การทำความเข้าใจเกี่ยวกับเครือข่าย (Network) เป็นเรื่องที่สำคัญมากในด้านการสื่อสารและการประมวลผลข้อมูล เนื่องจากเครือข่ายเป็นโครงสร้างพื้นฐานที่ช่วยให้การเชื่อมต่อและส่งผ่านข้อมูลเป็นไปได้อย่างมีประสิทธิภาพ เครือข่ายสามารถแบ่งออกได้เป็นหลายประเภทและมีองค์ประกอบสำคัญดังนี้:

ประเภทของเครือข่าย

1. **LAN (Local Area Network)**: เป็นเครือข่ายในพื้นที่เล็ก เช่น ในอาคารเดียวกันหรือสำนักงานเดียวกัน ความเร็วสูง ใช้สาย Ethernet หรือ Wi-Fi ในการเชื่อมต่อ

2. **WAN (Wide Area Network)**: เครือข่ายที่ครอบคลุมพื้นที่กว้างขึ้น เช่น เครือข่ายระหว่างเมืองหรือระหว่างประเทศ ตัวอย่างที่สำคัญคืออินเทอร์เน็ต

3. **MAN (Metropolitan Area Network)**: เครือข่ายที่ครอบคลุมพื้นที่ขนาดกลาง เช่น เมืองหรือภูมิภาคหนึ่ง เชื่อมต่อหลาย LAN เข้าด้วยกัน

4. **PAN (Personal Area Network)**: เครือข่ายที่เชื่อมต่ออุปกรณ์ส่วนบุคคลในพื้นที่จำกัด เช่น Bluetooth หรือเครือข่ายไร้สายระหว่างสมาร์ทโฟนและคอมพิวเตอร์

องค์ประกอบสำคัญของเครือข่าย

1. **อุปกรณ์เชื่อมต่อ (Networking Devices)**:
   - **Router**: อุปกรณ์ที่ทำหน้าที่เชื่อมต่อเครือข่ายต่างๆ เช่น LAN เข้ากับอินเทอร์เน็ต
   - **Switch**: อุปกรณ์ที่ใช้เชื่อมต่ออุปกรณ์ในเครือข่าย LAN และจัดการการส่งข้อมูลระหว่างอุปกรณ์
   - **Modem**: อุปกรณ์ที่ทำหน้าที่แปลงสัญญาณดิจิตอลให้เป็นสัญญาณอนาล็อกสำหรับการเชื่อมต่ออินเทอร์เน็ต
   - **Access Point (AP)**: อุปกรณ์ที่ช่วยให้เชื่อมต่อเครือข่ายแบบไร้สาย (Wi-Fi)

2. **Topology**: รูปแบบการเชื่อมต่ออุปกรณ์ในเครือข่าย มีหลายประเภท เช่น
   - **Bus Topology**: การเชื่อมต่ออุปกรณ์ทุกตัวเข้ากับสายสัญญาณหลักเดียว
   - **Star Topology**: อุปกรณ์ทุกตัวเชื่อมต่อกับอุปกรณ์กลาง (เช่น switch)
   - **Mesh Topology**: อุปกรณ์ทุกตัวเชื่อมต่อกันเป็นเครือข่ายเต็มรูปแบบ ทำให้มีความทนทานสูง

3. **Protocol (โพรโตคอล)**: เป็นกฎเกณฑ์และมาตรฐานที่ใช้ในการสื่อสารข้อมูล ตัวอย่างเช่น

- **TCP/IP (Transmission Control Protocol/Internet Protocol)**: ใช้ในการส่งข้อมูลผ่านอินเทอร์เน็ต
- **HTTP/HTTPS (HyperText Transfer Protocol)**: ใช้สำหรับการรับส่งข้อมูลบนเว็บ
- **FTP (File Transfer Protocol)**: ใช้สำหรับการโอนไฟล์

4. **IP Address**: ที่อยู่ที่ใช้ระบุตำแหน่งอุปกรณ์ในเครือข่าย มี 2 เวอร์ชันหลักคือ

- **IPv4**: ที่อยู่ 32 บิต (เช่น 192.168.1.1)
- **IPv6**: ที่อยู่ 128 บิต ใช้เพื่อรองรับจำนวนอุปกรณ์ที่มากขึ้น (เช่น 2001:0db8:85a3::8a2e:0370:7334)

Public IP Address มีอยู่ 2 รูปแบบหลัก คือ:

1. **IPv4 (Internet Protocol version 4)**
   - มีความยาว 32 บิต และถูกแบ่งออกเป็น 4 กลุ่ม (Octets) ซึ่งแต่ละกลุ่มมีค่า 0-255 ตัวอย่างเช่น 192.168.1.1
   - IPv4 สามารถรองรับได้ประมาณ 4.3 พันล้านที่อยู่ (2^32)
   - ปัจจุบันที่อยู่ IPv4 เริ่มไม่เพียงพอเนื่องจากจำนวนอุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตเพิ่มขึ้นอย่างรวดเร็ว

2. **IPv6 (Internet Protocol version 6)**
   - มีความยาว 128 บิต และแสดงในรูปแบบของเลขฐานสิบหก โดยมีเครื่องหมายโคลอน (:) แยกแต่ละกลุ่ม ตัวอย่างเช่น 2001:0db8:85a3:0000:0000:8a2e:0370:7334
   - IPv6 สามารถรองรับที่อยู่ได้จำนวนมหาศาล (2^128) ทำให้เพียงพอต่อการใช้งานในอนาคต

ดังนั้น **Public IP** จึงมี 2 เบอร์หลัก คือ IPv4 และ IPv6 ซึ่งทั้งสองแบบนี้ถูกใช้ในการเชื่อมต่ออุปกรณ์ผ่านอินเทอร์เน็ต

Network Services ที่สำคัญ

1. **DHCP (Dynamic Host Configuration Protocol)**: บริการที่ให้ IP Address อัตโนมัติแก่เครื่องที่เข้ามาในเครือข่าย

2. **DNS (Domain Name System)**: บริการที่แปลงชื่อโดเมน (เช่น google.com) เป็น IP Address ที่ใช้งานจริง

3. **NAT (Network Address Translation)**: ช่วยในการแปลง IP Address ภายในเครือข่ายให้สามารถเชื่อมต่อกับอินเทอร์เน็ตได้

ความปลอดภัยของเครือข่าย

1. **Firewall**: อุปกรณ์หรือซอฟต์แวร์ที่ทำหน้าที่กรองการเข้าถึงเครือข่ายและป้องกันการโจมตีจากภายนอก

2. **VPN (Virtual Private Network)**: การเชื่อมต่อเครือข่ายส่วนตัวผ่านอินเทอร์เน็ต โดยมีการเข้ารหัสข้อมูลเพื่อความปลอดภัย

3. **Intrusion Detection System (IDS)** และ **Intrusion Prevention System (IPS)**: ระบบตรวจสอบและป้องกันการโจมตีเครือข่ายจากภายในหรือภายนอก

การจัดการเครือข่าย (Network Management)

1. **Network Monitoring**: การตรวจสอบสถานะของเครือข่ายเพื่อให้แน่ใจว่าทำงานได้อย่างราบรื่น

2. **QoS (Quality of Service)**: การจัดการทราฟฟิกของเครือข่ายให้มีประสิทธิภาพ เช่น การจัดลำดับความสำคัญของการส่งข้อมูล

เครือข่าย (Network) จึงเป็นองค์ประกอบสำคัญที่ทำให้โลกดิจิทัลสามารถสื่อสารและทำงานได้อย่างมีประสิทธิภาพ

1. Network Link คืออะไร? (นาทีที่ 0.37)

Network Link หมายถึงการเชื่อมต่อทางกายภาพหรือการเชื่อมต่อทางตรรกะระหว่างอุปกรณ์สองตัวหรือมากกว่าในเครือข่าย ซึ่งสามารถเป็นการเชื่อมต่อแบบมีสาย (เช่น สาย Ethernet) หรือแบบไร้สาย (เช่น Wi-Fi) โดย Network Link นี้เป็นเส้นทางที่ใช้ในการส่งผ่านข้อมูลระหว่างอุปกรณ์

2. OSI Reference Model มีอะไรบ้าง? (นาทีที่ 1.54)

OSI Reference Model (Open Systems Interconnection) ประกอบด้วย 7 ชั้น ดังนี้:

1. **Physical Layer**: ชั้นกายภาพ จัดการการส่งข้อมูลแบบไฟฟ้าและการเชื่อมต่อกายภาพ
2. **Data Link Layer**: ชั้นเชื่อมโยงข้อมูล จัดการการถ่ายโอนข้อมูลที่ปราศจากข้อผิดพลาดระหว่างอุปกรณ์สองตัว
3. **Network Layer**: ชั้นเครือข่าย จัดการการกำหนดเส้นทางและการจัดการที่อยู่ IP
4. **Transport Layer**: ชั้นขนส่ง จัดการการรับประกันการส่งข้อมูลระหว่างต้นทางและปลายทาง
5. **Session Layer**: ชั้นเซสชัน จัดการการเริ่มและสิ้นสุดการเชื่อมต่อระหว่างผู้ใช้
6. **Presentation Layer**: ชั้นนำเสนอ จัดการการแปลงข้อมูลให้อยู่ในรูปแบบที่ใช้ได้
7. **Application Layer**: ชั้นประยุกต์ จัดการอินเตอร์เฟซกับผู้ใช้และแอปพลิเคชันต่างๆ

3. การเชื่อมต่อแบบ Point to Point คืออะไร? (นาทีที่ 15.38)

การเชื่อมต่อแบบ Point to Point คือการเชื่อมต่อที่เกิดขึ้นระหว่างอุปกรณ์สองตัวโดยตรงโดยไม่มีตัวกลาง เช่น การเชื่อมต่อระหว่างคอมพิวเตอร์สองเครื่องโดยใช้สาย Ethernet สายเดียว การเชื่อมต่อนี้ช่วยให้ข้อมูลถูกส่งไปถึงปลายทางโดยไม่ผ่านการกระจายข้อมูลไปยังอุปกรณ์อื่น

4. Anonymous FTP คืออะไร? (นาทีที่ 16.20)

Anonymous FTP เป็นบริการที่ช่วยให้ผู้ใช้สามารถเข้าถึงไฟล์ที่ถูกแชร์ผ่านเซิร์ฟเวอร์ FTP โดยไม่ต้องระบุชื่อผู้ใช้หรือรหัสผ่าน ผู้ใช้สามารถเข้าสู่ระบบด้วยชื่อผู้ใช้ว่า "anonymous" และมักใส่อีเมลเป็นรหัสผ่าน ทำให้เป็นวิธีการที่สะดวกในการแจกจ่ายไฟล์ต่อสาธารณะ

5. Subnet Mask คืออะไร? (นาทีที่ 17.41)

Subnet Mask คือค่าที่ใช้ในการแบ่งเครือข่ายออกเป็น subnet หรือเครือข่ายย่อย โดยใช้ร่วมกับ IP Address เพื่อแยกส่วนของที่อยู่ที่ใช้ระบุตัวอุปกรณ์ในเครือข่ายจากส่วนที่ใช้ระบุเครือข่าย ซึ่งช่วยให้มีการจัดการเครือข่ายอย่างมีประสิทธิภาพมากขึ้น เช่น Subnet Mask 255.255.255.0 แสดงว่ามี 256 IP Address ใน subnet นี้

6. ความยาวสูงสุดที่อนุญาตสำหรับสาย UTP คือเท่าใด? (นาทีที่ 19.26)

ความยาวสูงสุดที่อนุญาตสำหรับสาย UTP (Unshielded Twisted Pair) คือ **100 เมตร** การใช้สายยาวเกินกว่านี้อาจทำให้เกิดการสูญเสียสัญญาณหรือสัญญาณอ่อนเกินไปจนไม่สามารถสื่อสารได้อย่างมีประสิทธิภาพ

7. Data Encapsulation คืออะไร? (นาทีที่ 20.37)

Data Encapsulation คือกระบวนการที่ข้อมูลจากชั้นที่สูงกว่าถูกบรรจุหรือห่อหุ้มด้วยหัวข้อ (Header) ที่ชั้นล่างกว่าเพื่อเตรียมการส่งผ่านข้อมูล แต่ละชั้นใน OSI Model จะเพิ่มข้อมูลการควบคุมของตัวเองเข้าไปในส่วนหัวข้อมูลก่อนที่จะส่งไปยังชั้นล่าง กระบวนการนี้ช่วยให้ข้อมูลสามารถเดินทางผ่านเครือข่ายไปถึงปลายทางได้

1. Network Topology คืออะไร? (นาทีที่ 0.00)

Network Topology คือรูปแบบการจัดการเชื่อมต่อของอุปกรณ์ในเครือข่าย ซึ่งแสดงถึงวิธีการเชื่อมต่อระหว่างอุปกรณ์ต่างๆ ภายในเครือข่าย เช่น Star, Bus, Ring, Mesh หรือ Hybrid แต่ละแบบมีข้อดีและข้อเสียต่างกัน ขึ้นอยู่กับความต้องการของการใช้งานและประสิทธิภาพในการรับส่งข้อมูล

2. VPN คืออะไร? (นาทีที่ 1.07)

VPN (Virtual Private Network) คือเทคโนโลยีที่ใช้สร้างการเชื่อมต่อแบบปลอดภัยผ่านเครือข่ายอินเทอร์เน็ตสาธารณะ โดยการเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่าย ทำให้ผู้ใช้งานสามารถเชื่อมต่อกับเครือข่ายภายในองค์กรหรือเครือข่ายส่วนตัวได้อย่างปลอดภัยจากระยะไกล

3. NAT คืออะไร? (นาทีที่ 2.12)

NAT (Network Address Translation) คือกระบวนการแปลงที่อยู่ IP ภายในเครือข่ายส่วนตัวให้กลายเป็นที่อยู่ IP สาธารณะเมื่อข้อมูลถูกส่งออกไปยังอินเทอร์เน็ต และเมื่อได้รับข้อมูลกลับมา NAT จะทำการแปลงที่อยู่ IP สาธารณะกลับมา

เป็นที่อยู่ IP ภายในอีกครั้ง ทำให้สามารถเชื่อมต่อหลายอุปกรณ์ในเครือข่ายเดียวกันออกสู่อินเทอร์เน็ตได้โดยใช้ที่อยู่ IP สาธารณะเพียงหนึ่งเดียว

4. หน้าที่การทำงานของ Network Layer ใน OSI model คืออะไร? (นาทีที่ 3.22)

Network Layer (Layer 3) ใน OSI Model มีหน้าที่หลักในการกำหนดเส้นทางและการส่งต่อข้อมูลจากต้นทางไปยังปลายทางในเครือข่ายต่างๆ โดยใช้ที่อยู่ IP เพื่อระบุตำแหน่งของอุปกรณ์แต่ละตัวในเครือข่าย การทำงานของ Network Layer ยังรวมถึงการกำหนดเส้นทาง (Routing) และการจัดการการถ่ายโอนข้อมูลระหว่างเครือข่ายต่างๆ

5. Network Topology ส่งผลต่อการจัดตั้งระบบเครือข่ายได้อย่างไร? (นาทีที่ 4.43)

Network Topology ส่งผลต่อประสิทธิภาพและการจัดการเครือข่าย เช่น Star Topology จะมีความสามารถในการจัดการง่ายและมีความทนทาน หากอุปกรณ์ใดเสียสามารถตัดเฉพาะอุปกรณ์นั้นได้ แต่หากใช้ Bus Topology อุปกรณ์ทุกตัวจะเชื่อมต่อกับสายหลักเดียวกัน ทำให้เกิดปัญหาการจราจรของข้อมูลได้ง่ายหากอุปกรณ์หรือสายใดมีปัญหา รูปแบบ Topology จึงส่งผลโดยตรงต่อความเสถียร ความเร็ว และความยืดหยุ่นของเครือข่าย

6. Routing Protocol คืออะไร? (นาทีที่ 6.26)

Routing Protocol คือกฎเกณฑ์และวิธีการที่อุปกรณ์เครือข่าย (เช่น Router) ใช้ในการค้นหาเส้นทางที่ดีที่สุดสำหรับการส่งข้อมูลระหว่างเครือข่ายต่างๆ Routing Protocol ยังช่วยให้ Router สามารถแลกเปลี่ยนข้อมูลเกี่ยวกับเส้นทางกับ Router อื่นๆ ในเครือข่ายได้ ตัวอย่างของ Routing Protocol ได้แก่ RIP, OSPF และ BGP

7. RIP คืออะไร? (นาทีที่ 8.26)

RIP (Routing Information Protocol) เป็น Routing Protocol แบบดั้งเดิมที่ใช้ในการกำหนดเส้นทางบนเครือข่าย IP โดยใช้วิธีการส่งข้อมูลระยะทาง (Hop Count) เพื่อค้นหาเส้นทางที่ดีที่สุด เส้นทางที่มีจำนวน Hop น้อยที่สุดจะถูกเลือก อย่างไรก็ตาม RIP มีข้อจำกัดที่สามารถใช้ได้ในเครือข่ายที่มีขนาดเล็กหรือขนาดกลาง เพราะสามารถส่งข้อมูลได้เพียง 15 Hop เท่านั้น

8. Switch Capacity คืออะไร? (นาทีที่ 9.47)

Switch Capacity หมายถึงความสามารถในการจัดการและการส่งข้อมูลของ Switch ในเครือข่าย ซึ่งวัดจากจำนวนข้อมูลที่สามารถผ่านอุปกรณ์ Switch ในช่วงเวลาหนึ่งๆ รวมถึงจำนวนพอร์ตที่สามารถเชื่อมต่อกับอุปกรณ์อื่นๆ ความจุนี้มีผลโดยตรงต่อประสิทธิภาพในการรับส่งข้อมูลของเครือข่าย

9. MAC Address คืออะไร? (นาทีที่ 12.49)

MAC Address (Media Access Control Address) คือที่อยู่ทางกายภาพที่ไม่ซ้ำกัน ซึ่งถูกกำหนดให้กับอุปกรณ์เครือข่ายทุกตัว เช่น การ์ด LAN หรือ Wi-Fi Adapter โดย MAC Address มีความยาว 48 บิต และถูกใช้ใน Data Link Layer ในการระบุตัวตนของอุปกรณ์ในเครือข่าย

10. Layer 2 Switch ต่างกับ Layer 3 Switch อย่างไร? (นาทีที่ 14.13)

Layer 2 Switch ทำงานที่ Data Link Layer (Layer 2) ของ OSI Model ซึ่งจะทำหน้าที่ส่งข้อมูลตาม MAC Address ของอุปกรณ์ในเครือข่ายภายในเดียวกัน ส่วน Layer 3 Switch ทำงานที่ Network Layer (Layer 3) และมีความสามารถในการกำหนดเส้นทางข้อมูล (Routing) โดยใช้ IP Address ได้ด้วย ดังนั้น Layer 3 Switch จึงสามารถทำงานแทน Router ในบางเครือข่ายได้

1. Gateway คืออะไร? (นาทีที่ 0.00)

Gateway คืออุปกรณ์ที่ทำหน้าที่เป็นจุดเชื่อมต่อระหว่างเครือข่ายสองเครือข่ายที่แตกต่างกัน เช่น ระหว่างเครือข่ายภายในองค์กรกับอินเทอร์เน็ต หรือระหว่างสองเครือข่ายที่ใช้โปรโตคอลต่างกัน Gateway ทำหน้าที่แปลงข้อมูลให้สามารถสื่อสารกันได้ระหว่างเครือข่ายเหล่านั้น

2. Collision Domain คืออะไร? (นาทีที่ 0.54)

Collision Domain คือบริเวณในเครือข่ายที่มีการชนกันของสัญญาณหรือแพ็กเกจข้อมูลเกิดขึ้น เมื่ออุปกรณ์สองตัวหรือมากกว่าส่งข้อมูลพร้อมกันในเครือข่ายแบบ Half-Duplex การชนกันนี้ทำให้ข้อมูลต้องถูกส่งซ้ำ การจัดการ Collision Domain ช่วยลดปัญหาการชนกันของข้อมูลได้

3. Broadcast Domain คืออะไร? (นาทีที่ 3.35)

Broadcast Domain คือบริเวณในเครือข่ายที่ข้อมูลประเภท Broadcast สามารถส่งไปถึงอุปกรณ์ทุกตัวในเครือข่ายได้ หากอุปกรณ์ใดใน Broadcast Domain ส่งข้อมูลแบบ Broadcast แพ็กเกจข้อมูลนั้นจะถูกส่งไปยังอุปกรณ์ทุกตัวภายใน Domain นั้น การแบ่ง Broadcast Domain ทำได้โดยใช้ Router หรือ Switch ระดับ Layer 3

4. Ethernet Bridge คืออะไร? (นาทีที่ 5.50)

Ethernet Bridge คืออุปกรณ์ที่ใช้ในการเชื่อมต่อและกรองข้อมูลระหว่างสองหรือมากกว่าสองเครือข่ายภายใน LAN โดย Bridge จะทำงานที่ Data Link Layer (Layer 2) ของ OSI Model และใช้ MAC Address ในการตัดสินใจว่าส่งข้อมูลไปยังพอร์ตใดเพื่อให้การรับส่งข้อมูลมีประสิทธิภาพ

5. Bridge กับ Switch ต่างกันอย่างไร? (นาทีที่ 8.32)

Bridge และ Switch ทั้งสองทำงานที่ Layer 2 ของ OSI Model แต่มีความแตกต่างกันในด้านประสิทธิภาพและการใช้งาน:

- **Bridge**: มีพอร์ตน้อยกว่าและจัดการข้อมูลได้ช้ากว่า มักใช้ในการเชื่อมต่อเครือข่ายขนาดเล็ก
- **Switch**: มีหลายพอร์ตและสามารถจัดการการส่งข้อมูลได้รวดเร็วกว่าเพราะสามารถส่งข้อมูลพร้อมกันไปยังพอร์ตต่างๆ และจัดการการชนกันของสัญญาณได้ดีกว่า

6. เราสามารถระบุ Class ของ IP address ได้อย่างไร? โดยดูจากอะไร? (นาทีที่ 10.44)

เราสามารถระบุ Class ของ IP Address ได้โดยดูจากเลขในส่วนแรกของ IP Address โดยแบ่ง Class เป็น:

- **Class A**: เริ่มต้นด้วย 1-126 (เช่น 10.x.x.x)
- **Class B**: เริ่มต้นด้วย 128-191 (เช่น 172.16.x.x)
- **Class C**: เริ่มต้นด้วย 192-223 (เช่น 192.168.x.x)
- **Class D**: เริ่มต้นด้วย 224-239 ใช้สำหรับการ Broadcast
- **Class E**: เริ่มต้นด้วย 240-255 ใช้สำหรับการทดลองและการวิจัย

7. Firewall คืออะไร? (นาทีที่ 12.07)

Firewall คืออุปกรณ์หรือซอฟต์แวร์ที่ทำหน้าที่กรองและควบคุมการเข้าถึงข้อมูลระหว่างเครือข่ายภายในและเครือข่ายภายนอก (เช่น อินเทอร์เน็ต) Firewall จะทำหน้าที่ป้องกันภัยคุกคามและการโจมตีจากภายนอกโดยกำหนดกฎเกณฑ์ในการอนุญาตหรือปฏิเสธการเชื่อมต่อและการรับส่งข้อมูล

8. Star Topology มีข้อดี ข้อเสียอย่างไร? (นาทีที่ 13.18)

ข้อดีของ **Star Topology**:

- การจัดการง่าย เนื่องจากอุปกรณ์ทุกตัวเชื่อมต่อกับอุปกรณ์กลาง (เช่น Switch)
- หากอุปกรณ์ใดมีปัญหาจะไม่ส่งผลต่อการทำงานของอุปกรณ์อื่น
- ง่ายต่อการขยายเครือข่าย

ข้อเสีย:

- หากอุปกรณ์กลาง (เช่น Switch หรือ Hub) ล่ม เครือข่ายทั้งหมดจะหยุดทำงาน
- ใช้สายเคเบิลมากกว่ารูปแบบอื่น เช่น Bus Topology

9. Tracert มีไว้ทำอะไร? (นาทีที่ 14.30)

Tracert (หรือ Trace Route) เป็นคำสั่งที่ใช้ในการตรวจสอบเส้นทางที่ข้อมูลถูกส่งผ่านจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นๆ ในเครือข่าย โดยจะแสดงรายการของ Router ที่ข้อมูลผ่านในแต่ละจุด ช่วยให้เราทราบได้ว่ามีการชะลอตัวหรือปัญหาเกิดขึ้นในเครือข่ายที่ใด

1. DHCP คืออะไร? (นาทีที่ 0.00)

DHCP (Dynamic Host Configuration Protocol) คือโปรโตคอลที่ใช้ในการกำหนด IP Address อัตโนมัติให้กับอุปกรณ์ในเครือข่าย เมื่ออุปกรณ์เข้ามาเชื่อมต่อกับเครือข่าย DHCP Server จะทำการแจกจ่าย IP Address ให้แก่อุปกรณ์นั้น โดยไม่จำเป็นต้องกำหนดค่าเองแบบ Manual

2. งานหลักของ ARP คืออะไร? (นาทีที่ 1.10)

ARP (Address Resolution Protocol) มีหน้าที่ในการแปลงที่อยู่ IP (ใน Network Layer) ให้กลายเป็น MAC Address (ใน Data Link Layer) โดยเฉพาะในเครือข่าย Ethernet เมื่ออุปกรณ์ต้องการส่งข้อมูลไปยังอุปกรณ์อื่นในเครือข่าย ARP จะค้นหา MAC Address ที่ตรงกับ IP Address ที่ต้องการสื่อสาร

3. Default Gateway มีไว้ทำอะไร? (นาทีที่ 4.47)

Default Gateway คืออุปกรณ์ที่ใช้สำหรับส่งต่อข้อมูลจากเครือข่ายภายในไปยังเครือข่ายภายนอก หากอุปกรณ์ในเครือข่ายต้องการส่งข้อมูลไปยังที่อยู่ IP ที่อยู่นอกเครือข่ายของตนเอง ข้อมูลจะถูกส่งไปยัง Default Gateway ก่อนที่จะถูกส่งไปยังปลายทาง

4. จะเกิดอะไรขึ้นหากเดินสายสัญญาณเกินกว่ากำหนด? (นาทีที่ 7.02)

หากสายสัญญาณถูกเดินเกินระยะที่กำหนด (เช่น สาย UTP ระยะสูงสุดคือ 100 เมตร) จะทำให้เกิดการสูญเสียสัญญาณ สัญญาณที่ส่งอาจอ่อนเกินไปจนไม่สามารถสื่อสารกันได้อย่างมีประสิทธิภาพ หรืออาจทำให้เกิดความล่าช้าในการส่งข้อมูล

5. ปัญหาการทำงานของ Software อย่างไรบ้าง? ที่ส่งผลทำให้เครือข่ายทำงานบกพร่อง? (นาทีที่ 8.04)

ปัญหาของซอฟต์แวร์ที่ส่งผลให้เครือข่ายทำงานบกพร่อง เช่น:

- การกำหนดค่าโปรโตคอลผิดพลาด
- ซอฟต์แวร์เครือข่ายที่มี Bug หรือข้อผิดพลาด
- ระบบปฏิบัติการล้าสมัยหรือไม่รองรับการจัดการเครือข่ายอย่างมีประสิทธิภาพ
- การกำหนดค่าความปลอดภัยไม่เหมาะสม ทำให้เกิดการรั่วไหลของข้อมูลหรือการโจมตีเครือข่าย

6. ICMP คืออะไร? (นาทีที่ 9.21)

ICMP (Internet Control Message Protocol) เป็นโปรโตคอลที่ใช้ในการส่งข้อความควบคุมและแจ้งเตือนเมื่อเกิดปัญหาในกระบวนการส่งข้อมูล เช่น การแจ้งเตือนเมื่อไม่สามารถเข้าถึงปลายทางได้ หรือใช้ในการตรวจสอบการเชื่อมต่อผ่านคำสั่ง `ping`

7. เราสามารถเชื่อมต่อคอมพิวเตอร์ 2 เครื่อง เพื่อสื่อสารระหว่างกันโดยไม่ต้องเชื่อมต่อผ่าน Switch Hub ได้หรือไม่? (นาทีที่ 10.49)

ได้ สามารถเชื่อมต่อคอมพิวเตอร์ 2 เครื่องโดยตรงผ่านสาย **Crossover Ethernet Cable** ซึ่งเป็นสายที่เชื่อมต่อสายสัญญาณบางเส้นแบบไขว้กัน ทำให้สามารถสื่อสารกันได้โดยไม่ต้องผ่าน Switch หรือ Hub

8. CSMA/CD คืออะไร? (นาทีที่ 12.09)

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) เป็นกลไกที่ใช้ในเครือข่าย Ethernet แบบมีสายเพื่อควบคุมการส่งข้อมูล โดยตรวจสอบว่าช่องสัญญาณว่างก่อนจะส่งข้อมูล และหากพบว่ามีการชนกันของสัญญาณ (Collision) ก็จะหยุดส่งข้อมูลและรอเวลาสุ่มก่อนจะส่งใหม่

9. จุดประสงค์ของการใช้งาน Dynamic Routing Protocol คืออะไร? (นาทีที่ 15.51)

จุดประสงค์ของการใช้งาน Dynamic Routing Protocol คือเพื่อให้ Router ในเครือข่ายสามารถค้นหาและปรับเส้นทางที่ดีที่สุดในการส่งข้อมูลได้โดยอัตโนมัติ โดยจะทำการแลกเปลี่ยนข้อมูลเส้นทางกับ Router อื่นๆ ในเครือข่ายเพื่อปรับปรุงการทำงานให้เกิดประสิทธิภาพสูงสุด

10. ข้อดีและข้อด้อยของ Dynamic Routing คืออะไร? (นาทีที่ 16.42)

ข้อดีของ Dynamic Routing:

- ปรับเปลี่ยนเส้นทางการส่งข้อมูลโดยอัตโนมัติหากเส้นทางมีปัญหา
- ลดภาระในการจัดการเครือข่ายด้วยตนเอง (Manual Configuration)
- สามารถรองรับเครือข่ายขนาดใหญ่และซับซ้อนได้

ข้อด้อยของ Dynamic Routing:

- ใช้ทรัพยากรของระบบมากขึ้นในการประมวลผลข้อมูลเส้นทาง
- อาจเกิดการส่งข้อมูลวนซ้ำ (Routing Loop) หากมีการกำหนดค่าไม่ถูกต้อง

- การตั้งค่าเริ่มต้นซับซ้อนกว่าการใช้ Static Routing

11. Ipconfig คืออะไร? (นาทีที่ 18.00)

`Ipconfig` เป็นคำสั่งที่ใช้ในระบบปฏิบัติการ Windows เพื่อแสดงข้อมูลการตั้งค่า IP Address ของอุปกรณ์ที่ใช้งาน รวมถึงการแสดงข้อมูลที่เกี่ยวข้องกับการเชื่อมต่อเครือข่าย เช่น Subnet Mask, Default Gateway และ MAC Address นอกจากนี้ยังสามารถใช้เพื่อปล่อยและรับ IP Address ใหม่จาก DHCP Server ได้ด้วย

12. Port Address Translation คืออะไร? (นาทีที่ 19.28)

Port Address Translation (PAT) เป็นเทคนิคที่ใช้ในการแปลง IP Address ภายในเครือข่ายให้สามารถเชื่อมต่อกับภายนอกได้โดยใช้ IP Address สาธารณะเพียงตัวเดียว โดยการแปลงนี้จะใช้หมายเลขพอร์ตในการแยกแยะการเชื่อมต่อของอุปกรณ์ภายในแต่ละตัว ซึ่งเป็นรูปแบบหนึ่งของ NAT (Network Address Translation)

13. VPN คืออะไร? (นาทีที่ 21.32)

VPN (Virtual Private Network) คือการเชื่อมต่อเครือข่ายส่วนตัวผ่านเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต โดยการเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่าย ทำให้การเชื่อมต่อมีความปลอดภัยมากยิ่งขึ้น VPN ใช้สำหรับการเชื่อมต่อจากระยะไกลเพื่อเข้าถึงทรัพยากรภายในองค์กรอย่างปลอดภัย

1. Domain Name System คืออะไร? (นาทีที่ 0.00)

Domain Name System (DNS) คือระบบที่ทำหน้าที่แปลงชื่อโดเมน (เช่น www.example.com) ให้กลายเป็น IP Address ที่ใช้งานได้ในเครือข่ายอินเทอร์เน็ต DNS ทำให้ผู้ใช้สามารถจดจำชื่อเว็บไซต์ง่ายๆ แทนการจำ IP Address และทำหน้าที่เป็น "สมุดโทรศัพท์ของอินเทอร์เน็ต" ที่คอยแปลงชื่อให้กลายเป็นหมายเลข IP เพื่อให้อุปกรณ์เชื่อมต่อกันได้

2. Tunnel Mode หมายถึงอะไร? (นาทีที่ 1.51)

Tunnel Mode เป็นโหมดหนึ่งในการทำงานของ IPsec (Internet Protocol Security) ที่ใช้ในการเข้ารหัสข้อมูลสำหรับการส่งผ่านข้อมูลระหว่างสองเครือข่าย โดยทั้งข้อมูล Payload และ Header ของ IP Packet จะถูกเข้ารหัสใน Tunnel Mode ซึ่งทำให้ข้อมูลมีความปลอดภัยมากขึ้นในการส่งผ่านเครือข่ายสาธารณะ

3. Power Over Ethernet คืออะไร? (นาทีที่ 2.32)

Power over Ethernet (PoE) คือเทคโนโลยีที่ใช้ในการส่งพลังงานไฟฟ้าผ่านสาย Ethernet ทำให้สามารถจ่ายพลังงานให้กับอุปกรณ์ เช่น กล้องวงจรปิด (IP Camera) หรือ Access Point โดยไม่จำเป็นต้องใช้สายไฟแยกต่างหาก ซึ่งทำให้การติดตั้งอุปกรณ์ง่ายขึ้นและลดความซับซ้อน

4. เทคโนโลยี PoE มีประโยชน์อะไรบ้าง? (นาทีที่ 6.00)

ประโยชน์ของเทคโนโลยี PoE มีดังนี้:

- ลดการใช้สายไฟ เพราะสามารถส่งทั้งข้อมูลและพลังงานไฟฟ้าผ่านสาย Ethernet เส้นเดียว
- ช่วยให้การติดตั้งอุปกรณ์ในพื้นที่ที่ไม่มีแหล่งจ่ายไฟสะดวกขึ้น เช่น กล้องวงจรปิดในที่สูง
- ช่วยลดความซับซ้อนของการเดินสายและลดค่าใช้จ่ายในการติดตั้งระบบ
- ช่วยให้การจัดการและการควบคุมพลังงานของอุปกรณ์เครือข่ายทำได้ง่ายขึ้น

5. Forwarding Performance หรือ Transmit Rate คืออะไร? (นาทีที่ 7.47)

Forwarding Performance หรือ Transmit Rate หมายถึงความสามารถในการส่งต่อแพ็กเกจข้อมูลของ Switch หรือ Router โดยวัดจากจำนวนแพ็กเกจข้อมูลที่อุปกรณ์สามารถจัดการและส่งต่อได้ในหนึ่งวินาที มีหน่วยเป็น packets per second (pps) ประสิทธิภาพนี้มีผลต่อความเร็วและความสามารถในการจัดการข้อมูลในเครือข่าย

6. วิธีการ Switching ของ Switch มีกี่แบบ? (นาทีที่ 13.41)

วิธีการ Switching ของ Switch มี 3 แบบหลักๆ ดังนี้:

1. **Store-and-Forward**: Switch จะรับข้อมูลทั้งเฟรมก่อนแล้วจึงทำการตรวจสอบความถูกต้องและส่งต่อไปยังปลายทาง หากมีข้อผิดพลาดจะไม่ส่งข้อมูลออกไป
2. **Cut-Through**: Switch จะส่งข้อมูลออกไปทันทีหลังจากตรวจสอบที่อยู่ปลายทาง (MAC Address) โดยไม่รอรับเฟรมทั้งหมด ทำให้ส่งข้อมูลได้เร็วกว่า

3. **Fragment-Free**: เป็นการผสมระหว่าง Store-and-Forward และ Cut-Through โดย Switch จะตรวจสอบข้อมูลในช่วงแรกของเฟรมก่อนที่จะส่งต่อเพื่อลดข้อผิดพลาด

1. Static Routing คืออะไร? (นาทีที่ 0.00)

Static Routing คือการกำหนดเส้นทางการส่งข้อมูลระหว่างเครือข่ายโดยกำหนดด้วยตนเอง (Manual) ใน Router หรืออุปกรณ์เครือข่าย ผู้ดูแลระบบต้องทำการตั้งค่าเส้นทางแต่ละเส้นทางด้วยตนเอง ซึ่งทำให้ Static Routing มีความเสถียรและง่ายต่อการคาดการณ์ แต่ต้องการการจัดการที่ละเอียดในเครือข่ายขนาดใหญ่

2. คำสั่ง Ping มีไว้เพื่ออะไร? และให้ข้อมูลอะไรแก่เราบ้าง? (นาทีที่ 3.06)

คำสั่ง Ping ใช้ในการตรวจสอบการเชื่อมต่อระหว่างคอมพิวเตอร์สองเครื่องหรือระหว่างอุปกรณ์ในเครือข่าย โดยการส่ง ICMP Echo Request ไปยังปลายทางและรอการตอบกลับ คำสั่งนี้จะให้ข้อมูลเกี่ยวกับความหน่วง (Latency) และการสูญหายของแพ็กเกจ (Packet Loss) ซึ่งบ่งบอกถึงสภาพของการเชื่อมต่อเครือข่าย

3. ปัญหาเครือข่ายทำงานช้า มักมีสาเหตุจากอะไร? (นาทีที่ 4.27)

ปัญหาเครือข่ายทำงานช้ามักมีสาเหตุมาจากหลายปัจจัย เช่น:

- แบนด์วิธไม่เพียงพอสำหรับปริมาณการใช้งาน
- การชนกันของข้อมูลใน Collision Domain
- ปัญหาการตั้งค่าอุปกรณ์เครือข่ายผิดพลาด
- สายสัญญาณมีปัญหา เช่น สายสัญญาณชำรุดหรือระยะทางเกินกำหนด
- การใช้งานซอฟต์แวร์หรือระบบที่ไม่รองรับการทำงานเครือข่ายอย่างมีประสิทธิภาพ

4. Spanning-Tree มีไว้ทำอะไร? (นาทีที่ 6.42)

Spanning-Tree Protocol (STP) มีไว้เพื่อป้องกันการเกิด **Loop** ในเครือข่ายที่เชื่อมต่อด้วย Switch หลายตัว ซึ่งอาจทำให้ข้อมูลถูกส่งวนไปเรื่อยๆ และทำให้เครือข่ายทำงานไม่ปกติ STP จะทำการปิดพอร์ตที่เกิด Loop และทำให้เครือข่ายสามารถทำงานได้อย่างต่อเนื่องโดยไม่เกิดปัญหาการวนซ้ำของข้อมูล

5. SMTP คืออะไร? (นาทีที่ 8.35)

SMTP (Simple Mail Transfer Protocol) คือโปรโตคอลที่ใช้สำหรับการส่งอีเมลจากเครื่องผู้ส่งไปยัง Mail Server และระหว่าง Mail Server ด้วยกัน SMTP เป็นโปรโตคอลหลักที่ใช้ในการส่งอีเมลในเครือข่ายอินเทอร์เน็ต

6. หน้าที่หลักของ Transport Layer คืออะไร? (นาทีที่ 10.24)

หน้าที่หลักของ Transport Layer ใน OSI Model คือการจัดการการรับส่งข้อมูลระหว่างต้นทางและปลายทาง โดยการแบ่งข้อมูลออกเป็นส่วนๆ (Segments) ตรวจสอบการส่งข้อมูลให้ถูกต้อง และทำการจัดการการควบคุมการไหล (Flow Control) และการตรวจสอบข้อผิดพลาด (Error Control) ตัวอย่างโปรโตคอลในชั้นนี้ได้แก่ TCP และ UDP

7. หน้าที่การทำงานของ TCP คืออะไร? (นาทีที่ 18.12)

TCP (Transmission Control Protocol) เป็นโปรโตคอลใน Transport Layer ที่ทำหน้าที่รับประกันการส่งข้อมูลระหว่างต้นทางและปลายทาง โดย TCP จะตรวจสอบให้แน่ใจว่าข้อมูลถูกส่งครบถ้วน ถูกลำดับ และไม่มีข้อผิดพลาด นอกจากนี้ TCP ยังมีการควบคุมการไหลของข้อมูลและการจัดการการเชื่อมต่อแบบ Connection-Oriented

8. สาย UTP แบ่งเป็น Category อะไรบ้าง? (นาทีที่ 20.46)

สาย UTP (Unshielded Twisted Pair) แบ่งออกเป็นหลาย Category ขึ้นอยู่กับความเร็วและความถี่ที่รองรับ เช่น:

- **Cat 5**: รองรับความเร็ว 100 Mbps
- **Cat 5e**: รองรับความเร็ว 1 Gbps
- **Cat 6**: รองรับความเร็ว 10 Gbps ในระยะสั้น
- **Cat 6a**: รองรับความเร็ว 10 Gbps ในระยะที่ไกลขึ้น
- **Cat 7**: รองรับความเร็ว 10 Gbps ขึ้นไปและมีการป้องกันสัญญาณรบกวน

9. Permanent Link คืออะไร? (นาทีที่ 23.33)

Permanent Link คือส่วนของสายสัญญาณในโครงสร้างเครือข่ายที่มีการติดตั้งถาวรระหว่าง Patch Panel กับ Work Area Outlet โดยไม่รวมถึงสาย Patch Cable ที่เชื่อมต่ออุปกรณ์เข้ากับ Outlet เป็นส่วนสำคัญของการวางโครงสร้างพื้นฐานเครือข่ายที่มีความถาวรและเสถียร

10. Channel Link คืออะไร? (นาทีที่ 25.16)

Channel Link คือการรวมทุกองค์ประกอบของการเชื่อมต่อเครือข่ายระหว่างต้นทางและปลายทาง รวมทั้ง Permanent Link, Patch Cable, และสายเชื่อมต่ออื่นๆ ที่ใช้ในการเชื่อมอุปกรณ์กับเครือข่าย การจัดการ Channel Link จะช่วยให้สามารถวิเคราะห์ปัญหาและปรับปรุงประสิทธิภาพของเครือข่ายได้

11. โครงสร้างการเดินสายสัญญาณในอาคารประกอบด้วยอะไรบ้าง? (นาทีที่ 26.51)

โครงสร้างการเดินสายสัญญาณในอาคาร (Structured Cabling) ประกอบด้วย:

- **Work Area**: พื้นที่ที่มีการติดตั้งอุปกรณ์ปลายทาง เช่น คอมพิวเตอร์ โทรศัพท์
- **Horizontal Cabling**: การเดินสายสัญญาณจาก Work Area ไปยัง Telecom Room
- **Telecom Room**: ห้องที่มีอุปกรณ์เชื่อมต่อเครือข่าย เช่น Switch และ Patch Panel
- **Backbone Cabling**: สายสัญญาณที่เชื่อมต่อ Telecom Room แต่ละห้องในอาคารหรือระหว่างอาคาร
- **Equipment Room**: ห้องที่ใช้วางอุปกรณ์เครือข่ายหลัก เช่น Server หรือ Switch หลัก
- **Entrance Facility**: จุดที่สายสัญญาณภายนอกเข้ามาในอาคาร

12. ในกรณีที่เครื่องคอมพิวเตอร์ไม่สามารถเชื่อมต่อกับเครือข่ายเกิดจากอะไร? (นาทีที่ 30.09)

ปัญหาที่ทำให้คอมพิวเตอร์ไม่สามารถเชื่อมต่อกับเครือข่ายอาจเกิดจาก:

- การตั้งค่า IP Address หรือ Default Gateway ผิดพลาด
- สายสัญญาณชำรุดหรือหลุด
- อุปกรณ์เครือข่าย เช่น Switch หรือ Router มีปัญหาหรือไม่ทำงาน
- ปัญหาที่ NIC (Network Interface Card) ของคอมพิวเตอร์

- ปัญหาซอฟต์แวร์ เช่น การตั้งค่า Firewall ที่ไม่อนุญาตการเชื่อมต่อ

1. สาย Fiber Multimode กับ Single Mode ต่างกันอย่างไร? (นาทีที่ 0.00)

สาย Fiber Optic มีสองประเภทหลักคือ **Multimode** และ **Single Mode**:

- **Multimode Fiber**: รองรับการส่งแสงหลายโหมดพร้อมกันในสายเดียว ความยาวคลื่นแสงและระยะการส่งข้อมูลสั้นกว่า (เหมาะสำหรับการใช้งานในระยะใกล้ เช่น ภายในอาคาร) ความเร็วในการส่งข้อมูลอยู่ที่ 10 Gbps ในระยะไม่เกิน 550 เมตร

- **Single Mode Fiber**: ใช้สำหรับการส่งข้อมูลในระยะทางไกล เนื่องจากมีการส่งแสงเพียงโหมดเดียว ความเร็วสูงมาก และมีระยะการส่งข้อมูลไกลกว่ามาก เหมาะสำหรับเครือข่ายระยะไกลหรือเชื่อมต่อระหว่างเมือง ระยะทางได้ถึงหลายสิบกิโลเมตร

2. สาย Fiber Optic ที่มีขนาดต่างกัน สามารถนำมาเชื่อมต่อกันได้หรือไม่? (นาทีที่ 2.17)

โดยทั่วไป **ไม่แนะนำ** ให้นำสาย Fiber Optic ที่มีขนาดแตกต่างกันมาเชื่อมต่อกัน เพราะอาจทำให้ประสิทธิภาพการส่งข้อมูลลดลงหรือเกิดการสูญเสียสัญญาณ (Signal Loss) ได้ แต่ถ้าจำเป็นต้องเชื่อมต่อสามารถใช้ **อุปกรณ์แปลง** หรือ **Adapter** เพื่อปรับขนาดของสัญญาณระหว่างสายทั้งสองประเภทให้เข้ากันได้

3. Protocol คืออะไร? (นาทีที่ 4.18)

Protocol คือชุดของกฎเกณฑ์ที่ใช้ในการควบคุมและจัดการการสื่อสารระหว่างอุปกรณ์ในเครือข่าย โปรโตคอลจะกำหนดรูปแบบและวิธีการส่งข้อมูลเพื่อให้สามารถสื่อสารระหว่างกันได้อย่างถูกต้อง ตัวอย่างเช่น TCP/IP, HTTP, FTP เป็นต้น

4. Half Duplex กับ Full Duplex ต่างกันอย่างไร? (นาทีที่ 5.48)

- **Half Duplex**: การสื่อสารในลักษณะที่สามารถส่งข้อมูลได้ทีละทาง (ทางใดทางหนึ่ง) เช่น การใช้ Walkie-Talkie ที่ผู้ใช้ต้องสลับกันพูด

- **Full Duplex**: การสื่อสารที่สามารถส่งข้อมูลได้ทั้งสองทางพร้อมกัน เช่น การโทรศัพท์ ที่ทั้งสองฝ่ายสามารถพูดและฟังพร้อมกันได้

5. Server Virtualization คืออะไร? (นาทีที่ 7.57)

Server Virtualization คือการสร้างเซิร์ฟเวอร์เสมือนบนเซิร์ฟเวอร์ทางกายภาพหนึ่งเครื่อง เพื่อแบ่งทรัพยากรของเครื่องให้กับเซิร์ฟเวอร์หลายเครื่อง (Virtual Server) ซึ่งช่วยให้การใช้ทรัพยากรมีประสิทธิภาพมากขึ้น ลดการใช้ฮาร์ดแวร์ และการจัดการเซิร์ฟเวอร์ทำได้ง่ายขึ้น

6. Hypervisor คืออะไร? (นาทีที่ 8.33)

Hypervisor คือซอฟต์แวร์ที่ใช้จัดการการสร้างและการรันเครื่องเสมือน (Virtual Machines) บนเซิร์ฟเวอร์ทางกายภาพ Hypervisor ทำหน้าที่จัดการทรัพยากรของเซิร์ฟเวอร์ เช่น CPU, หน่วยความจำ และอุปกรณ์ I/O เพื่อให้แต่ละเครื่องเสมือนสามารถทำงานได้อย่างเป็นอิสระ ตัวอย่างของ Hypervisor ได้แก่ VMware, Hyper-V, และ KVM

7. Virtual Switch คืออะไร? (นาทีที่ 10.00)

Virtual Switch คือซอฟต์แวร์ที่ทำหน้าที่เหมือน Switch ในเครือข่ายทางกายภาพ แต่ทำงานในสภาพแวดล้อมเสมือนจริง (Virtual Environment) ทำหน้าที่เชื่อมต่อเครื่องเสมือนหลายๆ เครื่องภายในเซิร์ฟเวอร์เดียวกันหรือระหว่างเซิร์ฟเวอร์เสมือนต่างๆ ในเครือข่ายเดียวกัน

8. DHCP Relay Agent คืออะไร? (นาทีที่ 11.58)

DHCP Relay Agent คืออุปกรณ์หรือซอฟต์แวร์ที่ทำหน้าที่ส่งต่อคำขอ DHCP จากอุปกรณ์ในเครือข่ายย่อย (Subnet) ไปยัง DHCP Server ที่อยู่ในเครือข่ายอื่น DHCP Relay Agent ช่วยให้ DHCP Server สามารถแจกจ่าย IP Address ให้กับอุปกรณ์ในเครือข่ายที่ไม่ได้อยู่ใน Subnet เดียวกันได้

9. DHCP Snooping คืออะไร? (นาทีที่ 14.06)

DHCP Snooping คือเทคนิคความปลอดภัยที่ใช้ใน Switch เพื่อตรวจสอบและควบคุมการจ่าย IP Address ของ DHCP Server ที่ไม่ได้รับอนุญาต ช่วยป้องกันการโจมตีแบบ DHCP Spoofing ซึ่งอาจทำให้ผู้โจมตีสามารถควบคุมการแจกจ่าย IP Address ในเครือข่ายได้

1. Proxy Server คืออะไร? (นาทีที่ 0.00)

Proxy Server คือเซิร์ฟเวอร์ที่ทำหน้าที่เป็นตัวกลางระหว่างผู้ใช้และอินเทอร์เน็ต เมื่อผู้ใช้ร้องขอการเข้าถึงเว็บไซต์หรือทรัพยากรออนไลน์ Proxy Server จะทำการรับคำขอและส่งต่อไปยังปลายทาง แล้วนำข้อมูลที่ได้กลับมาให้ผู้ใช้ Proxy ช่วยให้สามารถเพิ่มความปลอดภัย ปกปิดที่อยู่ IP และควบคุมการเข้าถึงเว็บไซต์ได้

2. Access Network คืออะไร? (นาทีที่ 10.14)

Access Network คือส่วนของเครือข่ายที่เชื่อมต่อผู้ใช้ปลายทาง (End Users) เข้ากับเครือข่ายหลัก (Core Network) เช่น การเชื่อมต่อจากบ้านหรือสำนักงานเข้าสู่ ISP (Internet Service Provider) ผ่านสายโทรศัพท์, สายเคเบิล หรือเครือข่ายไร้สาย

3. Network Core คืออะไร? (นาทีที่ 14.12)

Network Core คือโครงสร้างส่วนกลางของเครือข่ายที่ทำหน้าที่จัดการการส่งข้อมูลระหว่าง Access Network ต่างๆ Network Core ประกอบไปด้วย Router และ Switch ที่ทำงานร่วมกันเพื่อส่งข้อมูลระหว่างจุดต้นทางและปลายทางในเครือข่าย ทำหน้าที่เป็นศูนย์กลางของการสื่อสารข้อมูลในเครือข่ายขนาดใหญ่

4. สถาปัตยกรรมการให้บริการระบบเครือข่าย มีอะไรบ้าง? (นาทีที่ 15.02)

สถาปัตยกรรมการให้บริการระบบเครือข่ายหลักๆ ประกอบด้วย:

- **Client-Server Architecture**: การให้บริการผ่านเซิร์ฟเวอร์ที่ทำหน้าที่จัดการข้อมูลและบริการต่างๆ ที่ลูกข่าย (Client) ร้องขอ
- **Peer-to-Peer (P2P) Architecture**: อุปกรณ์ทุกตัวในเครือข่ายสามารถทำหน้าที่ทั้งเป็นผู้ให้บริการและผู้ร้องขอบริการได้โดยตรง
- **Cloud-Based Architecture**: การให้บริการผ่านระบบคลาวด์ที่อยู่ในศูนย์ข้อมูลระยะไกล โดยผู้ใช้สามารถเข้าถึงได้ผ่านอินเทอร์เน็ต

5. SMTP คืออะไร? (นาทีที่ 17.11)

SMTP (Simple Mail Transfer Protocol) คือโปรโตคอลที่ใช้ในการส่งอีเมลระหว่างเซิร์ฟเวอร์และจากลูกข่ายไปยังเซิร์ฟเวอร์ เพื่อจัดการการส่งอีเมลจากต้นทางไปยังปลายทาง SMTP ถูกใช้ในกระบวนการส่งเมล แต่ไม่ใช่โปรโตคอลที่ใช้ในการรับเมล (เช่น IMAP หรือ POP3)

6. Quality of Service (QoS) คืออะไร? (นาทีที่ 18.05)

Quality of Service (QoS) คือเทคนิคที่ใช้ในการจัดลำดับความสำคัญของการส่งข้อมูลในเครือข่ายเพื่อให้แน่ใจว่าข้อมูลประเภทที่มีความสำคัญ (เช่น วิดีโอคอล หรือเสียง) ได้รับการส่งต่อก่อนข้อมูลที่มีความสำคัญน้อยกว่า เช่น การดาวน์โหลดไฟล์ QoS ช่วยปรับปรุงประสิทธิภาพของเครือข่ายในการรองรับปริมาณการใช้ที่สูง

7. Link Aggregation คืออะไร? (นาทีที่ 20.05)

Link Aggregation คือการรวมสายเครือข่ายหลายเส้นเข้าด้วยกันเพื่อเพิ่มความจุในการส่งข้อมูลและเพิ่มความน่าเชื่อถือของการเชื่อมต่อ ซึ่งช่วยให้ข้อมูลถูกส่งผ่านได้เร็วขึ้นและมีการกระจายการรับส่งข้อมูลระหว่างลิงก์ที่เชื่อมต่อกัน ทำให้ลดการแออัดในเครือข่าย

8. Port Mirroring คืออะไร? (นาทีที่ 23.58)

Port Mirroring คือฟังก์ชันใน Switch หรือ Router ที่ทำให้สามารถสำเนาการจราจรข้อมูล (Traffic) จากพอร์ตหนึ่งไปยังอีกพอร์ตหนึ่งเพื่อทำการตรวจสอบหรือวิเคราะห์ข้อมูลได้ ซึ่งมักใช้ในการตรวจสอบความปลอดภัยและการแก้ไขปัญหาเครือข่าย