การบริหารจัดการระบบเครือข่าย (Network Management System)

เครือข่ายคอมพิวเตอร์ (Computer Network) เป็นโครงสร้างพื้นฐานที่สำคัญของแทบทุกองค์กรธุรกิจ เป็นการเชื่อมโยงกัน ระหว่าง อุปกรณ์ ต่างๆ เช่น Router, Switch, Server, Clients รวมถึง ผู้ใช้งาน User โดยรูปแบบการเชื่อมต่อของเครือข่าย มีหลากหลายรูปแบบ มีทั้งที่ ต้องตั้งค่าการเชื่อมต่อ และไม่ตั้งค่าการเชื่อมต่อ รวมถึงการป้องกัน หรือการกำหนดสิทธิ์การเข้าถึงต่างๆ ดังนั้น จำเป็นที่จะต้องเข้าใจระบบ NMS (Network Management System)

การบริหารจัดการเครือข่าย (Network Management) เป็นกรอบงานที่มีจุดมุ่งหมายเพื่อให้มั่นใจได้ว่าระบบเครือข่ายจะมีประสิทธิภาพเต็มเปี่ยมในการทำงาน (Performance) มีความพร้อมใช้งานอยู่เสมอ (Availability) มีความเชื่อถือได้ (Reliability) และมีความมั่นคงปลอดภัย (Security) เพื่อเอื้อให้การดำเนินงานและธุรกิจขององค์กรเป็นไปอย่างราบรื่น ทั้งนี้เราอาจแบ่งเนื้องาน Network Management ออกเป็นภาคส่วนสำคัญ (Key Area) ได้ 5 ภาคส่วน ตามโมเดล FCAPS (เอฟแคปส์) ซึ่งได้รับการออกแบบโดย “องค์การระหว่างประเทศว่าด้วยการมาตรฐาน” หรือ “ISO” (International Organization for Standardization) ซึ่งมีมาตรฐาน ISO หลายมาตรฐานเช่น ISO27001,ISO27032,ISO27701 เป็นต้น

FCAPS (เอฟแคปส์) เป็นชื่อย่อของหลักการบริหาร และจัดการเครือข่ายห้าตัวคือ

Fault (ความผิดพลาด)

Configuration (การตั้งค่าอุปกรณ์)

Accounting (การจดบันทึกการใช้งาน)

Performance (ประสิทธิภาพการทำงาน)

Security (ความปลอดภัย)

ISO27001 : มาตรฐานที่ครอบคลุมการจัดการความปลอดภัยของข้อมูล (ISMS) ซึ่งเป็นหัวใจหลักของการรักษาความปลอดภัยในเครือข่าย

ISO27932 : มาตรฐานสำหรับความปลอดภัยทางไซเบอร์โดยเฉพาะ เน้นกรอบการทำงานเพื่อเสริมสร้างความปลอดภัยในสภาพแวดล้อมไซเบอร์

ISO27701 : มาตรฐานที่เกี่ยวข้องกับการจัดการข้อมูลส่วนบุคคล (PIMS) ซึ่งมีความสำคัญต่อองค์กรที่ต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูล

NMS **(Network Management System)** ซึ่งหมายถึง **ระบบบริหารจัดการเครือข่าย** เป็นซอฟต์แวร์หรือชุดโปรแกรมที่ช่วยให้ผู้ดูแลเครือข่ายสามารถตรวจสอบและจัดการอุปกรณ์ต่างๆ ในเครือข่ายได้อย่างมีประสิทธิภาพ เช่น การตรวจสอบสถานะของอุปกรณ์, การวิเคราะห์ปัญหา, และการแก้ไขปัญหาที่เกิดขึ้นได้อย่างรวดเร็ว

หน้าที่หลัก ของ การบริหารจัดการระบบเครือข่าย NMS ประกอบด้วย

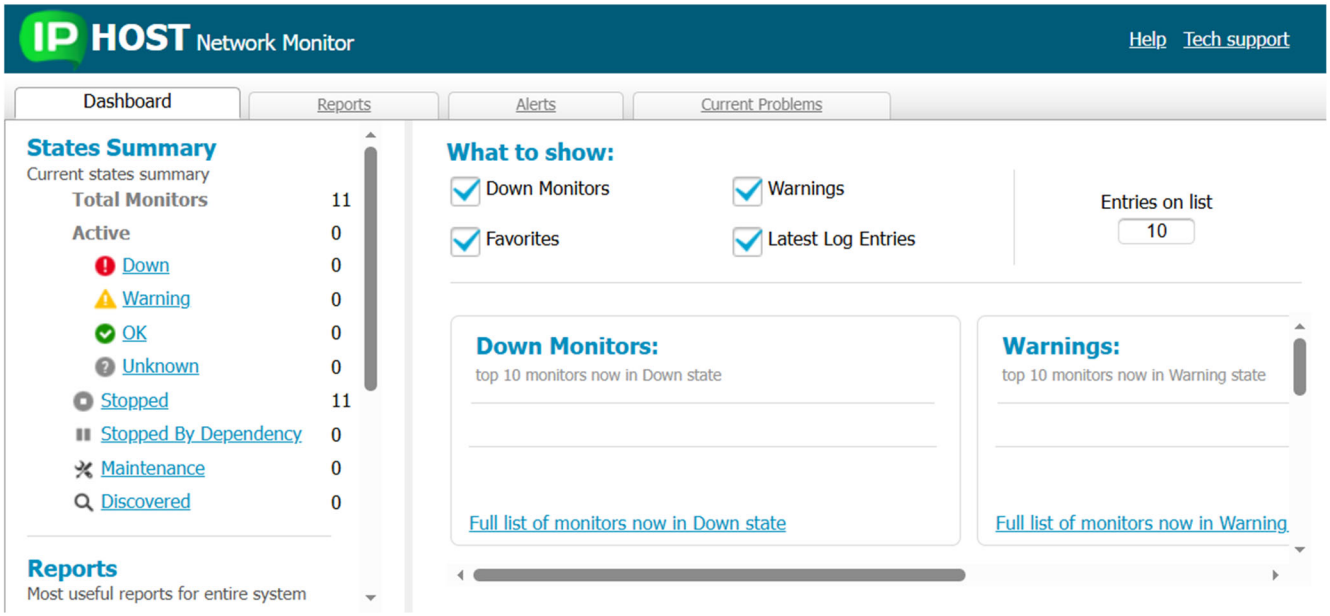
เฝ้าติดตาม (Monitoring): ตรวจสอบสถานะของอุปกรณ์ในเครือข่ายอย่างต่อเนื่อง เช่น การทำงานปกติหรือผิดปกติ

วิเคราะห์ปัญหา (Troubleshooting): วิเคราะห์ปัญหาที่เกิดขึ้น เช่น การแจ้งเตือนเมื่อมีอุปกรณ์ล่ม (interface down)

จัดการอุปกรณ์ (Device Management): ช่วยให้ผู้ดูแลสามารถตั้งค่า และจัดการอุปกรณ์เครือข่ายจากส่วนกลางได้

หลักทำงาน:

โดยทั่วไปใช้โปรโตคอล SNMP (Simple Network Management Protocol) ในการสื่อสารและรวบรวมข้อมูลจากอุปกรณ์เครือข่าย ข้อมูลที่เก็บรวบรวมจะถูกจัดเก็บไว้ในฐานข้อมูลที่เรียกว่า MIB (Management Information Base) ซึ่งมีอยู่ในระบบ NMS และบนอุปกรณ์แต่ละชิ้น แสดงผลในรูปแบบ GUI (Graphical User Interface) ทำให้ผู้ใช้สามารถมองเห็นภาพรวมและจัดการระบบได้ง่ายขึ้น



IP Host Network Monitor

โปรแกรมจัดการบริหารเครือข่าย ยังมีอีกมากที่มีทั้ง คุณภาพสูง, ใช้งานง่าย รวมถึงมีค่าใช้จ่ายหรือ ไม่มีค่าใช้จ่าย

พื้นฐานที่สำคัญของการบริหารจัดการระบบเครือข่าย สามารถแบ่งออกได้ดังนี้

1. การติดตั้งและกำหนดค่า

- การติดตั้งอุปกรณ์: ติดตั้งอุปกรณ์เครือข่ายที่จำเป็น เช่น เราเตอร์, สวิตช์, เซิร์ฟเวอร์ และ Access Point
- การกำหนดค่า: กำหนดค่าเครือข่ายเพื่อให้ทำงานได้อย่างถูกต้องและมีประสิทธิภาพตามความต้องการ

2. การตรวจสอบและบำรุงรักษา

- การตรวจสอบประจำวัน: ตรวจสอบการทำงานของระบบอย่างสม่ำเสมอเพื่อให้แน่ใจว่าระบบพร้อมใช้งานตลอดเวลา
- การอัพเดต: อัพเดตซอฟต์แวร์และฮาร์ดแวร์ให้เป็นเวอร์ชันล่าสุดอยู่เสมอเพื่อแก้ไขช่องโหว่และเพิ่มประสิทธิภาพ
- การสำรองข้อมูล: สำรองข้อมูลอย่างสม่ำเสมอเพื่อป้องกันการสูญหายจากปัญหาหรือการถูกทำลาย

3. การแก้ไขปัญหา

- การวิเคราะห์ปัญหา: เมื่อเกิดปัญหา เช่น เครือข่ายช้าหรือการเชื่อมต่อหลุด ผู้ดูแลระบบต้องสามารถวิเคราะห์หาสาเหตุและแก้ไขได้อย่างรวดเร็ว
- การใช้เครื่องมือ: ใช้เครื่องมือและเทคนิคที่เหมาะสมในการตรวจสอบฮาร์ดแวร์ ซอฟต์แวร์ และการตั้งค่าต่างๆ เพื่อแก้ไขปัญหา

4. การจัดการความปลอดภัย

- การป้องกันภัยคุกคาม: ป้องกันไวรัสและการโจมตีจากภายนอก เช่น การดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ หรือการใช้แผ่นดิสก์ที่ติดไวรัส
- การตั้งค่าความปลอดภัย: กำหนดค่าการรักษาความปลอดภัย เช่น การเข้ารหัสข้อมูลและการควบคุมสิทธิ์การเข้าถึง

5. การออกแบบและอัพเกรดระบบ

- การออกแบบโครงสร้าง: ออกแบบและวางแผนโครงสร้างเครือข่ายที่เหมาะสมกับความต้องการขององค์กร เช่น การเลือกใช้ Topology และสื่อกลางที่เหมาะสม
- การประเมินเทคโนโลยี: ประเมินและเลือกใช้เทคโนโลยีใหม่ๆ เช่น ระบบไร้สาย (Wireless) หรือระบบคลาวด์ (Cloud) เพื่อเพิ่มประสิทธิภาพและขยายเครือข่ายในอนาคต

1. การติดตั้งและกำหนดค่า

- การติดตั้งอุปกรณ์: ติดตั้งอุปกรณ์เครือข่ายที่จำเป็น เช่น เราเตอร์, สวิตช์, เซิร์ฟเวอร์ และ Access Point สิ่งที่จะเป็นตัวบ่งบอกว่า เราจะต้องติดตั้ง อุปกรณ์ใดบ้างในเครือข่าย จำเป็นต้องใช้ อุปกรณ์ หรือ เครื่องในเครือข่ายแบบใด คุณสมบัติต่ำสุดหรือสูงสุดที่ระบบต้องการมีอะไรบ้าง เป็นต้น

ตัวอย่างการออกแบบการบริหารจัดการระบบเครือข่าย

ในองค์กรหนึ่ง มีพนักงานที่ต้องใช้งานเครื่องคอมพิวเตอร์ในองค์กรทั้งหมด 3 แผนก โดยแต่ละแผนกจะมีเครื่องคอมพิวเตอร์ (Clients) ใช้งาน แผนกละ 3 เครื่อง โดยแต่ละเครื่องสามารถเชื่อมต่อเข้ากับ เครื่องศูนย์กลางข้อมูล (Server) และ แต่ละแผนก สามารถเข้าถึงข้อมูลส่วนกลางได้ ตามสิทธิ์ที่กำหนดไว้ จงออกแบบระบบเครื่องข่ายทั้งหมดนี้ ว่าต้องใช้ อุปกรณ์อะไรบ้าง และต้องใช้ Software อะไรบ้าง

ภาพรวมสถาปัตยกรรม (Concept)

- แต่ละแผนกอยู่ใน VLAN แยกกัน (เช่น VLAN 10, 20, 30) เพื่อแยก broadcast domain และควบคุมการเข้าถึง
- มีสวิตช์ระดับจัดการ (managed switch) รองรับ VLAN และ PoE (ถ้าต้องการกล้อง/โทรศัพท์)
- เราเตอร์/ไฟร์วอลล์ หน้าที่เชื่อมต่อระหว่าง VLAN และเชื่อมออกอินเทอร์เน็ต พร้อมนโยบาย ACL / NAT / VPN
- เซิร์ฟเวอร์ศูนย์กลาง (อาจเป็น Physical หรือ Virtual) ให้บริการ: AD/LDAP, DNS, DHCP (หรือ DHCP บนอุปกรณ์เครือข่าย), File Server / NAS, Backup, Authentication, และสามารถรันบริการอื่นได้ (เช่นฐานข้อมูล)
- โครงสร้างการอนุญาตใช้สิทธิ์โดยกลุ่ม (Group-based) เช่น AD Groups: DeptA_Users, DeptB_Users, DeptC_Users
- ระบบสำรองไฟ (UPS) และ Backup (on-site + off-site/cloud) เพื่อความทนทาน

Hardware/Device

อุปกรณ์เครือข่าย

1. Router / Next-Gen Firewall (1 เครื่อง)
    - ตัวอย่างฟีเจอร์: routing, inter-VLAN routing, stateful firewall, VPN (IPSec/SSL), IDS/IPS (ถ้าต้องการ)

    - ขนาดเล็ก-กลาง: Sophos, Fortinet, Cisco ASA/Firepower, Ubiquiti EdgeRouter / Ubiquiti Dream Machine Pro (ขึ้นกับงบ)
2. Managed Switch (เพียงพออย่างน้อย 12–24 พอร์ต)
    - Layer 2 (และบางรุ่นมี Layer 3) รองรับ VLAN, LACP, QoS
    - ตัวอย่าง: Cisco Catalyst/Symbol, HPE Aruba, Netgear ProSafe, Ubiquiti UniFi Switch
    - จำนวน: 1 ตัวสำหรับ 9 เครื่อง + พอร์ตเชื่อมไปเซิร์ฟเวอร์และอุปกรณ์เครือข่าย (เลือก 24-port)
3. Access Switches (ถ้าต้องแยกห้อง หรือระยะไกล) — ถ้าพื้นที่เล็กอาจไม่ต้องแยก

เซิร์ฟเวอร์ (Server) & การจัดเก็บข้อมูล (Data Storage)

1. Physical Server หรือ Virtual Host (1-2 เครื่อง)

- หน้าที่: Domain Controller (AD), DNS, DHCP (ถ้าตั้งบน Windows Server), File Server, Backup target, หรือรัน VM หลายตัว
- สเปคแนะนำ (สำหรับองค์กรขนาดเล็ก): CPU 4–8 cores, RAM 32–64 GB, Storage: SSD RAID 1/10 สำหรับ OS & apps, HDD RAID 5/6 สำหรับไฟล์ (หรือ SAN/NAS)

2. **NAS** (Network Attached Storage) หรือ **SAN** (Storage Area Network) (สำหรับไฟล์แชร์ และ backup)
    - ตัวอย่าง: Synology, QNAP, NetApp (องค์กรเล็ก Synology DS-series ก็พอ)
    - ควรมี RAID, hot-swap bays

ลูกข่าย (Clients)

1. Clients: 9 เครื่อง (เดสก์ท็อป/โน้ตบุ๊ก) — สเปคขึ้นกับงาน (Office: i3/i5, 8–16GB RAM)

อุปกรณ์เสริม

1. Wi-Fi Access Point(s) (ถ้าต้องการไวไฟภายในออฟฟิศ) และควรแยก SSID สำหรับผู้เยี่ยม/บุคคลภายนอกและสำหรับพนักงาน (VLAN แยก)

2. UPS (สำคัญ) — ให้กับ Server, Switch, Router
3. Rack / ตู้ พร้อมสายแลน (CAT6) และจุดติดตั้ง
4. สายแลน CAT6/CAT6a, Patch panel, Labeling

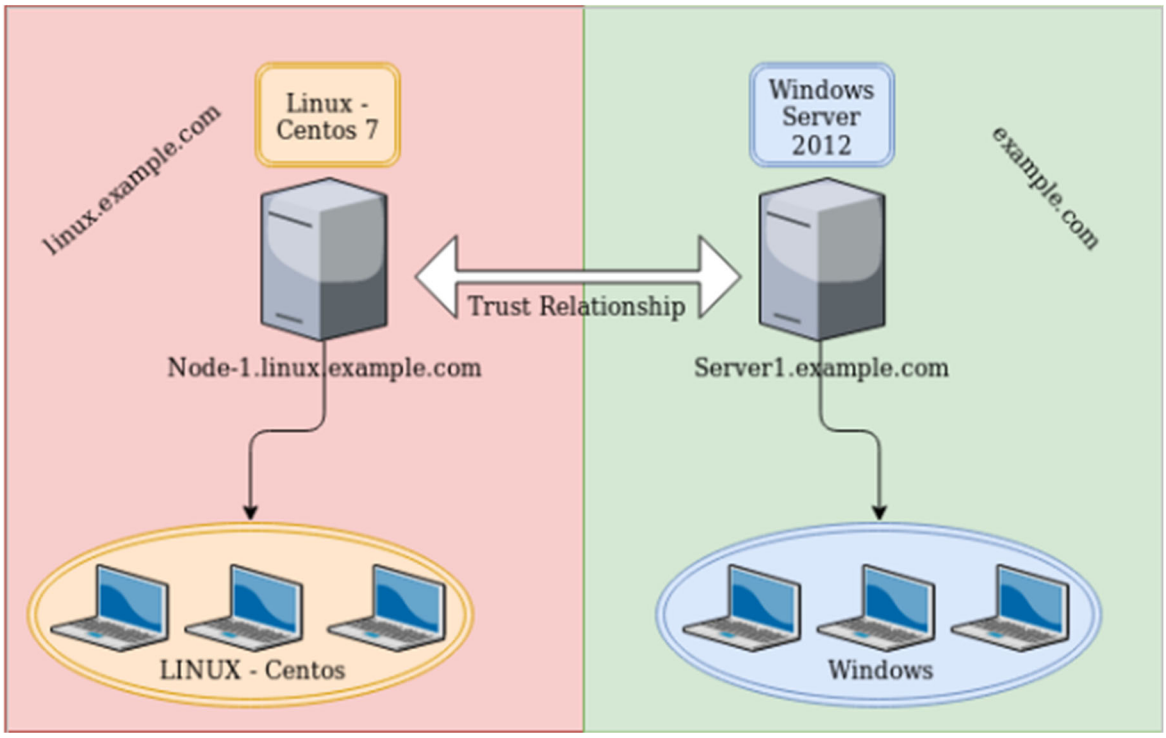
ซอฟต์แวร์และบริการที่ต้องใช้

ระบบปฏิบัติการเซิร์ฟเวอร์

- Windows Server (เช่น 2019/2022) หรือ Linux (Ubuntu Server, CentOS/Rocky) ขึ้นกับนโยบายองค์กร และงบประมาณ
    - หากใช้ Windows Server จะได้ AD, Group Policy, SMB File Sharing ง่าย
    - หากใช้ Linux สามารถใช้ Samba + LDAP/FreeIPA

Directory & Authentication

- Active Directory (Windows) หรือ LDAP/FreeIPA (Linux)



เปรียบเทียบ ระหว่าง Windows AD และ Lunux FreeIPA

- ใช้ Group Policy (GPO) ในกรณี Windows เพื่อจัดการนโยบายเครื่องลูกข่าย

ไฟล์แชร์และสิทธิ์

- File Server: SMB (Windows) หรือ Samba (Linux)
- ตั้งสิทธิ์บนไฟล์/โฟลเดอร์ตาม AD groups (เช่น DeptA_ReadWrite, DeptB_ReadOnly)

เครือข่ายพื้นฐาน

- DHCP (อาจใช้บน Router หรือ Windows Server) เพื่อการแจกจ่ายค่า IP อัตโนมัติกันการซ้ำซ้อน
- DNS (ภายใน) — ถ้าใช้ AD Windows Server จะทำ DNS การทำ DNS เพื่อสะดวกต่อการจำค่า IP Address ให้อาศัยการจำชื่อ Domain Name ง่ายกว่า
- NTP (เวลา) — ให้ทุกอุปกรณ์ sync เวลาจาก NTP server ภายใน/ภายนอก การกำหนดค่าเวลาอัตโนมัติตาม โซนเวลา (Time Zone) แต่ละประเทศ

ความมั่นคงปลอดภัย

- Endpoint Antivirus / EDR (ตัวอย่าง: Microsoft Defender for Business, ESET, Bitdefender)
- Firewall/UTM (ที่ฮาร์ดแวร์) สำหรับกรองทราฟิกและ VPN
- การจัดการแพตช์ (Windows Update Services — WSUS หรือ SCCM / หรือใช้ระบบจัดการแพตช์ของผู้ผลิต)
- MFA (multi-factor authentication) สำหรับ admin accounts หรือ VPN

สำรองข้อมูล (Backup)

- Backup software: Veeam (VMs/Servers), Acronis, Windows Server Backup, Duplicati (open-source) หรือใช้ NAS snapshot + cloud backup
- แนวทาง: full daily/weekly + incremental hourly/remote off-site (3-2-1 rule)

การตรวจสอบ/บันทึก

- Syslog / SIEM เบื้องต้น (เช่น Graylog, ELK) หรือ Logging บน Firewall
- Monitoring: Nagios/Zabbix/PRTG/Prometheus — ตรวจสถานะ server, disk, network

การเข้าถึงระยะไกล

- Remote Desktop Services (RDP) หรือ SSH (Linux)
- VPN server (IPSec/SSL) สำหรับการเชื่อมจากภายนอก

บริการอื่น ๆ (แนะนำ)

- File versioning / File server snapshots (NAS)

- Print server (ถ้ามีเครื่องพิมพ์ร่วม)
- Web-based management portal (ถ้าต้องการ)

การกำหนดค่า

การกำหนดค่าเครือข่ายเพื่อให้ทำงานได้อย่างถูกต้อง และมีประสิทธิภาพตามความต้องการเช่น

- File Server: SMB (Windows) หรือ Samba (Linux)
- ตั้งสิทธิ์บนไฟล์/โฟลเดอร์ตาม AD groups (เช่น DeptA_ReadWrite, DeptB_ReadOnly)
- การกำหนดค่า โปรโตคอลต่างๆ ที่จะใช้งาน เช่น TCP/IP, Subnet และค่า Gateway
- การกำหนดสิทธิ์การเข้าถึง และการใช้งานในส่วนต่างๆ เช่นการระบุ Folder ให้ผู้ใช้ การระบุ สิทธิ์การเปิดใช้ไฟล์หรือทรัพยากรต่างๆ

2. การตรวจสอบและบำรุงรักษา

- การตรวจสอบประจำวัน: ตรวจสอบการทำงานของระบบอย่างสม่ำเสมอเพื่อให้แน่ใจว่าระบบพร้อมใช้งานตลอดเวลา โดยใช้โปรแกรม บริหารจัดการระบบเครือข่าย NMS
- การอัพเดต: อัพเดตซอฟต์แวร์และฮาร์ดแวร์ให้เป็นเวอร์ชันล่าสุดอยู่เสมอเพื่อแก้ไขช่องโหว่และเพิ่มประสิทธิภาพ ในการอัพเดตซอฟต์แวร์ ให้เป็นปัจจุบัน เพื่อเป็นการอุดช่องโหว่ของ ระบบที่เกิดขึ้นและช่วยป้องกันการโจมตีได้
- การสำรองข้อมูล: สำรองข้อมูลอย่างสม่ำเสมอเพื่อป้องกันการสูญหายจากปัญหาหรือการถูกทำลาย ในการสำรองข้อมูล สำหรับเครื่องที่เป็นศูยน์กลางการจัดเก็บข้อมูล จำเป็นอย่างยิ่งที่จะต้องมีการสำรองข้อมูลอย่างมากเพราะ ปัญหาต่างๆที่เกิดขึ้นอาจทำข้อมูลเสียกายและไม่สามารถกู้กลับมาได้

3. การแก้ไขปัญหา

- การวิเคราะห์ปัญหา: เมื่อเกิดปัญหา เช่น เครือข่ายช้าหรือการเชื่อมต่อหลุด ผู้ดูแลระบบต้องสามารถวิเคราะห์หาสาเหตุและแก้ไขได้อย่างรวดเร็ว การหาสาเหตุสามารถทำได้ด้วยคำสั่งพื้นฐาน สำหรับการหาสาเหตุเบื้องต้น หรือการใช้โปรแกรมบริหารจัดการระบบเครือข่ายเป็นตัวช่วย
- การใช้เครื่องมือ: ใช้เครื่องมือและเทคนิคที่เหมาะสมในการตรวจสอบฮาร์ดแวร์ ซอฟต์แวร์ และการตั้งค่าต่างๆ เพื่อแก้ไขปัญหา การเลือกใช้เครื่องมือที่ถูกต้องสามารถหาสาเหตุของปัญหาได้ตรงจุด

4. การจัดการความปลอดภัย

- การป้องกันภัยคุกคาม: ป้องกันไวรัสและการโจมตีจากภายนอก เช่น การดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ หรือการใช้ อุปกรณ์ถายโอนไฟล์ที่ติดไวรัส การปิดตัวดักจับไวรัส หรือแม้แต่การปิด Firewall ของระบบ
- การตั้งค่าความปลอดภัย: กำหนดค่าการรักษาความปลอดภัย เช่น การเข้ารหัสข้อมูลและการควบคุมสิทธิ์การเข้าถึง ในการตั้งรหัสความปลอดภัย ควรตั้งให้คาดเดาได้ยาก ใช้อักขระปนกับตัวเลขตัวอักษรเพื่อความยากในการคาดเดา

5. การออกแบบและอัพเกรดระบบ

- การออกแบบโครงสร้าง: ออกแบบและวางแผนโครงสร้างเครือข่ายที่เหมาะสมกับความต้องการขององค์กร เช่น การเลือกใช้ Topology และสื่อกลางที่เหมาะสม การกำหนดและออกแบบเครือข่าย สามารถใช้โปรแกรมจำลองในการออกแบบเพื่อดูเส้นทาง การวางลำดับตำแหน่งอุปกรณ์ในระบบเครือข่าย
- การประเมินเทคโนโลยี: ประเมินและเลือกใช้เทคโนโลยีใหม่ๆ เช่น ระบบไร้สาย (Wireless) หรือระบบคลาวด์ (Cloud) เพื่อเพิ่มประสิทธิภาพและขยายเครือข่ายในอนาคต การเลือกระบบในการเชื่อมต่อตลอดจนการเลือก ทรัพยากรที่จะมารองรับการทำงานของระบบเครือข่าย

คำถามท้ายบท

1. การเลือกอุปกรณ์เครื่องข่ายที่มีไว้สำหรับการเชื่อมต่อข้อมูลที่ไม่ได้ระบุเส้นทางข้อมูลเราควรเลือกอุปกรณ์ชนิดใดแบบใด
2. การกำหนดค่าการเชื่อมต่อ Protocol เราควรเลือกว่าจะใช้ Protocol แบบใดสำหรับเครือข่ายและมีวิธีตั้งค่าอย่างไรบ้าง
3. การกำหนดสิทธิ์การเข้าถึงข้อมูล การเข้าถึง Folder และ Sub Folder