[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@699de712d6f5462d8b3e9129f25c2b06?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**What is SNMP?**

SNMP stands for "Simple Network Management Protocol." It’s an application layer protocol included in the internet protocol suite, a set of the most commonly used communication protocols online.

SNMP originated in the 1980s at a time when organizational networks were growing in both size and complexity. Today, it’s one of the most widely accepted protocols for network monitoring. Here’s a look at how SNMP works and why it matters to network professionals.

**What is SNMP used for?**

SNMP is used to collect data related to network changes or to determine the status of network-connected devices. Collecting this data can help IT professionals keep their finger on the pulse of all their managed devices and applications. Every device within the network can be queried in real-time with SNMP, TCP, and other types of probes for their performance metrics. When thresholds for certain values are exceeded, the software can alert system administrators of the issue, allowing them to drill into the data and troubleshoot a solution.

**What is Simple Network Management Protocol (SNMP)?**

Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN).

The purpose of SNMP is to provide network devices, such as routers, servers, and printers, with a common language for sharing information with a network management system ([NMS](https://www.techtarget.com/searchnetworking/definition/network-management-system)).

SNMP's client-server architecture has the three following components:

1. an SNMP manager;
2. an SNMP agent; and
3. a management information base ([MIB](https://www.techtarget.com/whatis/definition/management-information-base-MIB)).

The SNMP manager acts as the client, the SNMP agent acts as the server and the MIB acts as the server's database. When the SNMP manager asks the agent a question, the agent uses the MIB to supply the answer.

SNMP is so popular that most network devices come pre-bundled with SNMP agents. To make use of the protocol, however, network administrators must first change the default configuration settings of their network devices so SNMP agents can communicate with the network's management system.

SNMP is part of the original Internet Protocol (IP) suite as defined by the Internet Engineering Task Force (IETF). Multiple versions of the SNMP protocol exist. The most recent version, SNMPv3, includes [security mechanisms for authentication](https://www.techtarget.com/searchsecurity/answer/Is-upgrading-to-SNMP-v3-enough-to-secure-network-devices), encryption, and access control.

**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 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](https://www.techtarget.com/searchnetworking/definition/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, constantly collects status information but will only push information to the NMS 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 informed message type that enables a network monitoring tool to acknowledge messages from a device. Inform messages enable 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 enables the network manager to make change device configurations in response to new network events.

In most cases, SNMP functions in a synchronous model, with the communication initiated by the SNMP manager and the agent sending a response. Typically, SNMP uses User Datagram Protocol ([UDP](https://www.techtarget.com/searchnetworking/definition/UDP-User-Datagram-Protocol)) as its transport protocol. 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.

SNMP relays information between devices and network management systems.

SNMP is called "simple" because of the uncomplicated nature of the protocol's architecture. SNMP can issue read or write commands, such as resetting a password or changing a configuration setting. It can also report back how much bandwidth, CPU, and memory are in use.

One of the most widely used protocols, SNMP is supported on an extensive range of hardware -- from conventional network equipment like routers, switches, and wireless access points to endpoints like printers, scanners, and IoT devices.