นาย พัชระ อัลอุมารี รหัสนักศึกษา 6651630177

Assignment #5

อธิบายหลักการทำงานและความแตกต่างระหว่าง SNMP, NETCONF/YANG

SNMP (Simple Network Management Protocol)

SNMP เป็นโปรโตคอลมาตรฐานสำหรับการจัดการและตรวจสอบอุปกรณ์เครือข่าย เช่น เราเตอร์, สวิตช์, เซิร์ฟเวอร์ และอุปกรณ์ IoT โดย SNMP ทำงานบนโครงสร้างแบบ **Client-Server** ซึ่งมีองค์ประกอบหลักดังนี้:

1. องค์ประกอบหลักของ SNMP

1. **Managed Devices** (อุปกรณ์ที่ถูกจัดการ) - เป็นอุปกรณ์เครือข่ายที่รองรับ SNMP เช่น เราเตอร์, สวิตช์, ไฟร์วอลล์
2. **SNMP Agents** - ซอฟต์แวร์ที่ทำงานอยู่บนอุปกรณ์ที่ถูกจัดการ ทำหน้าที่เก็บข้อมูลและตอบสนองคำสั่งจาก SNMP Manager
3. **SNMP Manager** - เซิร์ฟเวอร์ที่ควบคุมและรวบรวมข้อมูลจาก SNMP Agents
4. **MIB (Management Information Base)** - ฐานข้อมูลที่กำหนดโครงสร้างของข้อมูลที่สามารถเรียกดูและจัดการได้ในอุปกรณ์ SNMP

2. วิธีการทำงานของ SNMP

SNMP ใช้กลไกการแลกเปลี่ยนข้อมูลผ่าน **UDP** พอร์ตมาตรฐานคือ **161** (สำหรับ SNMP Queries) และ **162** (สำหรับ SNMP Traps) โดยมีโหมดหลักดังนี้:

1. **Get Request** – SNMP Manager ขอข้อมูลจาก SNMP Agent
2. **Get Response** – SNMP Agent ส่งค่ากลับไปให้ SNMP Manager
3. **Set Request** – SNMP Manager เปลี่ยนค่าพารามิเตอร์บน SNMP Agent
4. **Trap** – SNMP Agent ส่งแจ้งเตือนไปยัง SNMP Manager โดยอัตโนมัติเมื่อเกิดเหตุการณ์สำคัญ
5. **Inform** – เหมือนกับ Trap แต่มีการยืนยันว่า SNMP Manager ได้รับข้อความ

3. เวอร์ชันของ SNMP

- **SNMPv1** – เวอร์ชันแรก ใช้ community string เป็นกลไกการรักษาความปลอดภัย (ง่ายต่อการถูกดักฟัง)
- **SNMPv2c** – ปรับปรุงการทำงานให้เร็วขึ้นและเพิ่ม Trap messages แต่ยังคงใช้ community string

- **SNMPv3** – เพิ่มระบบรักษาความปลอดภัยที่แข็งแกร่งขึ้น เช่น การเข้ารหัสและการตรวจสอบสิทธิ์ (Authentication & Encryption)

NETCONF/YANG

NETCONF (Network Configuration Protocol) และ YANG (Yet Another Next Generation) เป็นโซลูชันที่ออกแบบมาเพื่อการบริหารและจัดการการตั้งค่าอุปกรณ์เครือข่ายแบบโปรแกรมเมติกมากขึ้น โดยทำงานบนโปรโตคอลที่ปลอดภัย เช่น **SSH (พอร์ต 830)**

1. องค์ประกอบหลักของ NETCONF

1. **Network Device (Managed Device)** – อุปกรณ์ที่รองรับ NETCONF เช่น เราเตอร์, สวิตช์
2. **NETCONF Client** – ซอฟต์แวร์หรือระบบที่ใช้ในการสั่งการอุปกรณ์ผ่าน NETCONF
3. **NETCONF Server** – ทำงานบนอุปกรณ์เครือข่าย ทำหน้าที่รับคำสั่งและดำเนินการเปลี่ยนแปลงค่าการตั้งค่า
4. **YANG Model** – ภาษาโมเดลที่ใช้กำหนดโครงสร้างข้อมูลและการตั้งค่าเครือข่ายที่สามารถจัดการผ่าน NETCONF

2. วิธีการทำงานของ NETCONF

NETCONF ทำงานผ่าน **XML-based RPC (Remote Procedure Call)** และรองรับการทำงานหลัก 4 ประเภท:

1. **<get>** – ดึงข้อมูลการตั้งค่าของอุปกรณ์
2. **<edit-config>** – ปรับเปลี่ยนค่าการตั้งค่าอุปกรณ์
3. **<copy-config>** – คัดลอกการตั้งค่าระหว่าง running-config และ startup-config
4. **<delete-config>** – ลบการตั้งค่าบางส่วน

3. YANG และบทบาทใน NETCONF

YANG เป็นภาษาที่ใช้ในการกำหนดโครงสร้างข้อมูลสำหรับอุปกรณ์เครือข่าย ทำให้สามารถกำหนดค่าการตั้งค่าในรูปแบบที่เป็นโครงสร้าง เช่น **Tree-based Hierarchy** โดยข้อมูลที่กำหนดใน YANG จะถูกส่งผ่าน NETCONF ในรูปแบบ **XML**

คุณสมบัติ	**SNMP**	**NETCONF/YANG**
วัตถุประสงค์	Monitoring (เฝ้าระวังระบบ)	Configuration (ตั้งค่าและบริหารอุปกรณ์)
โปรโตคอลพื้นฐาน	UDP	TCP (SSH)
โครงสร้างข้อมูล	MIB (OID-based)	XML (YANG Model)
รูปแบบคำสั่ง	Get, Set, Trap, Inform	get, edit-config, copy-config
ความปลอดภัย	SNMPv3 รองรับการเข้ารหัส	ใช้ SSH (เข้ารหัสเป็นค่าเริ่มต้น)
ความสามารถในการตั้งค่าอุปกรณ์	จำกัดเฉพาะค่าที่รองรับใน MIB	สามารถกำหนดค่าอุปกรณ์แบบเต็มรูปแบบ
ความสามารถในการแจ้งเตือน	Trap, Inform (Asynchronous)	ใช้ **Notification Event** ผ่าน Subscription
ความยืดหยุ่น	มีข้อจำกัดในการกำหนดค่าการตั้งค่า	รองรับการตั้งค่าที่ซับซ้อนมากขึ้น

สรุป

SNMP เหมาะสำหรับการ Monitoring อุปกรณ์ เช่น การอ่านค่า CPU, RAM, Traffic ของ Router/Switch และรับแจ้งเตือนเมื่อเกิดเหตุการณ์ผิดปกติ

NETCONF/YANG เหมาะสำหรับการ Configuration และ Automation เช่น ตั้งค่า VLAN, Routing, Firewall Rules โดยรองรับการปรับแต่งค่าผ่าน API ที่ยืดหยุ่นกว่า SNMP

ปัจจุบันองค์กรหลายแห่งเริ่มเปลี่ยนจาก SNMP มาใช้ NETCONF/YANG เพื่อรองรับ Software-Defined Networking (SDN) และ Automation