4.1 Introduction

The Simple Network Management Protocol (SNMP) is a protocol designed for communicating with network elements, such as switches and multiplexers, and for managing their operation. Managing a network element includes detecting and diagnosing faults, provisioning capacity, activating service and suspending and re-activating service.

SNMP was introduced with the larger goal of allowing standardised, automated network management. The motivation for standardisation of management protocols is that independent vendors of

- NMSs
- SNMP-managed devices and
- other network equipment

may develop and supply devices that can interwork and communicate with other NMS and OSS software that support SNMP.

SNMP has been fairly successful in achieving its aims. The chief reason for the rise of SNMP has been its simplicity: implementing SNMP management in a network device is more straightforward than most other approaches to network management. In addition, SNMP was successfully “sold” by the Internet Engineering Task Force (IETF) as the chief Internet standard for network management. The IETF is influential in the Internet engineering and telecom communities. In the early days of SNMP, developing applications based on SNMP required significant effort to manage the variety of networked devices in use. This problem faded away as more development and other tools became available to support SNMP. SNMP is now the dominant communications protocol for end-to-end management of inter-networking devices.

SNMP facilitates communication between a managed device and the user of an SNMP management application. A managed device is any device with an SNMP agent. The SNMP agent is stored on a managed device. The agent gives access to data, or managed objects, that describe the state of a managed device. Through this access, the SNMP manager or management application can monitor and control the device.
The Oulu University Secure Programming Group of Finland has found several vulnerabilities in the decoding and processing of SNMP trap messages and SNMP request messages by SNMP managers. There are vulnerabilities in the decoding and the subsequent processing of SNMP trap messages and SNMP request messages.\(^5\) Vulnerabilities include denial-of-service conditions, format string vulnerabilities and buffer overflows. These may in turn result in service interruptions and may allow an attacker to gain access to the affected device. Owing to slight differences in SNMP implementations, the specific outcome arising from the vulnerabilities varies from product to product.

The development of the second version of SNMP (SNMPv2) standard addresses the lack of security of SNMP using mechanisms which focus on privacy, authentication and access control. SNMPv2 also allows more complex specification of variables and has some management commands not available in SNMP. SNMPv2 and SNMPv3 are now widely supported in new telecom equipment. Several of the products mentioned in this book, such as TEMPo by Tenor Networks, and AdventNet's products support many features of SNMPv2 and SNMPv3.

### 4.2 Object Management

Communication between an SNMP manager and a managed device occurs via SNMP in abstract units called Protocol Data Units (PDUs). The communication SNMP manager and a managed device are typically encapsulated in User Datagram Protocol (UDP) packets. There are four main kinds of operation between managers and agents:

1. The manager can perform a *get* (or read) to obtain information from the agent about an attribute of a managed object.
2. The manager can perform a *get-next* to do the same for the next object in the tree of objects on the managed device.
3. The manager can perform a *set* (or write) to set the value of an attribute of a managed object.
4. The agent can send a *trap*, or asynchronous notification, to the manager telling it about some event on the managed device.

SNMP management is achieved by making an SNMP call to the managed device in order to access a managed object. A managed object may be regarded as a value in a database of managed objects in the device. This database is maintained by the device and is populated with parameters that are relevant to the status, performance and configuration of the device (see Figure 4.1).

To specify managed objects to the SNMP agent, the SNMP manager or management application uses a rigorous naming syntax to specify variables. An object name is an object identifier (object ID or OID), which is like a serial number uniquely identifying an object to an SNMP agent.

\(^5\)These flaws have been documented by the CERT Coordination Center of the Software Engineering Institute operated by Carnegie Mellon University.