# Task A.4 - SNMP and Monitoring Protocols

## 1. SNMP Overview

SNMP (Simple Network Management Protocol) is a widely used protocol for managing and monitoring network devices such as routers, switches, and servers.  
  
Features:  
- Simple and widely supported  
- Compatible with most operating systems  
- Provides metrics for device health (CPU, Memory, Network)  
- Supports versions V1, V2c, and V3 (V3 includes encryption and authentication)  
  
Disadvantages:  
- Older versions (V1, V2c) are insecure.  
- Transmits data in plain text (unless using V3).  
- Limited functionality for modern automation.

## 2. Modern Alternatives to SNMP

| Protocol | Advantages | Disadvantages |  
|-------------------------|-------------------------------------------------------------|-----------------------------------------------|  
| NETCONF / RESTCONF | - Uses XML/JSON<br>- Secure (SSH/HTTPS)<br>- API friendly | - Complex setup on legacy devices |  
| Prometheus + Exporters | - Time-series monitoring<br>- Easy Grafana integration<br>- Supports automation | - Requires exporters on devices |

## 3. Modern Monitoring Trends

- Shift towards API-based monitoring instead of traditional SNMP.  
- Adoption of Prometheus and Grafana for performance metrics.  
- Support for automation and Infrastructure as Code (IaC).

## 4. Final Recommendation

For Rooman Technologies, the following approach is recommended:  
- Use Prometheus + SNMP Exporter for legacy device monitoring.  
- Use AWS CloudWatch for cloud infrastructure monitoring.  
- Avoid using SNMP V1/V2c due to security risks.  
- Prometheus is recommended as it:  
 - Scales efficiently.  
 - Supports modern security standards.  
 - Integrates well with DevOps pipelines and monitoring dashboards.