการที่เจาะจงลงไปโดยมีพื้นฐานจากข้อตกลงด้านระดับการให้บริการ (service level agreement: SLA) รายการต่อไปนี้แสดงคำศัพท์ต่าง ๆ ที่มักถูกหยิบยกขึ้นมากล่าวถึงเมื่อกำลังวิเคราะห์ performance ของเครือข่ายนั้น ๆ

2.5.3.1 ความจุ (แบนด์วิดธ์ : bandwidth) ความสามารถในการนำพาข้อมูลของเซอรกิตหรือเครือข่าย โดยทั่วไปจะถูกวัดในหน่อยบิตต่อวินาที (bps) หรือเมกะบิตต่อวินาที (Mbps) ค่านี้เป็นค่าเฉพาะตัวของเครือข่ายแต่ละประเภท ตัวอย่างเช่น เครือข่ายโทเค็นริง (token ring) มีแบนด์วิดธ์อยู่ที่ 4 Mbps และ 16 Mbps เครือข่ายอีเทอร์เน็ตก็จะมีตั้งแต่ 10 Mbps, 100 Mbps, 1 Gbps และ 10 Gbps เป็นต้น ค่านี้มักถูกเรียกอย่างง่าย ๆ ภาษาชาวบ้านว่า ความเร็ว (speed) ของเครือข่ายประเภทนั้น ๆ

2.5.3.2 เปอร์เซ็นต์การใช้งาน (utilization) เป็นเปอร์เซ็นต์ของแบนด์วิดธ์ทั้งหมดที่ถูกใช้งานอยู่ เปอร์เซ็นต์การใช้งานที่เหมาะสม (optimum utilization) เปอร์เซ็นต์การใช้งานเครือข่ายโดยเฉลี่ยสูงสุดก่อนที่จะถูกพิจารณาว่าเครือข่ายอิ่มตัว (saturated) เปอร์เซ็นต์การใช้งานเครือข่ายนั้นหมายถึงการวัดว่าแบนด์วิดธ์ถูกใช้ไปเท่าใดในระหว่างช่วงเวลาหนึ่ง ๆ ตัวอย่างเช่น เครื่องมือออนิเตอร์เครือข่ายอาจแสดงผลว่า network utilization บนอีเทอร์เน็ตเซ็กเมนต์ ณ ขณะนั้นเป็น 30 เปอร์เซ็นต์ นั่นหมายความว่า บนเซ็กเมนต์นั้น ๆ 30 เปอร์เซ็นต์กำลังถูกใช้งานอยู่ ถ้าเซ็กเมนต์นั้นมีแบบนด์วิดธ์ 100 Mbps ก็เท่ากับว่า แบนด์วิดธ์ประมาณ 30 Mbps กำลังถูกใช้

เครือข่ายแต่ละประเภทก็จะมีค่าเปอร์เซ็นต์การใช้งานแบนด์วิดธ์ที่เหมาะสมอยู่ ตัวอย่างเช่น บน Wide Area Network (WAN) ค่าเปอร์เซ็นต์การใช้งานควรอยู่ที่ประมาณ 70 เปอร์เซ็นต์ หากเกินกว่านี้ไปมากนั่นอาจเป็นไปได้ว่า WAN นั้นใกล้จะถึงจุดอิ่มตัวแล้ว WAN ที่มีเปอร์เซ็นต์การใช้งานอยู่ที่ประมาณ 70 เปอร์เซ็นต์นี้ สามารถรองรับทราฟฟิกสูงสุด (peak traffic) ที่เกิดขึ้นจากการโอนย้ายข้อมูลจำนวนมากโดยไม่คาดคิดได้จากรีโมตไซต์ได้ อย่าลืมว่า WAN มีแบนด์วิดธ์น้อยว่า LAN ดังนั้นจึงควรให้ความใส่ใจเป็นพิเศษ และอาจมีการนำเอาเทคโนโลยีพิเศษเข้ามาช่วยเพื่อลดปริมาณใช้งานแบนด์วิดธ์ เช่น ฟีเจอร์ของเราติ้งโพรโทคอล การบีบอัดข้อมูล และอื่น ๆ เป็นต้น

2.5.3.3 ทรูพุต (throughput) ปริมาณของข้อมูลที่รับส่งระหว่างโหนดได้สำเร็จโดยไม่มีข้อผิดพลาดต่อหนึ่งหน่วยเวลา (มักเป็นหน่อยข้อมูลต่อวินาที) ทรูพุตในระดับของอุปกรณ์เครือข่ายหมายถึง จำนวนของแพ็กเก็ตต่อหนึ่งวินาที (packet per second : pps) สูงสุดที่อุปกรณ์เครือข่ายสามารถประมวลผลได้โดยไม่มีการโยนแพ็กเก็ตใด ๆ ทิ้ง ผู้ผลิตอุปกรณ์เครือข่ายส่วนใหญ่มักมีการตีพิมพ์อัตรา pps ไว้สำหรับผลิตภัณฑ์ของตน โดยมีพื้นฐานจากทั้งการทดสอบของตนเองและจากองค์กรอิสระ ในการทดสอบอุปกรณ์เครือข่าย วิศวกรทดสอบจะวางอุปกรณ์สร้างทราฟฟิก (traffic generator) และตัววตรวจเช็กทราฟฟิก (traffic checker) ไว้ โดยอุปกรณ์สร้างทราฟฟิกจะทำการส่งแพ็กเก็ตที่มีความยาวตั้งแต่ 64-1,518 ไบต์สำหรับอีเทอร์เน็ต ตัวสร้างทราฟฟิกจะส่งทราฟฟิกจำนวนมาก (burst of traffic) ผ่านอุปกรณ์ที่อัตราเริ่มต้นซึ่งเป็นค่าครึ่งหนึ่งของค่าที่เป็นไปได้ในทางทฤษฎี ถ้าแพ็กเก็ตทั้งหมดได้รับอัตราจะถูกเพิ่มขึ้น แต่ถ้าแพ็กเก็ตทั้งหมดไม่ได้รับอัตราจะถูกลดระดับลงมา กระบวนการนี้จะถูกกระทำซ้ำไปเรื่อย ๆ จนกระทั่งได้ค่าอัตราสูงสุดที่แพ็กเก็ตสามารถถูกส่งไป และอุปกรณ์ได้รับทั้งหมดโดยไม่มีการสูญเสียแพ็กเก็ต (packet loss) ค่านี้มีถือเป็นค่า pps ทรูพุตในระดับแอปพลิเคชัน ผู้ใช้ปลายทางส่วนใหญ่มักคำนึงถึงทรูพุตของแปพลิเคชันว่า พวกเขารับส่งข้อมูลระหว่างกันขณะใช้งานแอปพลิเคชันได้รวดเร็วขนาดไหน

2.5.3.4 ประสิทธิภาพ (efficiency) เป็นตัววัดว่าต้องใช้ความพยายามเท่าใดในการทำให้เกิดปริมาณของทรูพุตที่กำหนด

2.5.3.5 เวลาหน่วง (delay, latency) ระยะเวลาที่นับจากเฟรมเริ่มเตรียมพร้อมสำหรับส่งจากโหนดต้นทางจนกระทั่งเดินทางไปถึงโหนดปลายทางในเครือข่าย

2.5.3.6 เวลาตอบสนอง (response time) ระยะเวลาระหว่างการร้องขอการให้บริการจากเครือข่ายไปจนถึงเวลาที่ได้รับการตอบสนองกลับ

2.5.4 ความสามารถในการสร้างความปลอดภัยให้กับข้อมูล (Security)

หมายถึง ความสามารถของระบบเครือข่ายในการปกป้องทรัพยากรต่าง ๆ ภายในไว้ให้ผู้ใช้ได้รับเฉพาะข้อมูลหรือใช้งานทรัพยากรได้ตามที่ตนมีสิทธิเท่านั้น Security นี้เป็นประเด็นที่กินความหมายได้กว้างมากกว้างกว่าประเด็นด้านเทคนิคอื่น ๆ เพราะเกี่ยวพันกันตั้งแต่อุปกรณ์เครือข่ายในระดับล่างไปจนถึงระดับของระบบปฏิบัติการ และระดับแอปพลิเคชัน อีกทั้งยังขยายความรวมไปถึงขอบเขตของการปกป้องความปลอดภัยทั้งในอินทราเน็ต อินเทอร์เน็ต หรือเอ็กซ์ทราเน็ต หัวข้อนี้สามารถถูกกล่าวแยกออกเป็นหนังสือได้หลายเล่มทีเดียว พึงระลึกไว้อย่างหนึ่งว่า Security ที่ดีนั้นจะต้องเอื้ออำนวยให้ผู้ใช้ใช้งานระบบได้อย่างสะดวกด้วย และระบบงานด้านธุรกิจสามารถดำเนินต่อไปได้โดยไม่สะดุดหรือปรับเปลี่ยนมากนัก และกระทำได้โดยไม่ส่งผลกระทบมากนักกับความสามารถด้านอื่น ๆ เช่น เรื่องของ Performance และความง่ายในการทำงานของผู้ใช้บนเครือข่าย

2.5.5 ความสามารถในการจัดการ (Manageability)

การจัดการเครือข่ายถือเป็นประเด็นด้านเทคนิคประการหนึ่งที่ผู้ออกแบบเครือข่ายขนาดกลางไปจนถึงขนาดใหญ่หรือใหญ่มากจำเป็นต้องคำนึงถึง มาตรฐาน ISO (International Standard Organization) ได้กล่าวไว้ว่า การจัดการเครือข่ายที่ดีควรประกอบไปด้วยแนวทางการจัดการ 5 ต่อไปนี้

2.5.5.1 Configuration Management เป็นการจัดการการเซตคอนฟิกูเรชันของอุปกรณ์เครือข่ายทั้งหมด โดยเป็นการจัดการจากศูนย์กลางเพื่ออำนวยความสะดวกให้กับผู้บริหารเครือข่าย ความสามารถในด้านการทำ Configuration Management จะช่วยให้ผู้บริหารเครือข่ายติดตาม (keep track) สถานการณ์คอนฟิกอุปกรณ์ และเก็บรักษาข้อมูลสถานะนั้นไว้ผู้บริหารเครือข่ายสามารถนิยามและเซฟดีฟอลต์คอนฟิกูเรชันสำหรับอุปกรณ์ประเภทเดียวกัน แก้ไขดีฟอลต์คอนฟิกูเรชันของอุปกรณ์ที่ต้องการได้ และโหลดคอนฟิกูเรชันลงไปบนอุปกรณ์ได้โดยไม่จำเป็นต้องเทลเน็ต (telnet) เข้าไปยังอุปกรณ์แล้วเซตคอนฟิกทีละตัว ความสามารถด้าน Configuration Management ยังช่วยให้ผู้บริหารเครือข่ายจัดทำ Inventory ของอุปกรณ์ต่างๆ ได้ รวมถึงการเก็บบันทึกล็อกไฟล์เพื่อการเก็บรายละเอียดของเวอร์ชันของระบบปฏิบัติการหรือเครือข่ายเซอร์วิสที่รันอยู่

ตัวอย่างของการเก็บบันทึกล็อกไฟล์ที่มีประโยชน์ ได้แก่ การจัดเก็บหมายเลขเวอร์ชันของระบบปฏิบัติการเครือข่ายรวมทั้งรันนิ่งคอนฟิกูเรชันของแต่ละอุปกรณ์ไว้ เพื่อความสะดวกในการปรับปรุงฟีเจอร์ต่าง ๆ ของอุปกรณ์หรือในการแก้ไขปัญหา

2.5.5.2 Performance Management เป็นการวิเคราะห์ประสิทธิภาพโดยรวมของระบบเพื่อนำไปสู่การวางแผนและการปรับปรุงคุณภาพของอุปกรณ์ให้ดีขึ้น การทำ Performance

Management จะรวมถึงการวิเคราะห์พฤติกรรมและประสิทธิผลในการทำงานของระบบเครือข่าย วิเคราะห์เวลาตอบสนอง (response time)

2.5.5.3 Fault Management เป็นการตรวจเช็ก แยกแยะและแก้ไขปัญหาที่เกิดขึ้น รายงานปัญหาที่เกิดให้ผู้จัดการเครือข่ายหรือรวมทั้งผู้ใช้เครือข่ายได้ทราบ

2.5.5.4 Security Management เป็นการมอนิเตอร์ และทดสอบมาตรการและนโนบายด้านการรักษาความปลอดภัย รวมถึงการรออดิตระบบรักษาความปลอดภัย

2.5.5.5 Accounting Management เป็นการจัดทำบันทึกปริมาณการใช้งานเครือข่าย ปริมาณทราฟฟิกที่วิ่งผ่าน รับเข้า / ส่งออกภายในเครือข่าย ซึ่งสามรถนำไปสู่การจัดเก็บหรือประเมินค่าใช้จ่าย (billing system) และการวางแผนในระยะยาว (capacity planning)

การทำให้บรรลุเป้าหมายในเรื่องของ Manageability นั้น จำเป็นต้องมีองค์ประกอบเสริมอื่น ๆ เข้ามาเกี่ยวข้องด้วย อย่างน้อยจำเป็นต้องมี “ซอฟต์แวร์จัดการเครือข่าย” ที่ดี

ซอฟต์แวร์จัดการเครือข่าย (Network Management Software) ที่มีใช้อยู่ในตลาดนั้นมีหลายยี่ห้อจากหลากหลายผู้ผลิต เช่น HP Open View ของ Hewlett-Packard, Cisco Works ของ Cisco System, Transcend ของ 3COM, Optivity NMS ของ Nortel Networks, SPETRUM ของ Enterasys Networks, Sun Net Manager ของ Sun

โดยทั่วไปแล้ว ซอฟต์แวร์จัดการเครือข่ายเหล่านี้จะอาศัยความสามารถของโพรโทคอล SNMP (simple Network Management Protocol) ซึ่งเป็นโพรโทคอลมาตรฐานระบบเปิดและบ่อยครั้งที่ซอฟต์แวร์จัดการเครือข่ายมักถูกเลือกโดยพิจารณาจากยี่ห้อของอุปกรณ์เครือข่ายที่ใช้งานอยู่ขณะนั้นให้เป็นผลิตภัณฑ์จากผู้ผลิตรายเดียวกัน ซอฟต์แวร์จัดการเครือข่ายที่ได้รับความนิยมมากมีอยู่ 2 ตัวได้แก่ HP Open View ของ Hewlett-Packard และ Cisco Works ของ Cisco Systems HP Open view นั้นเป็นซอฟต์แวร์จัดการเครือข่ายที่มีการวิวัฒนาการมาเป็นเวลายาวนาน อีกทั้งยังมีหลากหลายฟีเจอร์ที่ผู้บริหารเครือข่ายชื่นชอบ โดยเฉพาะในเรื่องของการแสดงแผนที่ที่ดูง่าย ส่วน Cisco work ของ Cisco นั้นได้รับความนิยมเนื่องจาก Cisco ถือเป็นผู้ผลิตอุปกรณ์เครือข่ายชั้นนำของโลกอยู่แล้ว ฐานการตลาดของซิสโก้นั้นมีอยู่มาก จึงมีผลต่อการเลือกใช้ซอฟต์แวร์จัดการเครือข่ายจากผู้ผลิตรายการเดียวกันไปด้วย ซอฟต์แวร์จัดการเครือข่ายที่กล่าวมานี้อาจทำได้ดีในบางเรื่องเช่น Configuration Management, Fault Management แต่ลำหรับบางความต้องการเช่น การออกรายงานหรือสร้าง Report สำหรับนำเสนอ

รวมทั้งการรวบรวมข้อมูลบางสอย่างเช่น Network Utilization นั้นอาจต้องมีซอฟต์แวร์อื่น ๆ เข้ามาเสริมด้วย เช่น MRTG และ Net Flow ของซิสโก้ เป็นต้น

2.5.6 ความสามารถในการรองรับการเปลี่ยนแปลงในอนาคต (Adaptability)

เครือข่ายที่ดีควรสามารถรองรับการเปลี่ยนแปลงในอนาคตได้เมื่อมีเทคโนโลยีใหม่ ๆ ที่จำเป็น หรือเอื้อประโยชน์ต่อการทำงานมากขึ้น ตัวอย่างเช่น ควรรองรับ Voice, QoS (Quality of Service) เหล่านี้ได้โดยไม่จำเป็นต้องเปลี่ยนอุปกรณ์ใหม่ เพียงแค่เพิ่มเติมการ์ดโมดูลเข้าไป

2.5.7 ประเด็นเกี่ยวกับต้นทุนค่าใช้จ่ายที่เหมาะสม (Affordability)

เป้าหมายนี้บางครั้งถูกเรียกว่า cost-effectiveness จุดประสงค์หลักของเป้าหมายนี้ก็คือ การทำให้เครือข่ายรองรับปริมาณทราฟฟิกให้ได้มากที่สุดภายในต้นทุนการเงินหรืองบประมาณที่มีอยู่ ใน Campus Networks ต้นทุนดังกล่าวมักไม่สูงนัก เพราะเครือข่ายประเภทนี้มักใช้งานสวิตช์เป็นส่วนใหญ่ แต่สำหรับใน Enterprise Networks ที่ประกอบด้วย Wide Area Network เป้าหมายด้าน Availability มักถือว่าเป็นเป้าหมายที่สำคัญกว่าเป้าหมายด้าน Availability องค์กรโดยทั่วไปจึงมักหาทางทำให้เป้าหมายด้าน Availability ดำเนินไปพร้อม ๆ กับด้าน Availability ให้ได้ เพราะค่าใช้จ่ายในแต่ละเดือนสำหรับการเช่าเซอร์กิตไม่ว่าจะเป็น Frame Relay, X.25 หรือ Leased Line ล้วนเป็นค่าใช้จ่ายที่มิใช่น้อยในการลดต้นทุนค่าใช้จ่ายในส่วนที่เกี่ยวกับ WAN Circuit สามารถทำได้โดยใช้เทคนิคต่าง ๆ เช่น

2.5.7.1 ใช้ Routing Protocol ที่ก่อให้เกิดทราฟฟิกบน WAN Circuit น้อยที่สุดเท่าที่เป็นไปได้

2.5.7.2 ลดปริมาณทราฟฟิกบน WAN Circuit ด้วยการใช้ฟีเจอร์อย่างเช่น การบีบอัดข้อมูล, Voice Activity Detection (VAD)

2.5.7.3 ใช้งาน WAN Circuit ให้คุ้มค่า เช่น ใช้รับส่งสัญญาณเสียง (voice signal) ไปด้วยโทรศัพท์ทางไกล

2.5.8 การใช้งานที่ง่ายดายและสะดวกสำหรับผู้ใช้ (Usability) เครือข่ายที่ดีควรทำให้ผู้ใช้ใช้งานทรัพยากรต่าง ๆ ได้โดยง่ายไม่ซับซ้อน สามารถเพิ่มการให้บริการอย่างเช่น Dynamic Host Configuration Protocol (DHCP) หรือ Windows Internet Naming Services (WINS), DNS ที่ดีเข้าไป เพื่อทำให้ผู้ใช้ใช้งานเครือข่ายได้ง่ายขึ้น

ประเด็นต่าง ๆ ที่กล่าวมาข้างต้นเป็นเพียงแค่แนวทางกว้าง ๆ เท่านั้น ในความเป็นจริงอาจไม่มีเครือข่ายใดที่มีคุณสมบัติต่าง ๆ พร้อมกันในเวลาเดียวกันได้ บางครั้งจำเป็นต้องถ่วงน้ำหนักต่าง ๆ ให้สมดุลกัน ตัวอย่างเช่น หากต้องการในแง่ของความสามารถในการให้บริการได้อย่างต่อเนื่อง

(Availability) จำเป็นต้องเพิ่มต้นทุนค่าใช้จ่ายให้สูงขึ้นตามไปด้วย คิดง่าย ๆ จากหัวข้อ “ตัวอย่างการเชื่อมต่อเครือข่ายจริงโดยใช้อุปกรณ์ประเภทต่าง ๆ”

บทสรุป

OSI Model เป็นรูปแบบความคิดที่กล่าวถึงคุณสมบัติพิเศษและมาตรฐานการทำงานภายในของระบบการสื่อสารโดยแบ่งเป็นชั้นนามธรรม และโพรโทคอลของระบบคอมพิวเตอร์

LAN Segmentation หมายถึงการแบ่ง LAN ออกเป็นเครือข่ายส่วนย่อย ๆ ซึ่งเรียกว่าแบ่งเป็น “เซกเมนต์ (segment)” โดยใช้อุปกรณ์เครือข่ายต่าง ๆ ได้แก่ บริดจ์/สวิตซ์ และเราเตอร์ ซึ่งแต่ละแบบนั้นจะมีผลต่อเรื่องของ Collision Domain และ Broadcast Domain

การออกแบบในลักษณะมีโครงสร้างตามลำดับชั้น ประกอบไปด้วยเลเยอร์ที่เรียกว่า Core Layer, Distribution Layer และ Access Layer ตามลำดับ

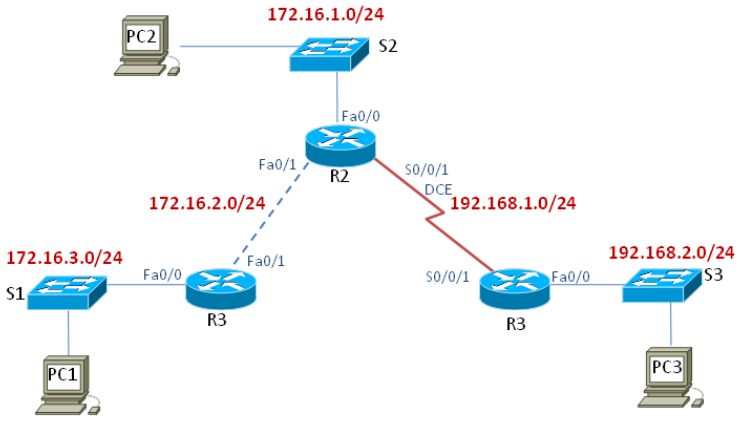
การออกแบบเครือข่ายต้องคำนึงถึงเครือข่ายที่จะใช้ในอนาคตด้วย ความพร้อมใช้ ความง่ายในการใช้งาน และความปลอดภัย

การจัดการเครือข่ายมี 5 แนวทาง คือ Configuration, Performance, Fault, Security และ Accounting

แบบฝึกหัด

จงตอบคำถามต่อไปนี้มาพอสังเขป

1. อธิบายการทำงานของโมเดล OSI ในแต่ละชั้นมาพอเข้าใจ?
2. อธิบายการทำงานของอุปกรณ์ที่ทำงานในแต่ละเลเยอร์ต่อไปนี้ Core Layer, Distribution Layer และ Access Layer?
3. การออกแบบเครือข่ายควรคำนึงถึงสิ่งใดบ้าง?
4. การจัดการคือข่ายมีแนวทางอย่างไรบ้าง?
5. ไดอะแกรมต่อไปนี้ มีกี่ Collision และ Broadcast Domain ?



อ้างอิง

IBM. (n.d). **OSI model.** Retrieved Nov 20, 2016, from https://www.ibm.com/support/knowledgecenter/en/SSCVHB_1.1.0/glossary/npi_osi_model.html

Tech-faq. (n.d). **Understanding the Cisco Three-Layer Hierarchical Model**. Retrieved Nov 23, 2016, from http://www.tech-faq.com/understanding-the-cisco-three-layer-hierarchical-model.html

วิกิพีเดีย. (2558).**แบบจำลองโอเอสไอ**. สืบค้นเมื่อ 20 พฤศจิกายน 2558, สืบค้นจาก https://th.wikipedia.org/wiki/แบบจำลองโอเอสไอ

Ryan. (2554). **Collision Domains vs. Broadcast Domains**. Retrieved Jun 20, 2017, from https://ciscoskills.net/2011/03/30/collision-domains-vs-broadcast-domains

เอกสิทธิ์ วิริยจารี .(2548). **เรียนรู้ระบบเครือข่ายจากอุปกรณ์ของ Cisco ภาคปฏิบัติ** กรุงเทพฯ .: ซีเอ็ดยูเคชั่น

จตุชัย แพงจันทร์. (2555). เจาะระบบ Network 3nd Edition. นนทบุรี: ไอดีซีฯ

สุชาติ คุ้มมะณี .ธวัชชัย ชมศิริ ,(2550). **เรียนรู้เครือข่ายและอุปกรณ์ Cisco ด้วยโปรแกรม Simulation**. กรุงเทพฯ : โปรวิชั่น