การออกแบบและวางระบบเครือข่ายคอมพิวเตอร์

กรณีศึกษา : อาคารโรงแรม

Network Design and Implementation

Case Study : Hotel Building

นายวรชน พนมชน

โครงงานสหกิจนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีสารสนเทศ

พ.ศ. 2561

การออกแบบและวางระบบเครือข่ายคอมพิวเตอร์

กรณีศึกษา : อาคารโรงแรม

Network Design and Implementation

Case Study : Hotel Building

นายวรชน พนมชน

โครงงานสหกิจนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

ปริญญาวิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีสารสนเทศ

พ.ศ. 2561

การออกแบบและวางระบบเครือข่ายคอมพิวเตอร์
กรณีศึกษา : อาคารโรงแรม
Network Design and Implementation Case Study : Hotel Building

นายวรชน พนมชน

โครงงานสหกิจศึกษานี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาเทคโนโลยีสารสนเทศบัณฑิต สาขาเทคโนโลยีสารสนเทศ
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย – ญี่ปุ่น
พ.ศ. 2561

คณะกรรมการสอบ

..... ประธานกรรมการสอบ
(ดร.โสภณ มงคลลักษมี)

..... กรรมการสอบ
(ดร.บุษราพร เหลืองมาลาวัฒน์)

..... อาจารย์ที่ปรึกษา
(รศ.ดร.อรรณพ หมั่นสกุล)

..... ประธานสหกิจศึกษาสาขาวิชา
(อาจารย์สลิลา ชีวกิดาการ)

ชื่อโครงงาน	การออกแบบและวางระบบเครือข่ายคอมพิวเตอร์ กรณีศึกษา : อาคารโรงแรม
ผู้เขียน	นายวรชน พนมชน
คณะวิชา	เทคโนโลยีสารสนเทศ สาขาเทคโนโลยีสารสนเทศ
อาจารย์ที่ปรึกษา	รองศาสตราจารย์ ดร.อรรณพ หมั่นสกุล
พนักงานที่ปรึกษา	นายศุภเดช สุทธิพงศ์คณาสัย
ชื่อบริษัท	VR Online Limited
ประเภทธุรกิจ/สินค้า	ให้บริการออกแบบและติดตั้งระบบเน็ตเวิร์ค

บทสรุป

จากผลการดำเนินงานของโครงการสำเร็จอย่างสมบรูณ์โดยสามารถงานที่ข้าพเจ้าได้รับหมอบหมายในโครงการสหกิจศึกษาเป็นงานในส่วนของออกแบบและติดตั้งระบบเครือข่าย ในช่วงแรกได้รับหมอบหมายให้ทำการศึกษาการและเรียนรู้วิธีการออกแบบและติดตั้งระบบ หลังจากนั้นเข้าสู่การทำงานจริง ได้ไปออกแบบระบบที่หน้างานและติดตั้งระบบให้กับบริษัทต่างๆรวมถึงได้รับหมอบหมายโครงงานสหกิจศึกษา คือออกแบบและวางระบบเครือข่ายคอมพิวเตอร์ให้กับโรงแรมแห่งหนึ่ง

ผลที่ได้รับจากการทำงานสหกิจ คือ ประสบการณ์การทำงานจริง ความรู้ทางด้านออกแบบและติดตั้งรวมไปถึงติดตามผลการใช้งานของระบบ เครือข่าย นอกจากนี้สิ่งที่ได้รับจากการทำงานสหกิจคือ ความรับผิดชอบในหน้าที่ที่ได้รับ รวมถึงการทำงานให้เสร็จภายในเวลาที่กำหนดและการทำงานให้ออกมามีประสิทธิภาพมากที่สุด

Project's name	Network Design and Implementation Case Study: Hotel Building
Writer	Mr.Worrachon Panomchon
Faculty	Information Technology, Information Technology
Faculty Advisor	Assoc. Prof. Dr.Annop Monsakul
Job Supervisor	Mr.Supadej Sutthiphongkanasai
Company's name	VR Online Limited
Business Type/Product	Network Design and Implementation

Summary

The work that I had been assigned in the cooperative education project is designing and installing the network. At the beginning, I was assigned to study how to design and install the system before practice the actual work to design the system at the site and to install the system for companies as well as the assignment of projects for cooperative education which is designing and installing computer network to the hotel.

The result of cooperative work is real work experience of design knowledge, installation, as well as monitors the performance of the network. In addition, the thing that I obtained from the co-operation is responsibility for the duty, punctuality on deadline of work and contributing the most effective productivity.

กิตติกรรมประกาศ

ตลอดการร่วมปฏิบัติงานสหกิจและการทำโครงงานต่างๆ ได้ลุล่วงไปได้ด้วยความอนุเคราะห์ ความเมตตา และความช่วยเหลือจากบุคคลหลายฝ่าย ซึ่งส่งผลให้โครงงานและการปฏิบัติงานดำเนินไปอย่างราบรื่น ซึ่งมีดังต่อไปนี้

1. คุณ จิดาภา พิทักษ์สัญญา (Managing Director) ที่ได้ให้การฝึกอบรมก่อนสหกิจศึกษา และให้โอกาสผู้เขียนเข้ามาสหกิจศึกษาและมอบหมายให้ร่วมปฏิบัติงานโครงการที่บริษัทแห่งนี้
2. คุณ ศุภเดช สุทธิพงศ์คณาสัย (Senior Network Engineer) ที่ค่อยสอนงานและมอบหมายให้ในการปฏิบัติงานสหกิจศึกษา
3. คุณ พิเชษฐ์ ปิวะพงษ์ (Network Engineer) ที่ค่อยสอนงานและมอบหมายให้ในการปฏิบัติงานสหกิจศึกษา

และบุคลากรอื่นๆ ที่ไม่ได้ร่วมเอ่ยนามด้วยทุกท่านที่ได้ให้คำแนะนำและความช่วยเหลือในการทำงานเป็นอย่างดี

ผู้เขียนใคร่ขอขอบพระคุณผู้ที่มีส่วนเกี่ยวข้องทุกท่าน ที่มีส่วนร่วมในการให้ข้อมูล เป็นที่ปรึกษาในการทำรายงานฉบับนี้จนเสร็จสมบูรณ์ ตลอดจนให้การดูแลและให้ความเข้าใจเกี่ยวกับชีวิตการทำงานจริง ผู้เขียนขอขอบคุณ ไว้ ณ ที่นี้ด้วย

วรชน พนมชน

ผู้จัดทำ

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูปประกอบ

รูปที่ **หน้า**

สารบัญภาพประกอบ (ต่อ)

ภาพที่ **หน้า**

สารบัญภาพประกอบ (ต่อ)

ภาพที่ **หน้า**

บทที่ 1

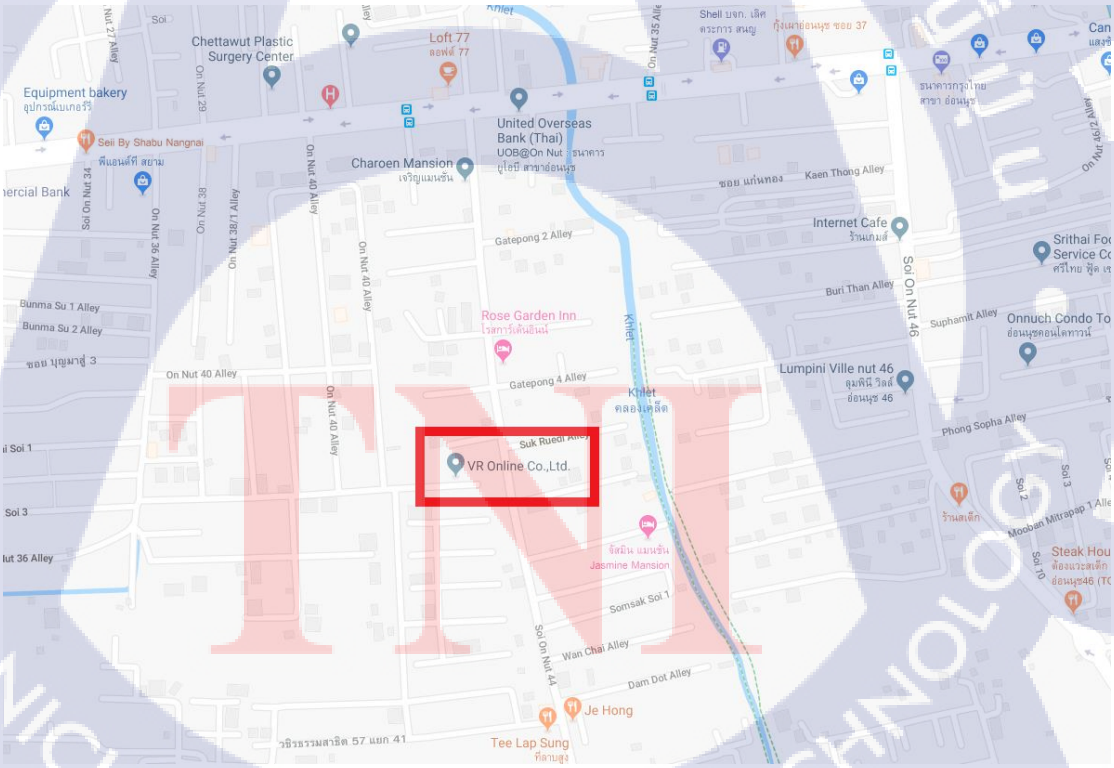
บทนำ

1.1 ชื่อและที่ตั้งสถานประกอบการ

ชื่อสถานประกอบการ : บริษัท วีอาร์ ออนไลน์ จำกัด

ที่ตั้งสถานประกอบการ : 107 ซอยอ่อนนุช 40 แขวงอ่อนนุช เขตสวนหลวง กรุงเทพมหานคร 10250

โทรศัพท์ : +662 006 8281



รูปที่ 1.1 แผนที่ตั้งบริษัท วีอาร์ ออนไลน์ จำกัด

1.2 ลักษระธุรกิจของสถานประกอบการ หรือการให้บริการขององค์กร

บริษัท วีอาร์ ออนไลน์ จำกัด (VR ONLINE Limited) ก่อตั้งใน ปี พ.ศ.2559 ดำเนินธุรกิจออกแบบและติดตั้งระบบเน็ตเวิร์ค พร้อมให้คำปรึกษากับสถานที่ใดๆที่ต้องการใช้เน็ตเวิร์คที่มีคุณภาพสูง

1.2.1 สินค้า

บริษัท วีอาร์ ออนไลน์ จำกัด (VR ONLINE Limited) มีการบริการ Solution ดังต่อไปนี้

1) Network Solution
2) Wireless Solution
3) Surveillance Solution
4) Network Security
5) Training

1.2.2 บริการด้านที่ปรึกษา

ลูกค้าจะได้รับการบริการที่ครบวงจร โดยเริ่มตั้งแต่การให้คำปรึกษา การติดตั้ง ไปจนถึงการบริการหลังการขาย

1) Consultation & Implementation

ทีมที่ปรึกษามากด้วยทักษะและประสบการณ์ทางด้านเน็ตเวิร์คที่สามารถที่จะให้โซลูชั่นและมุมมองที่มีประสิทธิภาพในการตอบสนองต่อความสำเร็จของลูกค้า

2) Training

ผู้ใช้งานจะได้รับการฝึกอบรมแบบ Workshop เพื่อให้ผู้อบรมทำความเข้าใจกับโซลูชั่นและสามารถใช้งานได้อย่างมีประสิทธิภาพ

3) Support

เรามีบริการหลังการขายที่จะให้บริการด้านคำปรึกษา ข้อเสนอแนะ และแก้ไขปัญหาให้กับลูกค้าทุกรายเพื่อช่วยให้ระบบงานของท่านทำงานได้อย่างราบรื่น

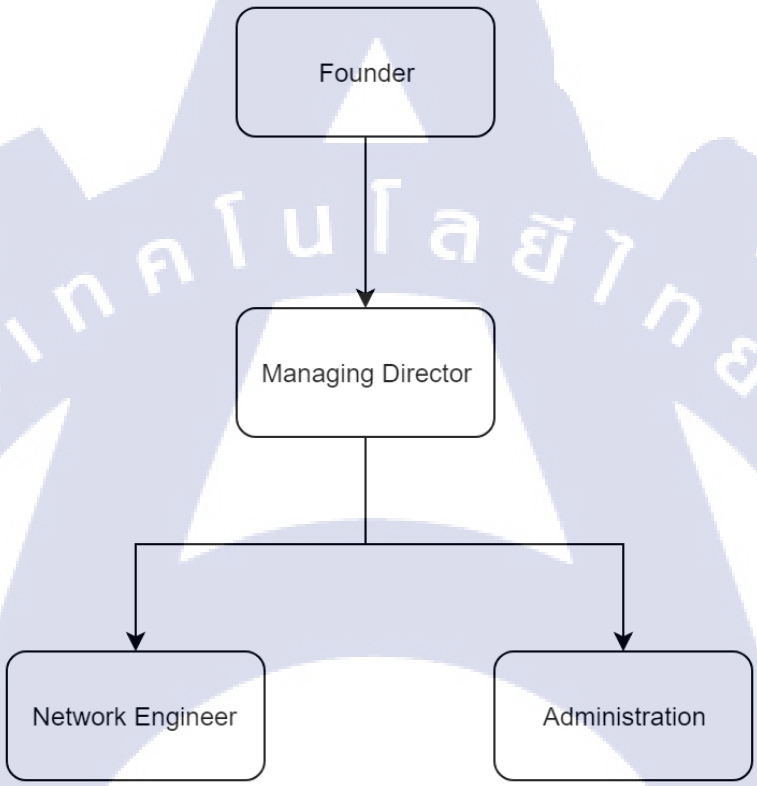
1.2.3 Experienced / Certified Resources

ทีมงานมืออาชีพที่มากด้วยประสบการณ์ในการออกแบบ และ ติดตั้งระบบเครือข่าย โดยที่ในทีมจะผ่านการฝึกอบรมและได้รับการรับรองดังนี้

1. MikroTik Certified Trainer
2. MikroTik Certified NetworTrainerk Associate
3. Mikrotik Certified Routing Engineer
4. MikroTik Certified Wireless Engineer
5. MiktoTik Certified Traffic Control Engineer
6. MiktoTik Certified User Management Engineer
7. MikroTik Certified IPv6 Engineer
8. Mikrotik Certified Internetworking Engineer
9. Ubiquiti Enterprise Wireless Admin
10. Draytek Certified Network Admin

1.3 รูปแบบการจัดองค์กรและการบริหารองค์กร

1.3 ผังโครงสร้างองค์กร



รูปที่ 1.2 แสดงแผนผัง โครงสร้างองค์กร

1.4 ตำแหน่งและหน้าที่งานที่นักศึกษาได้รับหมอบมาย

ตำแหน่ง : Network Engineer

หน้าที่ : ออกแบบและวางระบบเครือข่ายคอมพิวเตอร์

1.5 พนักงานที่ปรึกษาและตำแหน่งของพนักงานที่ปรึกษา

1) คุณ ศุภเดช สุทธิพงศ์คณาสัย : Senior Network Engineer

1.6 ระยะเวลาปฏิบัติงาน

1) ระยะเวลาอบรมก่อนปฏิบัติงานสหกิจศึกษาเป็นเวลา 2 เดือน

- เริ่มต้นอบก่อนปฏิบัติงานสหกิจ วันที่ 2 เมษายน พ.ศ. 2561
- สิ้นสุดอบรมก่อนปฏิบัติงานสหกิจ วันที่ 31 พฤษภาคม พ.ศ. 2561

2) ระยะเวลาปฏิบัติงานสหกิจศึกษาเป็นเวลา 4 เดือน

- เริ่มต้นปฏิบัติงานสหกิจศึกษา วันที่ 4 มิถุนายน พ.ศ. 2561
- สิ้นสุดงานสหกิจศึกษา วันที่ 28 กันยายน พ.ศ. 2561

1.7 ที่มาและความสำคัญของปัญหา

บริษัทเอ(นามสมมุติ) ดำเนินธุรกิจด้านโรงแรม มีปัญหาระบบอินเตอร์เน็ตไร้สายที่ให้บริการกับผู้มาเข้าพัก เช่น มีอาการหลุดออกจากระบบบ่อย , ความเร็วในการใช้งานอินเตอร์เน็ตช้า ทำให้มีความต้องการแก้ไขปัญหาดังกล่าว

1.8 วัตถุประสงค์ของการปฏิบัติงานและโครงงานที่ได้รับหมอบหมาย

1. เพื่อให้ได้เรียนรู้สภาพการทำงานจริงของการเป็น Network Engineer
2. เพื่อศึกษาการออกแบบระบบเครือข่ายคอมพิวเตอร์
3. เพื่อศึกษาการติดตั้งอุปกรณ์ต่างๆในระบบ
4. เพื่อศึกษาระบบเทคโนโลยี Software Defined Networks

1.9 ผลที่คาดว่าจะได้รับจากการปฏิบัติงาน หรือโครงการที่ได้รับหมอบหมาย

1. ได้รับประสบการณ์ในการทำงานจริงของการเป็น Network Engineer
2. ทำงานที่หมอบหมายให้เสร็จตามทันเวลา
3. ฝึกความรับผิดชอบต่องานที่ได้รับ และการจัดลำดับความสำคัญในการทำงาน
4. ได้ความรับรู้เกี่ยวกับการออกแบบระบบเครือข่ายคอมพิวเตอร์
5. สามารถนำความรู้และทักษะที่ได้รับจากการสหกิจศึกษานำไปใช้ประโยชน์ได้ในอนาคต

บทที่ 2
ทฤษฎีและเทคโนโลยีที่ใช้ในการปฏิบัติงาน

2.1 Computer Network

2.1.1 ความหมายของ Computer Network

Computer Network คือระบบเครือข่ายคอมพิวเตอร์ ซึ่งหมายถึงการเชื่อมต่อคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปเข้าด้วยกันด้วยสายเคเบิล หรือสื่ออื่นๆ ทำให้คอมพิวเตอร์สามารถรับส่งข้อมูลแก่กันและกันได้ ในกรณีที่เป็นการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์หลายๆ เครื่องเข้ากับเครื่องคอมพิวเตอร์ขนาดใหญ่ที่เป็นศูนย์กลาง เราเรียกคอมพิวเตอร์ที่เป็นศูนย์กลางนี้ว่า โฮสต์ (Host) และเรียกคอมพิวเตอร์ขนาดเล็กที่เข้ามาเชื่อมต่อว่า ไคลเอนต์ (Client/Terminal)

ระบบเครือข่าย (Network) จะเชื่อมโยงคอมพิวเตอร์เข้าด้วยกันเพื่อการติดต่อสื่อสาร เราสามารถส่งข้อมูลภายในอาคาร หรือข้ามระหว่างเมืองไปจนถึงอีกซีกหนึ่งของโลก ซึ่งข้อมูลต่างๆ อาจเป็นทั้งข้อความ รูปภาพ เสียง ก่อให้เกิดความสะดวกรวดเร็วแก่ผู้ใช้ ซึ่งความสามารถเหล่านี้ทำให้เครือข่ายคอมพิวเตอร์มีความสำคัญ และจำเป็นต่อการใช้งานในแวดวงต่างๆ

รูปแบบของเน็ตเวิร์คแบ่งได้เป็น 3 ลักษณะ ดังนี้

1.LAN(Local Area Network)

เป็นกลุ่มของคอมพิวเตอร์ที่เชื่อมต่อกันในพื้นที่จำกัด เช่นภายในตึกสำนักงาน หรือภายในโรงงาน ส่วนมากจะใช้สายเคเบิ้ลในการติดต่อสื่อสารกัน

2.MAN(Metropolitan Area Network)

เป็นการนำระบบ LAN หลายๆ LAN ที่มีพื้นที่อยู่ใกล้เคียงกันมาเชื่อมต่อกันให้มีขนาดใหญ่ขึ้น เช่นเชื่อมต่อกันในเมือง หรือในจังหวัด เป็นต้น

3.WAN(Wide Area Network)

เป็นกลุ่มของคอมพิวเตอร์ที่เชื่อมต่อกันแบบกว้างขวาง อาจจะเป็นภายในประเทศหรือระหว่างประเทศเป็นการใช้หลายๆ LAN หรือหลายๆ MAN ซึ่งอยู่คนละพื้นที่เชื่อมต่อเข้าหากัน เช่น สำนักงานที่ New York เชื่อมต่อกับที่ London การติดต่อสื่อสารกันอาจจะใช้ตั้งแต่สายโทรศัพท์จนกระทั่งถึงดาวเทียม

2.2 Open System Interconnection

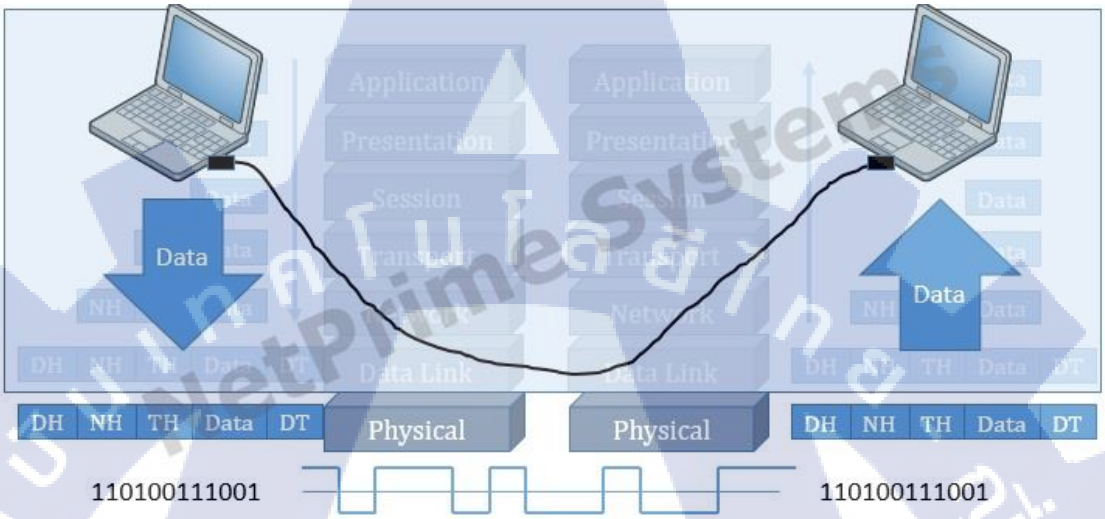
องค์กรมาตรฐานระหว่างประเทศ (The International Organization for Standardization) ได้พัฒนา Model ของการทำงานบนระบบเครือข่ายขึ้นมาเป็นมาตรฐานกลาง ในปัจจุบันใช้เพื่ออ้างอิงการสื่อสารและเปรียบเทียบการทำงานบนเครือข่าย บริษัท ที่ผลิตอุปกรณ์หรือ software ต่างๆขึ้นมาก็จะต้องผลิตตามมาตรฐานที่กำหนดขององค์ที่ดูแลในแต่ละส่วน ซึ่ง Model นี้ก็ถูกนำมาใช้มาเปรียบเทียบเพื่อให้เข้าใจและอธิบายการทำงานของแต่ละส่วนได้ง่ายขึ้น OSI Model ใช้อ้างอิงการสื่อสาร (Reference Model) แบ่งออกเป็นชั้น (Layer) โดยมีตั้งแต่ชั้นที่ 1 ถึงชั้น 7 (Layer 1 – 7) โดย Layer 1 จะอยู่ด้านล่างสุด และเรียงขึ้นไปจนถึง Layer 7 แต่ละ Layer ก็มีชื่อเรียกตามรูปแบบการสื่อสารและการทำงานของมันในแต่ละชั้น

	OSI Layer	TCP/IP	Datagrams are called
Software	Layer 7 Application	HTTP, SMTP, IMAP, SNMP, POP3, FTP	Upper Layer Data
	Layer 6 Presentation	ASCII Characters, MPEG, SSL, TSL, Compression (Encryption & Decryption)	
	Layer 5 Session	NetBIOS, SAP, Handshaking connection	
	Layer 4 Transport	TCP, UDP	Segment
	Layer 3 Network	IPv4, IPv6, ICMP, IPSec, MPLS, ARP	Packet
Hardware	Layer 2 Data Link	Ethernet, 802.1x, PPP, ATM, Fiber Channel, MPLS, FDDI, MAC Addresses	Frame
	Layer 1 Physical	Cables, Connectors, Hubs (DLS, RS232, 10BaseT, 100BaseTX, ISDN, T1)	Bits

ตารางที่ 2.1 OSI AND TCP/IP Modal

2.2.1 Layer 1 (Physical Layer)

เป็น ชั้นล่างสุด จะมีการกำหนดคุณสมบัติทางกายภาพของฮาร์ดแวร์ที่ใช้เชื่อมต่อระหว่าง คอมพิวเตอร์ทั้งสองระบบ เช่นสายที่ใช้รับส่งข้อมูลจะเป็นแบบไหน, ข้อต่อที่ใช้ในการรับส่งข้อมูลมีมาตรฐานอย่างไร,ความเร็วในการรับส่งข้อมูลเท่าใด สัญญาณที่ใช้ในการรับส่งข้อมูลมีรูปร่างอย่างไร,ใช้แรงดันไฟฟ้าเท่าไหร่ ข้อมูลใน Layer ที่ 1 นี้จะมองเห็นเป็นการรับส่งข้อมูลทีละบิตเรียงต่อกันไป



รูปที่ 2.1 อธิบายการส่งข้อมูลในชั้น Physical layer

จากรูปแสดงถึงการส่งข้อมูลบน Physical layer แสดงให้เห็นว่า ข้อมูลจะมาเป็นอย่างไรก็ตาม ก็จะถูกแปลงเป็นสัญญาณเพื่อส่งไปยังปลายทาง แล้วฝั่งปลายทางก็จะนำสัญญาณที่รับมาแปลงกลับเป็นข้อมูลเพื่อส่งให้เครื่อง Client ต่อไปเพราะ ฉะนั้น อุปกรณ์ต่างๆที่มีความสามารถในการนำพาสัญญาณไป ก็พวก Card LAN (NIC) , สาย UTP , สาย Fiber หรือพวกเต้าเสียบ หัวต่อต่างๆ RJ45 , RJ11 , RS323 จัดอยู่ใน Physical Layer

2.2.2 Layer 2 (Data-Link Layer)

เป็นชั้นที่ทำหน้ากำหนดรูปแบบของการส่งข้อมูลข้าม Physical Network โดยใช้ Physical Address อ้างอิงที่อยู่ต้นทางและปลายทาง ซึ่งก็คือ MAC Address นั่นเอง รวมถึงทำการตรวจสอบและจัดการกับ error ในการรับส่งข้อมูล ข้อมูลที่ถูกส่งบน Layer 2 เราจะเรียกว่า Frame ซึ่งบน Layer 2 ก็จะแบ่งเป็น LAN และ WAN ครับ

ซึ่ง ปัจจุบัน บน Layer 2 LAN เรานิยมใช้เทคโนโลยีแบบ Ethernet มากที่สุด ส่วน WAN ก็จะมีหลายแบบแตกต่างกันไป เช่น Lease Line (HDLC , PPP) , MPLS , 3G และอื่นๆ

8 Bytes	6 Bytes	6 Bytes	2 Bytes	46-1500 Bytes	4 Bytes
Preamble	Destination Address	Source Address	Type	Data	FCS

รูปที่ 2.2 อธิบายส่วนประกอบของ Ethernet Frame

สำหรับ LAN ยังมีการแบ่งย่อยออกเป็น 2 sublayers คือ

Logical Link Control (LLC)

IEEE 802.2 ซึ่งจะให้บริการกับ Layer ด้านบนในการเข้าใช้สัญญาณใน การรับ-ส่งข้อมูล ตามมาตรฐาน IEEE802 แล้ว จะอนุญาตให้สถาปัตยกรรมของ LAN ที่ต่างกันสามารถทำงานร่วมกันได้ หมายความว่า Layer ด้านบนไม่จำเป็นต้องทราบว่า Physical Layer ใช้สายสัญญาณประเภทใดในการรับ-ส่งข้อมูล เพราะ LLC จะรับผิดชอบในการปรับ Frame ข้อมูลให้สามารถส่งไปได้ในสายสัญญาณประเภทนั้นได้ และไม่จำเป็นต้องสนใจว่าข้อมูลจะส่งผ่านเครือข่ายแบบไหน เช่น Ethernet , Token Ring บลาๆๆ และไม่จำเป็นต้องรู้ว่าการส่งผ่านข้อมูลใน Physical Layer จะใช้การรับส่งข้อมูล แบบใด LLC จะเป็นผู้จัดการเรื่องเหล่านี้ได้ทั้งหมดครับ Media Access Control (MAC) IEEE 802.3 ใช้ควบคุมการติดต่อสื่อสารกับ Layer 1 และรับผิดชอบในการรับ-ส่งข้อมูลให้สำเร็จและถูกต้อง โดยมีการระบุ MAC Address ของอุปกรณ์เครือข่าย ซึ่งใช้อ้างอิงในการส่งข้อมูลจากต้นทางไปยังปลายทาง เช่น

จาก ต้นทางส่งมาจาก MAC Address หมายเลข AAAA:AAAA:AAAA ส่งไปหาปลายทาง หมายเลข BBBB:BBBB:BBBB เมื่อปลายทางได้รับข้อมูลก็จะรู้ว่าใครส่งมา เพื่อจะได้ตอบกลับไปถูกต้อง

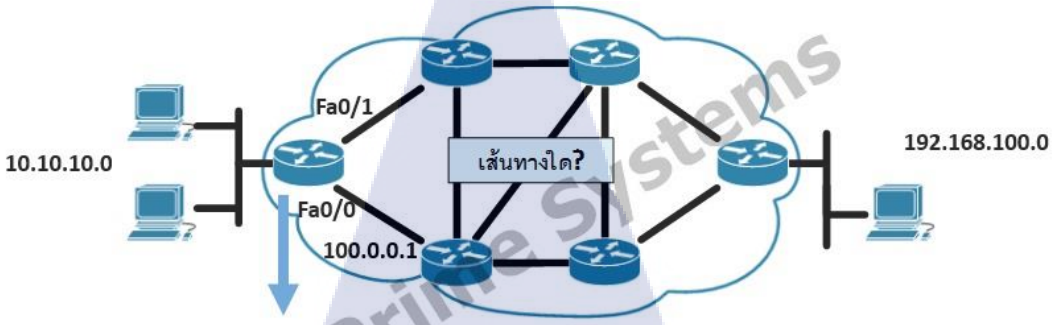
Layer2 บน Ethernet (IEEE802.3) เมื่อมันมีหน้าที่ในการรับผิดชอบการรับ-ส่งข้อมูลให้สำเร็จและถูกต้อง มันจึงมีการตรวจสอบข้อผิดพลาดในการส่งข้อมูลด้วย ที่เราเรียกว่า Frame Check Sequence (FCS) และยังตรวจสอบกับ Physical ด้วยว่าช่องสัญญาณพร้อมสำหรับส่งข้อมูลไหม ถ้าว่างก็ส่งได้

ถ้าไม่ว่างก็ต้องรอ CSMA/CD คือกลไลการตรวจสอบการชนกันของข้อมูล บน Ethernet ถ้าเกิดมีการชนกันเกิดขึ้น มันก็จะส่งสัญญาณ (jam signal) ออกไปเพื่อให้ทุกคนหยุดส่งข้อมูล แล้วสุ่มรอเวลา (back off) เพื่อส่งใหม่อีกครั้ง

2.2.3 Layer 3 (Network Layer)

ทำหน้าที่ส่งข้อมูลข้ามเครือข่าย หรือ ข้าม network โดยส่งข้อมูลผ่าน Internet Protocol (IP) โดยมีการสร้างที่อยู่ขึ้นมา (Logical Address) เพื่อใช้อ้างอิงเวลาส่งข้อมูล เราเรียกว่า IP address ข้อมูลที่ถูกส่งมาจากต้นทาง เพื่อไปยังปลายทาง ที่ไม่ได้อยู่บนเครือข่ายเดียวกัน จำเป็นจะต้องพึ่งพาอุปกรณ์ที่ทำงานบน Layer 3 นั่นก็คือ Router หรือ Switch Layer 3 โดยใช้ Routing Protocol

(OSPF , RIP,BGP) เพื่อหาเส้นทางและส่งข้อมูลนั้น (IP) ข้ามเครือข่ายไป



Network Protocol	Destination	Exit Interface	Next Hop
Connected	10.10.10.0	Fa0/1	
Learned	192.168.100.0	Fa0/0	100.0.0.1

รูปที่ 2.3 อธิบายการทำงานของ Network Layer

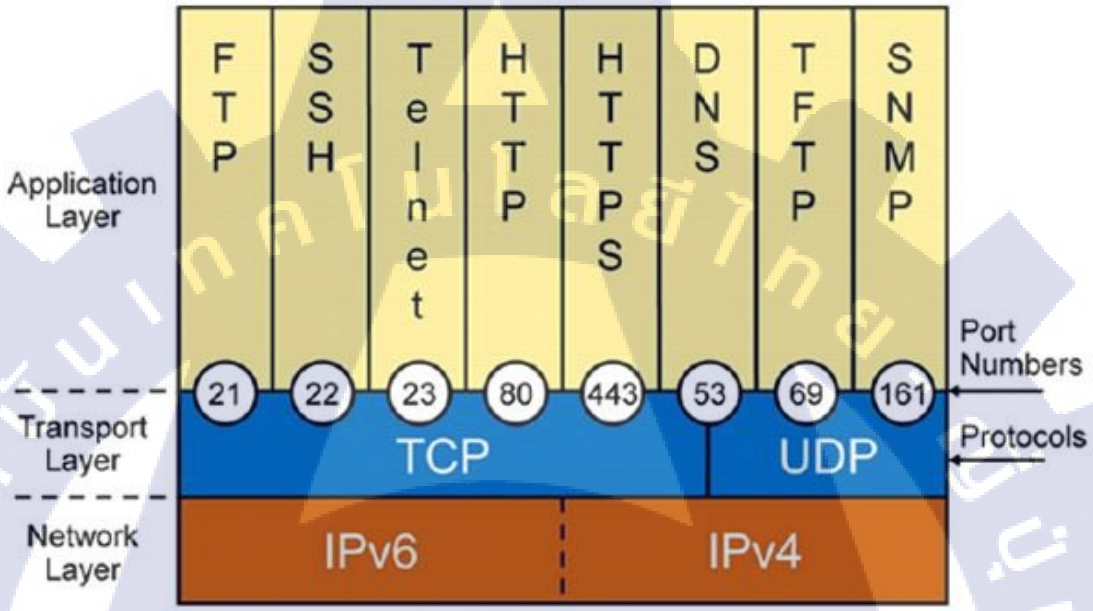
โดยการทำงานของ Internet Protocol (IP) เป็นการทำงานแบบ Connection-less หมายความว่า IP ไม่มีการตรวจสอบข้อมูลว่าส่งไปถึงปลายทางไหม แต่มันจะพยายามส่งข้อมูลออกไปด้วยความพยายามที่ดีที่สุด (Best-Effort) เพราะฉะนั้น ข้อมูลที่ส่งออกไปแล้วไม่ถึงปลายทาง ต้นทางก็จะไม่รู้เลย ถ้าส่งไปแล้วข้อมูลไม่ถึงปลายทาง ฝั่งต้นทางจะต้องทำการส่งไปใหม่บน Layer 3

จึงมี Protocol อีกตัวหนึ่งเพื่อใช้ตรวจสอบว่าปลายทางยังมีชีวิตอยู่ไหม ก่อนที่จะส่งข้อมูล นั่นคือ ICMP ครับ แต่ผู้ใช้งานจะต้องเป็นคนเรียกใช้ protocol ตัวนี้เองนะครับ

จริงๆ แล้ว ก็ยังมีรายละเอียดของ ICMP , ARP อีกที่ทำงานบน Layer 3

2.2.4 Layer 4 (Transport Layer)

ทำหน้าที่เชื่อมต่อกับ Upper Layer ในการใช้งาน network services ต่างๆ หรือ Application ต่าง จากต้นทางไปยังปลายทาง (end-to-end connection) ในแต่ละ services ได้ โดยใช้ port number ในการส่งข้อมูลของ Layer 4 จะใช้งานผ่าน protocol 2 ตัว คือ TCP และ UDP



รูปที่ 2.4 อธิบายการทำงานของ Transport Layer

Transmission Control Protocol (TCP) มีคุณลักษณะที่สำคัญ ดังนี้

จัดแบ่งข้อมูลจากระดับ Application ให้มีขนาดพอเหมาะที่จะส่งไปบนเครือข่าย (Segment)

มีการสร้าง Connection กันก่อนที่จะมีการรับส่งข้อมูลกัน (Connection-oriented)

มีการใช้ Sequence Number เพื่อจัดลำดับการส่งข้อมูล

มีการตรวจสอบว่าข้อมูลที่ส่งไปถึงปลายทางหรือไม่ (Recovery)

บน TCP ก่อนจะส่งข้อมูลนั้นจะต้องทำการตรวจสอบก่อนว่า ปลายทางสามารถติดต่อได้ โดยจะทำการสร้างการเชื่อมต่อระหว่างผู้ส่งและผู้รับก่อน โดยใช้กลไล Three-Way Handshake เพื่อให้แน่ใจว่าข้อมูลที่ส่งจะสามารถส่งถึงผู้รับแน่นอน นอกจาก Three-Way Handshake แล้ว TCP ยังมีกลไก Flow Control เพื่อควบคุมการส่งข้อมูลเมื่อเกิดปัญหาบนเครือข่ายระหว่างที่ส่งข้อมูลอยู่ หรือ กลไล Error Recovery ในกรณีที่มีข้อมูลบางส่วน

หายไปขณะส่ง ก็ให้ทำการส่งมาใหม่ (Retransmission) นอก จากนั้นยังสามารถทำการจัดสรรค์หรือแบ่งส่วนของข้อมูลออกเป็นส่วนๆ (Segmentation) ก่อนที่จะส่งลงไปที่ Layer 3 อีกด้วยและข้อมูลที่ถูกแบ่งออก ก็จะใส่ลำดับหมายเลขเข้าไป(Sequence number) เพื่อให้ปลายทางนำข้อมูลไปประกอบกันได้อย่างถูกต้อง

User Datagram Protocol (UDP) มีคุณลักษณะที่สำคัญ ดังนี้

ไม่มีการสร้าง Connection กันก่อนที่จะมีการรับส่งข้อมูลกัน (Connectionless)

ส่งข้อมูลด้วยความพยายามที่ดีที่สุด (Best-Effort)

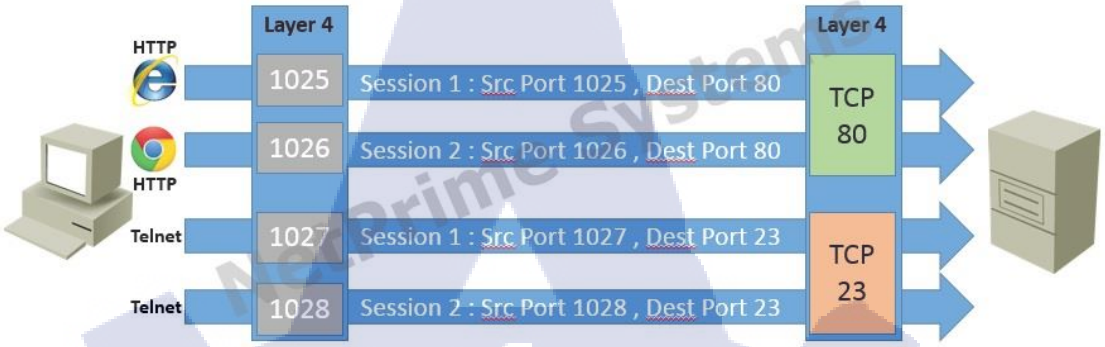
ไม่มีการตรวจสอบว่าข้อมูลที่ส่งไปถึงปลายทางหรือไม่ (No Recovery)

บน UDP จะตรงข้ามกับ TCP เลยครับ เพราะ ไม่มีการสร้างการเชื่อมต่อกันก่อน หมายความว่าถ้า services ใดๆ ใช้งานผ่าน UDP ก็จะถูกส่งออกไปทันทีด้วยความพยายามที่ดีที่สุด (Best-Effort) และไม่มีการส่งใหม่เมื่อข้อมูลสูญหาย (No Recovery) หรือส่งไม่ถึงปลายทางอีกด้วย

ข้อดีของมันก็คือ มีความรวดเร็วในการส่งข้อมูล เพราะฉะนั้น services ที่ใช้งานผ่าน UDP ก็มีมากมาย เช่น TFTP , DHCP , VoIP และอื่นๆ เป็นต้น

2.2.5 Layer 5 (Session Layer)

ทำหน้าที่ควบคุมการเชื่อมต่อ session เพื่อติดต่อจากต้นทาง กับ ปลายทาง



รูปที่ 2.5 อธิบายการทำงานของ Session Layer

เมื่อฝั่งต้นทางต้องการติดต่อไปยังปลายทางด้วย port 80 (เปิด Internet Explorer) ฝั่งต้นทางก็จะทำการติดต่อไปยังปลายทาง โดยการสร้าง session ขึ้นมา เป็น session ที่ 1 ส่งผ่าน Layer 4 โดย random port ต้นทางขึ้นมาเป็น 1025 ส่งไปหาปลายทางด้วย port 80 ระหว่าง ที่ session ที่ 1 ใช้งานอยู่เราติดต่อไปยังปลายทางอีกครั้งด้วย port 80 (เปิด Google Chrome) ฝั่งต้นทางก็จะทำการสร้าง session ที่ 2 ขึ้นมา ส่งผ่าน Layer 4 โดย random port ต้นทางขึ้นมาเป็น 1026 ส่งไปหาปลายทางด้วย port 80 แล้วแต่ละ session ฝั่งปลายทาง ก็จะตอบกลับมาด้วย port ที่ฝั่งต้นทางส่งมา ทำให้สามารถแยก session ออกได้ เมื่อเราส่งข้อมูลบนเครือข่าย

2.2.6 Layer 6 (Presentation Layer)

ทำหน้าที่ในการแปล หรือ นำเสนอ structure , format , coding ต่างๆของข้อมูลบน application ที่จะส่งจากต้นทางไปยังปลายทาง ให้อยู่ในรูปแบบที่ฝั่งต้นทางและปลายทางสามารถเข้าใจได้ทั้ง 2 ฝั่ง

2.2.7 Layer 7 (Application Layer)

ทำหน้าที่ติดต่อระหว่างผู้ใช้ (User) กับ Application ที่ใช้งานบนเครือข่าย เช่น HTTP,HTTPS , FTP , Telnet เป็นต้น สรุปแล้วคือ Application ที่ใช้งานผ่านระบบ Network

2.3 Local Area Network (IEEE 802.3)

มาตรฐานของ LAN ถูกกำหนดโดยคณะกรรมการจาก IEEE ซึ่งมีชื่ออย่างเป็นทางการว่า IEEE 802 Local and Metropolitan Area Network Standard Committee โดยจะเน้นการกำหนดคุณสมบัติในระดับของ Physical Layer และ Data Link Layer ใน OSI Reference Model มาตรฐานจำนวนมากถูกกำหนดออกมาจากกรรมการกลุ่มนี้ และได้นำมาใช้กำหนดรูปแบบโครงสร้างของระบบเครือข่ายในปัจจุบัน มาตรฐานดังนี้

IEEE 802.3: Ethernet นับเป็นต้นกำเนิดของเทคโนโลยี LAN เนื่องจาก LAN ส่วนมากหรือเกือบทั้งหมดในปัจจุบันใช้ พื้นฐานของเทคโนโลยีนี้ คุณลักษณะเฉพาะในการทำงานของ Ethernet คือการทำงานแบบที่เรียกว่า การเข้าใช้ระบบเครือข่ายโดยวิธีช่วงชิง หรือ CSMA/CD (Carrier Sense Multiple Access with Collision Detection) โดยมีหลักการทำงานดังนี้

ก่อนที่สถานีงานของผู้ใช้จะส่งข้อมูลออกไปยังเครือข่าย จะต้องมีการแจ้งออกไปก่อนเพื่อตรวจสอบดูว่ามีสัญญาณพาหะของผู้ใช้รายอื่นอยู่ในสายหรือไม่

เมื่อไม่พบสัญญาณของผู้ใช้อื่น จึงจะเริ่มส่งข้อมูลออกไปได้หากตรวจพบสัญญาณพาหะของผู้ใช้รายอื่นอยู่ จะต้องรอจนกว่าสายจะว่างถึงจะส่งข้อมูลได้ ในกรณีที่เกิดปัญหาในการตรวจสอบสัญญาณพาหะ ซึ่งอาจเนื่องมาจากระยะทางของสถานีงานอยู่ห่างกันมาก อาจจะเกิดการชนกันของข้อมูลขึ้นได้ ในกรณีนี้ให้ทั้งทุกๆ สถานีหยุดการส่งข้อมูลขณะนั้น แต่ละสถานีจะทำการสุ่มช่วงระยะเวลาในการรอ เพื่อทำการส่งข้อมูลออกไปใหม่เพื่อ ไม่ให้มีการชนกันเกิดขึ้นอีก หากยังมีเหตุการณ์ชนกันเกิดขึ้นอีก ก็จะต้องหยุดรอโดยเพิ่มช่วงระยะเวลาในการสุ่มเป็นสองเท่าเพื่อให้ลดโอกาสการชนกันลงและส่งข้อมูลออกไปใหม่ และทำซ้ำเช่นนี้ จนกว่าข้อมูลจะถูกส่งออกไปได้อย่างสมบูรณ์ แม้ว่าระบบ CSMA/CD ดูเหมือนจะเป็นวิธีจัดระเบียบการส่งสัญญาณในระบบเครือข่ายที่ไม่เรียบร้อยนัก แต่ก็ทำงานได้ผลเป็นอย่างดี แต่เมื่อมีจำนวนโหนดบนเครือข่ายมากขึ้น ก็จะทำให้ความน่าจะเป็นในการปะทะกันของ ข้อมูลเพิ่มมากขึ้นด้วย ซึ่งจะส่งผลให้เครือข่ายทำงานช้าลงอย่างหลีกเลี่ยงไม่ได้ ระบบเครือข่าย Ethernet ยังสามารถแบ่งประเภทได้อีก ตามความเร็วและชนิดของสายเคเบิล

ดังนี้

- IEEE 802.3 10Base5 (Thick Ethernet)

  เป็นระบบเครือข่ายแบบบัส ใช้สายโคแอ็กเชียลอย่างหนา (3/8 นิ้ว) สามารถส่งข้อมูลได้ที่อัตราเร็ว 10 เมกะบิตต่อวินาที ในระยะทางสูงสุดไม่เกิน 500 เมตร และเนื่องจากสายโคแอ็กเชียลอย่างหนาสามารถนำสัญญาณไปได้ไกลกว่าจึงมักถูกใช้เป็นแบคโบน (Backbone) ของระบบเครือข่าย

- IEEE 802.3 10Base2 (Thin Ethernet)

  เป็นระบบเครือข่ายแบบบัส ใช้สายโคแอ็กเชียลอย่างบาง (3/16 นิ้ว) สามารถติดตั้งได้ง่ายกว่าแบบแรกและราคาต่ำกว่า สามารถส่งข้อมูลได้ที่อัตราเร็ว 10 เมกะบิตต่อวินาที ระยะทางสูงสุดไม่เกิน 200 เมตร

- IEEE 802.3 10BaseT (Twisted-pair Ethernet)

  เป็นระบบที่จัดการเชื่อมต่อโหนดต่างๆ เข้ากับ Hub เป็นรูปแบบดาว ใช้สายคู่พันเกลียวโดยอาจเป็นแบบไม่มีสิ่งห่อหุ้ม(Unshielded Twisted-pair) หรือแบบมีสิ่งห่อหุ้ม (Shielded Twisted-pair)ก็ได้ มีหัวเชื่อมต่อเป็นแบบ RJ-45 มีลักษณะคล้ายปลั๊กโทรศัพท์ สามารถส่งข้อมูลได้ที่อัตราเร็ว 10 เมกะบิตต่อวินาที โดยมีความยาวของสายระหว่างสถานีงานกับ Hub ไม่เกิน 100 เมตร

- IEEE 802.3u 100BaseX (Fast Ethernet)

  มีระบบการเชื่อมต่อแบบดาว สามารถรับส่งข้อมูลได้ที่อัตราเร็ว 100 เมกะบิตต่อวินาที

- IEEE 802.3ab (1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s)

  มีระบบการเชื่อมต่อแบบดาว สามารถรับส่งข้อมูลได้ที่อัตราเร็ว 1,000 เมกะบิตต่อวินาที

- IEEE 802.3an (10GBASE-T 10 Gbit/s Ethernet over unshielded twisted pair)

มีระบบการเชื่อมต่อแบบดาว สามารถรับส่งข้อมูลได้ที่อัตราเร็ว 10,000 เมกะบิตต่อวินาที

2.3.2 Power over Ethernet (IEEE 802.3af/at)

เทคโนโลยี Power over Ethernet (PoE) นั้น การติดตั้งอุปกรณ์ IT หรืออุปกรณ์เครือข่ายใดๆ ต่างก็ต้องมีการเผื่อการเชื่อมต่อกับปลั๊กไฟเอาไว้เสมอ ทำให้ในการใช้งานหลายๆ กรณีนั้นจะต้องมีการเผื่อไว้ทั้งสาย LAN และสายไฟพร้อมๆ กัน ส่งผลต่อเนื่องให้การติดตั้งมีค่าใช้จ่ายเพิ่มขึ้นเพราะอาจต้องเดินระบบไฟฟ้าเพิ่มสำหรับแต่ละอุปกรณ์ รวมถึงความรกของสาย LAN และสายไฟพี่มีจำนวนมากภายในอาคารหรือบนโต๊ะทำงาน

แนวคิดของ PoE จึงถือกำเนิดขึ้นมาเพื่อรวมการรับส่งข้อมูลและการจ่ายพลังงานไฟฟ้าเอาไว้ภายในสาย LAN เส้นเดียวกันเลย ทำให้การออกแบบและติดตั้งใช้งานอุปกรณ์ต่างๆ นั้นสามารถลดค่าใช้จ่ายในการเดินระบบไฟลงไปได้ และช่วยให้ปริมาณสายต่างๆ ภายในองค์กรลดลงไปด้วย มาตรฐานของการจ่ายไฟผ่านสาย LAN นี้จะเป็นที่รู้จักสากลกันภายใต้มาตรฐาน 802.3af (PoE) ที่มีกำลังจ่ายไฟประมาณ 15.4 Watt และมาตรฐาน 802.3at (High Power PoE+) ที่มีกำลังจ่ายไฟประมาณ 30 Watt และรองรับการทำงานแบบ Backward Compatible กับ 802.3af ได้ ทั้งนี้ในการคำนวณใดๆ นั้นก็ต้องประเมินเผื่อความสูญเสียของกำลังไฟฟ้าที่เกิดขึ้นจากการส่งผ่านสาย LAN เอาไว้ด้วยประมาณ 10% ก่อนที่จะไปถึงอุปกรณ์ตัวรับพลังงานที่จะนำมาเชื่อมต่อ

Comparison of PoE parameters

Property	802.3af (802.3at Type 1) "PoE"	802.3at Type 2 "PoE+"	802.3bt Type 3 "4PPoE"[25]	802.3bt Type 4
Power available at PD[note 1]	12.95 W	25.50 W	51 W	71 W
Maximum power delivered by PSE	15.40 W	30.0 W	60 W	100 W
Voltage range (at PSE)	44.0–57.0 V[26]	50.0–57.0 V[26]	50.0–57.0 V	52.0–57.0 V
Voltage range (at PD)	37.0–57.0 V[27]	42.5–57.0 V[27]	42.5–57.0 V[28]	41.1–57.0 V
Maximum current I_{max}	350 mA[29]	600 mA[29]	600 mA per pair[28]	960 mA per pair[28]
Maximum cable resistance per pairset	20 Ω[30] (Category 3)	12.5 Ω[30] (Category 5)	12.5 Ω[28]	12.5 Ω[28]
Power management	Three power class levels negotiated by signature	Four power class levels negotiated by signature or 0.1 W steps negotiated by LLDP	Three power class levels negotiated by signature or 0.1 W steps negotiated by LLDP[31]	0.1 W steps negotiated by LLDP
Derating of maximum cable ambient operating temperature	None	5 °C (9 °F) with one mode (two pairs) active	10 °C (20 °F) with more than half of bundled cables pairs at I_{max}[32]	10 °C (20 °F) with temperature planning required
Supported cabling	Category 3 and Category 5[24]	Category 5[24][note 2]	Category 5	Category 5
Supported modes	Mode A (endspan), Mode B (midspan)	Mode A, Mode B	Mode A, Mode B, 4-pair mode	4-pair mode

Notes:

1. ^ Most switched power supplies within the powered device will lose another 10 to 25% of the available power.
2. ^ More stringent cable specification allows assumption of more current carrying capacity and lower resistance (20.0 Ω for Category 3 versus 12.5 Ω for Category 5).

ตารางที่ 2.2 เปรียบเทียบ Power over Ethernet

รูปที่ 2.6 อธิบายการทำงานของ PoE

สำหรับอุปกรณ์ที่สามารถจ่ายไฟบนสาย LAN ด้วย PoE หรือ High Power PoE+ ได้นั้น ปัจจุบันมีด้วยกัน 2 ประเภท ได้แก่ อุปกรณ์ Switch ที่รองรับการทำงานแบบ PoE และ High Power PoE+ โดยสามารถจ่ายไฟให้กับอุปกรณ์ต่างๆ ได้ผ่านสาย LAN ทีละหลายๆ เส้น และอุปกรณ์ PoE และ High Power PoE+ Injector ที่ส่วนใหญ่จะมีหน้าที่ในการจ่ายไฟให้กับสาย LAN ทีละ 1 เส้นเท่านั้น

2.4 Wireless Local Area Network (IEEE802.11)

IEEE802.11 คือมาตรฐานการทำงานของระบบเครือข่ายไร้สายกำหนดขึ้นโดย สถาบันวิชาชีพวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (Institute of Electrical and Electronics Engineers: IEEE) เป็นมาตรฐานกลาง ที่ได้นำมาปฏิบัติใช้ เพื่อที่จะทำการเชื่อมโยงอุปกรณ์เครือข่ายไร้สายเข้าด้วยกันบนระบบ ในทางปกติแล้ว การเชื่อมต่อระบบเครือข่ายไร้สายจำเป็นต้องใช้อุปกรณ์สองชิ้น นั่นคือ

- แอคเซสพอยต์ คือตัวกลางที่ช่วยในการติดต่อระหว่าง ตัวรับ-ส่งสัญญาญไวเลส ของผู้ใช้ กับ เราต์เตอร์ผ่านทางสายนำสัญญาณที่ทำจากทองแดงที่ได้รับการเชื่อมต่อกับระบบเครือข่าย เช่น สายแลนหรือสายโทรศัพท์ ADSL หรือผ่านทางสายใยแก้วนำแสง
- ตัวรับ-ส่งสัญญาณไวเลส ทำหน้าที่รับ-ส่ง สัญญาณ ระหว่างตัวรับส่งแต่ละตัวด้วยกัน หรือระหว่างตัวลูกข่ายกับแอคเซสพอยต์

2.4.1 มาตรฐานที่อยู่ภายใต้ กรอบของเทคโนโลยี IEEE 802.11

ปัจจุบันนี้มีมาตรฐานออกมาหลายอย่าง แต่ที่ได้รับความนิยมทั้งในอดีตและปัจจุบันนั้น แบ่งออกเป็น 7 มาตรฐานด้วยกัน ได้แก่

- IEEE 802.11a - เสร็จสมบูรณ์เมื่อปี ค.ศ. 1999 โดยออกเผยแพร่ช้ากว่าของมาตรฐาน IEEE 802.11b ใช้เทคโนโลยีที่เรียกว่า OFDM (Orthogonal Frequency Division Multiplexing) เพื่อปรับปรุงความเร็วในการส่งข้อมูลให้วิ่งได้สูงถึง 54 Mbps บนความถี่ 5Ghz ซึ่งจะมีคลื่นรบกวนน้อยกว่าความถี่ 2.4 Ghz ที่มาตรฐานอื่นใช้กัน ที่ความเร็วนี้สามารถทำการแพร่ภาพและข่าวสารที่ต้องการความละเอียดสูงได้ อัตราความเร็วในการรับส่งข้อมูลสามารถปรับระดับให้ช้าลงได้ เพื่อเพิ่มระยะทางการเชื่อมต่อให้มากขึ้น แต่ทว่าข้อเสียก็คือ ความถี่ 5 Ghz นั้น หลายๆ ประเทศไม่อนุญาตให้ใช้ เช่นประเทศไทยเพราะได้จัดสรรให้อุปกรณ์ประเภทอื่นไปแล้ว และเนื่องด้วยการที่มาตรฐานนี้ ใช้การเชื่อมต่อที่ความถี่สูงๆ ทำให้มาตรฐานนี้ มีระยะการรับส่งที่ค่อนข้างใกล้ คือ ประมาณ 35 เมตร ในโครงสร้าง

ปิด(เช่น ในตึก ในอาคาร) และ 120 เมตรในที่โล่งแจ้งและด้วยความที่ส่งข้อมูลด้วยความถี่สูงนี้ ทำให้การส่งข้อมูลนั้นไม่สามารถทะลุทะลวงโครงสร้างของตึกได้มากนัก อุปกรณ์ไร้สายที่รองรับเทคโนโลยี IEEE 802.11a นี้ไม่สามารถเข้ากันได้กับอุปกรณ์ที่รองรับมาตรฐาน IEEE 802.11b และ IEEE 802.11g ที่จะอธิบายด้านล่างนี้ได้ อีกทั้งอุปกรณ์ของ IEEE 802.11a ยังมีราคาสูงกว่า IEEE 802.11b ด้วย ดังนั้นอุปกรณ์ IEEE 802.11a จึงได้รับความนิยมน้อยกว่า IEEE 802.11b มาก จึงทำให้ไม่ค่อยเป็นที่ได้รับความนิยมเท่าที่ควร

- IEEE 802.11b - เสร็จสมบูรณ์เมื่อปี ค.ศ. 1999 ใช้เทคโนโลยีที่เรียกว่า CCK (Complimentary Code Keying) ผนวกกับ DSSS (Direct Sequence Spread Spectrum) เพื่อปรับปรุงความสามารถของอุปกรณ์ให้รับส่งข้อมูลได้ด้วยความเร็วสูงสุดที่ 11 Mbps ผ่านคลื่นวิทยุความถี่ 2.4 GHz เนื่องจากการใช้คลื่นความถี่ที่ต่ำกว่าอุปกรณ์ที่รองรับมาตรฐาน IEEE 802.11a ทำให้อุปกรณ์ที่ใช้มาตรฐานนี้จะมีความสามารถในการส่งคลื่นสัญญาณไปได้ไกลกว่าคือประมาณ 38 เมตรในโครงสร้างปิดและ 140 เมตรในที่โล่งแจ้ง รวมถึง สัญญาณสามารถทะลุทะลวงโครงสร้างตึกได้มากกว่าอุปกรณ์ที่รองรับกั
- IEEE 802.11a ด้วย ปัจจุบันผลิตภัณฑ์อุปกรณ์เครือข่ายไร้สายภายใต้มาตรฐานนี้ได้รับการผลิตออกมาเป็นจำนวนมาก โดยอุปกรณ์ที่ใช้ความถี่ย่านนี้ก็เช่น IEEE 802.11, Bluetooth, โทรศัพท์ไร้สาย, และเตาไมโครเวฟ และที่สำคัญแต่ละผลิตภัณฑ์มีความสามารถทำงานร่วมกันได้ อุปกรณ์ของผู้ผลิตทุกยี่ห้อต้องผ่านการตรวจสอบจากสถาบัน Wi-Fi Alliance เพื่อตรวจสอบมาตรฐานของอุปกรณ์และความเข้ากันได้ของแต่ละผู้ผลิต ปัจจุบันนี้นิยมนำอุปกรณ์ WLAN ที่มาตรฐาน 802.11b ไปใช้ในองค์กรธุรกิจ สถาบันการศึกษา สถานที่สาธารณะ และกำลังแพร่เข้าสู่สถานที่พักอาศัยมากขึ้น มาตรฐานนี้มีระบบเข้ารหัสข้อมูลแบบ WEP ที่ 128 บิต
- IEEE 802.11g - เสร็จสมบูรณ์ในปี ค.ศ. 2003 ทางคณะทำงาน IEEE 802.11g ได้นำเอาเทคโนโลยี OFDM ของ 802.11a มาพัฒนาบนความถี่ 2.4 Ghz จึงทำให้ใช้ความเร็ว 36-54 Mbps ซึ่งเป็นความเร็วที่สูงกว่ามาตรฐาน 802.11b ซึ่ง 802.11g สามารถปรับระดับ

ความเร็วในการสื่อสารลงเหลือ 2 Mbps ได้ตามสภาพแวดล้อมของเครือข่ายที่ใช้งาน มาตรฐานนี้เป็นที่ยอมรับจากผู้ใช้เป็นจำนวนมากและกำลังจะเข้ามาแทนที่ 802.11b ในอนาคตอันใกล้ นอกจากที่กล่าวมาข้างต้นนี้มีบางผลิตภัณฑ์ใช้เทคโนโลยีเฉพาะตัวเข้ามาเสริม ทำให้ความเร็วเพิ่มขึ้นจาก 54 Mbps เป็น 108 Mbps แต่ต้องทำงานร่วมกันเฉพาะอุปกรณ์ที่ผลิตจากบริษัทเดียวกันเท่านั้น ซึ่งความสามารถนี้เกิดจากชิป (Chip) กระจายสัญญาณของตัวอุปกรณ์ที่ผู้ผลิตบางรายสามารถเพิ่มประสิทธิภาพการรับส่งสัญญาณเป็น 2 เท่าของการรับส่งสัญญาณได้แต่ปัญหาของการกระจายสัญญาณนี้จะมีผลทำให้อุปกรณ์ไร้สายในมาตรฐาน 802.11b มีประสิทธิภาพลดลงด้วยเช่นกัน

- IEEE 802.11n - เสร็จสมบูรณ์ในปี ค.ศ. 2009 ทำงานบนย่านความถี่ 2.4 และ 5 GHz โดยที่สามารถให้อัตราการส่งถ่ายข้อมูลสูงสุดถึง 300 Mbps มีความสามารถในการส่งคลื่นสัญญาณ ได้ระยะประมาณ 70 เมตรในโครงสร้างปิด และ 250 เมตรในที่โล่งแจ้ง เพิ่มความสามารถในการกันสัญญาณกวนจากอุปกรณ์อื่นๆ ที่ใช้ความถี่ 2.4GHz เหมือนกัน และสามารถรองรับอุปกรณ์มาตรฐาน IEEE 802.11b และ IEEE 802.11g ได้ 802.11-2012 - ในปี 2007 กลุ่มงาน TGmb ได้รับการอนุมัติให้รวบรวมการแก้ไขทั้งหมดให้เป็นเวอร์ชันที่เรียกว่า REVmb หรือ 802.11mb ที่ประกอบด้วย 802.11k, r, y, n, w, p, z, v, u, s ตีพิมพ์วันที่ 29 มีนาคม 2012
- 802.11ac - เป็นมาตรฐานที่ 5 GHz ให้ทรูพุทกับแลนไร้สายแบบหลายสถานีสูงกว่าที่อย่างน้อย 1 Gbps และสำหรับลิงก์เดี่ยวที่อย่างน้อย 500 Mbps โดยการใช้ RF แบนด์วิธที่กว้างกว่า(80 หรือ 160 MHz) สตรีมมากกว่า (สูงถึง 8 สตรีม) และมอดูเลทที่ความจุสูงกว่า(สูงถึง 256 QAM)
- 802.11ad - หรือ "WiGig" เกิดจากการผลักดันจากผู้ผลิตฮาร์ดแวร์ ในวันที่ 24 กรกฎาคม 2012 Marvell และ Wilocity ได้ประกาศการเป็นคู่ค้าใหม่เพื่อนำ Wi-Fi solution แบบ tri-band ใหม่ออกสู่ตลาด โดยการใช้ความถี่ที่ 60 GHz ทรูพุททางทฤษฎีสูงสุดถึง 7 Gbps มาตรฐานนี้จะออกสู่ตลาดได้ราวต้นปี 2014

Wireless Technology Comparison Chart

Wireless Standard	802.11b		802.11a		802.11g		802.11n		802.11ac	
Popularity	+++	Widely adopted, readily available everywhere	+	Limited adoption	++	Medium adoption, replaced b as commonplace	++	Many products, some based on a draft specification, later finalized Oct, 2009	+	Draft, only a few manufactures have chips based on draft specification
Speed (theoretical)	11Mbps	Up to 11Mbps	54Mbps	Up to 54Mbps	54Mbps	Up to 54Mbps	300Mbps	Up to 300Mbps	1Gbps	Up to 1000Mbps, theoretically
Relative Cost	$	Inexpensive	$$$	Expensive	$$	Moderate	$$	Moderate	$$$	Expensive
Frequency	2.4Ghz	Crowded 2.4GHz band, may conflict with other 2.4GHz devices like cordless phones, microwave ovens, etc.	5Ghz	5GHz band only	2.4Ghz	Crowded 2.4GHz band, may conflict with other 2.4GHz devices like cordless phones, microwave ovens, etc	5Ghz and/or 2.4Ghz	Only some devices support 5Ghz or include dual-band radios	5Ghz	5GHz band only
Range	100-150ft	Good Range, typically up to 100-150 feet indoors, depending on construction, building materials, room layout	25-75ft	Limited range, typically no more than 25 to 75 feet indoors	100-150ft	Good Range, typically up to 100-150 feet indoors, depending on construction, building materials, room layout	~230ft	Promises great range, but varies depending on indoor objects and nearby devices using the same frequency	?ft	No real-world test data at this time
Public Access	+++	Public "Hot Spots" growing rapidly, allowing WiFi access in airports, hotels, college campuses, restaurants, etc.	X	None at this time	++	Compatible with current 802.11b "Hot Spots" which may convert to 802.11g Realize ISP may not be providing access anywhere near 54Mbps	+	Very limited, more likely that your n device is associating to b/g AP at 2.4Ghz	X	None at this time
Compatibility	OK 802.11b	Widest adoption	OK 802.11a	Incompatible with 802.11b or 802.11g	OK 802.11b 802.11g	Interoperates with 802.11b networks (at 11Mbps) incompatible with 802.11a unless supported by certain dual-radio APs	OK 802.11b 802.11g 802.11a	Interoperates with b/g/a, small performance hit when mixed-mode is enabled and legacy devices are associated	OK 802.11a 802.11n	Interoperates with a/n APs (only when n is a dual-band 5Ghz radio)

ตารางที่ 2.3เปรียบเทียบเทคโนโลยีไร้สาย

2.5 Software-defined Network

Software-defined Network เป็นสิ่งที่ถูกคิดขึ้นมาเพื่อแก้ไขปัญหานี้ ในคำจำกัดความที่สั้นที่สุด SDN คือสถาปัตยกรรมของเครือข่าย ที่ดึงการจัดการเครือข่ายทั้งหมดมารวมอยู่ที่ซอฟต์แวร์โดยไ ม่สนใจอุปกรณ์และความแตกต่างของผู้ผลิต ในแง่นี้ SDN จะแก้ไขปัญหาตรงที่ผู้ดูแลเครือข่ายสามารถจัดการตั้งค่าอุปกรณ์ในจุดเดียว แล้วสามารถนำไปใช้ได้เลย เมื่อมีอุปกรณ์ใหม่ๆ เพิ่มเข้ามาในระบบ ก็ไม่จำเป็นที่จะต้องแก้ไขที่ตัวเครื่อง นอกจากแก้ไขซอฟต์แวร์เล็กๆ น้อยๆ เท่านั้น

วิธีคิดของ SDN ที่เข้ามาแก้ไขปัญหาของผู้ดูแลเครือข่าย กำลังเป็นแนวทางใหม่ในอุตสาหกรรมคอมพิวเตอร์ และเป็นแนวคิดที่บริษัทขนาดใหญ่หรือผู้ให้บริการโครงข่าย ให้ความสนใจเป็นอย่างมาก เนื่องจากสิ่งที่เป็นผลลัพธ์ของโครงสร้างนี้คือความยืดหยุ่นและเอื้อต่อการขยายตัวของโครงข่ายเมื่อจำเป็นที่จะต้องเพิ่มความสามารถในการรองรับการใช้งานเข้าไป

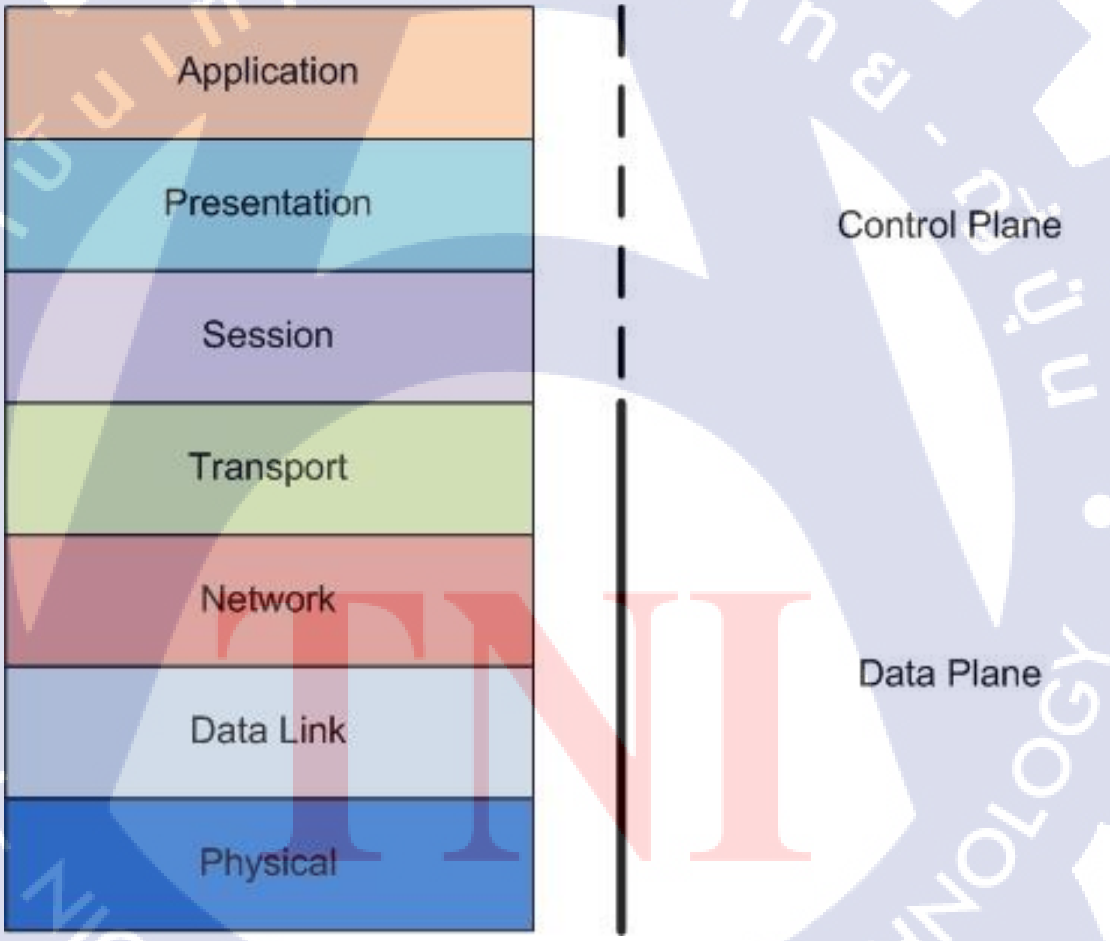
บทความนี้จะเป็นการแนะนำให้รู้จักกับ SDN โดยพื้นฐานในแง่ของความเป็นมาและแนวคิดในเชิงสถาปัตยกรรม ซึ่งจะทำให้เข้าใจถึงลักษณะของ SDN ได้ดียิ่งขึ้น

ประวัติและพัฒนาการของ SDN

SDN เป็นผลพวงจากความพยายามในการพัฒนาแนวคิดด้านเครือข่ายตั้งแต่ในช่วงทศวรรษที่ 1990 ซึ่งในช่วงเวลานั้น แนวคิดเกี่ยวกับ Active Networking เกิดขึ้นมา โดยตอบโจทย์ที่ว่าเครือข่ายจะสามารถทำให้ “กำหนด” หรือ “สามารถโปรแกรม” (programmable) ได้อย่างไร แนวคิดของ Active Networking คือการมองว่าเครือข่ายนั้นสามารถที่จะเหมือนเครื่องคอมพิวเตอร์ตามปกติได้ ซึ่งก็คือการที่ผู้ดูแลระบบ/นักพัฒนา สามารถเขียนโปรแกรมเพื่อเข้าเรียกใช้งานทรัพยากร (resources) ของเครือข่ายให้ได้เต็มที่ วิธีการสำคัญคือการทำให้เครือข่ายมี API (Application Programming Interface) ในฐานะช่องทางการเข้าถึง และการถอดรหัส (demultiplex) หัวแพ็กเก็ตเพื่อส่งไปให้ถูกที่ ซึ่งที่สุดทั้งสองอย่างนี้อยู่ภายใต้แนวคิดที่ว่าโครงสร้างทั้งหมดของอุปกรณ์ต่างๆ จะต้องถูกรวมกัน (unified) จากนั้นจึงเริ่มมีแนวคิดในการแบ่งชั้นของเครือข่าย โดยแบ่งออกเป็น control plane ซึ่งก็คือชั้นที่ควบคุมเส้นทางของข้อมูล และ data plane ซึ่งเป็นชั้นของข้อมูล (จะกล่าวเพิ่มเติมในภายหลัง) โดยอยู่ในช่วงระหว่างปี 2000 ที่เริ่มมีแนวคิดดังกล่าว โดยมองว่า การมองลักษณะเครือข่ายแยกกันดังนี้จะส่งผลดีเพื่อให้มีความคล่องตัวในการบริหารและจัดการมากขึ้น ภายใต้กรอบคิดเช่นนี้ ชั้นทั้งสองที่แยกกันจะมีส่วนที่ประสานงานกันซึ่งเป็นส่วนที่เปิด และรวบรวมการควบคุมระบบเครือข่ายให้มาอยู่ในจุดเดียวกันทั้งหมด ซึ่งกลายมาเป็นแนวทางที่สำคัญสำหรับ SDN ซึ่งก็คือแนวคิดของการมี API เปิดซึ่งประสานงานเข้ากับ control plane และ data plane ในการจัดการ และการจัดการแบบกึ่งรวมศูนย์กึ่งกระจายตัว กล่าวคือ ในแง่หนึ่งเรารวมศูนย์เพื่อจัดการ แต่ในเวลาเดียวกันการรวมศูนย์นี้จะต้องป้องกันไม่ให้เกิดความล้มเหลวแบบจุดเดียว (single point failure) อันจะนำมาซึ่งการล่มของระบบนั่นเอง แนวคิดทั้งสองมีผลทำให้เกิดโครงการที่เรียกว่า OpenFlow ซึ่งเป็น API มาตรฐานในการเรียกใช้งานที่ตอบสนองกับแนวคิดดังกล่าวข้างต้น โดยโครงการ OpenFlow ที่ภายหลังไปอยู่ภายใต้การดูแลของ Open Network Foundation กลายเป็นแกนสำคัญของระบบ SDN นั่นเอง

โครงสร้างของ SDN

SDN นั้นสร้างตัวเองอยู่บนฐานของแนวคิดที่ว่า ส่วนที่ควบคุม (control plane) และส่วนของข้อมูล (data plane) แยกออกจากกันอย่างชัดเจน โดยมีส่วนของการจัดการ (management) เป็นตัวเชื่อมโดยใช้ API ในการเชื่อมต่อทั้งสองส่วนนี้เข้าด้วยกัน Control plane เป็นส่วนที่จะทำหน้าที่ในการตัดสินใจว่า แพ็กเก็ตที่วิ่งอยู่ภายในระบบหรือเข้าถึงระบบแล้ว จะต้องจัดการส่งต่อหรือทำอย่างไรก็ต่อไป ส่วน Data plane คือส่วนที่จะอนุญาต หรือทำหน้าที่ในการส่งข้อมูลไปตามการตัดสินใจของ control plane นั่นเอง เพื่อให้เห็นภาพชัดเจนขึ้น เราลองมาดูภาพด้านล่างที่เป็น OSI Model เทียบกับแนวคิดดังกล่าว



รูปที่ 2.7 อธิบายโครงสร้างของ SDN

แม้การแบ่งเช่นนี้อาจจะไม่ถูกต้องเสมอไป แต่ก็พอให้ภาพคร่าวๆ ถึงแนวคิดดังกล่าวได้ โดยในสภาพปัจจุบัน อุปกรณ์เครือข่ายแทบจะทุกชิ้นจำเป็นที่จะต้องมี control และ data plane อยู่ด้วยกันตลอดเวลา ซึ่งแน่นอนว่าอาจจะต้องอยู่ในสภาพที่ปิดและต่างผู้ผลิตกัน

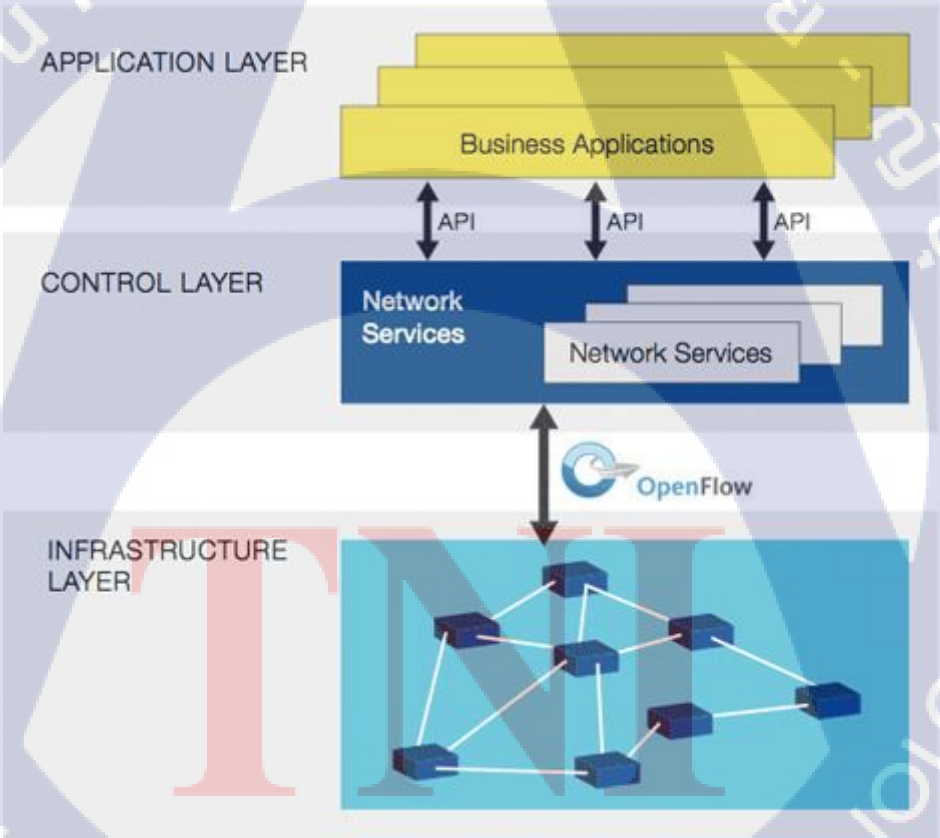
ปัจจุบันอุปกรณ์ต่างๆจะมีมาตรฐานบางอย่างกำหนดให้ทำงานร่วมกัน แต่สิ่งที่เกิดขึ้นก็คืออุปกรณ์แต่ละตัวมีการตัดสินใจจาก control plane ที่แตกต่างกันโดยสิ้นเชิง และในหลายครั้งเราก็มักจะพบว่า โปรโตคอลอย่าง TCP หรือ IP (ถ้าแยกกัน) มักจะไม่ได้รับรองว่าข้อมูลที่ได้จะ ไปถึงปลายทางได้ (TCP ให้ความน่าเชื่อถือ ขณะที่ IP มีหน้าที่ควบคุม แต่กลับไม่มีความน่าเชื่อถือ) และหลายครั้งเมื่ออุปกรณ์หนึ่งตัดสินใจส่งแพ็กเก็ตผิดพลาด ผลที่เกิดขึ้นคือแพ็กเก็ตเหล่านั้นต้องใช้ control plane ของอุปกรณ์อื่นในการหาเส้นทางไปในแต่ละจุด (hop) ซึ่งสิ่งที่ตามมาคือการเสียเวลาโดยไม่จำเป็นที่การเดินทางของข้อมูลซึ่งสมควรจะเดินทางสั้นๆ แต่เมื่อเจอข้อผิดพลาด กลับต้องใช้ระยะทางในการเดินทางนานกว่าที่คิด

เพื่อให้เห็นภาพ สมมติว่าผมได้รับมอบหมายจากแม่ให้เดินทางจากห้างสรรพสินค้าเอ็มโพเรียม นำเอกสารชิ้นหนึ่งไปส่งให้กับเจ้าหน้าที่ของกรมสรรพากรที่ซอยอารีย์สัมพันธ์ ผมทราบแต่เพียงว่าผมจะต้องไปซอยอารีย์สัมพันธ์ แต่ไม่ทราบว่าเส้นทางที่จะไปนั้นมีอะไรบ้าง และเส้นทางไหนที่ดีที่สุดบ้าง ในกรณีแบบนี้ถ้าผมต้องขับรถไป สิ่งที่เกิดขึ้นคือผมอาจจะต้องสอบถามเส้นทางจากคนในท้องที่ ซึ่งถ้าเส้นทางที่ได้รับมาจากการสอบถามถูกต้อง ก็จะไปได้ถึงที่ แต่จะมั่นใจได้อย่างไรว่าเป็นเส้นทางที่รวดเร็วที่สุดและดีที่สุด? จะมั่นใจได้อย่างไรว่าเส้นทางที่ผมเลือกใช้นี้ เป็นเส้นทางที่ไม่มีรถติดหรืออุบัติเหตุ? บางคนที่ผมถามอาจจะ ไม่รู้จักเส้นทางเหล่านั้น และก็ต้องโยนการสอบถามไปให้คนอื่นๆ ทำให้ผมเสียเวลาเพิ่มขึ้น กล่าวคือ ผมไม่มีหลักประกันใดๆ เลยที่จะมั่นใจได้ว่าเอกสารที่ผมถือไปส่งนั้น จะไปถึงปลายทางในระยะเวลาที่กำหนด หรือถ้าถึง ก็ไม่ได้มั่นใจว่าเส้นทางที่ผมเลือกใช้โดยการสอบถามจากคนอื่นนั้น ดีที่สุด

เช่นเดียวกัน ในกรณีแพ็กเก็ตที่ถูกส่งออกไป แม้ว่าจะทราบว่าปลายทางอยู่ที่ใด แต่การที่ต้องผ่านอุปกรณ์ต่างๆ ซึ่งทำหน้าที่อยู่ในเครือข่ายจำนวนมากในแต่ละจุด และหลายครั้งแต่ละอุปกรณ์มีระบบการควบคุมในการส่งต่อแพ็กเก็ตไปถึงปลายทางที่แตกต่างกัน ซึ่งทำให้การตัดสินใจในแต่ละจุดนั้นอาจจะไม่ได้หมายถึงว่าเป็นเส้นทางที่ดีที่สุดเสมอไปนั่นเอง

ในแง่นี้ ถ้าเป็น SDN สิ่งที่เกิดขึ้นคือดึงเอาการทำงานในส่วนของ control plane ทั้งหมด ขึ้นมารวมไว้ที่จุดเดียว ผลที่ได้คือเราจะสามารถจัดการการเคลื่อนไหวของแพ็กเก็ตในเครือข่ายได้ และเราสามารถกำหนดหรือควบคุม (program) เส้นทางของแต่ละแพ็กเก็ตโดยผ่านการกำหนดเงื่อนไขต่างๆ ผลที่เกิดขึ้นก็คือการจัดการเครือข่ายที่มีประสิทธิภาพได้ดีมากยิ่งขึ้นนั่นเอง

ภาพดังกล่าวสะท้อนถึงลักษณะของ SDN ที่เน้นไปที่การควบคุมจากส่วนกลางและเส้นทางที่ดีที่สุดและสามารถเปลี่ยนแปลงเส้นทางให้สอดรับกับความหนาแน่นของเครือข่ายนั่นเอง ในแง่นี้ก็แปลว่าผู้ดูแลระบบสามารถเข้าจัดการเครือข่ายได้และกำหนดเส้นทางโดยใช้ซอฟต์แวร์ที่เรียกใช้งาน API ณ จุดเดียว ซึ่งทำให้สามารถใช้งานเครือข่ายได้อย่างเต็มที่และมีประสิทธิภาพนั่นเอง ลองดูภาพอธิบายจาก Open Networking Foundation

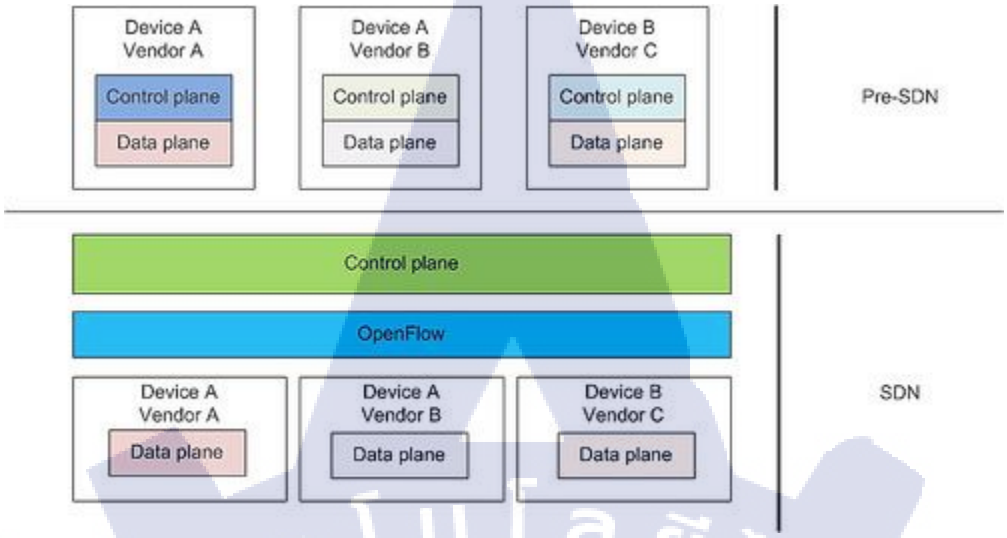


รูปที่ 2.8 อธิบายการทำงานของ SDN

ผลที่ได้จากการใช้งาน SDN

อย่างที่ได้กล่าวไปแล้วว่าสิ่งที่ SDN ทำขึ้นนั่นก็คือระบบเครือข่ายที่แยกตัวโครงสร้างการไหลของข้อมูล ออกจากโครงสร้างการตัดสินใจว่าจะให้ข้อมูลไหลไปในทิศทางใด โดยมี API อย่าง OpenFlow เป็นตัวกลางในการประสานระหว่างตัวโครงสร้างของเครือข่ายและส่วนควบคุมของระบบเครือข่ายนั่นเอง ซึ่งผลที่ได้จากการใช้งาน SDN ที่พอจะกล่าวถึงได้มีอยู่สามอย่าง ดังนี้

ผู้ดูแลระบบไม่ต้องสนใจอุปกรณ์โดยดูที่ผู้ผลิตอีกต่อไป ในแง่นี้หมายถึงว่า แต่เดิม แต่ละอุปกรณ์จะมีระบบการควบคุมและจัดการเครือข่ายที่แยกออกไปจากกันเอง ซึ่งก็แปลว่าอุปกรณ์แต่ละชิ้นจะมีระบบการทำงานที่แตกต่างกัน แม้ว่าจะมีโปรโตคอลหรือมาตรฐานกลางที่สามารถทำให้ใช้งานร่วมกันได้ แต่เมื่อต้องแก้ไขปัญหา อุปกรณ์แต่ละตัวกลับมีวิธีการที่แตกต่างกัน เมื่อมีการใช้งาน SDN สิ่งที่เกิดขึ้นคือไม่ว่าอุปกรณ์ของผู้ผลิตรายใดก็ตาม ควบคุมจัดการให้ด้วยโปรโตคอลกลางที่เรียกว่า OpenFlow Configuration



รูปที่ 2.9 เปรียบเทียบการใช้ก่อนและหลังมี SDN

ระบบมีคุณสมบัติที่ยืดหยุ่นและขยายตัวได้ง่ายขึ้น ด้วยเหตุผลจากข้อแรกที่เราไม่ต้องคำนึงว่าอุปกรณ์ต้องมาจากผู้ผลิตรายเดียวกัน สิ่งที่เกิดขึ้นคือการจัดซื้ออุปกรณ์เครือข่ายและปรับเปลี่ยนขนาดของเครือข่ายสามารถทำได้เร็วขึ้นและวางแผนได้ง่ายมากขึ้นกว่าเดิมอีกทั้งมีต้นทุนที่ถูกลง (เพราะไม่ต้องถูกผูกขาดด้วยผู้ผลิตรายใดรายหนึ่ง)

ผู้ดูแลระบบสามารถจัดการเครือข่ายให้มีประสิทธิภาพ เนื่องจากตัว control plane สามารถที่จะกำหนดค่าในการใช้งานต่างๆ ได้ผ่านทางซอฟต์แวร์ที่ควบคุมจากศูนย์กลาง สวิตซ์แต่ละชุดจะสามารถควบคุมผ่าน API สำหรับการควบคุม

แนวโน้มและบทสรุปของ SDN

แนวคิดของ SDN ที่นำเอาซอฟต์แวร์ไปจัดการระบบเครือข่ายและควบคุม เป็นสิ่งที่เกิดขึ้นภายใต้ความพยายามยาวนานมากว่า 2 ทศวรรษเป็นอย่างน้อย การเติบโตของ SDN ที่กลายมาเป็นสิ่งที่หลายคนเริ่มให้ความสนใจในเวลานี้ ไม่ใช่เพราะความยืดหยุ่นในการทำงานเท่านั้น แต่ยังรวมไปถึงแนวทางในการใช้งานที่ปรับใช้มาเป็นฐานของ Network Virtualization ได้เป็นอย่างดี

บทที่ 3

แผนงานการปฏิบัติงานและขั้นตอนการดำเนินงาน

3.1 แผนงานปฏิบัติงาน

ตารางที่ 3.1 แสดงแผนการปฏิบัติงานสหกิจศึกษาเป็นเวลา 4 เดือน

หัวข้องาน	เดือนที่ 1				เดือนที่ 2				เดือนที่ 3				เดือนที่ 4			
ศึกษาและเรียนรู้การออกแบบระบบและการใช้งานอุปกรณ์																
ออกไปสำรวจหน้างาน																
ออกแบบระบบเครือข่าย																
จัดเตรียมอุปกรณ์ก่อนไปติดตั้ง																
ติดตั้งระบบ																
ทดสอบระบบและนำเสนอระบบ																
ติดตามผลและปรับปรุงตามความต้องการของลูกค้า																

3.2 รายละเอียดงานที่นักศึกษาปฏิบัติในงานสหกิจศึกษา หรือรายละเอียดโครงงานที่ได้รับหมอบหมาย

3.2.1 รายละเอียดโครงการที่ได้รับหมอบหมาย

รายละเอียดในการดำเนินโครงการ

บริษัท A (นามสมมุติ) ดำเนินธุรกิจโรงแรมมีความต้องให้ปรับปรุงระบบอินเตอร์เน็ตไร้สาย (Wi-Fi) ที่ให้บริการกับลูกค้าที่มาเข้าพักและพนักงาน

เนื่องจากระบบที่มีอยู่เดิมนั่นมีปัญหาดังนี้

1.เชื่อมต่อแล้วหลุดออกจากระบบบ่อย

2.สัญญาณ Wi-Fi ไม่ครอบคลุมไม่ครอบคลุมพื้นทั้งหมดของทางโรงแรม

3.เชื่อมต่อแล้วไม่สามารถอินเตอร์เน็ตได้อย่างเต็มประสิทธิภาพ

4.ส่วนพนักงานมีปัญหาในการเข้าใช้งานระบบบริหารจัดของทางโรงแรมที่อยู่บนระบบคลาวด์ (Cloud Computing)

5.ไม่มีระบบสำรองในกรณีอินเตอร์เน็ตหรือระบบไฟฟ้ามีปัญหา

6.ไม่มีระบบพิสูจน์ตัวตนและจัดเก็บข้อมูลการใช้งาน (Log)

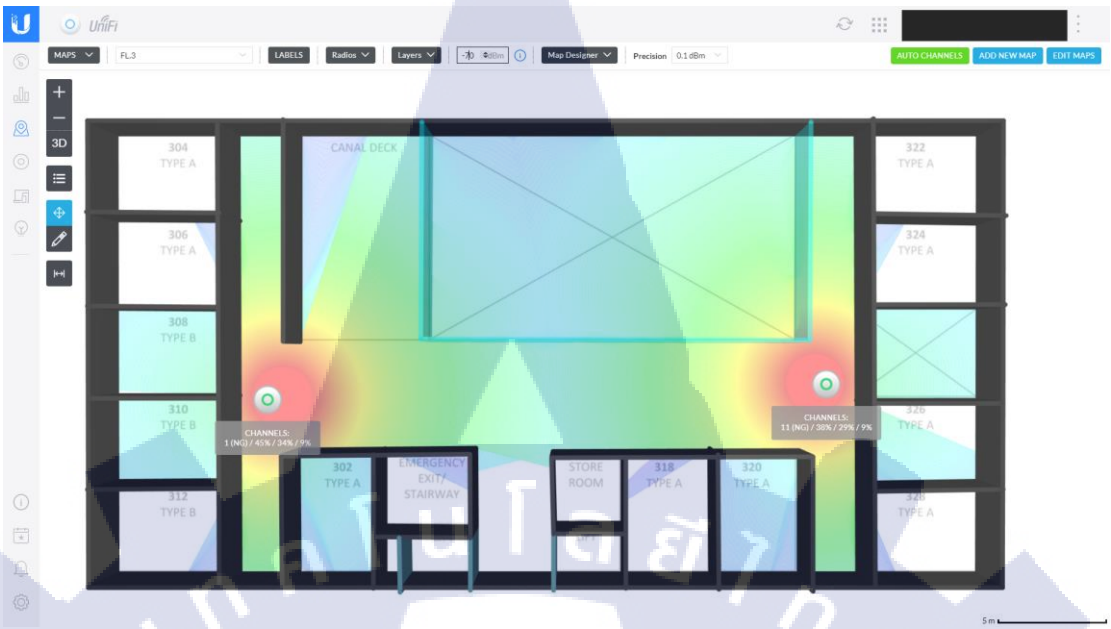
7.Wi-Fi เดิมไม่มีระบบโรมมิ่งในกรณีที่ใช้งานข้ามโซน

3.3 ขั้นตอนการดำเนินงานที่นักศึกษาปฏิบัติงานในโครงงาน\

3.3.1 ศึกษาความต้องการของระบบ (Get Requirement)

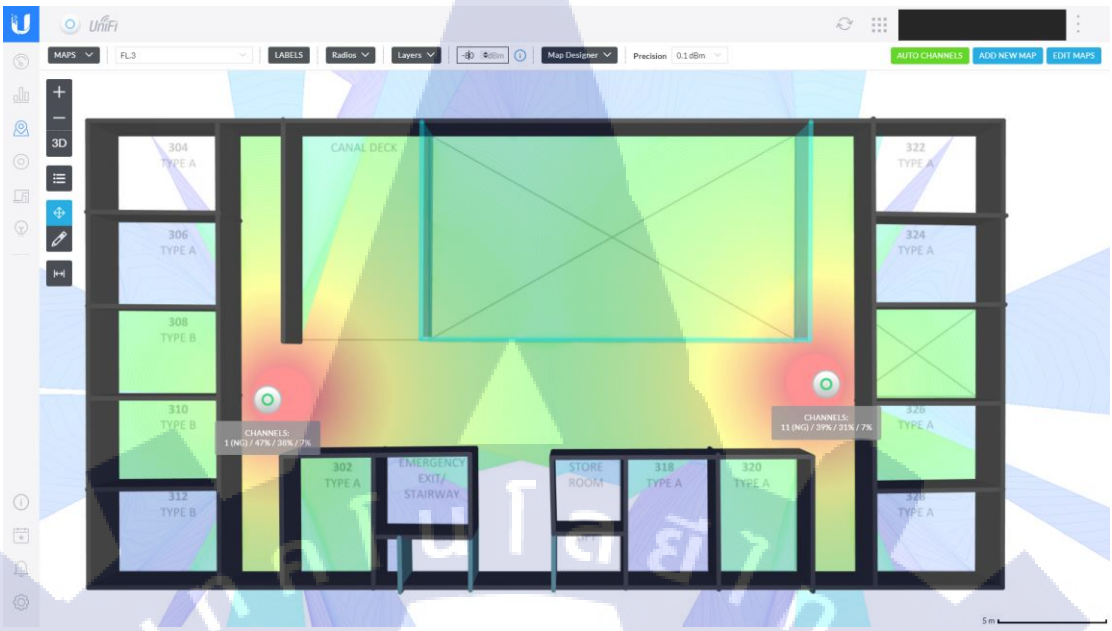
รูปที่ 3.1 Old Network Wi-Fi Heat Map RSSI -60 dBm

จากภาพที่ 3.1 จะเห็นได้ว่าที่การรับสัญญาณที่ความแรง -60dBm ระบบเดิมนั่นที่สัญญาณ Wi-Fi ไม่สามารถครอบคลุมในบริเวณห้องพักสามารถใช้ได้เพียงแค่ส่วนระเบียงสำหรับพักผ่อน (Canal Deck) เท่านั่น



รูปที่ 3.2 Old Network Wi-Fi Heat Map RSSI -70 dBm

จากรูปที่ 3.2 จะเห็นได้ว่าที่การรับสัญญาณที่ความแรง -70dBm ระบบเดิมนั่นที่สัญญาณ Wi-Fi สามารถครอบคลุมได้เพียงห้อง 5 ห้องเท่านั่นและส่วนระเบียงสำหรับพักผ่อน (Canal Deck) เท่านั่น



รูปที่ 3.3 Old Network Wi-Fi Heat Map RSSI -80 dBm

จากรูปที่ 3.3 จะเห็นได้ว่าที่การรับสัญญาณที่ความแรง -80dBm ระบบเดิมนั่นที่สัญญาณ Wi-Fi สามารถครอบคลุมได้เกือบทั้งหมดยกเว้นห้องพัก 2 ห้องสุดที่ไม่สามารถใช้งานได้ แต่ก็ไม่สามารถใช้ความเร็วได้เต็มประสิทธิภพเป็นสัญญาณมีความเข้มน้อยมาก

รายละเอียดความต้องการของระบบ

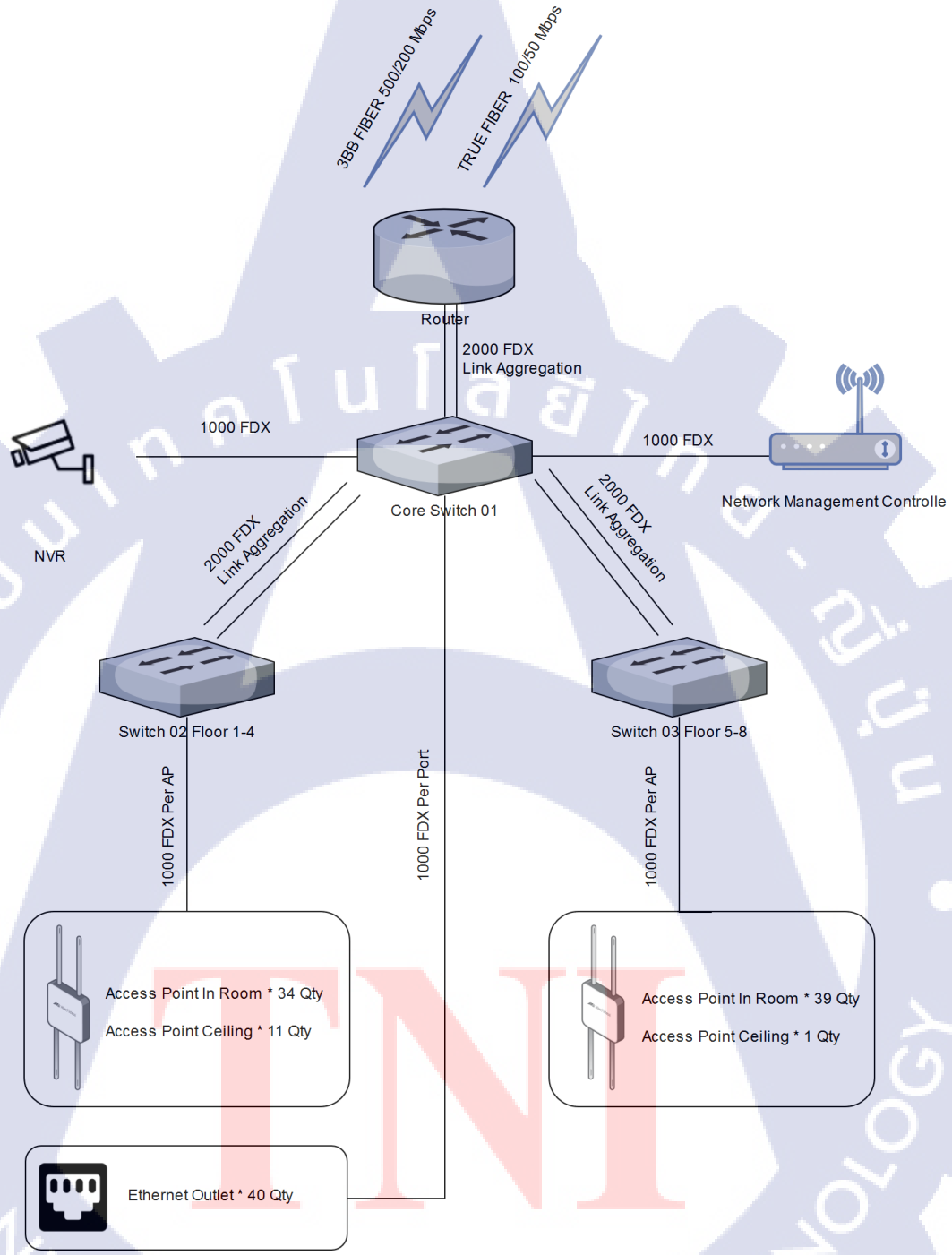
1) ระบบเน็ตเวิร์คที่มีความเสถียร
2) ความเร็วโดยรวมของระบบที่สูงขึ้น
3) ระบบอินเตอร์เน็ตไร้สาย (Wi-Fi) ครอบคลุมทุกพื้นที่
4) ระบบพิสูจน์ตัวตน
5) เก็บข้อมูลการใช้งาน (Log)
6) สามารถใช้งานระบบบริหารจัดการโรงแรมได้เสถียร
7) ระบบสำรอง

3.3.2 วางแผนการทำงานหรือสิ่งที่ต้องมีภายในระบบ (Planning)

1. ติดตั้ง Gateways
2. ระบบ Load Balance เพื่อกระจายการใช้งานข้อมูลและสำรองในกรณี
3. Internet ของผู้ให้บริการ (ISP) เจ้าใดเจ้าหนึ่งมีปัญหาให้สามารถใช้งานแทนกันได้
4. ระบบ QOS (Quality of Service) เพื่อจัดการข้อมูลที่ส่งภายในระบบ
5. ให้มีการจัดความสำคัญของข้อมูลแต่ละประเภทให้มีการใช้งานได้มีความเสถียร
6. ระบบ Hotspot เพื่อพิสูจน์ตัวตนของลูกค้า, พนักงาน
7. และจัดเก็บ Log การใช้งานระบบอินเตอร์เน็ต
8. ระบบ Firewall เพื่อป้องกันการโจมตีทางไซเบอร์
9. ติดตั้ง Switch
10. ระบบ VLAN (Virtual Local Area Network)
    เพื่อแบ่งแยกกลุ่มของผู้ใช้งานระบบและอุปกรณ์ต่างๆในระบบ
    ทำให้สามารถบริหารจัดการได้ง่าย
11. ระบบ PoE (Power over Ethernet) เป็นระบบจ่ายไฟฟ้าให้กับอุปกรณ์ปลายทาง
    ไปกับสาย LAN (Ethernet Cable)
12. ติดตั้ง Wireless Controller เพื่อความบริหารจัดการอุปกรณ์ Access Point
    ภายในระบบทั้งหมดได้จากศูนย์กลาง
13. ติดตั้ง Access Point ในห้องพักแต่ละห้องและบริเวณพื้นที่ส่วนกลางต่างๆ
14. ระบบ Roaming ของระบบ Wireless Network เพื่อที่เวลาผู้ใช้งาน
    เดินไปยังจุดต่างๆของโรงแรมสามารถใช้งาน Wireless Network ได้อย่างราบรื่น
15. ติดตั้ง UPS (Uninterruptible Power Supply) เพื่อเป็นระบบไฟฟ้าสำรองให้กับ
    ทั้งระบบในกรณีไฟฟ้าดับหรือขัดข้อง
16. ระบบ UPS Monitor เพื่อแจ้งเตือนกรณีไฟฟ้าดับหรือขัดข้อง
    และปิดระบบในอัตโนมัติในกรณี Battery ของ UPS ใกล้หมด
17. ระบบ Cloud เพื่อที่สามารถ Monitor ระบบจากภายนอกได้

18. ระบบ VPN (Virtual Private Network) เพื่อให้ผู้บริหารสามารถเข้ามาใช้งานระบบภายในของโรมแรมจากภายนอกได้
19. วางแผนการย้ายระบบเก่ามาเป็นระบบใหม่ ให้ผู้ใช้ได้รับผลกระทบน้อยที่สุด
20. วางแผนการติดตั้งอุปกรณ์เข้ากับห้องพักแต่ละห้อง

3.3.3 การออกแบบระบบ (Design)



รูปที่ 3.4 โครงสร้างระบบ

VLAN ID	CIDR	Default Gateway	Note.
10	192.168.10.0/24	192.168.10.1	Management
1101	192.168.11.0/24	192.168.11.1	Office
1102	192.168.12.0/24	192.168.12.1	Floor 2
1103	192.168.13.0/24	192.168.13.1	Floor 3
1104	192.168.14.0/24	192.168.14.1	Floor 4
1105	192.168.15.0/24	192.168.15.1	Floor 5
1106	192.168.16.0/24	192.168.16.1	Floor 6
1107	192.168.17.0/24	192.168.17.1	Floor 7
1108	192.168.18.0/24	192.168.18.1	Floor8
1109	192.168.19.0/24	192.168.19.1	Public area
1110	192.168.110.0/24	192.168.110.1	CCTV
1120	192.168.120.0/24	192.168.120.1	Guest
1199	192.168.199.0/24	192.168.199.1	Old Network

ตารางที่ 3.2 แสดงหมายเลข IP Address ในระบบที่ออกแบบ

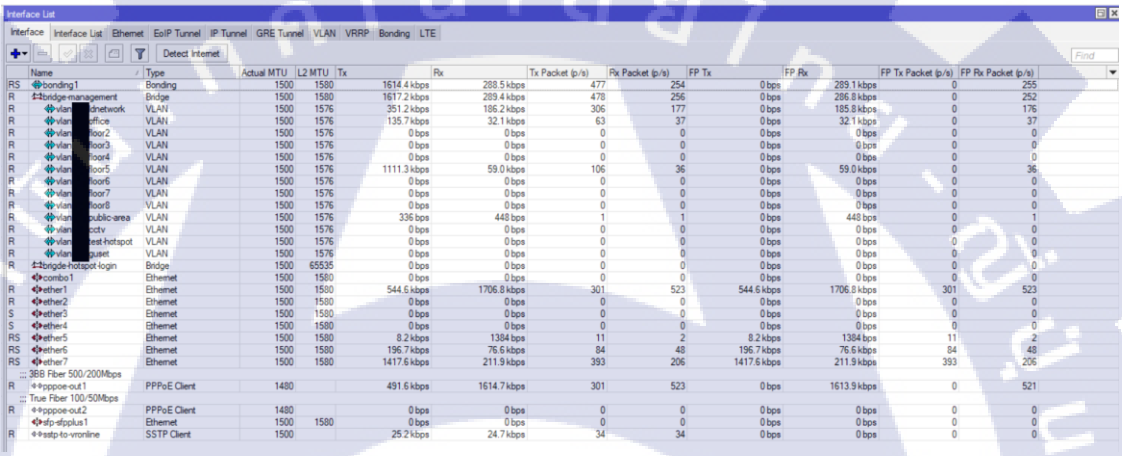
3.3.4 ติดตั้งระบบ (Integration)

1.ตั้งชื่อ (Identity) ให้กับแต่ละอุปกรณ์ในระบบ

2.เปลี่ยนรหัสผ่าน (Password) ให้กับแต่ละอุปกรณ์ในระบบ

3.ปิดบริการ (Service) ที่ไม่ใช้งานและเป็นอันตรายต่อการโจมตีทางไซเบอร์

3.3.4.1 Router

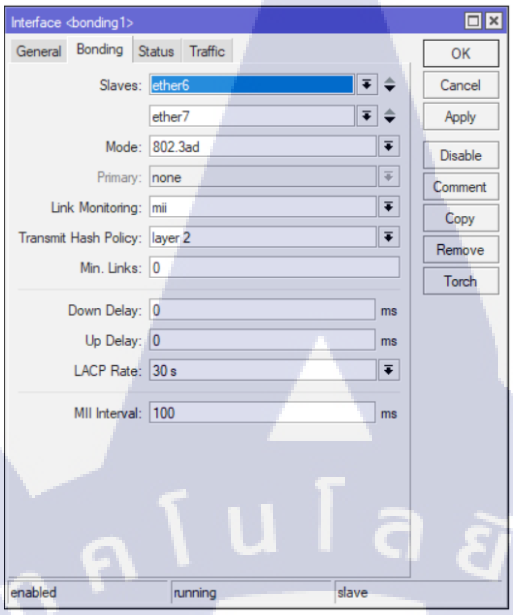


รูปที่ 3.5 Interface ในระบบทั้งหมด

1.สร้าง Bridge Management เพื่อเป็นวงของเน็ตเวิร์คในการบริหารจัดการระบบ

2.สร้าง VLAN ตามที่ได้ออกแบบไว้

3.เพิ่ม VLAN (Tag VLAN) เข้าใน Bridge Management เพื่อให้ดูแลและจัดการได้

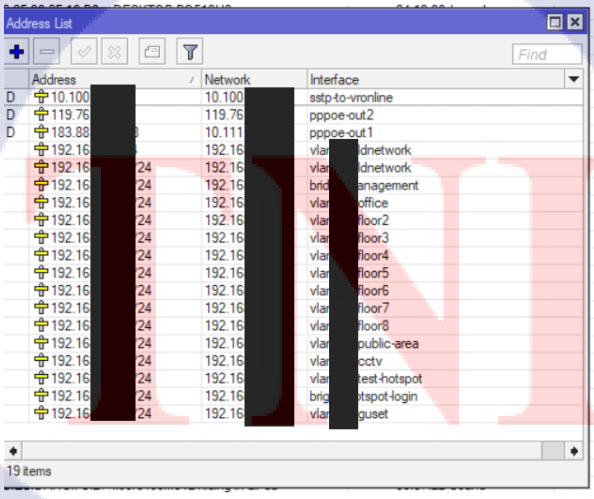


รูปที่ 3.6 Bonding Interface

4.สร้าง Bonding Interface (Link aggregation)

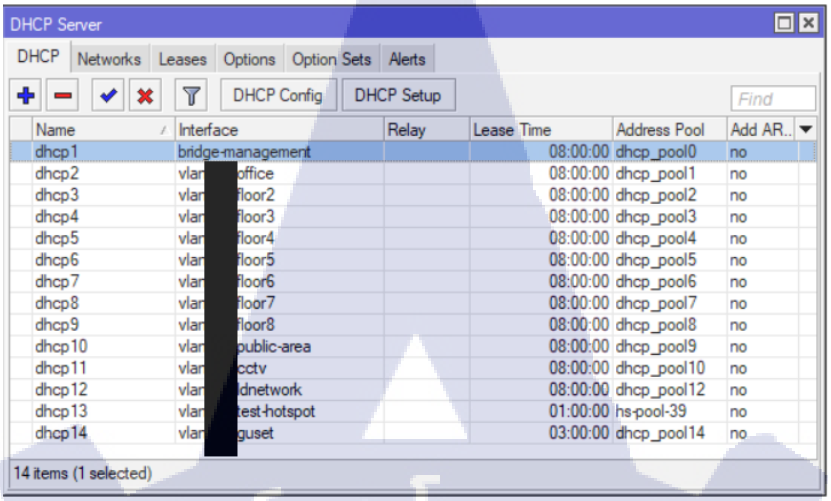
โดยใช้มาตรฐาน IEEE802.3ad เพื่อใช้เชื่อมต่อกับ Switch

5.เพิ่ม VLAN เข้าใน Bonding Interface (Trunk)



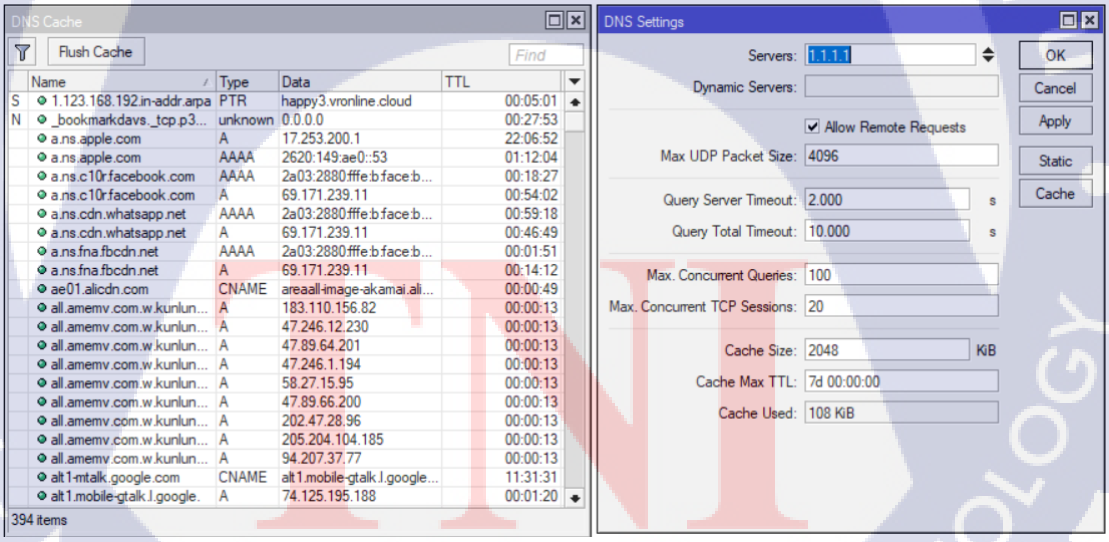
รูปที่ 3.7 Address list

6.สร้าง IP Address ให้กับแต่ละ VLAN ตามที่ออกแบบไว้



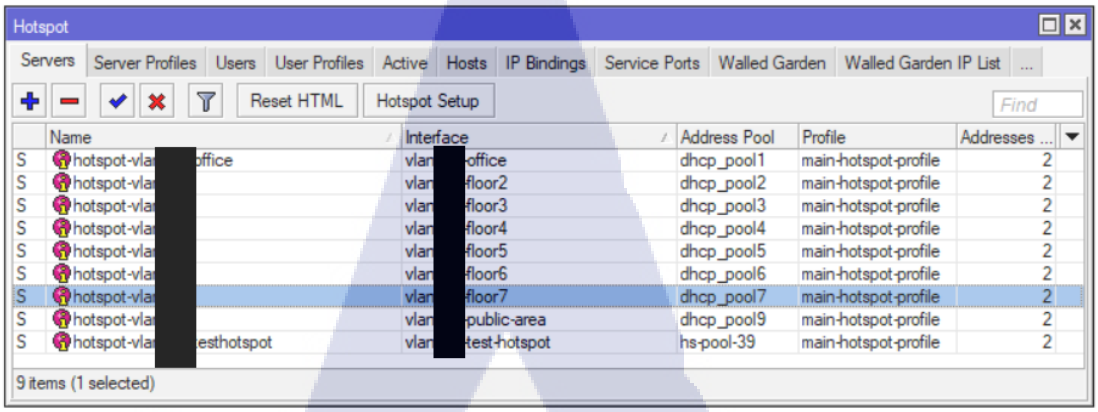
รูปที่ 3.8 DHCP Server

7.สร้าง DHCP Server ให้แต่ละ Interface โดยสร้าง IP Pool ให้แต่ละ Interface และกำหนดค่า Gateway, DNS Server, Lease Time ของแต่ละ DHCP Server



รูปที่ 3.9 DNS Settings

8.กำหนด DNS Server เป็น 1.1.1.1 (Cloudflare DNS) ในการใช้งานบริการ DNS

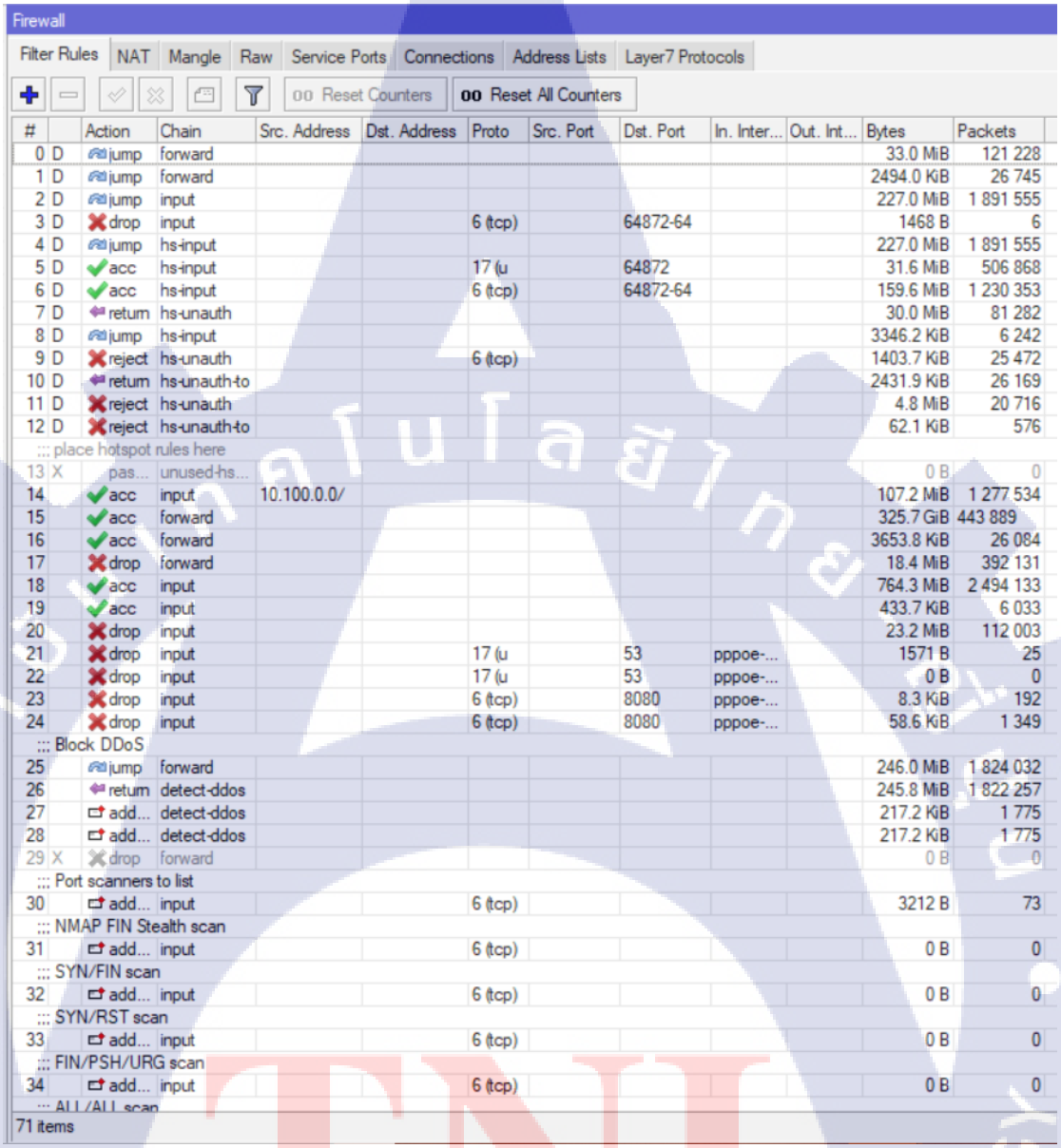


รูปที่ 3.10 Hotspot Server

9.สร้าง Hotspot Server เพื่อเป็นระบบยืนยันตัวตนในระบบให้กับผู้มาพักอาศัยและพนักงานของทางโรงแรม

10.เพิ่ม SSL Certificate เข้าในระบบ Hotspot เพื่อใช้ในการเข้าสู่ระบบแบบเข้ารหัสข้อมูลผ่าน HTTPS ได้อย่าถูกต้องสมบูรณ์

11.สร้าง User Admin ในระบบ Hotspot ให้กับทางโรงแรมเพื่อเข้าไปบริหารจัดการข้อมูลผู้เข้าใช้ในระบบ



Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

oo Reset Counters | oo Reset All Counters

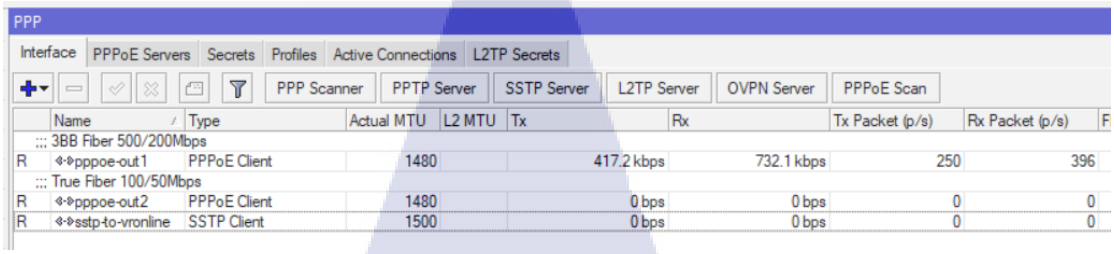
#		Action	Chain	Src. Address	Dst. Address	Proto	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0	D	jump	forward								33.0 MiB	121 228
1	D	jump	forward								2494.0 KiB	26 745
2	D	jump	input								227.0 MiB	1 891 555
3	D	drop	input			6 (tcp)		64872-64			1468 B	6
4	D	jump	hs-input								227.0 MiB	1 891 555
5	D	acc	hs-input			17 (u		64872			31.6 MiB	506 868
6	D	acc	hs-input			6 (tcp)		64872-64			159.6 MiB	1 230 353
7	D	return	hs-unauth								30.0 MiB	81 282
8	D	jump	hs-input								3346.2 KiB	6 242
9	D	reject	hs-unauth			6 (tcp)					1403.7 KiB	25 472
10	D	return	hs-unauth-to								2431.9 KiB	26 169
11	D	reject	hs-unauth								4.8 MiB	20 716
12	D	reject	hs-unauth-to								62.1 KiB	576
		;;; place hotspot rules here										
13	X	pas...	unused-hs...								0 B	0
14		acc	input	10.100.0.0/							107.2 MiB	1 277 534
15		acc	forward								325.7 GiB	443 889
16		acc	forward								3653.8 KiB	26 084
17		drop	forward								18.4 MiB	392 131
18		acc	input								764.3 MiB	2 494 133
19		acc	input								433.7 KiB	6 033
20		drop	input								23.2 MiB	112 003
21		drop	input			17 (u		53	pppoe-...		1571 B	25
22		drop	input			17 (u		53	pppoe-...		0 B	0
23		drop	input			6 (tcp)		8080	pppoe-...		8.3 KiB	192
24		drop	input			6 (tcp)		8080	pppoe-...		58.6 KiB	1 349
		;;; Block DDoS										
25		jump	forward								246.0 MiB	1 824 032
26		return	detect-ddos								245.8 MiB	1 822 257
27		add...	detect-ddos								217.2 KiB	1 775
28		add...	detect-ddos								217.2 KiB	1 775
29	X	drop	forward								0 B	0
		;;; Port scanners to list										
30		add...	input			6 (tcp)					3212 B	73
		;;; NMAP FIN Stealth scan										
31		add...	input			6 (tcp)					0 B	0
		;;; SYN/FIN scan										
32		add...	input			6 (tcp)					0 B	0
		;;; SYN/RST scan										
33		add...	input			6 (tcp)					0 B	0
		;;; FIN/PSH/URG scan										
34		add...	input			6 (tcp)					0 B	0
		;;; ALL/ALL scan										

71 items

รูปที่ 3.11 Firewall

12.สร้างกฎของ Firewall ตามที่ออกแบบเอาไว้ให้เข้ากับความต้องการของลูกค้า โดย มีการทำระบบ Load Balance และป้องกันการโจมตีดังต่อไปนี้

DDoS, Port Scan, FTP Brute Forcers, SSH Brute Forcers, Bogon IP addresses, DNS Amplifier Attack, Ransomware, Deny Protocol ที่มีความปลอดภัยต่ำทั้งหมด

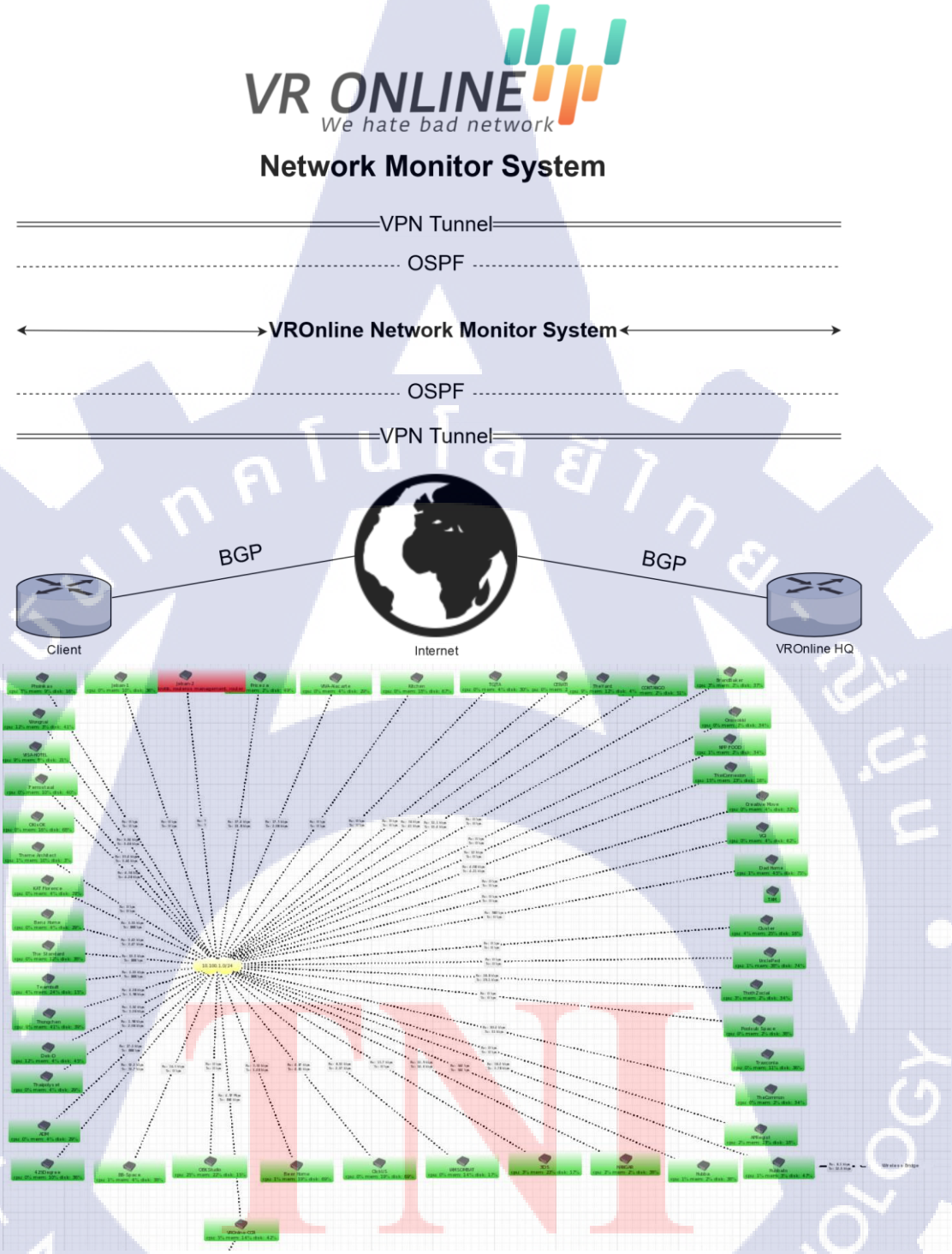


รูปที่ 3.12 Point to Point Protocol

13.เชื่อมต่อ Internet ผ่านระบบ PPPoE

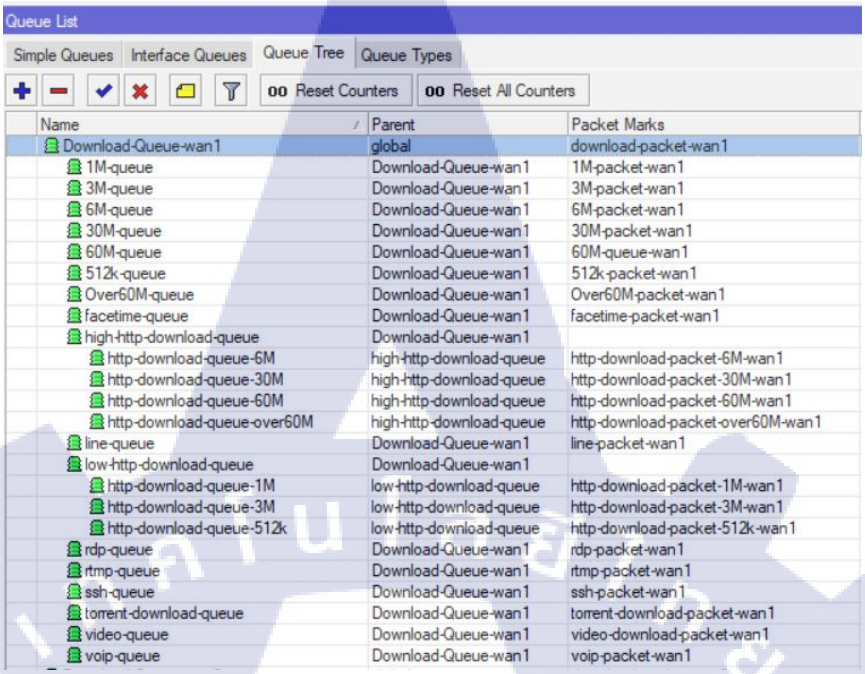
14.เชื่อมต่อ VPN ไปที่ Cloud ของบริษัท เพื่อใช้ในการติดตามสถานของระบบ (Monitoring)

15.ทำ OSPF Routing บน VPN ให้สามารถเข้าสู่ระบบติดตามสถาน (Monitoring) ของบริษัท



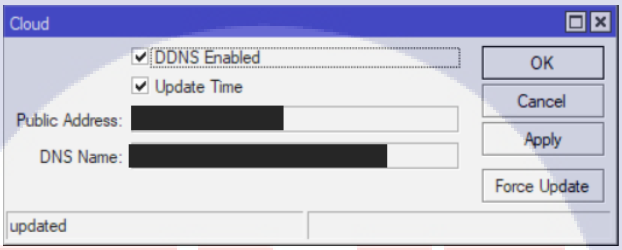
รูปที่ 3.13 Monitoring System

16.ส่งข้อมูล Router กลับไปที่ บริษัทเพื่อเพิ่มเข้าสู่ระบบติดตามสถาน (Monitoring System)



รูป 3.14 Quality of Service

17.ทำระบบ Quality of Service โดยแบ่งตาม บริการ (Service) ที่เข้ามาใช้งานระบบ จะให้บริการ (Service) ที่ต้องการความเสถียรมีลำดับที่สูงกว่าจะได้เป็นลำดับแรก



รูปที่ 3.15 Dynamic DNS

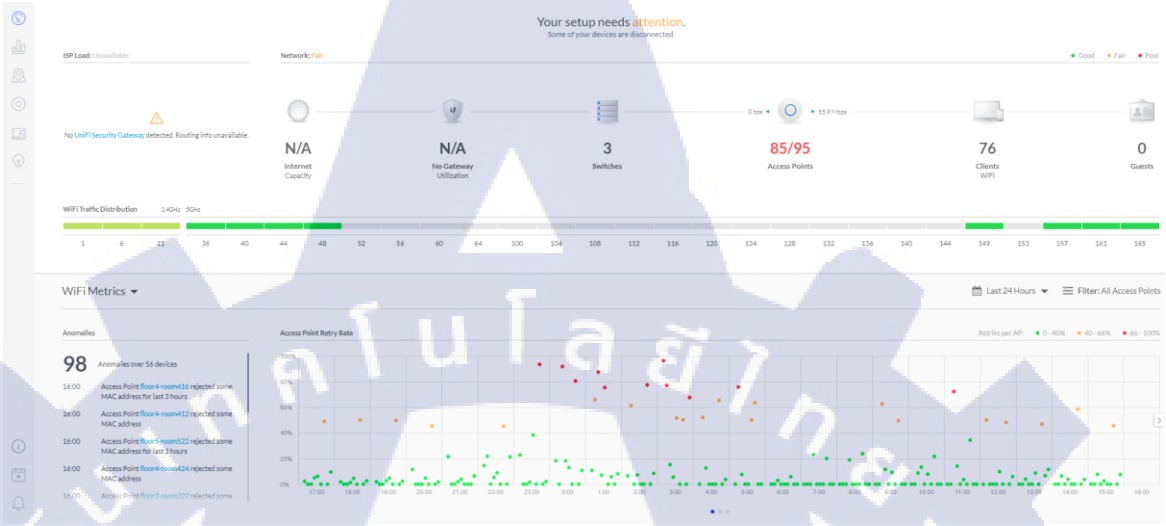
18.ทำระบบ Dynamic DNS ให้สามารถเชื่อมต่อมาจากภายนอกได้

19.ทำระบบ VPN โดยใช้ มาตรฐาน L2TP/IPsec เพื่อเป็นระบบยืนยันตัวในการเชื่อมต่อจากภายนอกเข้ามายังระบบ

20.ทำระบบ Log เพื่อเก็บข้อมูลผู้ใช้ในระบบ

21.ทำระบบ Daily Backup เพื่อป้องกันในกรณีฉุกเฉิน

3.3.4.2 Network Management Controlle



รูปที่ 3.16 Dashboard Network Management Controller

Network Management Controller ที่เลือกใช้คือ “ UniFi® Software-Defined Networking ” สามารถติดตามสถาน, ควบคุมและสั่งการได้ทั้ง Gateway, Switch, Access Points ได้จากศูนย์กลาง ในงานนี้เราเลือกมาควบคุมและสั่งการเฉพาะ Switch และ Access Points

รูปที่ 3.17 SDN Site Configuration

1.ตั้งชื่อ Site

2.เลือกประเทศเป็น ประเทศไทย และเวลาเป็น UTC+7 Bangkok

3.เลือก Enable advanced features เพื่อให้ใช้ความสามารถดังต่อไปนี้ได้

Airtime fairness, Bandsteering, minimum RSSI, Load balancing and opening terminal after clicking on device's ip.

4.เลือก Automatically upgrade AP firmware เพื่อที่เวลามี firmware ใหม่ของ Access Points

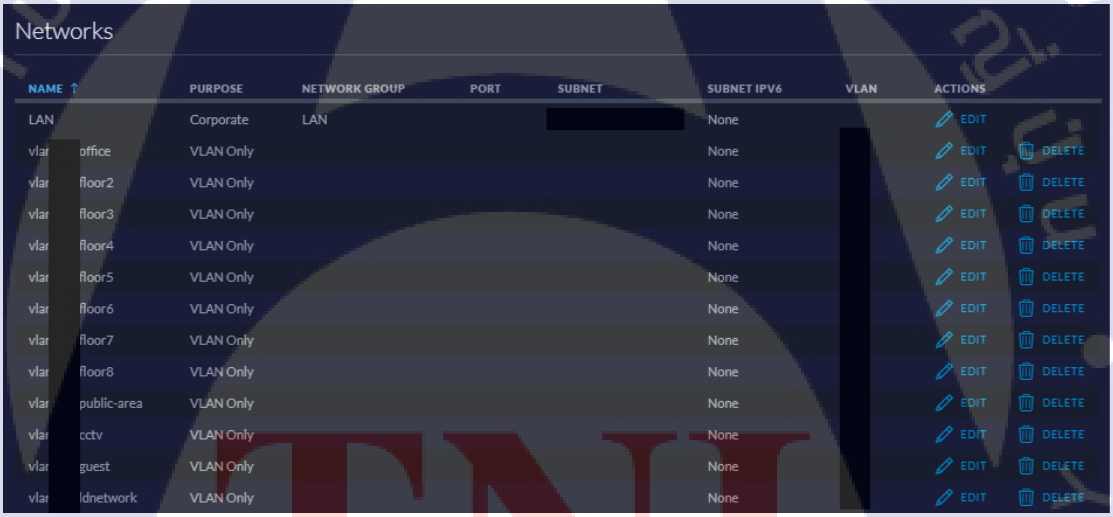
ระบบจะทำการ อัพเดทให้อัตโนมัติ

5.เลือก Enable status LED เพื่อให้ อุปกรณ์แต่ละตัวเปิกไฟแสดงสถาน

6.เลือก Enable alert emails เพื่อให้ส่ง E-Mail แจ้งเตือนให้ในกรณีตรวจพบปัญหาในระบบ

7.เลือก Enable connectivity monitor and wireless uplink เพื่อให้ค่อยตรวจสอบ Gateway ยังทำงานอยู่ปกติ ในกรณี Gateway ไม่สามารถติดต่อ Gateway ได้ระบบจะทำการปิดการส่งสัญญาณ Wi-Fi ให้อัตโนมัติ

8.กำหนดค่า ปริมาณ Internet ที่มีในระบบ



รูปที่ 3.18 SDN Network Configuration

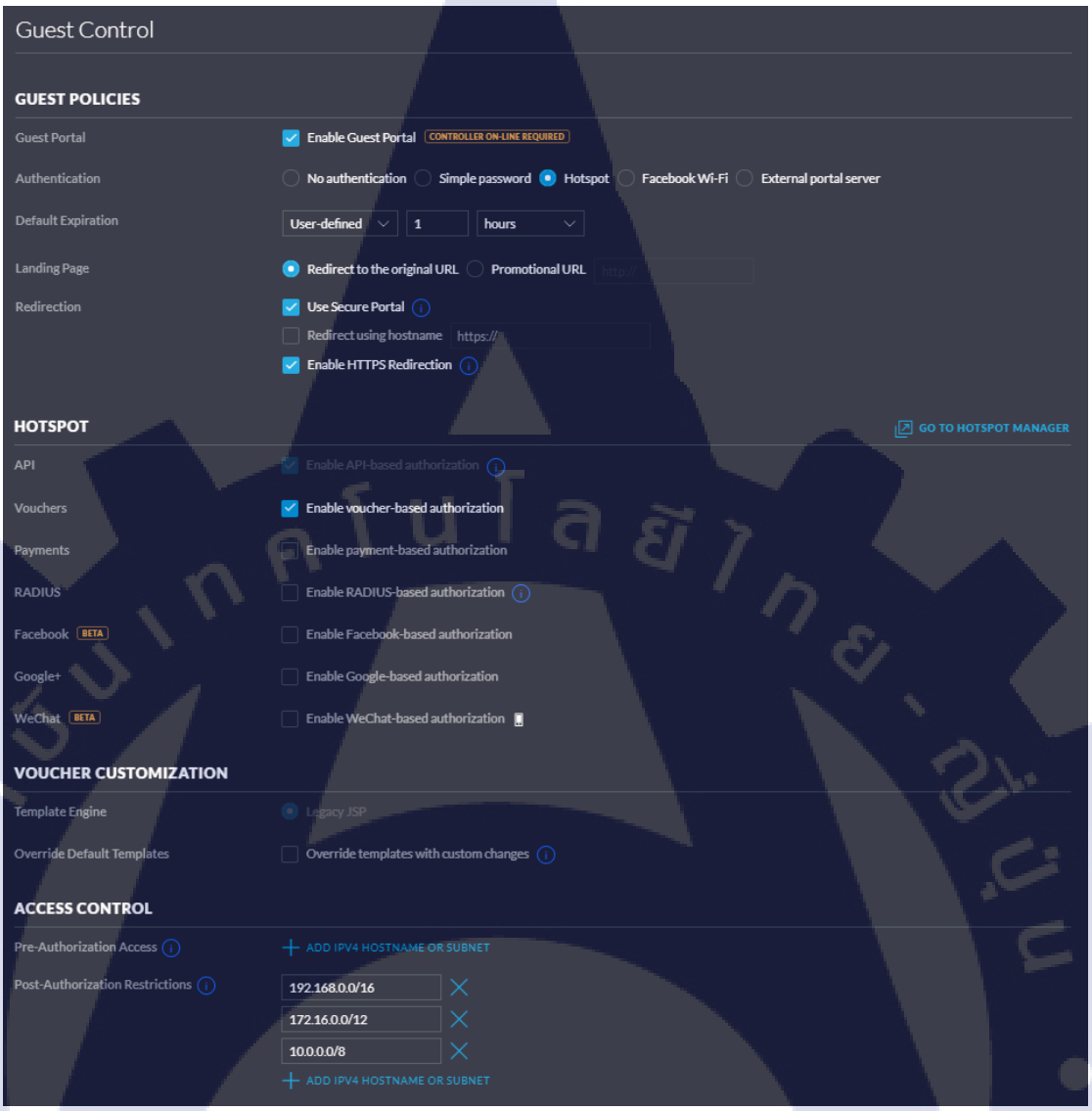
9.สร้าง VLAN ตามที่ได้ออกแบบไว้

10.กำหนด DHCP Guarding ให้แต่ละ VLAN เพื่อป้องกันการมี DHCP Server ภายนอกเข้ามาปลอมแปลงเป็นของระบบ

รูปที่ 3.19 SDN Switch Ports

11.สร้าง Switch Ports Profile สำหรับให้ Access Points ในแต่ละชั้น

12. สร้าง Switch Ports Profile สำหรับ Port ที่ต่อเชื่อม Access Points กับ Switch เป็นแบบ Isolation เพื่อป้องกัน Broadcast Storm เกิดขึ้นในระบบ



รูปที่ 3.20 SDN Guest Control

13.เลือก Enable Guest Portal เพื่อใช้งานระบบ Guest ให้กับคนที่เข้ามาใช้บริการโรงแรม แต่ไม่ได้เข้าพัก เช่น ห้องอาหารหรือร้านกาแฟ

14.เลือกวิธีการยืนยันตัวตนแบบ Hotspot

15.เลือกเวลาที่อยู่ในระบบได้เป็น 1 ชม.

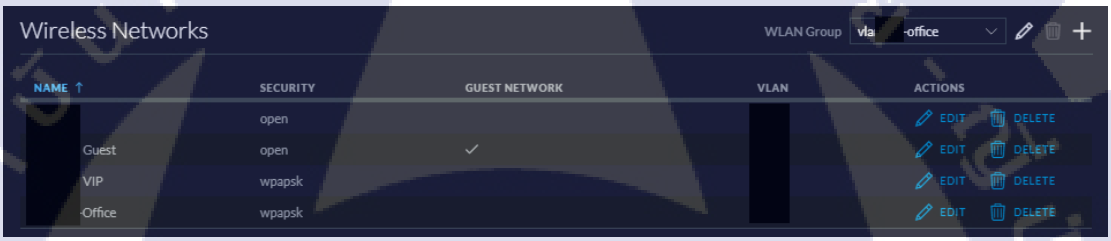
16. Landing Page เลือกเป็น Redirect to the original URL

16. ตั้งค่า Redirection เป็น Use Secure Portal และ Enable HTTPS Redirection เพื่อให้เวลาเชื่อมต่อและข้อมูลการยืนยันตัวตนถูกเข้ารหัสทั้งหมด

17. Hotspot เลือกรูปแบบการยืนยันแบบ Vouchers

18. Post-Authorization Restrictions ใส่ IP Address ในระบบที่เราออกแบบไว้ เพื่อป้องกันไม่คนที่อยู่ในเครื่องข่าย Guest Network เข้าถึงเครื่องข่ายภายในได้

19. สร้าง User Admin สำหรับบริหารจัดการ Vouchers

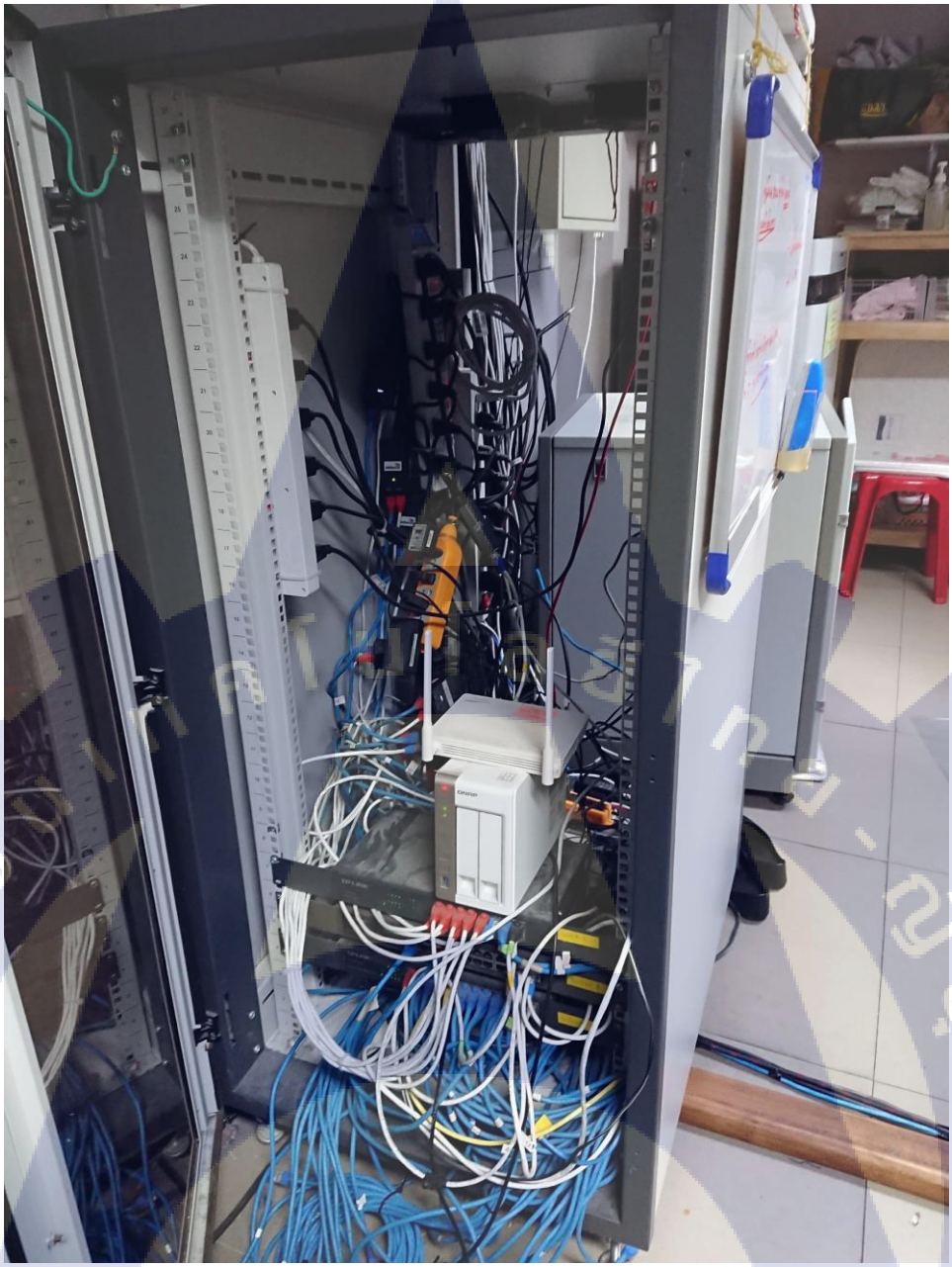


รูปที่ 3.21 SDN Wireless Networks

20.สร้าง WLAN Group ให้แต่ละส่วนของอาคาร

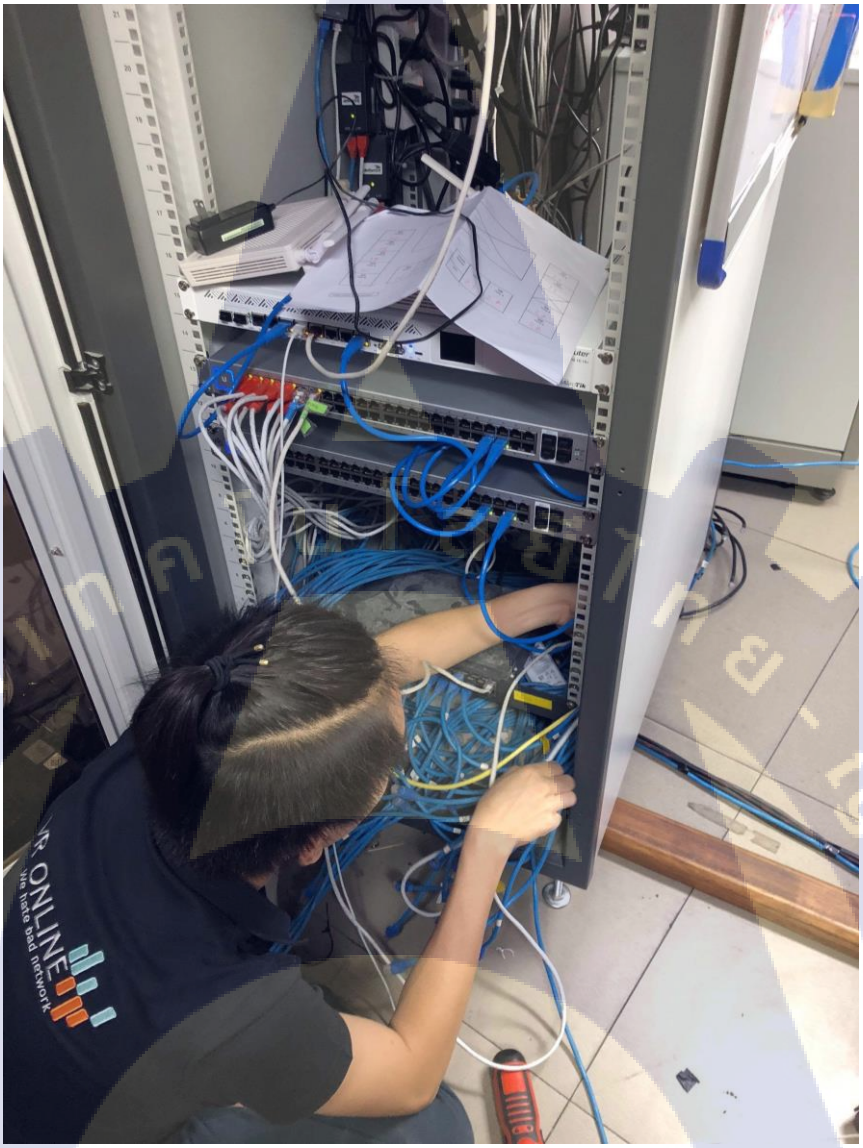
21.สร้าง SSID ของแต่ละ VLAN ใน WLAN Group ทุกอัน

22.SSID สำหรับ Guest เลือก Guest Network เพื่อใช้งานความสามารถ Guest Control



รูปที่ 3.22 สภาพตู้ Rack แต่เดิมที่มีอยู่

หลังเตรียมทุกอย่างเรียบร้อยแล้วก็ได้แจ้งทางโรงแรมเพื่อเปลี่ยนระบบจากระบบเก่าเข้าระบบใหม่ โดยใช้เวลาประมาณ 15 นาที เพื่อสลับสายไปยัง อุปกรณ์ชุดใหม่



รูปที่ 3.23 ติดตั้งอุปกรณ์และย้ายสู่ระบบใหม่

จากรูปที่ 3.23 นั่นตอนย้ายระบบนั่นต้องเตรียมระบบเก่าให้ โรงแรงยังสามารถให้บริการได้อยู่ โดยการ จำลอง Network เก่าขึ้นมาแล้วย้ายสายของส่วนนั่นมายังอุปกรณ์ใหม่

หลังจากนั่นก็เริ่มย้ายสายของส่วนห้องพักและในห้องพักแต่ละห้องก็

ให้ทีมติดตังเข้าไปติดตั้ง Access Point ไปพร้อมกัน

รูปที่ 3.24 ติดตั้งอุปกรณ์เรียบร้อย

หลังจากติดตั้งอุปกรณ์เรียบร้อยแล้วก็เริ่มทำการทดสอบระบบต่างๆที่ออกแบบไว้ว่าเป็นไปตามที่ออกแบบไว้หรือไม่

รูปที่ 3.25 ก่อนติดตั้ง Access Point

จากที่ออกแบบ คือ ห้องพัก 1 ห้องมี Access Point 1 ตัว เพื่อให้สัญญาณครอบคลุมทั้งห้อง และใช้งานได้อย่างมีประสิทธิภาพ เนื่องจากห้องพักทุกห้องมี Lan Outlet อยู่แล้วทำให้ติดตั้ง Access Points เข้าไปได้เลยไม่ต้องเดินสายใหม่

รูปที่ 3.26 ติดตั้ง Access Point เรียบร้อย

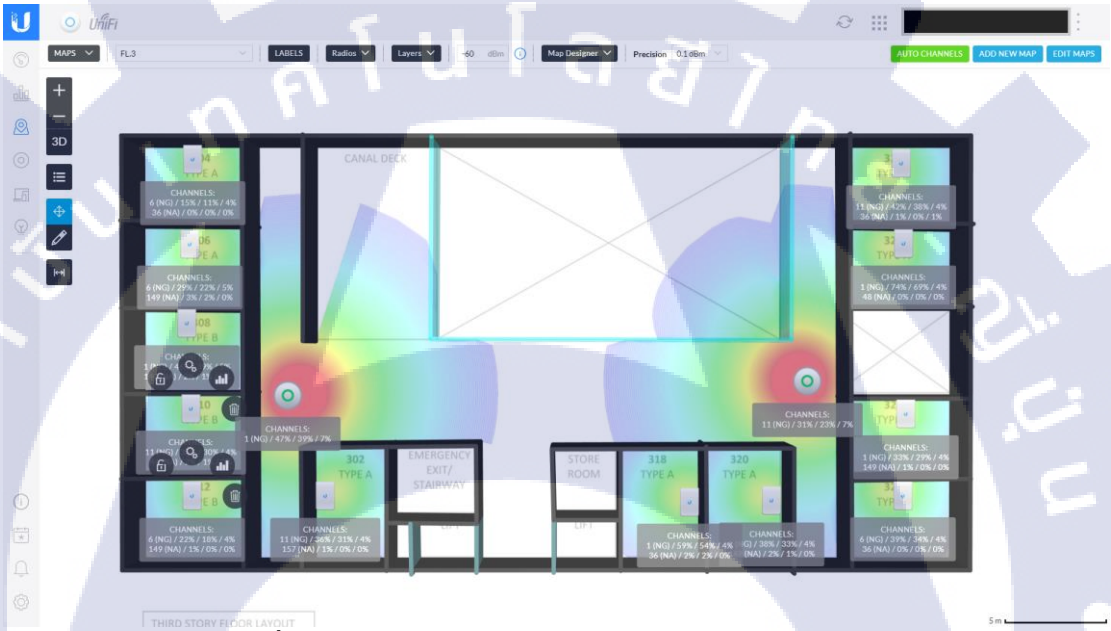
หลังจาก Access Point เรียบร้อยก็ให้ทางทีมติดตั้งตรวจสอบสัญญาณ

ว่าครอบคลุมหรือแรงไปรบกวนห้องอื่นหรือไม่จะได้ปรับกำลังส่งได้อย่างถูกต้อง

บทที่ 4

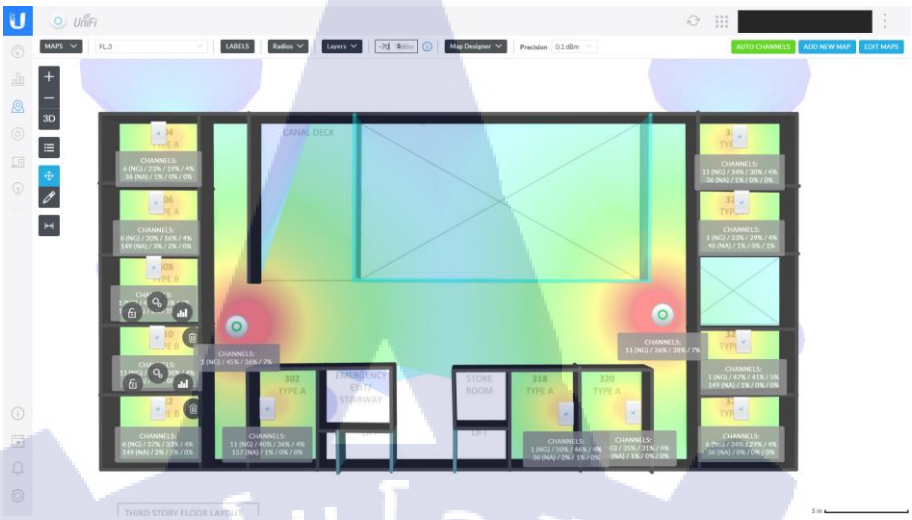
ผลการดำเนินงาน และสรุปผลต่างๆ

4.1 ผลการดำเนินงาน



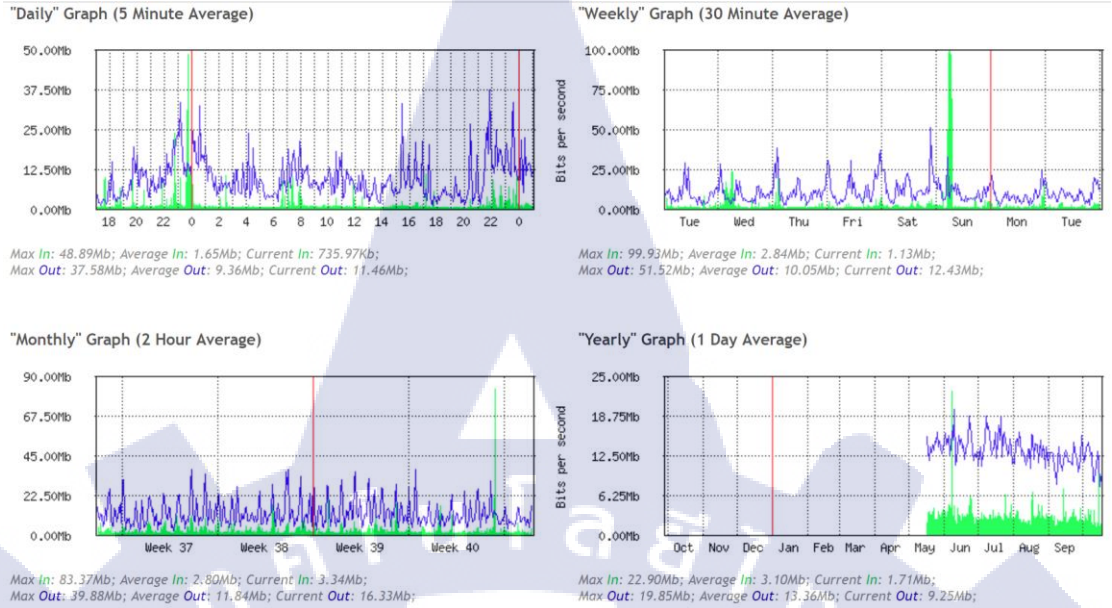
รูปที่ 4.1 New Network Wi-Fi Heat Map RSSI -60 dBm

จากรูปที่ 4.1 จะเห็นได้ว่าหลังได้ติดตั้ง Access Point ไปยังห้องพักทุกห้อง ที่การรับสัญญาณที่ความแรง -60dBm สัญญาณ Wi-Fi สามารถครอบคลุมในบริเวณห้องพักได้ทั้งหมด



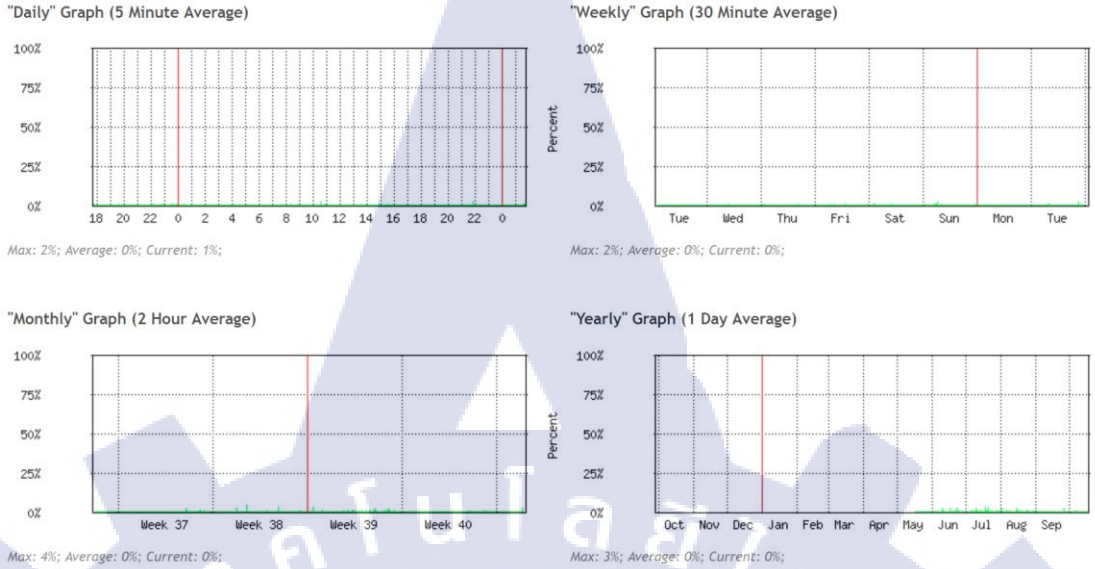
รูปที่ 4.2 New Network Wi-Fi Heat Map RSSI -70 dBm

จากรูปที่ 4.2 จะเห็นได้ว่าหลังได้ติดตั้ง Access Point ไปยังห้องพักทุกห้องที่การรับสัญญาณที่ความแรง -70dBm สัญญาณ Wi-Fi สามารถครอบคลุมในบริเวณห้องพักได้ทั้งหมดและยังสามารถครอบคลุมไปยังบริเวณทางเดินได้อีกด้วย เพื่อช่วยในฟังก์ชั่น Roaming ทำให้ลูกค้าสามารถใช้งานได้อย่างไม่ขาดช่วง



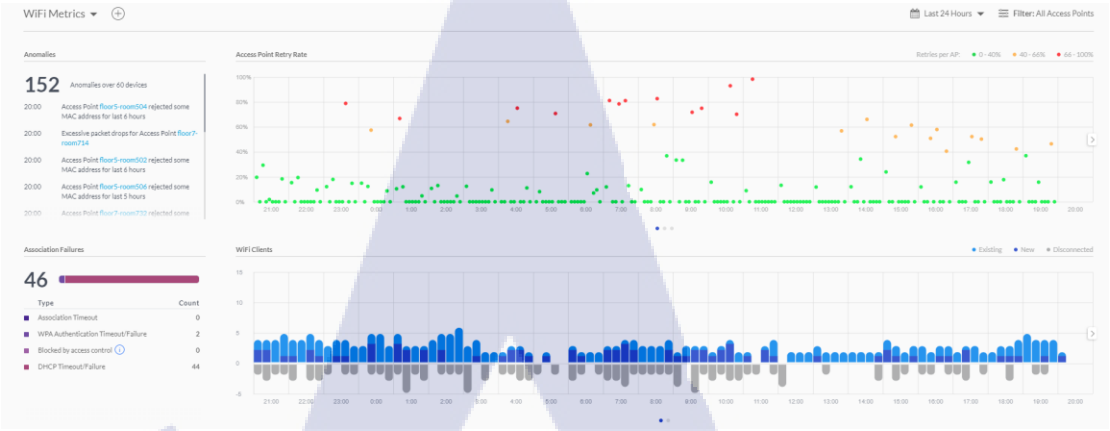
รูปที่ 4.3 Network Statistics

จากรูปที่ 4.3 แสดงให้เห็นถึงปริมาณเฉลี่ยของ Bandwidth ที่ใช้ โดยรวมของทั้งระบบจะเห็นว่าต่อเดือนใช้ Bandwidth 20-40 Mbps และมีบ้างช่วงเท่านั้นที่เห็นว่ามีความต้องการ Bandwidth สูงถึง 100 Mbps ทำให้สามารถปรับแพ็จเกจอินเตอร์เน็ตได้อย่างถูกต้องเพื่อลดค่าใช้จ่ายของทางโรมแรม



รูปที่ 4.4 Gateway CPU Usage

จากภาพที่ 4.4 แสดงให้เห็นว่ามีการใช้ CPU เพียง 4% ทำให้เห็นได้ว่า ตัว Gateway **ยังสามารถรับลูกข่ายและ** Bandwidth ได้อีกในอนาคต



รูปที่ 4.5 Wi-FI Metrics

รูปที่ 4.5 ภาพเป็นการแสดงความผิดปกติต่างๆในการใช้งานระบบ Wi-Fi และแสดงความหนาแน่นของการใช้งาน Access Point แต่ละตัวอีกด้วย

รูปที่ 4.6 Devices

จากรูปที่ 4.6 ภาพเป็นการแสดงสถานของ อุปกรณ์ แต่ละตัวในระบบ และยังสามารถสั่งงานไปยัง อุปกรณ์ ได้จากตรงนี้เลย

บทที่ 5
บทสรุปและข้อเสนอแนะ

5.1 สรุปผลการดำเนินงาน

จากผลการดำเนินงานของโครงการสำเร็จอย่างสมบรูณ์โดยการไปติดตั้งระบบอินเตอร์เน็ตให้กับโรงแรมแห่งหนึ่งเพื่อแก้ปัญหาระบบอินเตอร์เน็ตไม่มีความเสถียรและสัญญาณ Wi-Fi ไม่ครอบคลุม

โครงการที่ได้รับมอบหมายจากทางบริษัทสามารถทำสำเร็จไปได้ด้วยดี อาจจะติดปัญหาระหว่างการดำเนินการ เนื่องจากข้าพเจ้าไม่ชำนาญในการติดตั้งระบบ แต่พี่หัวหน้างานรวมถึงพี่ในบริษัทค่อยให้คำแนะนำและค่อยให้คำปรึกษาในเรื่องการพัฒนาระบบตามที่ได้มอบหมายรวมถึงในการทำงานในระยะเวลาทั้งหมด

จากการปฏิบัติงานตลอดระยะเวลาภายใน 4 เดือนทำให้ได้รับประสบการณ์ในการทำงานจริง ความรู้และทักษะในการติดตั้ง,ออกแบบระบบ สภาพแวดล้อมความมีน้ำใจที่พี่ๆในบริษัทช่วยสอนหรือให้คำปรึกษาในตลอดระยาเวลา 4 เดือน ซึ่งเป็นสิ่งที่ไม่สามารถหาได้ในห้องเรียนและมีประโยชน์อย่างมากในการเข้ารับสหกิจศึกษา

5.2 แนวทางการแก้ไขปัญหา

ในระยะเวลาที่ปฏิบัติงานปัญหาที่พบอยู่คือทักษะในแก้ไขปัญหาทางเทคนิคบางอย่างของข้าพเจ้า ส่งผลให้ต้องพี่หัวหน้างานค่อยอธิบายเป็นรอบที่สองอยู่บ่อยครั้งทำให้ข้าพเจ้าต้อง เรียนรู้มาตรฐานเน็ตเวิร์คและทักษะหรือเทคนิคใหม่ๆในการติดตั้งระบบเน็ตเวิร์ค เมื่อเข้าใจแล้วข้าพเจ้าต้องไปอธิบายให้กับพี่หัวหน้างานเพื่อเป็นการฝึกฝนทักษะซึ่งส่งผลให้สามารถพัฒนาความสามารถและติดตั้งระบบตามที่ได้มอบหมายได้สำเร็จ

5.3 ข้อเสนอแนะจากการดำเนินงาน

ในการดำเนินงานทุกครั้งต้องมีลำดับขั้นตอนที่ชัดเจนและมีการจดบันทึกเสมอเพื่อที่เวลาส่งมอบงานหรือกลับมาแก้ไขระบบที่ติดตั้งไปนั้นสามารถมีข้อมูลที่เพียงพอและทุกงานต้องไม่บกพร่องมาตรฐานเน็ตเวิร์ครวมถึงการออกแบบที่รองรับไปถึงการเติบโตขององค์กรในอนาคตอีกด้วย

เอกสารอ้างอิง

[1] ความหมายของ Computer Network [Online], Available : http://www.mindphp.com/%E0%B8%84%E0%B8%B9%E0%B9%88%E0%B8%A1%E0%B8%B7%E0%B8%AD/73-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3/2221-computer-network-%E0%B8%84%E0%B8%B7%E0%B8%AD%E0%B8%AD%E0%B8%B0%E0%B9%84%E0%B8%A3.html [2018, September 5]

[2] Open System Interconnection [Online], Available : http://netprime-system.com/osi-model-7-layers/ [2018,September 5]

[3] Local Area Network (IEEE 802.3) [Online], Available : http://irrigation.rid.go.th/rid15/ppn/Knowledge/Networks%20Technology/network7.htm [2018, September 5]

[4] Power over Ethernet (IEEE 802.3af/at) [Online], Available : https://www.techtalkthai.com/4-steps-in-choosing-right-poe-and-high-power-poe-plus-switch-by-zyxel/ [2018,September 7].

[5] Wireless Local Area Network (IEEE802.11) [Online], Available : https://th.wikipedia.org/wiki/IEEE_802.11 [2018,September 7]

[6] Software-defined Network [Online], Available : https://www.blognone.com/node/56144 [2018, September 9]

ภาคผนวก ก

รายงานการปฏิบัติงานประจำสัปดาห์ (Weekly Report)

ประวัติผู้จัดทำโครงงาน

ชื่อ – สกุล นายวรชน พนมชน

วัน เดือน ปี เกิด 7 ตุลาคม พ.ศ. 2539

ประวัติการศึกษา

ระดับประถมศึกษา ประถมศึกษาตอนต้น
โรงเรียนสาธิตมหาวิทยาลัยรามคำแหง
ประถมศึกตอนปลาย
โรงเรียนสาธิตมหาวิทยาลัยรามคำแหง

ระดับมัธยมศึกษา มัธยมศึกษาตอนต้น
โรงเรียนสาธิตมหาวิทยาลัยรามคำแหง
มัธยมศึกษาตอนปลาย
โรงเรียนสาธิตมหาวิทยาลัยรามคำแหง

ระดับอุดมศึกษา คณะเทคโนโลยีสารสนเทศ สาขา เทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย – ญี่ปุ่น

ทุนการศึกษา - ไม่มี –

ประวัติการฝึกอบรม

1. MikroTik Certified Network Associate
2. MikroTik Certified User Management Engineer
3.Ubiquiti Enterprise Wireless Admin
4.Draytek Certified Network Admin
5. CCNA Routing and Switching Essentials

ผลงานที่ได้รับการตีพิมพ์ - ไม่มี -