# Lecture 10. Simple Network Management Protocol (SNMP)

# Simple Network Management Protocol(SNMP)

**Simple Network Management Protocol** (**SNMP**) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more.

# SNMP for monitoring

SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB) which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications.

Three significant versions of SNMP have been developed and deployed. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security.

SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

# How SNMP works

SNMP software agents on network devices and services communicate with a network management system to relay status information and configuration changes. The NMS provides a single interface from which administrators can issue batch commands and receive automatic alerts.

SNMP relies on the concept of a management information base (MIB) to organize how information about device metrics gets exchanged. The MIB is a formal description of a network device's components and status information. MIBs can be created for any network device in the Internet of Things (IoT), including IP video cameras, vehicles, industrial equipment and medical equipment. In addition to hardware, SNMP can be used to monitor services such as Dynamic Host Configuration Protocol (DHCP).

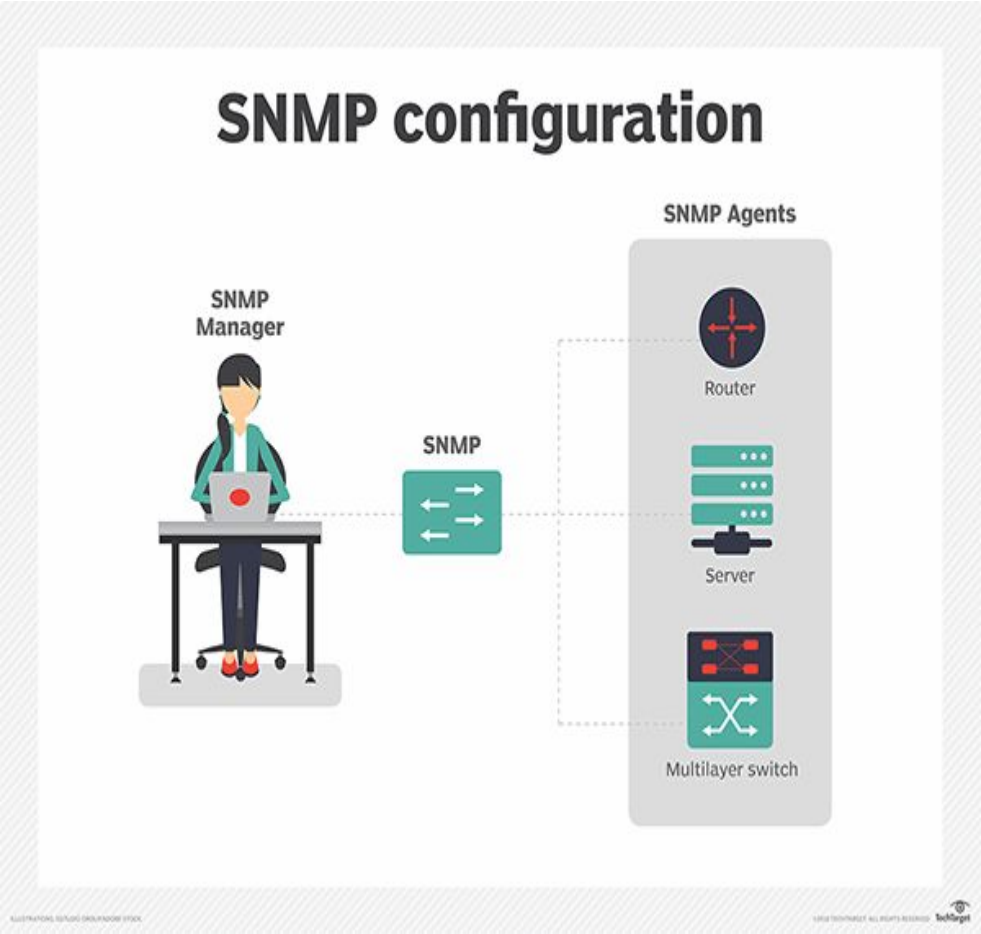
SNMP uses a blend of pull and push communications between network devices and the network management system. The SNMP Agent, which resides with the MIB on a network device, collects status information constantly but will only push information to the network monitoring system upon request or when some aspect of the network crosses a pre-defined threshold known as a trap. Trap Messages are typically sent to the management server when something significant, such as a serious error condition, occurs.

SNMP also includes an "inform" message type that allows a network monitoring tool to acknowledge messages from a device. Inform messages allow the Agent to reset a triggered alert. Network management tools can also use a "set" message to make changes to a network device through the SNMP Agent. This capability allows the network manager to make change device configurations in response to new network events.

# 3 elements of SNMP

SNMP consists of three key components: managed devices, agents, and the **network management** station (NMS).

In most cases, SNMP functions in a synchronous model, with communication initiated by the SNMP Manager and the Agent sending a response. Typically, SNMP uses UDP as its transport protocol. The well known UDP ports for SNMP traffic are 161 (SNMP) and 162 (SNMPTRAP). These two ports are fundamental defaults and are the same in all versions of SNMP.



# Components of SNMP

There are four main components in an SNMP-managed network:

**SNMP agent:** This software runs on the hardware or service being monitored, collecting data about disk space, bandwidth use and other important network performance metrics. When queried by the SNMP manager, the agent sends the requested information back to the management system. An agent may also proactively notify the NMS if an error occurs. Most devices come with an SNMP agent pre-installed but it typically needs to be turned on and configured.

**SNMP-managed network nodes:** These are the network devices and services upon which the agents run.

**SNMP manager:** The network management system (NMS) is a software platform that functions as a centralized console to which agents feed information. The NMS will actively request agents to send updates at regular intervals, and what a network manager can do with that information depends heavily on how feature-rich the NMS is. There are several free SNMP managers available, but they are typically limited in their capabilities or the number of nodes they can support. At the other end of the spectrum, enterprise-grade platforms offer advanced features for more complex networks, with some products supporting up to tens of thousands of network nodes.

Most of the time, SNMP functions in a synchronous model, with communication initiated by the SNMP manager and the agent sending a response. These commands and messages, typically transported over User Datagram Protocol (UDP) or Transmission Control Protocol/Internet Protocol (TCP/IP), are known as protocol data units (PDUs):

- **GETRequest:** Generated by the SNMP manager and sent to an agent to obtain the value of a variable, identified by its OID, in an MIB .
- **RESPONSE:** Sent by the agent to the SNMP manager, issued in reply to a GETRequest, GETNEXTRequest, GETBULKRequest, and a SETRequest. Contains the values of the requested variables.
- **GETNEXTRequest:** Sent by the SNMP manager to agent to retrieve the values of the next OID in the MIB's hierarchy.
- **GETBULKRequest:** Sent by the SNMP manager to the agent to efficiently obtain a potentially large amount of data, especially large tables.
- **SETRequest:** Sent by the SNMP manager to the agent to issue configurations or commands.
- **TRAP:** An asynchronous alert sent by the agent to the SNMP manager to indicate a significant event, such as an error or failure, has occurred.
- **INFORMRequest:** An asynchronous alert similar to a TRAP, but requires confirmation of receipt by the SNMP manager.

# Why we need network monitoring

Network availability monitoring tools help networking teams assess the health and availability of their network devices, as well as the overall network. Network monitoring systems can track bandwidth utilization, uptime, availability and response times of networked devices, and they provide detailed reports and analytics that can assist network managers with troubleshooting.

The market for network management systems can be confusing, however, as there's a wide variety of software and integrated hardware appliances that offer similar functionality, but with varying degrees of integration and performance. Some network availability monitoring tools have fully integrated architectures that require only a single piece of software, whereas other tools may include several individual components, such as a polling engine, a database, an analytics server or user console that must be installed and managed separately.

Thank you for your attention!