แผนการจัดการเรียนรู้

หลักสูตรประกาศนียบัตรวิชาชีพชั้นสูง พุทธศักราช 2567
สาขาวิชา เทคโนโลยีสารสนเทศ
กลุ่มอาชีพ ซอฟต์แวร์และการประยุกต์
ประเภทวิชา อุตสาหกรรมดิจิทัลและเทคโนโลยีสารสนเทศ

รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย

จัดทำโดย
นายสุรชาติ ลิ้มรัตนพันธ์
ครูผู้สอน

แผนกวิชาเทคโนโลยีสารสนเทศ

ภาคเรียนที่ 1 ปีการศึกษา 2569
วิทยาลัยอาชีวศึกษานครปฐม
สำนักงานคณะกรรมการการอาชีวศึกษา
กระทรวงศึกษาธิการ

คำนำ

แผนการจัดการเรียนรู้รายวิชา ระบบปฏิบัติการเครื่องแม่ข่าย รหัสวิชา 31901-2002 จัดทำขึ้นตามหลักสูตรประกาศนียบัตรวิชาชีพชั้นสูง พุทธศักราช 2567 สาขาวิชาเทคโนโลยีสารสนเทศ โดยมุ่งพัฒนาผู้เรียนให้ติดตั้ง กำหนดค่า ตรวจสอบ และดูแลระบบปฏิบัติการเครื่องแม่ข่าย รวมถึงบริการเครือข่ายและระบบเสมือนได้ตามหลักการและความต้องการของงาน

กิจกรรมการเรียนรู้ยึดการลงมือปฏิบัติบน Ubuntu Server, Proxmox VE และ LXC Container ควบคู่กับการอธิบายหลักการจากสไลรายวิชา ผู้เรียนจะได้ฝึกตั้งแต่เครือข่ายและสายสัญญาณ Linux CLI บริการ DNS/DHCP, Nginx, MariaDB, Node.js, SSH, Firewall, FTP, การนำเว็บขึ้นใช้งาน และการ Clone ระบบจาก GitHub มาติดตั้งบน Server โดยใช้หลักฐานจาก Service, Port, Log, Permission และการทดสอบจาก Client จริง

ผู้จัดทำหวังว่าแผนฉบับนี้จะช่วยให้การจัดการเรียนรู้มีลำดับชัดเจน ผู้เรียนเข้าใจว่าคำสั่งและไฟล์ตั้งค่าแต่ละส่วนส่งผลต่อระบบอย่างไร

สามารถตรวจสอบและแก้ปัญหาอย่างมีเหตุผล พร้อมพัฒนาความรับผิดชอบ ความรอบคอบ การสื่อสาร และการทำงานเป็นทีมสำหรับงานด้านระบบเครื่องแม่ข่าย

ลงชื่อ

(สุรชาติ ลิ้มรัตนพันธ์)

สารบัญ

หน้า

คำนำ ก
สารบัญ ข
หลักสูตรรายวิชา ก
มาตรฐานอาชีพ ข
ตารางวิเคราะห์หน่วยการเรียนรู้ ค
หน่วยการเรียนรู้ จ
ตารางวิเคราะห์พฤติกรรมการเรียนรู้ ฉ
หน่วยที่ 1 เรื่อง/งาน พื้นฐานระบบปฏิบัติการเครื่องแม่ข่าย เครือข่าย และสาย LAN 1
แผนการจัดการเรียนรู้ 1
ใบความรู้ 4
ใบงานที่ 1 6
หน่วยที่ 2 เรื่อง/งาน การติดตั้ง Ubuntu Server คำสั่ง Linux และบริการ DNS/DHCP 7
แผนการจัดการเรียนรู้ 7
ใบความรู้ 10
ใบงานที่ 2 12
หน่วยที่ 3 เรื่อง/งาน การติดตั้ง Web Server, Database และ Node.js Server Stack 13
แผนการจัดการเรียนรู้ 13
ใบความรู้ 16
หน่วยที่ 4 เรื่อง/งาน การจัดการผู้ใช้ SSH เครือข่าย และความปลอดภัย Server 19
แผนการจัดการเรียนรู้ 19
ใบความรู้ 22
ใบงานที่ 4 24
หน่วยที่ 5 เรื่อง/งาน การติดตั้งและทดสอบ FTP Server 25
แผนการจัดการเรียนรู้ 25
ใบความรู้ 28
ใบงานที่ 5 30
หน่วยที่ 6 เรื่อง/งาน Proxmox VE, LXC Container และการนำเว็บขึ้นใช้งาน 31
แผนการจัดการเรียนรู้ 31
ใบความรู้ 34
ใบงานที่ 6 36

หน่วยที่ 7 เรื่อง/งาน การติดตั้ง Git และ Clone ระบบจาก GitHub มารันบน Server 37
แผนการจัดการเรียนรู้ 37
ใบความรู้ 40
ใบงานที่ 7 42

หลักสูตรรายวิชา

หลักสูตร ประกาศนียบัตรวิชาชีพชั้นสูง พุทธศักราช 2567
ประเภทวิชา อุตสาหกรรมดิจิทัลและเทคโนโลยีสารสนเทศ กลุ่มอาชีพ ซอฟต์แวร์และการประยุกต์
รหัส 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย (Network Operating System for Server)
ทฤษฎี 1 ชั่วโมง/สัปดาห์ ปฏิบัติ 4 ชั่วโมง/สัปดาห์ จำนวน 1-4-3 หน่วยกิต

อ้างอิงมาตรฐาน

มาตรฐานอาชีพ รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และมาตรฐานสมรรถนะรายวิชาตามหลักสูตร ปวส. พ.ศ. 2567

ผลลัพธ์การเรียนรู้ระดับรายวิชา

ติดตั้ง กำหนดค่า และสนับสนุนการใช้งานระบบปฏิบัติการเครื่องแม่ข่าย บริการเครือข่าย ระบบเสมือน และเว็บแอปพลิเคชันตามหลักการ โดยปฏิบัติงานด้วยความละเอียดรอบคอบ รับผิดชอบ สื่อสารและทำงานร่วมกับผู้อื่นได้

จุดประสงค์รายวิชา เพื่อให้

1. เข้าใจ NOS, OSI 7 Layer, TCP/IP อุปกรณ์เครือข่าย และหลักการของบริการเครื่องแม่ข่าย
2. มีทักษะติดตั้ง Ubuntu Server, Proxmox VE, LXC และจัดการ User, Permission, SSH, Firewall และ Network Service
3. มีทักษะให้บริการ DNS, DHCP, Web, Database, File, FTP, Proxy, AAA, IoT และ Deploy Web Application อย่างเป็นระบบ
4. มีเจตคติที่ดี ปฏิบัติงานละเอียด รอบคอบ รับผิดชอบ สื่อสาร และทำงานร่วมกับผู้อื่นได้

สมรรถนะรายวิชา

1. แสดงความรู้เกี่ยวกับ NOS, OSI/TCP-IP เครือข่าย Virtualization, Container และบริการ Server ตามหลักการ
2. ติดตั้ง กำหนดค่า ควบคุม และรักษาความปลอดภัยระบบปฏิบัติการเครื่องแม่ข่ายและบริการเครือข่ายได้
3. Deploy ตรวจสอบ แก้ปัญหา สำรองข้อมูล และบูรณาการ Web Application/Server Service ตามโจทย์ได้

คำอธิบายรายวิชา

ศึกษาและปฏิบัติเกี่ยวกับโมเดล OSI 7 Layer และ TCP/IP Protocol ระบบปฏิบัติการบนเครื่องแม่ข่าย การเข้าหัวสาย LAN ตามมาตรฐาน TIA/EIA การติดตั้ง Proxmox Hypervisor การสร้างและจัดการเครื่องเสมือน และ LXC Container การตั้งค่าพื้นฐาน การจัดการผู้ใช้งาน Firewall และ SSH การตรวจสอบระบบเครือข่ายและพอร์ตบริการ การติดตั้ง DNS Server, Web Server, Database Server, DHCP Server และ File and Resource Sharing Server การประยุกต์ Proxy Server, AAA Server,

Container Platform และ IoT Platform ตามความต้องการของระบบ การใช้ SSL Certificate เพื่อปกป้องการสื่อสาร การตั้งค่า Nginx Reverse Proxy และการ Deploy Web Application ด้วย Git, Node.js และ MariaDB ตามแนวคิด DevOps เบื้องต้น

มาตรฐานอาชีพ

หน่วยงานรับรองมาตรฐานอาชีพ สถาบันคุณวุฒิวิชาชีพ (องค์การมหาชน)

มาตรฐานอาชีพ สาขาวิชาชีพเทคโนโลยีสารสนเทศและการสื่อสาร

อาชีพ ช่างสนับสนุนด้านเทคนิค รหัส 40106 ระดับ 5

หน่วยสมรรถนะ		สมรรถนะย่อย		เกณฑ์การปฏิบัติงาน	วิธีประเมิน
รหัส	**คำอธิบาย**	**รหัส**	**คำอธิบาย**		
40106	ช่างสนับสนุนด้านเทคนิค ระดับ 5	NOS-01	อธิบาย NOS, OSI / TCP-IP และเครือข่าย	วิเคราะห์การสื่อสารและจัดทำสาย LAN ได้	แบบทดสอบและตรวจชิ้นงาน
		NOS-02	ติดตั้ง Ubuntu Server และใช้ Linux CLI	ติดตั้งและตั้งค่าพื้นฐานได้	Checklist และปฏิบัติจริง
		NOS-03	ตรวจสอบ DNS และ DHCP	อธิบายและตรวจสอบบริการพื้นฐานได้	สถานการณ์และผลคำสั่ง
		NOS-04	ติดตั้ง Web / Database / Application Server	ติดตั้ง Nginx, MariaDB และ Node.js ได้	ตรวจ Service / Port / Config
		NOS-05	จัดการ User, Permission และ SSH	กำหนดสิทธิ์และเข้าถึงระยะไกลอย่างปลอดภัย	ทดสอบบัญชีและ SSH Key
		NOS-06	ตรวจเครือข่ายและใช้ Firewall	เปิดเฉพาะพอร์ตจำเป็นและยืนยันด้วย Nmap	Firewall Audit
		NOS-07	ให้บริการ FTP	ตั้งค่า vsftpd และส่งไฟล์ผ่าน FileZilla ได้	ทดสอบ Upload / Download
		NOS-08	ติดตั้ง Proxmox VE และสร้าง LXC	จัดการ Hypervisor, Network และ Container ได้	ตรวจ Web GUI / LXC
		NOS-09	Deploy Web Application และ HTTPS	นำเว็บขึ้นใช้ผ่าน Nginx / PM2/SSL ได้	ทดสอบจาก Client

	NOS-10	ติดตั้ง Git และ Clone ระบบจาก GitHub	ดาวน์โหลด Public Repository ลง Server ได้	Git Clone Checklist
	NOS-11	ติดตั้งและเปิดระบบที่ Clone มา	ติดตั้ง Dependencies และเปิดบริการได้	Deployment Checklist

ตารางวิเคราะห์หน่วยการเรียนรู้

ผลลัพธ์การเรียนรู้ระดับรายวิชา (Job) ระบบปฏิบัติการเครื่องแม่ข่าย

งานหลัก (Duty)	**งานย่อย (Task)**	**สมรรถนะย่อย** (มาตราฐานอาชีพ)	**ความรู้ในการปฏิบัติงาน**	**ทักษะในการปฏิบัติงาน**
	1.1 อธิบาย NOS, Client-Server และอุปกรณ์	NOS-01	บทบาท Server/Client/Switch/Router	วิเคราะห์แผนผังเครือข่าย
	1.2 วิเคราะห์ OSI/TCP-IP และ Protocol		Layer, Encapsulation, Port	ติดตามเส้นทางข้อมูล
	1.3 เข้าหัวและทดสอบสาย LAN		UTP, T568A/B, RJ-45	ย้ำหัวและใช้ LAN Tester
	2.1 ติดตั้ง Ubuntu Server	NOS-02/NOS-03	Installation, Directory, User, Network	ติดตั้งและตรวจระบบหลังติดตั้ง
	2.2 ใช้ Linux CLI และตรวจ DNS/DHCP		Command, DORA, DNS Record	จัดการไฟล์และวิเคราะห์ Name/IP
3. Server Stack	3.1 ติดตั้ง Git และ Nginx	NOS-04	Package, Document Root, systemd	สร้างและให้บริการหน้าเว็บ
	3.2 ตั้ง MariaDB, Node.js และ Reverse Proxy		SQL, Runtime, proxy_pass	สร้าง Stack และตรวจ Log

ผลลัพธ์การเรียนรู้ระดับรายวิชา (Job) ระบบปฏิบัติการเครื่องแม่ข่าย

งานหลัก (Duty)	**งานย่อย (Task)**	**สมรรถนะย่อย** (มาตราฐานอาชีพ)	**ความรู้ในการปฏิบัติงาน**	**ทักษะในการปฏิบัติงาน**
	4.1 จัดการ User, Permission และ SSH Key	NOS-06	Least Privilege, chmod/chown, sshd	กำหนดสิทธิ์และ Hardening
	4.2 ตรวจ Port และตั้ง UFW/Nmap		TCP/UDP, Bind, Rule, Scan	วิเคราะห์และลดพอร์ตเปิด

	5.1 ติดตั้ง vsftpd และ Passive Port	NOS-07	Control/Data Connection, Config	สร้างผู้ใช้ โฟลเดอร์ และ Firewall
	5.2 ทดสอบ FileZilla และแก้ปัญหา		Message Log, Listing, Transfer	Upload/Download และวิเคราะห์ Error
6. Proxmox/LXC/Deployment	6.1 ติดตั้ง Proxmox VE และสร้าง LXC	NOS-09	Hypervisor, Bridge, Storage, Template	Provision Container และ Network
	6.2 Deploy Web Application และ HTTPS		Build, Nginx, PM2, TLS	นำเว็บขึ้นใช้และตรวจหลัง Restart

ผลลัพธ์การเรียนรู้ระดับรายวิชา (Job) ระบบปฏิบัติการเครื่องแม่ข่าย

งานหลัก (Duty)	**งานย่อย (Task)**	**สมรรถนะย่อย** (มาตราฐานอาชีพ)	**ความรู้ในการปฏิบัติงาน**	**ทักษะในการปฏิบัติงาน**
	7.1 ติดตั้ง Git และ Clone Public Repository	NOS-11	Git, HTTPS URL, Repository, Clone	ดาวน์โหลดระบบลง Container
	7.2 ติดตั้ง Dependencies และเปิดระบบ		README, package.json, npm, PM2/Nginx	เปิดระบบและตรวจ Process/Port

หน่วยการเรียนรู้

รหัส 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย

ทฤษฎี 1 ชั่วโมง/สัปดาห์ ปฏิบัติ 4 ชั่วโมง/สัปดาห์ จำนวน 1-4-3 หน่วยกิต รวม 15 สัปดาห์ 75 ชั่วโมง

สัดส่วนคะแนน: คะแนนเก็บ/ใบงาน 35 คะแนน สอบปลายภาค 20 คะแนน โครงงาน 15 คะแนน จิตพิสัย 20 คะแนน และสอบปฏิบัติ 10 คะแนน รวม 100 คะแนน

หน่วยที่	**หน่วยการเรียนรู้**	**เวลาเรียน (ชม.)**		
		ทฤษฎี	**ปฏิบัติ**	**รวม**
1	**พื้นฐานระบบปฏิบัติการเครื่องแม่ข่าย เครือข่าย และสาย LAN**	**2**	**3**	**5**
2	**การติดตั้ง Ubuntu Server คำสั่ง Linux และบริการ DNS/DHCP**	**2**	**8**	**10**
3	**การติดตั้ง Web Server, Database และ Node.js Server Stack**	**3**	**12**	**15**
4	**การจัดการผู้ใช้ SSH เครือข่าย และความปลอดภัย Server**	**2**	**8**	**10**
5	**การติดตั้งและทดสอบ FTP Server**	**2**	**8**	**10**

6	Proxmox VE, LXC Container และการนำเว็บขึ้นใช้งาน	2	13	15
7	การติดตั้ง Git และ Clone ระบบจาก GitHub มารันบน Server	2	8	10
รวม		15	60	75

ตารางวิเคราะห์พฤติกรรมการเรียนรู้

รหัส 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย
ทฤษฎี 1 ชั่วโมง/สัปดาห์ ปฏิบัติ 4 ชั่วโมง/สัปดาห์ จำนวน 1-4-3 หน่วยกิต รวม 75 ชั่วโมง

หน่วยการเรียนรู้	ระดับความสามารถที่คาดหวัง				จำนวนชั่วโมง ท/ป	ร้อยละประเมินผล
	พุทธิพิสัย	ทักษะพิสัย	จิตพิสัย	ประยุกต์ใช้		
1. พื้นฐานระบบปฏิบัติการเครื่องแม่ข่าย เครือข่าย และสาย LAN	K2	S2	A2	Ap2	2/3	7
2. การติดตั้ง Ubuntu Server คำสั่ง Linux และบริการ DNS/DHCP	K2	S3	A2	Ap2	2/8	10
3. การติดตั้ง Web Server, Database และ Node.js Server Stack	K3	S3	A3	Ap3	3/12	16
4. การจัดการผู้ใช้ SSH เครือข่าย และความปลอดภัย Server	K3	S3	A3	Ap3	2/8	13
5. การติดตั้งและทดสอบ FTP Server	K3	S3	A3	Ap3	2/8	13
6. Proxmox VE, LXC Container และการนำเว็บขึ้นใช้งาน	K3	S3	A3	Ap3	2/13	18
7. การติดตั้ง Git และ Clone ระบบจาก GitHub มารันบน Server	K3	S3	A3	Ap3	2/8	23
รวมการจัดการเรียนรู้ตลอดภาคเรียน					75	100%

ประเมินผลลัพธ์การเรียนรู้ระดับรายวิชา

ผู้เรียนสามารถติดตั้ง กำหนดค่า และตรวจสอบระบบปฏิบัติการเครื่องแม่ข่าย บริการเครือข่าย ระบบเสมือน และเว็บแอปพลิเคชันบน Ubuntu Server, Proxmox VE และ LXC ได้อย่างเป็นระบบและปลอดภัย โดยจัดการผู้ใช้ สิทธิ์ SSH Firewall Port Service Log การสำรองและกู้คืนข้อมูล พร้อมสื่อสารและทำงานร่วมกับผู้อื่นอย่างรับผิดชอบ

ระดับความสามารถที่คาดหวัง.....วิเคราะห์ให้สอดคล้องจุดประสงค์รายวิชาหรือสูงกว่า

พุทธิพิสัย	ทักษะพิสัย	จิตพิสัย
K1 = ความรู้ ความจำ	S1 = เลียนแบบ	A1 = รับรู้
K2 = ความเข้าใจ	S2 = ทำได้ตามแบบ	A2 = ตอบสนอง
	S3 = ทำได้ถูกต้อง	A3 = การสร้างคุณค่า
K3 = การนำไปใช้	S4 = ทำได้อย่างต่อเนื่อง	A4 = จัดระบบคุณค่านิยม
K4 = การวิเคราะห์		
K5 = การประเมินค่า	S5 = ทำได้อย่างเป็นธรรมชาติ	A5 = การสร้างลักษณะนิสัย
K6 = การสร้างสรรค์		
<u>หมายเหตุ</u> ใส่ได้มากกว่า 1 ระดับ	<u>หมายเหตุ</u> ใส่ระดับที่คาดหวังระดับเดียว	<u>หมายเหตุ</u> ใส่ระดับที่คาดหวังระดับเดียว

ด้านความสามารถประยุกต์ใช้และรับผิดชอบ

Ap1 = สามารถปฏิบัติงานตามแบบแผนที่กำหนด

Ap2 = สามารถปฏิบัติงานตามแบบแผน และปรับตัวภายใต้ความเปลี่ยนแปลงที่ไม่ซับซ้อน

Ap3 = สามารถวางแผนการปฏิบัติงานที่ได้รับมอบหมายและแก้ไขปัญหาการปฏิบัติงานที่ไม่อยู่ภายใต้การควบคุมในบางเรื่อง โดยประยุกต์ใช้ความรู้ ทักษะทางวิชาชีพ เทคโนโลยีสารสนเทศและการสื่อสาร

Ap4 = สามารถวางแผนการปฏิบัติงานที่รับผิดชอบ ปรับตัวและแก้ไขปัญหาการปฏิบัติงานที่ไม่คุ้นเคยหรือซับซ้อนและเป็นนามธรรม โดยประยุกต์ใช้ความรู้ ทักษะทางวิชาชีพ เทคโนโลยีสารสนเทศและการสื่อสาร

Ap5 = สามารถประยุกต์ใช้ความรู้ ทักษะทางวิชาชีพ เทคโนโลยีสารสนเทศและการสื่อสารในการวางแผนแก้ไขปัญหาและพัฒนานวัตกรรมตามสายอาชีพ

<u>หมายเหตุ</u> ใส่ระดับที่คาดหวังระดับเดียว

2

	แผนการจัดการเรียนรู้	หน่วยที่ 1
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 1
	ชื่อหน่วยการเรียนรู้ พื้นฐานระบบปฏิบัติการเครื่องแม่ข่าย เครือข่าย และสาย LAN	ทฤษฎี 2 ชม. ปฏิบัติ 3 ชม.
ชื่อเรื่อง/งาน NOS, OSI/TCP-IP, อุปกรณ์เครือข่าย และการเข้าหัว RJ-45		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนอธิบายบทบาทของระบบปฏิบัติการเครื่องแม่ข่าย อุปกรณ์เครือข่าย และการไหลของข้อมูลตามโมเดล OSI/TCP-IP พร้อมเข้าหัวสาย UTP ตามมาตรฐาน T568A/T568B และทดสอบสายด้วย LAN Tester ได้ถูกต้อง

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: อธิบายความสัมพันธ์ของ Server, Client, Protocol และ OSI ได้ถูกต้องไม่น้อยกว่าร้อยละ 70 และสาย LAN ที่จัดทำต้องเรียงพินครบ 1-8 โดยเครื่องทดสอบไม่พบสายขาดหรือสลับคู่

2) วิธีประเมิน: แบบทดสอบความรู้ การสังเกตระหว่างปฏิบัติ และการตรวจชิ้นงานสาย LAN รายบุคคล

3) หลักฐานการปฏิบัติงาน (Performance Evidence): ใบงานที่ 1 แผนผังการสื่อสารเครือข่าย และสาย LAN ที่ผ่านการทดสอบ

4) หลักฐานความรู้ (Knowledge Evidence): แบบสรุปหน้าที่ OSI 7 Layer อุปกรณ์เครือข่าย และมาตรฐานสีสาย T568A/T568B

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงานช่างสนับสนุนด้านเทคนิคที่ต้องติดตั้งและตรวจสอบโครงสร้างพื้นฐานเครือข่ายก่อนให้บริการ Server

3. สมรรถนะประจำหน่วย

3.1 อธิบายความหมายและหน้าที่ของ Network Operating System ได้

3.2 จำแนกบทบาท Server, Client, Switch, Router, Gateway และ Access Point ได้

3.3 อธิบายหน้าที่ของ OSI 7 Layer และ TCP/IP Protocol ได้

3.4 วิเคราะห์การ Encapsulation และ De-encapsulation ของข้อมูลได้

3.5 เข้าหัวและทดสอบสาย UTP ตามมาตรฐานได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบายความแตกต่างระหว่างระบบปฏิบัติการทั่วไปกับระบบปฏิบัติการเครื่องแม่ข่ายได้

4.2 ระบุหน้าที่ของอุปกรณ์เครือข่ายจากสถานการณ์ที่กำหนดได้

4.3 เรียงลำดับ OSI 7 Layer และยกตัวอย่าง Protocol ที่เกี่ยวข้องได้

4.4 อธิบายเส้นทางข้อมูลจากเครื่อง Client ไปยัง Server ได้

4.5 บอกความแตกต่างของ T568A และ T568B ได้

4.6 เข้าหัว RJ-45 และตรวจสอบผลด้วย LAN Tester ได้

4.7 ปฏิบัติงานอย่างเป็นระเบียบและดูแลเครื่องมือร่วมกันได้

5. สาระการเรียนรู้

ความหมายและบทบาทของ Network Operating System, โครงสร้าง Client-Server, อุปกรณ์เครือข่าย, OSI 7 Layer, TCP/IP, Protocol และ Port, การ Encapsulation, โครงสร้างสาย UTP, มาตรฐาน T568A/T568B, Straight-Through/Crossover และขั้นตอนเข้าหัว RJ-45

6. กิจกรรมการเรียนรู้

6.1 ครูใช้ภาพเครือข่ายใกล้ตัวตั้งคำถามว่าอุปกรณ์ใดทำหน้าที่เป็น Server, Client และตัวกลางสื่อสาร

6.2 ครูอธิบาย NOS อุปกรณ์เครือข่าย และสาธิต Animation การเดินทางของข้อมูลผ่าน OSI 7 Layer

6.3 ผู้เรียนจับคู่ Protocol, Port และอุปกรณ์กับ Layer แล้วร่วมกันอธิบายเหตุผล

6.4 ครูสาธิตการปอกสาย เรียงสี ตัดปลาย และย้ำหัว RJ-45 ตามมาตรฐาน T568B

6.5 ผู้เรียนเข้าหัวสายรายบุคคลและทดสอบลำดับพิน 1-8 ด้วย LAN Tester พร้อมแก้ไขเมื่อพบข้อผิดพลาด

6.6 ผู้เรียนสรุปสิงที่ค้นพบในใบงานและเชื่อมโยงว่าสายสัญญาณมีผลต่อการเข้าถึง Server อย่างไร

7. สื่อและแหล่งการเรียนรู้

7.1 สไลรายวิชาสัปดาห์ที่ 1 เรื่อง NOS, อุปกรณ์เครือข่าย และ OSI Model

7.2 สาย UTP, หัว RJ-45, คีมย้ำหัว, อุปกรณ์ปอกสาย และ LAN Tester

7.3 แผนผังเครือข่ายตัวอย่าง ใบความรู้ที่ 1 และใบงานที่ 1

8. หลักฐานการเรียนรู้

8.1 หลักฐานความรู้

แบบสรุปหน้าที่ OSI 7 Layer อุปกรณ์เครือข่าย และมาตรฐานสีสาย T568A/T568B

8.2 หลักฐานการปฏิบัติงาน

ใบงานที่ 1 แผนผังการสื่อสารเครือข่าย และสาย LAN ที่ผ่านการทดสอบ

9. การวัดและประเมินผล

9.1 เกณฑ์การปฏิบัติงาน

ตอบคำถามหลักได้อย่างน้อยร้อยละ 70 ระบุอุปกรณ์และ Layer ได้ถูกต้อง และชิ้นงานสาย LAN ใช้งานได้จริง

9.2 วิธีการประเมิน

ตรวจแบบทดสอบ ตรวจใบงาน สังเกตขั้นตอนการใช้เครื่องมือ และทดสอบสายต่อหน้าครู

9.3 เครื่องมือประเมิน

แบบทดสอบ แบบตรวจใบงาน แบบสังเกตการปฏิบัติ และ LAN Tester

10. บันทึกผลหลังการจัดการเรียนรู้

10.1 ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

10.2 ปัญหา อุปสรรคที่พบ

10.3 การแก้ไขปัญหา

1) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

2) แนวทางแก้ปัญหาในครั้งต่อไป

	ใบความรู้ที่ 1	หน่วยที่ 1
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 1
	ชื่อหน่วยการเรียนรู้ พื้นฐานระบบปฏิบัติการเครื่องแม่ข่าย เครือข่าย และสาย LAN	ทฤษฎี 2 ชม. ปฏิบัติ 3 ชม.
ชื่อเรื่อง/งาน NOS, OSI/TCP-IP, อุปกรณ์เครือข่าย และการเข้าหัว RJ-45		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนอธิบายบทบาทของระบบปฏิบัติการเครื่องแม่ข่าย อุปกรณ์เครือข่าย และการไหลของข้อมูลตามโมเดล OSI/TCP-IP พร้อมเข้าหัวสาย

UTP ตามมาตรฐาน T568A/T568B และทดสอบสายด้วย LAN Tester ได้ถูกต้อง

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: อธิบายความสัมพันธ์ของ Server, Client, Protocol และ OSI ได้ถูกต้องไม่น้อยกว่าร้อยละ 70 และสาย LAN ที่จัดทำต้องเรียงพินครบ 1-8 โดยเครื่องทดสอบไม่พบสายขาดหรือสลับคู่

2) วิธีประเมิน: แบบทดสอบความรู้ การสังเกตระหว่างปฏิบัติ และการตรวจชิ้นงานสาย LAN รายบุคคล

3) หลักฐานการปฏิบัติงาน (Performance Evidence): ใบงานที่ 1 แผนผังการสื่อสารเครือข่าย และสาย LAN ที่ผ่านการทดสอบ

4) หลักฐานความรู้ (Knowledge Evidence): แบบสรุปหน้าที่ OSI 7 Layer อุปกรณ์เครือข่าย และมาตรฐานสีสาย T568A/T568B

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงานช่างสนับสนุนด้านเทคนิคที่ต้องติดตั้งและตรวจสอบโครงสร้างพื้นฐานเครือข่ายก่อนให้บริการ Server

3. สมรรถนะประจำหน่วย

3.1 อธิบายความหมายและหน้าที่ของ Network Operating System ได้

3.2 จำแนกบทบาท Server, Client, Switch, Router, Gateway และ Access Point ได้

3.3 อธิบายหน้าที่ของ OSI 7 Layer และ TCP/IP Protocol ได้

3.4 วิเคราะห์การ Encapsulation และ De-encapsulation ของข้อมูลได้

3.5 เข้าหัวและทดสอบสาย UTP ตามมาตรฐานได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบายความแตกต่างระหว่างระบบปฏิบัติการทั่วไปกับระบบปฏิบัติการเครื่องแม่ข่ายได้

4.2 ระบุหน้าที่ของอุปกรณ์เครือข่ายจากสถานการณ์ที่กำหนดได้

4.3 เรียงลำดับ OSI 7 Layer และยกตัวอย่าง Protocol ที่เกี่ยวข้องได้

4.4 อธิบายเส้นทางข้อมูลจากเครื่อง Client ไปยัง Server ได้

4.5 บอกความแตกต่างของ T568A และ T568B ได้

4.6 เข้าหัว RJ-45 และตรวจสอบผลด้วย LAN Tester ได้

4.7 ปฏิบัติงานอย่างเป็นระเบียบและดูแลเครื่องมือร่วมกันได้

5. เนื้อหาสาระ

5.1 ระบบปฏิบัติการเครื่องแม่ข่ายและโครงสร้าง Client-Server

Network Operating System คือระบบปฏิบัติการที่ออกแบบเพื่อให้บริการผู้ใช้หลายคนและควบคุมทรัพยากรเครือข่าย เช่น Web, Database, File และ DNS Server โดย Client เป็นฝ่ายร้องขอและ Server เป็นฝ่ายประมวลผลคำขอ ตอบกลับ และบันทึกเหตุการณ์ของระบบ

5.2 อุปกรณ์เครือข่ายและหน้าที่

Switch เชื่อมอุปกรณ์ภายใน LAN, Router เชื่อมคนละเครือข่าย, Gateway เป็นทางออกของเครือข่าย และ Access Point เชื่อมอุปกรณ์ไร้สาย การเลือกและต่ออุปกรณ์ผิดตำแหน่งทำให้ Client ไปไม่ถึง Server แม้บริการจะทำงานอยู่ก็ตาม

5.3 OSI 7 Layer, TCP/IP และการเดินทางของข้อมูล

OSI แบ่งการสื่อสารเป็น 7 ชั้นเพื่อช่วยออกแบบและแก้ปัญหา ข้อมูลจาก Application จะถูกเติมข้อมูลควบคุมลงทีละชั้นเรียกว่า Encapsulation แล้วส่งผ่านสื่อ เมื่อถึงปลายทางจะถอดข้อมูลย้อนกลับ เรียกว่า De-encapsulation การวิเคราะห์ทีละ Layer ช่วยหาว่าปัญหาเกิดที่สาย IP Port หรือ Application

5.4 สาย UTP มาตรฐาน T568A/T568B และการเข้าหัว RJ-45

สาย UTP มีลวดทองแดง 4 คู่เพื่อลดสัญญาณรบกวน มาตรฐาน T568A และ T568B กำหนดลำดับสีที่พิน 1-8 งานทั่วไปนิยมสาย Straight-Through ที่ปลายทั้งสองใช้มาตรฐานเดียวกัน หลังย้ำหัวต้องใช้ LAN Tester ตรวจสายขาด สายสลับ และคู่สายผิดก่อนนำไปใช้งาน

6. แบบฝึกหัด/แบบทดสอบ

6.1 อธิบายว่าเหตุใดการแก้ปัญหาเครือข่ายจึงควรตรวจจาก Physical Layer ขึ้นไป

6.2 จับคู่ Switch, Router, Gateway และ Access Point กับหน้าที่ที่ถูกต้อง

6.3 เขียนลำดับสี T568B และปฏิบัติการเข้าหัวสายพร้อมบันทึกผล LAN Tester

7. เอกสารอ้างอิง

สำนักงานคณะกรรมการการอาชีวศึกษา. หลักสูตร ปวส. พ.ศ. 2567; Cisco Networking Academy. Networking Basics; สไลรายวิชา สัปดาห์ที่ 1

8. ภาคผนวก (เฉลยแบบฝึกหัด เฉลยแบบทดสอบ ฯ)

8.1 แนวคำตอบ: เริ่มจากสายและสัญญาณ เพราะหาก Layer ล่างไม่ทำงาน Layer บนจะสื่อสารไม่ได้

8.2 แนวคำตอบ: Switch เชื่อม LAN, Router เชื่อมเครือข่าย, Gateway เป็นทางออก, AP ให้บริการไร้สาย

8.3 ประเมินจากความถูกต้องของลำดับสี ขั้นตอนย้ำหัว และผลทดสอบพิน 1-8

	แผนการจัดการเรียนรู้	**หน่วยที่ 2**
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	**สอนครั้งที่** 2-3
	ชื่อหน่วยการเรียนรู้ การติดตั้ง Ubuntu Server คำสั่ง Linux และบริการ DNS/DHCP	ทฤษฎี 2 ชม. ปฏิบัติ 8 ชม.
ชื่อเรื่อง/งาน Ubuntu Server, Linux CLI, DNS และ DHCP Fundamentals		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนติดตั้งและตั้งค่า Ubuntu Server ใช้คำสั่ง Linux จัดการไฟล์ แพ็กเกจ และเครือข่าย พร้อมอธิบายและตรวจสอบการทำงานของ DNS และ DHCP ได้ตามหลักการ

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: ติดตั้งระบบจนเข้าสู่ระบบได้ ใช้คำสั่งตามภารกิจได้ไม่น้อยกว่าร้อยละ 80 และวิเคราะห์ขั้นตอน DHCP

DORA กับ DNS Record ได้ถูกต้อง

2) วิธีประเมิน: ตรวจ Checklist การติดตั้ง สังเกตการใช้คำสั่ง ตรวจผลลัพธ์บน Terminal และแบบทดสอบสถานการณ์ DNS/DHCP

3) หลักฐานการปฏิบัติงาน (Performance Evidence): Ubuntu Server ที่พร้อมใช้งาน ภาพผลคำสั่ง ใบงาน CLI และแผนภาพ DHCP/DNS

4) หลักฐานความรู้ (Knowledge Evidence): บันทึกโครงสร้าง Directory คำสั่งพื้นฐาน ขั้นตอน DORA และหน้าที่ของ DNS Record

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงานติดตั้งระบบปฏิบัติการและตรวจสอบบริการเครือข่ายของช่างสนับสนุนด้านเทคนิค

3. สมรรถนะประจำหน่วย

3.1 เตรียมสื่อและติดตั้ง Ubuntu Server ตามขั้นตอนได้

3.2 อธิบายโครงสร้าง Directory และสิทธิ์ผู้ใช้ Linux ได้

3.3 ใช้คำสั่งจัดการไฟล์ ไดเรกทอรี และแพ็กเกจได้

3.4 ตรวจสอบ IP Address, Route, DNS และสถานะ Service ได้

3.5 อธิบายหลักการ DHCP DORA และ DNS Record ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบายความแตกต่างระหว่าง GUI และ CLI สำหรับงาน Server ได้

4.2 ติดตั้ง Ubuntu Server และกำหนดค่าเครือข่ายเบื้องต้นได้

4.3 ใช้ pwd, ls, cd, mkdir, touch, cp, mv, rm และ nano ได้ถูกต้อง

4.4 ใช้ apt และ systemctl เพื่อติดตั้งและตรวจสอบบริการได้

4.5 ใช้ ip a, ip route, ping และคำสั่งตรวจสอบชื่อเครื่องได้

4.6 อธิบาย DHCP DORA และจำแนก A, CNAME, MX, TXT Record ได้

4.7 บันทึกคำสั่งและผลการทดลองอย่างเป็นระบบได้

5. สาระการเรียนรู้

สถาปัตยกรรม Linux, GUI/CLI, Root และผู้ใช้ทั่วไป, โครงสร้าง Directory, Absolute/Relative Path, คำสั่งจัดการไฟล์และแพ็กเกจ, systemd, การตั้งค่าเครือข่ายเบื้องต้น, DHCP DORA, Scope, Lease, Reservation, DNS Recursive/Authoritative และ DNS Record

6. กิจกรรมการเรียนรู้

6.1 ครูทบทวนองค์ประกอบเครื่อง Server และอธิบายเหตุผลที่งานดูแลระบบนิยมใช้ Linux CLI

6.2 ครูสาธิตขั้นตอนติดตั้ง Ubuntu Server และจุดที่ต้องตรวจ เช่น Disk, User, Hostname และ Network

6.3 ผู้เรียนติดตั้งหรือเปิด Ubuntu Server ของตนเอง แล้วทำภารกิจสำรวจ Directory และเส้นทางไฟล์

6.4 ผู้เรียนปฏิบัติคำสั่งจัดการไฟล์ แก้ไขไฟล์ด้วย nano อัปเดตแพ็กเกจ และตรวจสถานะระบบ

6.5 ครูใช้แผนภาพ/Animation อธิบาย DHCP DORA และการถามตอบชื่อโดเมนของ DNS จากนั้นให้ผู้เรียนจำลองลำดับเหตุการณ์

6.6 ผู้เรียนตรวจ IP, Route และ DNS สรุปผลลงใบงาน พร้อมอธิบายว่าควรตรวจจุดใดเมื่อเข้าเว็บไซต์ไม่ได้

7. สื่อและแหล่งการเรียนรู้

7.1 สไลด์สัปดาห์ที่ 2-3 เรื่อง Ubuntu Server, Linux CLI, DHCP และ DNS

7.2 Ubuntu Server ISO, เครื่อง Server/VM/LXC, Terminal และ Network Diagram

7.3 ใบความรู้ที่ 2 ใบงานคำสั่ง Linux และแบบจำลอง DHCP/DNS

8. หลักฐานการเรียนรู้

8.1 หลักฐานความรู้

บันทึกโครงสร้าง Directory คำสั่งพื้นฐาน ขั้นตอน DORA และหน้าที่ของ DNS Record

8.2 หลักฐานการปฏิบัติงาน

Ubuntu Server ที่พร้อมใช้งาน ภาพผลคำสั่ง ใบงาน CLI และแผนภาพ DHCP/DNS

9. การวัดและประเมินผล

9.1 เกณฑ์การปฏิบัติงาน

ติดตั้งและบูตระบบสำเร็จ ทำภารกิจคำสั่งครบอย่างน้อยร้อยละ 80 และอธิบาย DHCP/DNS จากสถานการณ์ได้

9.2 วิธีการประเมิน

ตรวจระบบจริง ตรวจประวัติคำสั่งและผลลัพธ์ สอบถามเหตุผล และตรวจใบงานรายบุคคล

9.3 เครื่องมือประเมิน

Installation Checklist, Command Checklist, แบบทดสอบ และแบบประเมินความรับผิดชอบ

10. บันทึกผลหลังการจัดการเรียนรู้

10.1 ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

10.2 ปัญหา อุปสรรคที่พบ

10.3 การแก้ไขปัญหา

1) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

2) แนวทางแก้ปัญหาในครั้งต่อไป

	ใบความรู้ที่ 2	หน่วยที่ 2
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 2-3
	ชื่อหน่วยการเรียนรู้ การติดตั้ง Ubuntu Server คำสั่ง Linux และบริการ DNS/DHCP	ทฤษฎี 2 ชม. ปฏิบัติ 8 ชม.
ชื่อเรื่อง/งาน Ubuntu Server, Linux CLI, DNS และ DHCP Fundamentals		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนติดตั้งและตั้งค่า Ubuntu Server ใช้คำสั่ง Linux จัดการไฟล์ แพ็กเกจ และเครือข่าย พร้อมอธิบายและตรวจสอบการทำงานของ DNS และ DHCP ได้ตามหลักการ

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: ติดตั้งระบบจนเข้าสู่ระบบได้ ใช้คำสั่งตามภารกิจได้ไม่น้อยกว่าร้อยละ 80 และวิเคราะห์ขั้นตอน DHCP DORA กับ DNS Record ได้ถูกต้อง

2) วิธีประเมิน: ตรวจ Checklist การติดตั้ง สังเกตการใช้คำสั่ง ตรวจผลลัพธ์บน Terminal และแบบทดสอบสถานการณ์ DNS/DHCP

3) หลักฐานการปฏิบัติงาน (Performance Evidence): Ubuntu Server ที่พร้อมใช้งาน ภาพผลคำสั่ง ใบงาน CLI และแผนภาพ DHCP/DNS

4) หลักฐานความรู้ (Knowledge Evidence): บันทึกโครงสร้าง Directory คำสั่งพื้นฐาน ขั้นตอน DORA และหน้าที่ของ DNS Record

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงานติดตั้งระบบปฏิบัติการและตรวจสอบบริการเครือข่ายของช่างสนับสนุนด้านเทคนิค

3. สมรรถนะประจำหน่วย

3.1 เตรียมสื่อและติดตั้ง Ubuntu Server ตามขั้นตอนได้

3.2 อธิบายโครงสร้าง Directory และสิทธิ์ผู้ใช้ Linux ได้

3.3 ใช้คำสั่งจัดการไฟล์ ไดเรกทอรี และแพ็กเกจได้

3.4 ตรวจสอบ IP Address, Route, DNS และสถานะ Service ได้

3.5 อธิบายหลักการ DHCP DORA และ DNS Record ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบายความแตกต่างระหว่าง GUI และ CLI สำหรับงาน Server ได้

4.2 ติดตั้ง Ubuntu Server และกำหนดค่าเครือข่ายเบื้องต้นได้

4.3 ใช้ pwd, ls, cd, mkdir, touch, cp, mv, rm และ nano ได้ถูกต้อง

4.4 ใช้ apt และ systemctl เพื่อติดตั้งและตรวจสอบบริการได้

4.5 ใช้ ip a, ip route, ping และคำสั่งตรวจสอบชื่อเครื่องได้

4.6 อธิบาย DHCP DORA และจำแนก A, CNAME, MX, TXT Record ได้

4.7 บันทึกคำสั่งและผลการทดลองอย่างเป็นระบบได้

5. เนื้อหาสาระ

5.1 Linux และการติดตั้ง Ubuntu Server

Linux เป็นระบบปฏิบัติการที่เหมาะกับ Server เพราะเสถียร จัดการจากระยะไกลได้ และมีระบบแพ็กเกจที่ชัดเจน การติดตั้งต้องเตรียม ISO เลือกภาษา คีย์บอร์ด Network Storage สร้างผู้ใช้และตั้ง Hostname ให้สื่อความหมาย หลังติดตั้งควรอัปเดตรายการแพ็กเกจและตรวจ IP ก่อนเริ่มติดตั้งบริการ

5.2 โครงสร้างคำสั่ง Linux และการจัดการไฟล์

คำสั่ง Linux มีรูปแบบ command option argument ตัวอย่าง ls -la /etc คำสั่งสำคัญ ได้แก่ pwd, ls, cd, mkdir, touch, cp, mv, rm และ nano เส้นทางที่ขึ้นต้นด้วย / เป็น Absolute Path ส่วน Relative Path อ้างอิงจากตำแหน่งปัจจุบัน การใช้ sudo หมายถึงการขอสิทธิ์ผู้ดูแลเฉพาะคำสั่งที่จำเป็น

5.3 แพ็กเกจ บริการ และการตรวจสอบเครือข่าย

ใช้ sudo apt update เพื่ออ่านรายการแพ็กเกจล่าสุด และ apt install เพื่อติดตั้งโปรแกรม บริการส่วนใหญ่ควบคุมด้วย systemctl start, stop, restart, enable และ status ตรวจเครือข่ายด้วย ip a, ip route, ping และ hostname -I โดยต้องอ่านผลลัพธ์ ไม่ตัดสินจากข้อความเพียงบรรทัดเดียว

5.4 DHCP และ DNS

DHCP แจกค่า IP, Subnet Mask, Gateway และ DNS อัตโนมัติผ่าน Discover, Offer, Request, Acknowledge หรือ DORA ส่วน DNS แปลงชื่อเป็น IP Recursive DNS ช่วยค้นหาคำตอบ ขณะที่ Authoritative DNS เก็บข้อมูลจริง Record ที่พบบ่อยคือ A, CNAME, MX และ TXT การเข้าเว็บได้ต้องอาศัยทั้ง IP Route และ DNS ทำงานร่วมกัน

6. แบบฝึกหัด/แบบทดสอบ

6.1 เขียนคำสั่งสร้าง /home/student/lab2 และไฟล์ note.txt จากนั้นแสดงตำแหน่งปัจจุบัน

6.2 เรียงลำดับขั้นตอน DHCP DORA พร้อมอธิบายข้อมูลที่ Client ได้รับ

6.3 วิเคราะห์กรณี ping IP ได้แต่เปิดชื่อเว็บไซต์ไม่ได้ว่าควรตรวจส่วนใดและใช้คำสั่งอะไร

7. เอกสารอ้างอิง

Ubuntu Server Documentation; man pages ของคำสั่ง Linux; ISC DHCP Documentation; Cloudflare Learning Center: DNS; สไลด์สัปดาห์ที่ 2-3

8. ภาคผนวก (เฉลยแบบฝึกหัด เฉลยแบบทดสอบ ฯ)

8.1 ตัวอย่าง: mkdir -p /home/student/lab2, cd /home/student/lab2, touch note.txt, pwd และ ls -l

8.2 Discover ขอผู้ให้บริการ, Offer เสนอค่า, Request เลือกค่า, Acknowledge ยืนยัน Lease

8.3 ควรตรวจ DNS Server และ Name Resolution ด้วย resolvectl, nslookup หรือ dig พร้อมตรวจ /etc/resolv.conf

-
-
-

	แผนการจัดการเรียนรู้	หน่วยที่ 3
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 4-6
	ชื่อหน่วยการเรียนรู้ การติดตั้ง Web Server, Database และ Node.js Server Stack	ทฤษฎี 3 ชม. ปฏิบัติ 12 ชม.
ชื่อเรื่อง/งาน Git, Nginx, MariaDB, Node.js และ Nginx Reverse Proxy		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนติดตั้งและกำหนดค่า Git, Nginx, MariaDB และ Node.js บน Ubuntu Server สร้างฐานข้อมูลและเว็บแอปพลิเคชันเบื้องต้น พร้อมตั้งค่า Nginx Reverse Proxy และตรวจสอบบริการได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: บริการทุกตัวต้องทำงานหลัง Restart ระบบ หน้าเว็บต้องเข้าจากเครื่องอื่นได้ ฐานข้อมูลใช้บัญชีที่กำหนดสิทธิ์เฉพาะงาน และ Reverse Proxy ส่งคำขอไปยัง Node.js ได้

2) วิธีประเมิน: ตรวจสถานะ Service, Port, Config และผลการเข้าถึงจาก Client พร้อมประเมินการอธิบายหน้าที่ของแต่ละส่วน

3) หลักฐานการปฏิบัติงาน (Performance Evidence): หน้าเว็บบน Nginx ฐานข้อมูล/ตารางตัวอย่าง Node.js Application และไฟล์ Nginx Site Configuration

4) หลักฐานความรู้ (Knowledge Evidence): แผนผัง Server Stack บันทึกคำสั่งติดตั้ง และคำอธิบายเส้นทาง Request จาก Client ถึง Application/Database

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงาน Web/Database Server และการ Deploy Web Application ตามแนวคิด DevOps เบื้องต้น

3. สมรรถนะประจำหน่วย

3.1 ติดตั้งและควบคุม Nginx Web Server ได้

3.2 สร้างฐานข้อมูล ผู้ใช้ และกำหนดสิทธิ์ MariaDB ได้

3.3 ติดตั้ง Node.js และรัน HTTP Application ได้

3.4 ใช้ Git นำ Source Code มายัง Server ได้

3.5 ตั้งค่า Nginx Reverse Proxy และวิเคราะห์ Log ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบายบทบาทของ Nginx, MariaDB, Node.js และ Git ใน Server Stack ได้

4.2 ติดตั้ง Nginx และแก้ไข Document Root ได้

4.3 ใช้ systemctl และ nginx -t เพื่อตรวจสอบบริการและไฟล์ตั้งค่าได้

4.4 สร้าง Database, Table และ User ที่มีสิทธิ์เหมาะสมได้

4.5 สร้างและรัน Node.js HTTP Server ได้

-

-

4.6 ตั้งค่า proxy_pass และทดสอบจาก Client ได้

4.7 เก็บหลักฐานและอธิบายปัญหาที่พบระหว่าง Deploy ได้

5. สาระการเรียนรู้

บทบาทของ Server Stack, การติดตั้ง Git/Nginx/MariaDB/Node.js, Document Root และ Virtual Host, SQL เบื้องต้นและหลักสิทธิ์ขั้นต่ำ, Node.js HTTP Server, npm, Nginx Reverse Proxy, systemctl, Port และ Log

6. กิจกรรมการเรียนรู้

6.1 ครูใช้แผนภาพอธิบายเส้นทางคำขอจาก Browser ผ่าน Nginx ไปยัง Node.js และ MariaDB

6.2 ผู้เรียนติดตั้ง Git และ Nginx ตรวจหน้าเริ่มต้น แล้วแก้ไขหน้า HTML ให้แสดงชื่อ Server ของตนเอง

6.3 ครูสาธิตการสร้าง Database, User และ Grant เฉพาะฐานข้อมูล จากนั้นผู้เรียนสร้างตารางและเพิ่มข้อมูลตัวอย่าง

6.4 ผู้เรียนติดตั้ง Node.js สร้าง HTTP Server และตรวจว่ากำลังฟังพอร์ตใดด้วย ss -tulpn

6.5 ครูสาธิต Nginx Reverse Proxy ผู้เรียนสร้าง Site Configuration ตรวจด้วย nginx -t และ Reload

6.6 ผู้เรียนทดสอบจากเครื่อง Client อ่าน Access/Error Log และจัดทำแผนผังพร้อมหลักฐานการทำงานของทั้ง Stack

7. สื่อและแหล่งการเรียนรู้

7.1 สไลเรื่อง Nginx, MariaDB, Node.js, Git และ Reverse Proxy

7.2 Ubuntu Server/LXC, Web Browser, Terminal และ Source Code ตัวอย่าง

7.3 ใบความรู้ที่ 3 ใบงาน Server Stack และแผนผัง Request Flow

8. หลักฐานการเรียนรู้

8.1 หลักฐานความรู้

แผนผัง Server Stack บันทึกคำสั่งติดตั้ง และคำอธิบายเส้นทาง Request จาก Client ถึง Application/Database

8.2 หลักฐานการปฏิบัติงาน

หน้าเว็บบน Nginx ฐานข้อมูล/ตารางตัวอย่าง Node.js Application และไฟล์ Nginx Site Configuration

9. การวัดและประเมินผล

9.1 เกณฑ์การปฏิบัติงาน

ติดตั้งครบทุกบริการ ตรวจ Config ผ่าน เข้าหน้าเว็บจาก Client ได้ และอธิบายหน้าที่แต่ละส่วนถูกต้องไม่น้อยกว่าร้อยละ 80

9.2 วิธีการประเมิน

ตรวจ Service/Port/Config จริง ทดลอง Request จาก Client ตรวจฐานข้อมูล และสัมภาษณ์สั้นรายบุคคล

9.3 เครื่องมือประเมิน

Server Stack Checklist, แบบตรวจ Config, แบบประเมินชิ้นงาน และแบบบันทึกการแก้ปัญหา

10. บันทึกผลหลังการจัดการเรียนรู้

10.1 ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

10.2 ปัญหา อุปสรรคที่พบ

10.3 การแก้ไขปัญหา

1) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

2) แนวทางแก้ปัญหาในครั้งต่อไป

	ใบความรู้ที่ 3	หน่วยที่ 3
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 4-6
	ชื่อหน่วยการเรียนรู้ การติดตั้ง Web Server, Database และ Node.js Server Stack	ทฤษฎี 3 ชม. ปฏิบัติ 12 ชม.
ชื่อเรื่อง/งาน Git, Nginx, MariaDB, Node.js และ Nginx Reverse Proxy		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนติดตั้งและกำหนดค่า Git, Nginx, MariaDB และ Node.js บน Ubuntu Server สร้างฐานข้อมูลและเว็บแอปพลิเคชันเบื้องต้น พร้อมตั้งค่า Nginx Reverse Proxy และตรวจสอบบริการได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: บริการทุกตัวต้องทำงานหลัง Restart ระบบ หน้าเว็บต้องเข้าจากเครื่องอื่นได้ ฐานข้อมูลใช้บัญชีที่กำหนดสิทธิ์เฉพาะงาน และ Reverse Proxy ส่งคำขอไปยัง Node.js ได้

2) วิธีประเมิน: ตรวจสถานะ Service, Port, Config และผลการเข้าถึงจาก Client พร้อมประเมินการอธิบายหน้าที่ของแต่ละส่วน

3) หลักฐานการปฏิบัติงาน (Performance Evidence): หน้าเว็บบน Nginx ฐานข้อมูล/ตารางตัวอย่าง Node.js Application และไฟล์ Nginx Site Configuration

4) หลักฐานความรู้ (Knowledge Evidence): แผนผัง Server Stack บันทึกคำสั่งติดตั้ง และคำอธิบายเส้นทาง Request จาก Client ถึง Application/Database

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงาน Web/Database Server และการ Deploy Web Application ตามแนวคิด DevOps เบื้องต้น

3. สมรรถนะประจำหน่วย

3.1 ติดตั้งและควบคุม Nginx Web Server ได้

3.2 สร้างฐานข้อมูล ผู้ใช้ และกำหนดสิทธิ์ MariaDB ได้

3.3 ติดตั้ง Node.js และรัน HTTP Application ได้

3.4 ใช้ Git นำ Source Code มายัง Server ได้

3.5 ตั้งค่า Nginx Reverse Proxy และวิเคราะห์ Log ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบายบทบาทของ Nginx, MariaDB, Node.js และ Git ใน Server Stack ได้

4.2 ติดตั้ง Nginx และแก้ไข Document Root ได้

4.3 ใช้ systemctl และ nginx -t เพื่อตรวจสอบบริการและไฟล์ตั้งค่าได้

4.4 สร้าง Database, Table และ User ที่มีสิทธิ์เหมาะสมได้

4.5 สร้างและรัน Node.js HTTP Server ได้

4.6 ตั้งค่า proxy_pass และทดสอบจาก Client ได้

4.7 เก็บหลักฐานและอธิบายปัญหาที่พบระหว่าง Deploy ได้

5. เนื้อหาสาระ

5.1 ภาพรวม Server Stack และเส้นทางของ Request

Nginx รับ HTTP Request ที่พอร์ต 80/443 และส่ง Static File หรือส่งต่อไปยัง Application ผ่าน Reverse Proxy, Node.js ประมวลผลตรรกะของแอปพลิเคชัน ส่วน MariaDB เก็บข้อมูลแบบตาราง Git ใช้รับและติดตาม Source Code การแยกหน้าที่ทำให้ดูแลและแก้ปัญหาได้เป็นส่วน ๆ

5.2 Nginx Web Server

ติดตั้งด้วย apt install nginx แล้วตรวจ systemctl status nginx หน้าเว็บหลักมักอยู่ที่ /var/www/html ไฟล์ Site Configuration อยู่ใน /etc/nginx/sites-available และเปิดใช้ผ่าน sites-enabled ทุกครั้งที่แก้ Config ต้องใช้ nginx -t ก่อน Reload เพื่อป้องกันบริการหยุดจาก Syntax Error

5.3 MariaDB และ Node.js

MariaDB ควรสร้างฐานข้อมูลและบัญชีแยกจาก root แล้ว GRANT เฉพาะสิทธิ์ที่งานต้องใช้ Node.js ใช้ JavaScript ฝั่ง Server จัดการแพ็กเกจด้วย npm และเปิด HTTP Server บนพอร์ตภายใน เช่น 3000 ต้องตรวจ Process, Port และ Error Message เมื่อ Application ไม่ตอบสนอง

5.4 Git และ Nginx Reverse Proxy

Git clone นำโครงการลง Server และ git pull อัปเดตโค้ด Reverse Proxy ใช้ location / และ proxy_pass http://127.0.0.1:3000 เพื่อซ่อนพอร์ตภายในและรวมจุดเข้าใช้งานไว้ที่ Nginx หากเกิดปัญหาให้ตรวจ nginx -t, systemctl status, ss -tulpn, curl และ Log ตามลำดับ

6. แบบฝึกหัด/แบบทดสอบ

6.1 อธิบายเส้นทาง Request เมื่อผู้ใช้เปิดเว็บไซต์ที่ Nginx ส่งต่อไป Node.js และอ่านข้อมูลจาก MariaDB

6.2 เขียนลำดับการตรวจสอบเมื่อ Nginx แสดง 502 Bad Gateway

6.3 ปฏิบัติสร้างหน้าเว็บ ฐานข้อมูล และ Reverse Proxy พร้อมแนบผล systemctl, ss และ curl

7. เอกสารอ้างอิง

Nginx Documentation; MariaDB Server Documentation; Node.js Documentation; Git Documentation; สไล Server Stack และ Reverse Proxy

8. ภาคผนวก (เฉลยแบบฝึกหัด เฉลยแบบทดสอบ ฯ)

8.1 Browser -> Nginx -> Node.js -> MariaDB และส่งผลย้อนกลับตามเส้นทางเดิม

8.2 ตรวจ Application Process/Port, curl 127.0.0.1:3000, proxy_pass, nginx -t และ Error Log

8.3 ประเมินจาก Checklist การติดตั้ง ความถูกต้องของ Config และผลทดสอบจาก Client

-

-

-

	แผนการจัดการเรียนรู้	หน่วยที่ 4
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 7-8
	ชื่อหน่วยการเรียนรู้ การจัดการผู้ใช้ SSH เครือข่าย และความปลอดภัย Server	ทฤษฎี 2 ชม. ปฏิบัติ 8 ชม.
ชื่อเรื่อง/งาน User/Permission, SSH Hardening, Port Monitoring, UFW และ Nmap		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนสร้างผู้ใช้และกลุ่ม กำหนด Owner/Permission ใช้ SSH Key ปรับความปลอดภัย SSH ตรวจสอบพอร์ตและกำหนด UFW Firewall Rule พร้อมยืนยันผลด้วย Nmap ได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: บัญชีและสิทธิ์ต้องเป็นไปตามโจทย์ SSH Key ใช้งานได้ พอร์ตที่ไม่อนุญาตต้องเข้าถึงไม่ได้ และผู้เรียนอธิบายผลของ Rule ได้

2) วิธีประเมิน: สถานการณ์ปฏิบัติ ตรวจ Permission/SSH/UFW จริง เปรียบเทียบผลก่อนและหลัง และตรวจรายงาน Nmap

3) หลักฐานการปฏิบัติงาน (Performance Evidence): บัญชีผู้ใช้ โฟลเดอร์ที่กำหนดสิทธิ์ SSH Key Configuration UFW Rule และผล Port Scan

4) หลักฐานความรู้ (Knowledge Evidence): ตารางเลขสิทธิ์ chmod หลัก Least Privilege หน้าที่พอร์ต และลำดับวิเคราะห์ Network Service

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงานดูแลบัญชีผู้ใช้ การเข้าถึงระยะไกล และการลดพื้นที่โจมตีของเครื่องแม่ข่าย

3. สมรรถนะประจำหน่วย

3.1 จัดการ User, Group และ sudo ตามหลักสิทธิ์ขั้นต่ำได้
3.2 ใช้ chmod และ chown กำหนดสิทธิ์ไฟล์ได้
3.3 สร้างและใช้ SSH Key พร้อมปิด Root Login ได้
3.4 ตรวจ IP, Route, Socket, Port และ Service ได้
3.5 กำหนดและตรวจสอบ UFW Rule ด้วย Nmap ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 สร้างผู้ใช้และกลุ่มตามโจทย์ได้
4.2 คำนวณและกำหนดสิทธิ์ Read/Write/Execute ได้
4.3 เปลี่ยน Owner/Group ของไฟล์และตรวจผลด้วย ls -l ได้
4.4 ตั้งค่า SSH Key และอธิบาย Public/Private Key ได้
4.5 อธิบาย TCP/UDP, Port และการ Bind ที่ 127.0.0.1/0.0.0.0 ได้
4.6 ใช้ ss, curl, ping, nmap และ UFW วิเคราะห์ระบบได้

4.7 ปรับ Rule โดยไม่ตัดการเข้าถึงที่จำเป็นและบันทึกเหตุผลได้

5. สาระการเรียนรู้

User/Group/sudo, Least Privilege, Linux Permission, chmod/chown, SSH Key, sshd_config, TCP/UDP, Port และ Bind Address, ip/ss/ping/curl/nmap, UFW Default Policy, Allow/Deny และ IP Whitelisting

6. กิจกรรมการเรียนรู้

6.1 ครูยกกรณีใช้บัญชี root ทำงานทุกอย่าง แล้วให้ผู้เรียนวิเคราะห์ความเสี่ยงและสิทธิ์ที่ควรมี

6.2 ผู้เรียนสร้าง User/Group กำหนด Owner และ Permission ของโฟลเดอร์ร่วมตามสถานการณ์

6.3 ครูสาธิต SSH Key และอธิบายตำแหน่ง Private/Public Key จากนั้นผู้เรียนทดสอบเข้าสู่ระบบ

6.4 ผู้เรียนตรวจ IP, Route, Service และ Port ด้วย ip a, ip route, systemctl และ ss -tulpn

6.5 ครูสาธิต UFW Default Deny และการ Allow เฉพาะบริการ ผู้เรียนกำหนด Rule โดยรักษาช่องทางบริหารระบบไว้

6.6 ผู้เรียนสแกนพอร์ตจากเครื่องอื่นด้วย Nmap เปรียบเทียบก่อน/หลัง Firewall และเขียนเหตุผลของผลที่เห็น

7. สื่อและแหล่งการเรียนรู้

7.1 สไลด์สัปดาห์ที่ 6-7 เรื่อง User, Permission, SSH, Network Diagnostics และ UFW

7.2 Ubuntu Server/LXC สองเครื่อง เครือข่าย LAN และโปรแกรม Terminal

7.3 ใบความรู้ที่ 4 ใบงาน Permission/SSH และแบบบันทึก Firewall Audit

8. หลักฐานการเรียนรู้

8.1 หลักฐานความรู้

ตารางเลขสิทธิ chmod หลัก Least Privilege หน้าทีพอร์ต และลำดับวิเคราะห์ Network Service

8.2 หลักฐานการปฏิบัติงาน

บัญชีผู้ใช้ โฟลเดอร์ที่กำหนดสิทธิ์ SSH Key Configuration UFW Rule และผล Port Scan

9. การวัดและประเมินผล

9.1 เกณฑ์การปฏิบัติงาน

Permission ถูกตามโจทย์ SSH Key ใช้งานได้ UFW คงพอร์ตจำเป็นและปิดพอร์ตอื่น ผล Nmap สอดคล้องกับ Rule

9.2 วิธีการประเมิน

ตรวจคำสั่งและไฟล์ตั้งค่า ทดสอบ Login/Access จริง และเปรียบเทียบผล Port Scan

9.3 เครื่องมือประเมิน

Permission Checklist, SSH Hardening Checklist, UFW/Nmap Audit Sheet และแบบสังเกตความรอบคอบ

-

10. บันทึกผลหลังการจัดการเรียนรู้

10.1 ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

10.2 ปัญหา อุปสรรคที่พบ

10.3 การแก้ไขปัญหา

1) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

2) แนวทางแก้ปัญหาในครั้งต่อไป

	ใบความรู้ที่ 4	หน่วยที่ 4
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 7-8
	ชื่อหน่วยการเรียนรู้ การจัดการผู้ใช้ SSH เครือข่าย และความปลอดภัย Server	ทฤษฎี 2 ชม. ปฏิบัติ 8 ชม.
ชื่อเรื่อง/งาน User/Permission, SSH Hardening, Port Monitoring, UFW และ Nmap		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนสร้างผู้ใช้และกลุ่ม กำหนด Owner/Permission ใช้ SSH Key ปรับความปลอดภัย SSH ตรวจสอบพอร์ตและกำหนด UFW Firewall Rule พร้อมยืนยันผลด้วย Nmap ได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: บัญชีและสิทธิ์ต้องเป็นไปตามโจทย์ SSH Key ใช้งานได้ พอร์ตที่ไม่อนุญาตต้องเข้าถึงไม่ได้ และผู้เรียนอธิบายผลของ Rule ได้

2) วิธีประเมิน: สถานการณ์ปฏิบัติ ตรวจ Permission/SSH/UFW จริง เปรียบเทียบผลก่อนและหลัง และตรวจรายงาน Nmap

3) หลักฐานการปฏิบัติงาน (Performance Evidence): บัญชีผู้ใช้ โฟลเดอร์ที่กำหนดสิทธิ์ SSH Key Configuration UFW Rule และผล Port Scan

4) หลักฐานความรู้ (Knowledge Evidence): ตารางเลขสิทธิ์ chmod หลัก Least Privilege หน้าที่พอร์ต และลำดับวิเคราะห์ Network Service

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงานดูแลบัญชีผู้ใช้ การเข้าถึงระยะไกล และการลดพื้นที่โจมตีของเครื่องแม่ข่าย

3. สมรรถนะประจำหน่วย

3.1 จัดการ User, Group และ sudo ตามหลักสิทธิ์ขั้นต่ำได้
3.2 ใช้ chmod และ chown กำหนดสิทธิ์ไฟล์ได้
3.3 สร้างและใช้ SSH Key พร้อมปิด Root Login ได้
3.4 ตรวจ IP, Route, Socket, Port และ Service ได้
3.5 กำหนดและตรวจสอบ UFW Rule ด้วย Nmap ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 สร้างผู้ใช้และกลุ่มตามโจทย์ได้
4.2 คำนวณและกำหนดสิทธิ์ Read/Write/Execute ได้
4.3 เปลี่ยน Owner/Group ของไฟล์และตรวจผลด้วย ls -l ได้
4.4 ตั้งค่า SSH Key และอธิบาย Public/Private Key ได้
4.5 อธิบาย TCP/UDP, Port และการ Bind ที่ 127.0.0.1/0.0.0.0 ได้
4.6 ใช้ ss, curl, ping, nmap และ UFW วิเคราะห์ระบบได้
4.7 ปรับ Rule โดยไม่ตัดการเข้าถึงที่จำเป็นและบันทึกเหตุผลได้

5. เนื้อหาสาระ

5.1 User, Group, sudo และหลัก Least Privilege
แต่ละบริการและผู้ดูแลควรมีสิทธิ์เท่าที่จำเป็น adduser ใช้สร้างบัญชี usermod -aG เพิ่มสมาชิกกลุ่ม และ sudo ให้สิทธิ์ผู้ดูแลเฉพาะคำสั่ง การใช้ root ตลอดเวลาทำให้ความผิดพลาดกระทบทั้งระบบและตรวจสอบผู้กระทำได้ยาก

5.2 Linux Permission, chmod และ chown
Permission แบ่ง Owner, Group, Others และสิทธิ์ r=4, w=2, x=1 เช่น 750 หมายถึง Owner ทำได้ทั้งหมด Group อ่าน/เข้าได้ Others ไม่มีสิทธิ์ chmod เปลี่ยน Permission ส่วน chown เปลี่ยน Owner และ Group ต้องตรวจผลด้วย ls -l ทุกครั้ง

5.3 SSH Key และ SSH Hardening
SSH Key มี Private Key ซึ่งต้องเก็บที่ Client และ Public Key ที่บันทึกใน ~/.ssh/authorized_keys ของ Server เมื่อทดสอบ Key สำเร็จจึงค่อยปิด PasswordAuthentication และ PermitRootLogin ใน sshd_config ต้องเปิด Session เดิมไว้ระหว่างทดสอบเพื่อป้องกันล็อกตัวเองออกจากระบบ

5.4 Port Monitoring, UFW และ Nmap
Port คือจุดรับบริการ TCP/UDP การ Bind ที่ 127.0.0.1 รับเฉพาะภายในส่วน 0.0.0.0 รับทุก Interface ใช้ ss -tulpn ดู Process/Port, curl ทดสอบบริการ, UFW กำหนด Default Deny และเปิดเฉพาะพอร์ตจำเป็น จากนั้นใช้ Nmap จากเครื่องอื่นยืนยันผลจริง

6. แบบฝึกหัด/แบบทดสอบ
6.1 กำหนด Permission ให้ Owner อ่าน/เขียน/เข้า Group อ่าน/เข้า และ Others ไม่มีสิทธิ์ พร้อมอธิบายเลขที่ใช้
6.2 อธิบายเหตุผลที่ต้องทดสอบ SSH Key ก่อนปิด Password Login

6.3 สร้าง UFW Rule สำหรับ SSH และ Web แล้วใช้ Nmap ยืนยันพอร์ตที่เปิดจาก Client
7. เอกสารอ้างอิง
Ubuntu Server Guide: Users and SSH; OpenSSH Manual; UFW Manual; Nmap Reference Guide;
สไลด์สัปดาห์ที่ 6-7
8. ภาคผนวก (เฉลยแบบฝึกหัด เฉลยแบบทดสอบ ฯ)
8.1 ใช้ chmod 750 เพราะ Owner=7, Group=5, Others=0
8.2 หาก Key หรือ Permission ผิด การปิด Password ก่อนจะทำให้ผู้ดูแลกลับเข้า Server ไม่ได้

8.3 ประเมินจาก ufw status numbered, ss -tulpn และผล Nmap ที่สอดคล้องกัน

-
-

-
-

-
-

	แผนการจัดการเรียนรู้	หน่วยที่ 5
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 9-10
	ชื่อหน่วยการเรียนรู้ การติดตั้งและทดสอบ FTP Server	ทฤษฎี 2 ชม. ปฏิบัติ 8 ชม.
ชื่อเรื่อง/งาน vsftpd, User Permission, Passive Ports, Firewall และ FileZilla		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนอธิบาย Control/Data Connection และ Passive Mode ติดตั้ง vsftpd สร้างผู้ใช้และโฟลเดอร์ กำหนดสิทธิ์ เปิด Firewall และทดสอบ Upload/Download ด้วย FileZilla ได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: เข้าสู่ระบบได้ เห็นรายการไฟล์ อัปโหลดและดาวน์โหลดสำเร็จ ไฟล์บน Server มี Owner/Permission ถูกต้อง และ Firewall เปิดเฉพาะพอร์ตที่กำหนด

2) วิธีประเมิน: ตรวจ Config และ Service ทดสอบ FileZilla จาก Client อ่าน Message Log และแก้สถานการณ์ Login/Listing/Transfer Error

3) หลักฐานการปฏิบัติงาน (Performance Evidence): ไฟล์ vsftpd.conf ผู้ใช้ FTP โฟลเดอร์ upload ไฟล์ทดสอบ ผล UFW และภาพ Transfer Successful ใน FileZilla

4) หลักฐานความรู้ (Knowledge Evidence): แผนภาพ Control/Data Connection ความหมาย Passive Port และตารางวิเคราะห์อาการผิดพลาด

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงานให้บริการ File Transfer และการวิเคราะห์ร่วมกันระหว่าง Service, Permission, Port และ Firewall

3. สมรรถนะประจำหน่วย

3.1 อธิบาย FTP Control และ Data Connection ได้
3.2 ติดตั้งและตรวจสอบบริการ vsftpd ได้
3.3 สร้าง FTP User และกำหนดโฟลเดอร์/สิทธิ์ได้
3.4 ตั้งค่า Passive Port Range และ UFW ได้
3.5 ใช้ FileZilla ทดสอบและอ่าน Message Log ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบายเหตุผลที่ FTP ใช้มากกว่าหนึ่ง Connection ได้
4.2 อธิบาย Passive Port และความสัมพันธ์กับ Firewall ได้
4.3 ติดตั้ง vsftpd และสำรองไฟล์ตั้งค่าก่อนแก้ไขได้
4.4 สร้างผู้ใช้และโฟลเดอร์ upload พร้อมกำหนด Owner ได้
4.5 อธิบายค่า local_enable, write_enable และ chroot_local_user ได้
4.6 เชื่อมต่อด้วย FileZilla และส่งไฟล์ได้ทั้งสองทิศทาง

4.7 วิเคราะห์ Message Log และแก้ปัญหาตามหลักฐานได้

5. สาระการเรียนรู้

หลักการ FTP, Port 21, Control/Data Connection, Active/Passive Mode, Passive Port Range, การติดตั้ง vsftpd, Local User, chroot, Directory/Owner/Permission, UFW และการใช้ FileZilla Site Manager, Transfer Queue และ Message Log

6. กิจกรรมการเรียนรู้

6.1 ครูทบทวนปัญหาจากคาบก่อนและใช้ Animation แสดงคำสั่ง Login ทาง Port 21 กับการส่งไฟล์ผ่าน Passive Port แยกกัน
6.2 ผู้เรียนตรวจ IP ของ Container อัปเดตแพ็กเกจ ติดตั้ง vsftpd และตรวจ Service/Port
6.3 ครูอธิบายค่าใน vsftpd.conf ทีละบรรทัด ผู้เรียนสำรองไฟล์เดิม และแก้เฉพาะค่าที่จำเป็น
6.4 ผู้เรียนสร้าง ftpstudent โฟลเดอร์ ftp/upload และไฟล์ welcome.txt โดยตรวจ Owner/Permission ด้วย ls -l
6.5 ผู้เรียนกำหนด pasv_min_port/pasv_max_port เปิด UFW สำหรับ Port 21 และช่วง Passive Port แล้ว Reload บริการ
6.6 ผู้เรียนใช้ FileZilla เชื่อมต่อ ดู Local/Remote Site อัปโหลด/ดาวน์โหลด และใช้ Message Log ระบุว่าขั้นตอนใดสำเร็จหรือผิดพลาด

7. สื่อและแหล่งการเรียนรู้

7.1 สไลด์สัปดาห์ที่ 9-10 เรื่อง FTP Flow, Passive Port และ vsftpd
7.2 Ubuntu Server LXC, Proxmox Console, เครื่อง Client ที่ติดตั้ง FileZilla และเครือข่าย LAN
7.3 ใบความรู้ที่ 5 คู่มือคำสั่งทีละขั้น และใบงานวิเคราะห์ FileZilla Message Log

8. หลักฐานการเรียนรู้

8.1 หลักฐานความรู้

แผนภาพ Control/Data Connection ความหมาย Passive Port และตารางวิเคราะห์อาการผิดพลาด

8.2 หลักฐานการปฏิบัติงาน

ไฟล์ vsftpd.conf ผู้ใช้ FTP โฟลเดอร์ upload ไฟล์ทดสอบ ผล UFW และภาพ Transfer Successful ใน FileZilla

9. การวัดและประเมินผล

9.1 เกณฑ์การปฏิบัติงาน

Service Active, Port/Firewall ถูกต้อง Login/Directory Listing/Upload/Download สำเร็จ และอธิบาย Passive Port ได้

9.2 วิธีการประเมิน

ตรวจคำสั่งและ Config ทดสอบด้วย FileZilla ต่อหน้าครู ตรวจไฟล์จริงบน Server และถามเหตุผลของแต่ละค่า

9.3 เครื่องมือประเมิน

FTP Setup Checklist, FileZilla Test Sheet, แบบวิเคราะห์ Error และแบบสังเกตการแก้ปัญหา

10. บันทึกผลหลังการจัดการเรียนรู้

10.1 ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

10.2 ปัญหา อุปสรรคที่พบ

10.3 การแก้ไขปัญหา

1) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

2) แนวทางแก้ปัญหาในครั้งต่อไป

-

	ใบความรู้ที่ 5	หน่วยที่ 5
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 9-10
	ชื่อหน่วยการเรียนรู้ การติดตั้งและทดสอบ FTP Server	ทฤษฎี 2 ชม. ปฏิบัติ 8 ชม.
ชื่อเรื่อง/งาน vsftpd, User Permission, Passive Ports, Firewall และ FileZilla		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนอธิบาย Control/Data Connection และ Passive Mode ติดตั้ง vsftpd สร้างผู้ใช้และโฟลเดอร์ กำหนดสิทธิ์ เปิด Firewall และทดสอบ Upload/Download ด้วย FileZilla ได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: เข้าสู่ระบบได้ เห็นรายการไฟล์ อัปโหลดและดาวน์โหลดสำเร็จ ไฟล์บน Server มี Owner/Permission ถูกต้อง และ Firewall เปิดเฉพาะพอร์ตที่กำหนด

2) วิธีประเมิน: ตรวจ Config และ Service ทดสอบ FileZilla จาก Client อ่าน Message Log และแก้สถานการณ์ Login/Listing/Transfer Error

3) หลักฐานการปฏิบัติงาน (Performance Evidence): ไฟล์ vsftpd.conf ผู้ใช้ FTP โฟลเดอร์ upload ไฟล์ทดสอบ ผล UFW และภาพ Transfer Successful ใน FileZilla

4) หลักฐานความรู้ (Knowledge Evidence): แผนภาพ Control/Data Connection ความหมาย Passive Port และตารางวิเคราะห์อาการผิดพลาด

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงานให้บริการ File Transfer และการวิเคราะห์ร่วมกันระหว่าง Service, Permission, Port และ Firewall

3. สมรรถนะประจำหน่วย

3.1 อธิบาย FTP Control และ Data Connection ได้

3.2 ติดตั้งและตรวจสอบบริการ vsftpd ได้

3.3 สร้าง FTP User และกำหนดโฟลเดอร์/สิทธิ์ได้

3.4 ตั้งค่า Passive Port Range และ UFW ได้

3.5 ใช้ FileZilla ทดสอบและอ่าน Message Log ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบายเหตุผลที่ FTP ใช้มากกว่าหนึ่ง Connection ได้

4.2 อธิบาย Passive Port และความสัมพันธ์กับ Firewall ได้

4.3 ติดตั้ง vsftpd และสำรองไฟล์ตั้งค่าก่อนแก้ไขได้

4.4 สร้างผู้ใช้และโฟลเดอร์ upload พร้อมกำหนด Owner ได้

4.5 อธิบายค่า local_enable, write_enable และ chroot_local_user ได้

4.6 เชื่อมต่อด้วย FileZilla และส่งไฟล์ได้ทั้งสองทิศทาง

4.7 วิเคราะห์ Message Log และแก้ปัญหาตามหลักฐานได้

5. เนื้อหาสาระ

5.1 FTP, Control Connection และ Data Connection

FileZilla เริ่มเชื่อมต่อไปยัง vsftpd ที่ TCP Port 21 เพื่อ Login และส่งคำสั่ง เช่น USER, PASS และ LIST เส้นทางนี้เรียก Control Connection เมื่อขอดูรายการหรือส่งไฟล์ Server จะสร้าง Data Connection แยกต่างหาก ดังนั้น Login สำเร็จยังไม่ยืนยันว่าจะส่งไฟล์ได้

5.2 Passive Mode และ Passive Port

Passive Port คือพอร์ตชั่วคราวที่ FTP Server เลือกจากช่วงที่กำหนดเพื่อรับ Data Connection จาก Client เช่น 40000-40100 Server แจ้งหมายเลขพอร์ตผ่าน Control Connection แล้ว FileZilla เป็นฝ่ายเปิดการเชื่อมต่อใหม่เข้าไป วิธีนี้เหมาะกับ Client ที่อยู่หลัง Firewall/NAT แต่ Server ต้องเปิดทั้ง Port 21 และช่วง Passive Port

5.3 การตั้งค่า vsftpd ผู้ใช้ และสิทธิ์โฟลเดอร์

ค่าหลัก ได้แก่ local_enable=YES ให้ผู้ใช้ Linux Login, write_enable=YES อนุญาตเขียน และ chroot_local_user=YES จำกัดผู้ใช้ให้อยู่ภายใน Home Directory ของบัญชีตนเอง สร้างโฟลเดอร์ upload และใช้ chown/chmod กำหนดเจ้าของให้ถูกต้อง จากนั้น Restart และตรวจ status

5.4 การทดสอบด้วย FileZilla และการอ่านหลักฐาน

FileZilla แสดง Local Site, Remote Site, Transfer Queue และ Message Log ในหน้าจอเดียว จึงเห็นทั้งผลการ Login การเปิด Passive Port และสถานะส่งไฟล์ กรอก Host, Username, Password และ Port 21 แล้วทดสอบ Upload/Download หากผิดพลาดให้แยกว่าเกิดที่ Login, Directory Listing, Permission หรือ Data Connection ก่อนแก้ไข

6. แบบฝึกหัด/แบบทดสอบ

6.1 อธิบายความแตกต่างระหว่าง Control Connection และ Data Connection ของ FTP

6.2 อธิบายว่าเหตุใดเปิดเฉพาะ Port 21 แล้ว Login ได้ แต่ FileZilla อาจแสดงรายการไฟล์หรือส่งไฟล์ไม่ได้

6.3 ปฏิบัติติดตั้ง vsftpd ตั้ง Passive Port 40000-40100 และทดสอบ Upload/Download พร้อมแนบ Message Log

7. เอกสารอ้างอิง

Ubuntu Server Guide; vsftpd Manual; FileZilla Client Documentation;

สไลด์สัปดาห์ที่ 9-10

8. ภาคผนวก (เฉลยแบบฝึกหัด เฉลยแบบทดสอบ ฯ)

8.1 Control ใช้ Login/คำสั่งที่ Port 21 ส่วน Data ใช้รายการไฟล์และข้อมูลไฟล์จริง

8.2 เพราะ Data Connection ใช้ Passive Port แยก หาก Firewall ปิดช่วงดังกล่าวการส่งข้อมูลจะไม่สำเร็จ

8.3 ประเมินจาก Config, UFW, ไฟล์บน Server และข้อความ Successful transfers ใน FileZilla

-
-
-

-
-
-

-

-
-
-

	แผนการจัดการเรียนรู้	หน่วยที่ 6
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 11-13
	ชื่อหน่วยการเรียนรู้ Proxmox VE, LXC Container และการนำเว็บขึ้นใช้งาน	ทฤษฎี 2 ชม. ปฏิบัติ 13 ชม.
ชื่อเรื่อง/งาน Proxmox Installation, LXC, Production Build, Nginx, PM2 และ HTTPS		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนอธิบายสถาปัตยกรรม Proxmox VE ติดตั้งบนเครื่อง Server ตั้ง Management Network สร้าง LXC Container และนำ Web Application ขึ้นใช้งานผ่าน Nginx/PM2 พร้อม HTTPS ได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: เข้า Proxmox Web GUI ได้ Container มี IP และออกเครือข่ายได้ Web Application เข้าจาก LAN ได้หลัง Restart และ HTTPS ใช้งานตาม Config

2) วิธีประเมิน: ตรวจ Proxmox/Network/Storage/LXC จริง ตรวจ Production Build, Process, Nginx Configuration และทดสอบจาก Client

3) หลักฐานการปฏิบัติงาน (Performance Evidence): Proxmox Node, LXC Container, Web Application ที่ Deploy แล้ว Nginx/PM2 Config และผล HTTPS

4) หลักฐานความรู้ (Knowledge Evidence): แผนภาพ Type-1 Hypervisor ความแตกต่าง KVM/LXC ขั้นตอน Provisioning และ Deployment Runbook

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงาน Virtualization, Container Platform และการ Deploy Web Application บนโครงสร้างพื้นฐานจริง

3. สมรรถนะประจำหน่วย

3.1 อธิบาย Proxmox VE, KVM และ LXC ได้
3.2 ติดตั้ง Proxmox และตั้ง Management IP ได้
3.3 ดาวน์โหลด Template และสร้าง LXC Container ได้
3.4 Deploy Production Build ด้วย Nginx/PM2 ได้
3.5 ตั้งค่า HTTPS/Reverse Proxy และทดสอบจาก LAN ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบาย Type-1 Hypervisor และข้อแตกต่าง KVM/LXC ได้
4.2 เตรียม USB Boot และตั้ง BIOS/UEFI สำหรับติดตั้งได้
4.3 กำหนด Hostname, IP, Gateway, DNS และ Storage ได้
4.4 สร้าง LXC กำหนด CPU/RAM/Disk/Network ตามโจทย์ได้
4.5 อธิบาย Development Mode กับ Production Build ได้
4.6 ตั้งค่า Nginx/PM2 และแก้ React Routing 404 ได้

4.7 สร้าง Certificate และบังคับ Redirect HTTP ไป HTTPS ได้

5. สาระการเรียนรู้

Proxmox VE Type-1 Hypervisor, KVM/LXC, ISO/USB Boot, Management IP, Linux Bridge, Storage, OS Template, LXC Provisioning, React/Node Production Build, Nginx try_files/Reverse Proxy, PM2, SSL/TLS และ Port 443

6. กิจกรรมการเรียนรู้

6.1 ครูใช้แผนภาพอธิบาย Bare-metal Hypervisor และให้ผู้เรียนเปรียบเทียบ KVM กับ LXC จากการใช้ทรัพยากร

6.2 ผู้เรียนเตรียม USB Boot ติดตั้ง Proxmox VE และบันทึกค่า Hostname, Management IP, Gateway และ DNS

6.3 ผู้เรียนเข้า https://IP:8006 ตรวจ Node/Storage/Bridge ดาวน์โหลด Template และสร้าง LXC ตามทรัพยากรที่กำหนด

6.4 ครูสาธิต npm install, npm run build, Nginx Document Root/try_files และ PM2 สำหรับ Node.js

6.5 ผู้เรียน Deploy Web Application ทดสอบจากเครื่องอื่นใน LAN และตรวจ Process/Port/Log เมื่อมีปัญหา

6.6 ครูอธิบาย SSL/TLS ผู้เรียนสร้าง Self-signed Certificate ตั้ง Port 443 และ Redirect 80 -> 443 พร้อมบันทึกข้อจำกัดของ Certificate

7. สื่อและแหล่งการเรียนรู้

7.1 สไลด์สัปดาห์ที่ 11-13 เรื่อง Proxmox VE, LXC และ Web Deployment

7.2 เครื่อง Server จริง, Proxmox ISO, USB Drive, Switch, Client Browser และ Source Code

7.3 ใบความรู้ที่ 6 Installation Checklist, LXC Worksheet และ Deployment Runbook

8. หลักฐานการเรียนรู้

8.1 หลักฐานความรู้

แผนภาพ Type-1 Hypervisor ความแตกต่าง KVM/LXC ขั้นตอน Provisioning และ Deployment Runbook

8.2 หลักฐานการปฏิบัติงาน

Proxmox Node, LXC Container, Web Application ที่ Deploy แล้ว Nginx/PM2 Config และผล HTTPS

9. การวัดและประเมินผล

9.1 เกณฑ์การปฏิบัติงาน

ติดตั้งและเข้า GUI ได้ LXC ทำงานและมี Network Application เข้าจาก LAN ได้ Config ผ่าน และระบบกลับมาทำงานหลัง Restart

9.2 วิธีการประเมิน

ตรวจระบบจริง ทดลอง Restart/Access ตรวจ Resource/Network/Port/Log และประเมิน Runbook ที่ผู้เรียนจัดทำ

9.3 เครื่องมือประเมิน

Proxmox Installation Checklist, LXC/Deployment Rubric, HTTPS Test Sheet และแบบประเมินการแก้ปัญหา

-

10. บันทึกผลหลังการจัดการเรียนรู้

10.1 ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

10.2 ปัญหา อุปสรรคที่พบ

10.3 การแก้ไขปัญหา

1) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

2) แนวทางแก้ปัญหาในครั้งต่อไป

	ใบความรู้ที่ 6	หน่วยที่ 6
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 11-13
	ชื่อหน่วยการเรียนรู้ Proxmox VE, LXC Container และการนำเว็บขึ้นใช้งาน	ทฤษฎี 2 ชม. ปฏิบัติ 13 ชม.
ชื่อเรื่อง/งาน Proxmox Installation, LXC, Production Build, Nginx, PM2 และ HTTPS		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนอธิบายสถาปัตยกรรม Proxmox VE ติดตั้งบนเครื่อง Server ตั้ง Management Network สร้าง LXC Container และนำ Web Application ขึ้นใช้งานผ่าน Nginx/PM2 พร้อม HTTPS ได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: เข้า Proxmox Web GUI ได้ Container มี IP และออกเครือข่ายได้ Web Application เข้าจาก LAN ได้หลัง Restart และ HTTPS ใช้งานตาม Config

2) วิธีประเมิน: ตรวจ Proxmox/Network/Storage/LXC จริง ตรวจ Production Build, Process, Nginx Configuration และทดสอบจาก Client

3) หลักฐานการปฏิบัติงาน (Performance Evidence): Proxmox Node, LXC Container, Web Application ที่ Deploy แล้ว Nginx/PM2 Config และผล HTTPS

4) หลักฐานความรู้ (Knowledge Evidence): แผนภาพ Type-1 Hypervisor ความแตกต่าง KVM/LXC ขั้นตอน Provisioning และ Deployment Runbook

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงงาน Virtualization, Container Platform และการ Deploy Web Application บนโครงสร้างพื้นฐานจริง

3. สมรรถนะประจำหน่วย

3.1 อธิบาย Proxmox VE, KVM และ LXC ได้
3.2 ติดตั้ง Proxmox และตั้ง Management IP ได้
3.3 ดาวน์โหลด Template และสร้าง LXC Container ได้
3.4 Deploy Production Build ด้วย Nginx/PM2 ได้
3.5 ตั้งค่า HTTPS/Reverse Proxy และทดสอบจาก LAN ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบาย Type-1 Hypervisor และข้อแตกต่าง KVM/LXC ได้
4.2 เตรียม USB Boot และตั้ง BIOS/UEFI สำหรับติดตั้งได้
4.3 กำหนด Hostname, IP, Gateway, DNS และ Storage ได้
4.4 สร้าง LXC กำหนด CPU/RAM/Disk/Network ตามโจทย์ได้
4.5 อธิบาย Development Mode กับ Production Build ได้
4.6 ตั้งค่า Nginx/PM2 และแก้ React Routing 404 ได้
4.7 สร้าง Certificate และบังคับ Redirect HTTP ไป HTTPS ได้

5. เนื้อหาสาระ

5.1 Proxmox VE, KVM และ LXC

Proxmox VE เป็น Type-1 Hypervisor ติดตั้งบนฮาร์ดแวร์โดยตรง และจัดการผ่าน Web GUI KVM จำลองเครื่องเสมือนเต็มรูปแบบและมี Kernel ของตนเอง ส่วน LXC ใช้ Kernel ร่วมกับ Host จึงเบาและเริ่มทำงานเร็ว เหมาะกับบริการ Linux ที่แยกสภาพแวดล้อมกัน

5.2 การติดตั้งและสร้าง LXC Container

ขั้นตอนหลักคือเตรียม ISO/USB เปิด Virtualization ใน BIOS ติดตั้ง Proxmox กำหนด Management IP และเข้า https://IP:8006 จากนั้นตรวจ Storage, Linux Bridge, ดาวน์โหลด OS Template และสร้าง LXC โดยกำหนด CPU, RAM, Disk, Password/SSH Key และ Network ให้สอดคล้องกับแผน

5.3 การ Deploy Web Application

Development Mode เหมาะกับการพัฒนา ส่วน Production Build สร้างไฟล์ที่ปรับให้เหมาะกับการใช้งานจริง React ใช้ npm run build แล้วให้ Nginx บริการ Static File พร้อม try_files $uri /index.html สำหรับ Client-side Routing ส่วน Node.js ใช้ PM2 ดูแล Process ให้เริ่มใหม่เมื่อหยุดหรือ Restart ระบบ

5.4 HTTPS และ Nginx Reverse Proxy

HTTPS ใช้ TLS เข้ารหัสข้อมูลระหว่าง Client/Server Certificate ระบุชื่อและ Public Key Self-signed เหมาะกับ Lab แต่ Browser ยังไม่เชื่อถือโดยอัตโนมัติ Nginx รับ Port 443 อ้างอิง Certificate/Private Key

และอาจ Redirect Port 80 ไป HTTPS ทุกครั้งต้องตรวจ nginx -t และทดสอบจาก Client

6. แบบฝึกหัด/แบบทดสอบ

6.1 เปรียบเทียบ KVM และ LXC โดยพิจารณา Kernel ทรัพยากร และกรณีใช้งาน

6.2 เขียนลำดับสร้าง LXC ตั้งแต่ Template จนเข้า Console และทดสอบ Network

6.3 Deploy Web Application ผ่าน Nginx/PM2 และ HTTPS พร้อมจัดทำ Runbook สำหรับกู้ระบบหลัง Restart

7. เอกสารอ้างอิง

จุดตรวจ	คำสั่ง/ตำแหน่ง	วัตถุประสงค์
Proxmox Web GUI	https://IP:8006	จัดการ Node, Storage, Network และ LXC
LXC Network	ip a / ip route / ping	ตรวจ IP, Gateway และการออกเครือข่าย
GitHub Clone/Build	git clone / npm ci / npm run build	รับระบบ ติดตั้งแพ็กเกจ และสร้างไฟล์ใช้งานจริง
Nginx Config	nginx -t / systemctl reload nginx	ตรวจและนำ Config ใหม่มาใช้
Node.js Process	pm2 start / pm2 save / pm2 status	ดูแล Process ให้ทำงานต่อเนื่อง
HTTPS	curl -k https://IP / ss -tulpn	ยืนยัน Port 443 และการตอบกลับแบบเข้ารหัส

Proxmox VE Administration Guide; Nginx Documentation; PM2 Documentation; MDN TLS;

สไลด์สัปดาห์ที่ 11-13

8. ภาคผนวก (เฉลยแบบฝึกหัด เฉลยแบบทดสอบ ฯ)

8.1 KVM แยก OS เต็มรูปแบบและยืดหยุ่นกว่า LXC เบากว่าและเหมาะกับ Linux Service

8.2 Template -> Create CT -> Resource -> Network -> Start -> Console -> update -> test IP/DNS

8.3 ประเมินจากการเข้าถึงจริง Config/Process ที่ถูกต้อง การเริ่มอัตโนมัติ และ Runbook ที่ผู้อื่นทำตามได้

-
-
-
-
-

-

-
-
-

	แผนการจัดการเรียนรู้	หน่วยที่ 7
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 14-15
	ชื่อหน่วยการเรียนรู้ การติดตั้ง Git และ Clone ระบบจาก GitHub มารันบน Server	ทฤษฎี 2 ชม. ปฏิบัติ 8 ชม.
ชื่อเรื่อง/งาน Git Installation, GitHub Public Repository, HTTPS Clone, Dependencies และ Deployment		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนติดตั้ง Git บน Ubuntu Server รับ HTTPS URL ของ Public Repository ที่ผู้สอนกำหนด ใช้ git clone ดาวน์โหลดระบบ ตรวจสอบคู่มือและโครงสร้างโปรเจกต์ ติดตั้ง Dependencies และเปิดระบบด้วย PM2 หรือ Nginx ได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: ติดตั้ง Git และ Clone Repository ได้โดยไม่มีข้อผิดพลาด ระบุหน้าที่ของ README.md และ package.json ได้ เลือกวิธีเปิดระบบตรงกับประเภทโปรเจกต์ และยืนยันผลด้วย Process, Port, curl หรือ Browser ได้

2) วิธีประเมิน: ตรวจผลคำสั่งและ Checklist รายขั้น สังเกตการปฏิบัติ สอบถามเหตุผล และตรวจการเปิดระบบจาก Client

3) หลักฐานการปฏิบัติงาน (Performance Evidence): โฟลเดอร์ระบบที่ Clone จาก GitHub ผลการติดตั้ง Dependencies สถานะ PM2/Nginx พอร์ตบริการ และหน้าเว็บที่เปิดได้

4) หลักฐานความรู้ (Knowledge Evidence): ใบงานลำดับ GitHub URL ถึง Server ตารางบันทึกคำสั่ง ผลลัพธ์ และการวิเคราะห์ข้อผิดพลาดที่พบ

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงคำอธิบายรายวิชาในส่วนการติดตั้งและบริหารจัดการโปรแกรมให้บริการในระบบเครือข่าย พร้อมฝึกความรอบคอบในการอ่านคู่มือและตรวจผลก่อนเปิดบริการ

3. สมรรถนะประจำหน่วย

3.1 อธิบายความหมายของ Public Repository, HTTPS URL และ git clone ได้

3.2 ติดตั้ง Git และตรวจสอบเวอร์ชันบน Ubuntu Server ได้

3.3 Clone ระบบจาก GitHub ลง Home Directory ของ Container ได้

3.4 ตรวจ README.md, package.json และ Dependencies ของระบบได้

3.5 นำระบบที่ Clone มาเปิดด้วย PM2 หรือ Build และ Nginx ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบายความแตกต่างระหว่าง Git ซึ่งติดตั้งบน Server กับ GitHub ซึ่งเป็นแหล่งเก็บ Repository ได้

4.2 ตรวจสอบว่า Repository ที่กำหนดเป็น Public และคัดลอก HTTPS URL ได้ถูกต้อง

4.3 ติดตั้ง Git ด้วย apt และยืนยันผลด้วย git --version ได้

4.4 ใช้ git clone ดาวน์โหลดระบบและตรวจโฟลเดอร์ที่สร้างขึ้นได้

4.5 อ่าน README.md และ package.json เพื่อหาวิธีติดตั้งและเปิดระบบได้

4.6 เลือกใช้ npm ci หรือ npm install ตามไฟล์ที่มีใน Repository ได้

4.7 ตรวจสถานะ Process, Port และการตอบกลับของระบบ พร้อมอธิบายข้อผิดพลาดพื้นฐานได้

5. สาระการเรียนรู้

Git และ GitHub ในขอบเขตการดาวน์โหลดระบบ, Public Repository, HTTPS URL, git clone, README.md, package.json, package-lock.json, Dependencies, npm ci, npm install, Node.js Application, PM2, React/Vite Production Build, Nginx, Process, Port, curl, Browser และการแก้ปัญหาจากข้อความ Error

6. กิจกรรมการเรียนรู้

6.1 ครูกำหนดขอบเขตว่าบทนี้ใช้ GitHub เป็นแหล่งดาวน์โหลดระบบเท่านั้น และอธิบายคำว่า Repository, HTTPS URL และ Clone จากสไลด์

6.2 ครูใช้ภาพเคลื่อนไหวแสดงเส้นทาง Repository จาก GitHub มายัง Proxmox Container แล้วให้ผู้เรียนเรียงลำดับขั้นตอน

6.3 ผู้เรียนเปิด Public Repository ที่กำหนด คัดลอก HTTPS URL เปิด Proxmox GUI Console ติดตั้ง Git และตรวจเวอร์ชัน

6.4 ผู้เรียนใช้ git clone ดาวน์โหลดระบบ เข้าโฟลเดอร์ ตรวจ README.md, package.json และบันทึกคำสั่งที่โปรเจกต์รองรับ

6.5 ผู้เรียนติดตั้ง Dependencies แล้วเลือกเปิดระบบด้วย PM2 หรือ Build และ Nginx ตามประเภทของ Repository

6.6 ผู้เรียนตรวจ Process, Port, curl และ Browser พร้อมวิเคราะห์ Error จาก URL, Network, npm, PM2 หรือ Nginx ตาม Checklist

7. สื่อและแหล่งการเรียนรู้

7.1 สไลด์หน่วยที่ 7 เรื่องการติดตั้ง Git และ Clone ระบบจาก GitHub มารันบน Server

7.2 Public GitHub Repository, Proxmox/LXC, Ubuntu Server, Proxmox GUI Console, Node.js, PM2, Nginx และ Browser

7.3 ใบความรู้ที่ 7 ใบงานลำดับการ Clone และ Checklist ตรวจ Repository, Dependencies, Process, Port และหน้าเว็บ

8. หลักฐานการเรียนรู้

8.1 หลักฐานความรู้

ใบงานลำดับ GitHub URL ถึง Server ตารางบันทึกคำสั่ง ผลลัพธ์ และการวิเคราะห์ข้อผิดพลาดที่พบ

8.2 หลักฐานการปฏิบัติงาน

โฟลเดอร์ระบบที่ Clone จาก GitHub ผลการติดตั้ง Dependencies สถานะ PM2/Nginx พอร์ตบริการ และหน้าเว็บที่เปิดได้

9. การวัดและประเมินผล

9.1 เกณฑ์การปฏิบัติงาน

Clone Repository ได้ถูกต้อง ติดตั้ง Dependencies สำเร็จ เลือกวิธีรันตรงกับโปรเจกต์ และแสดงหลักฐานว่า Process, Port และหน้าเว็บทำงานจริง

9.2 วิธีการประเมิน

ตรวจ Checklist คำสั่งและผลลัพธ์ สังเกตการปฏิบัติ สอบถามความหมายของแต่ละขั้น และทดสอบเปิดระบบจาก Browser

9.3 เครื่องมือประเมิน

Git Clone Checklist, Deployment Checklist, ใบงานที่ 7 แบบสังเกตการปฏิบัติ และแบบบันทึกข้อผิดพลาด

10. บันทึกผลหลังการจัดการเรียนรู้

10.1 ผลการจัดการเรียนรู้ที่เกิดขึ้นกับผู้เรียน

10.2 ปัญหา อุปสรรคที่พบ

10.3 การแก้ไขปัญหา

1) ผลการแก้ไขปัญหาที่ส่งผลลัพธ์ที่ดีต่อผู้เรียน

2) แนวทางแก้ปัญหาในครั้งต่อไป

	ใบความรู้ที่ 7	หน่วยที่ 7
	รหัสวิชา 31901-2002 ชื่อวิชา ระบบปฏิบัติการเครื่องแม่ข่าย	สอนครั้งที่ 14-15
	ชื่อหน่วยการเรียนรู้ การติดตั้ง Git และ Clone ระบบจาก GitHub มารันบน Server	ทฤษฎี 2 ชม. ปฏิบัติ 8 ชม.
ชื่อเรื่อง/งาน Git Installation, GitHub Public Repository, HTTPS Clone, Dependencies และ Deployment		

1. ผลลัพธ์การเรียนรู้ระดับหน่วยการเรียน

ผู้เรียนติดตั้ง Git บน Ubuntu Server รับ HTTPS URL ของ Public Repository ที่ผู้สอนกำหนด ใช้ git clone ดาวน์โหลดระบบ ตรวจสอบคู่มือและโครงสร้างโปรเจกต์ ติดตั้ง Dependencies และเปิดระบบด้วย PM2 หรือ Nginx ได้

2. อ้างอิงมาตรฐาน/เชื่อมโยงกลุ่มอาชีพ

2.1 มาตรฐานอาชีพ: รหัส 40106 ช่างสนับสนุนด้านเทคนิค ระดับ 5 และสมรรถนะรายวิชาระบบปฏิบัติการเครื่องแม่ข่าย

1) เกณฑ์การปฏิบัติงาน: ติดตั้ง Git และ Clone Repository ได้โดยไม่มีข้อผิดพลาด ระบุหน้าที่ของ README.md และ package.json ได้ เลือกวิธีเปิดระบบตรงกับประเภทโปรเจกต์ และยืนยันผลด้วย Process, Port, curl หรือ Browser ได้

2) วิธีประเมิน: ตรวจผลคำสั่งและ Checklist รายขั้น สังเกตการปฏิบัติ สอบถามเหตุผล และตรวจการเปิดระบบจาก Client

3) หลักฐานการปฏิบัติงาน (Performance Evidence): โฟลเดอร์ระบบที่ Clone จาก GitHub ผลการติดตั้ง Dependencies สถานะ PM2/Nginx พอร์ตบริการ และหน้าเว็บที่เปิดได้

4) หลักฐานความรู้ (Knowledge Evidence): ใบงานลำดับ GitHub URL ถึง Server ตารางบันทึกคำสั่ง ผลลัพธ์ และการวิเคราะห์ข้อผิดพลาดที่พบ

2.2 บูรณาการกลุ่มอาชีพ: เชื่อมโยงคำอธิบายรายวิชาในส่วนการติดตั้งและบริหารจัดการโปรแกรมให้บริการในระบบเครือข่าย พร้อมฝึกความรอบคอบในการอ่านคู่มือและตรวจผลก่อนเปิดบริการ

3. สมรรถนะประจำหน่วย

3.1 อธิบายความหมายของ Public Repository, HTTPS URL และ git clone ได้

3.2 ติดตั้ง Git และตรวจสอบเวอร์ชันบน Ubuntu Server ได้

3.3 Clone ระบบจาก GitHub ลง Home Directory ของ Container ได้

3.4 ตรวจ README.md, package.json และ Dependencies ของระบบได้

3.5 นำระบบที่ Clone มาเปิดด้วย PM2 หรือ Build และ Nginx ได้

4. จุดประสงค์เชิงพฤติกรรม

4.1 อธิบายความแตกต่างระหว่าง Git ซึ่งติดตั้งบน Server กับ GitHub ซึ่งเป็นแหล่งเก็บ Repository ได้

4.2 ตรวจสอบว่า Repository ที่กำหนดเป็น Public และคัดลอก HTTPS URL ได้ถูกต้อง

4.3 ติดตั้ง Git ด้วย apt และยืนยันผลด้วย git --version ได้

4.4 ใช้ git clone ดาวน์โหลดระบบและตรวจโฟลเดอร์ที่สร้างขึ้นได้

4.5 อ่าน README.md และ package.json เพื่อหาวิธีติดตั้งและเปิดระบบได้

4.6 เลือกใช้ npm ci หรือ npm install ตามไฟล์ที่มีใน Repository ได้

4.7 ตรวจสถานะ Process, Port และการตอบกลับของระบบ พร้อมอธิบายข้อผิดพลาดพื้นฐานได้

5. เนื้อหาสาระ

5.1 Git, GitHub Repository และการ Clone ระบบ

Git เป็นโปรแกรมที่ติดตั้งบน Ubuntu Server ส่วน GitHub เป็นบริการที่เก็บ Repository ออนไลน์ ในหน่วยนี้ผู้เรียนใช้เฉพาะ Public Repository ที่ผู้สอนเตรียมไว้ ไม่สร้างหรืออัปโหลด Repository ใหม่ การ Clone คือการใช้ HTTPS URL ดาวน์โหลดไฟล์และโครงสร้างของระบบทั้งชุดลงเป็นโฟลเดอร์ใหม่บน Server

5.2 การติดตั้ง Git และใช้ HTTPS URL

ติดตั้ง Git ด้วย sudo apt update และ sudo apt install git -y แล้วตรวจด้วย git --version บนหน้า Proxmox GUI Console จากหน้า Repository กด Code เลือก HTTPS และคัดลอก URL ที่ลงท้าย .git จากนั้นเข้า Home Directory และใช้ git clone URL หากสำเร็จจะเห็นข้อความ Cloning into และมีโฟลเดอร์ชื่อเดียวกับ Repository

5.3 การตรวจไฟล์และติดตั้ง Dependencies

หลัง Clone ต้องเข้าโฟลเดอร์ ใช้ ls -la ตรวจไฟล์ อ่าน README.md และ package.json เพื่อดูวิธีติดตั้งและ scripts ของระบบ โฟลเดอร์ node_modules มักไม่เก็บใน Repository จึงต้องติดตั้งใหม่ ใช้ npm ci เมื่อมี package-lock.json เพื่อให้ได้เวอร์ชันตามที่กำหนด และใช้ npm install เมื่อไม่มี lock file

5.4 การเปิดระบบและตรวจสอบผล

Node.js Application ที่มี start script ใช้ PM2 ดูแล Process และตรวจด้วย pm2 status, ss และ curl ส่วน React/Vite Static Website ใช้ npm run build แล้วคัดลอกไฟล์ใน dist ไปยัง /var/www/html จากนั้นตรวจ nginx -t และ reload Nginx การแก้ปัญหาควรแยกเป็นช่วง URL/Network, Clone, Dependencies, Process, Port และ Nginx

6. แบบฝึกหัด/แบบทดสอบ

6.1 อธิบายเส้นทางจาก Public Repository บน GitHub จนเกิดโฟลเดอร์ระบบบน Ubuntu Server

6.2 เขียนลำดับคำสั่งติดตั้ง Git, Clone Repository, ตรวจ README/package.json และติดตั้ง Dependencies

6.3 วิเคราะห์กรณี Clone สำเร็จแต่หน้าเว็บยังเปิดไม่ได้ โดยระบุจุดตรวจและคำสั่งที่เกี่ยวข้อง

7. เอกสารอ้างอิง

GitHub Docs: Cloning a repository; Git Documentation: git-clone; npm Docs: npm ci; PM2 Documentation; Nginx Documentation; สไลด์หน่วยที่ 7

8. ภาคผนวก (เฉลยแบบฝึกหัด เฉลยแบบทดสอบ ฯ)

8.1 เปิด Repository -> คัดลอก HTTPS URL -> ติดตั้ง Git -> git clone URL -> ตรวจโฟลเดอร์ที่สร้างขึ้น

8.2 ตัวอย่าง: sudo apt update, sudo apt install git -y, git --version, cd ~, git clone URL, cd REPOSITORY, ls -la, cat README.md, cat package.json และ npm ci หรือ npm install

8.3 ตรวจตามลำดับ ได้แก่ README/package.json, npm error, pm2 status/logs, ss -lntp, curl localhost และ Nginx config/port ที่ใช้งาน

-

-

-

-

-

-