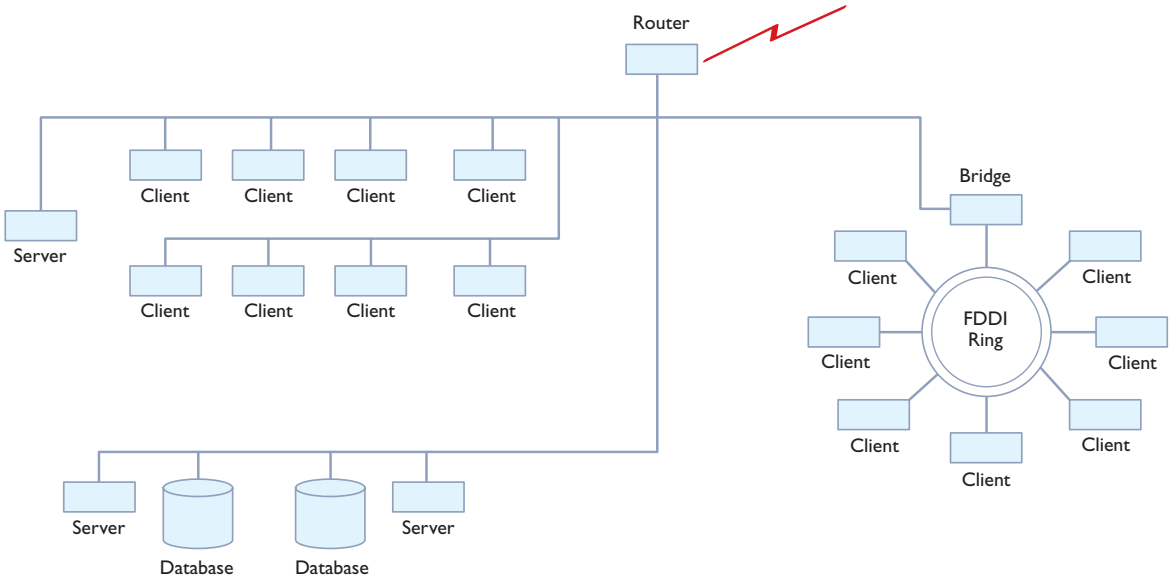
## SNMP

SNMP stands for **S**imple **N**etwork **M**anagement **P**rotocol. SNMP makes it possible to manage devices on a network. A device that can be monitored is called an agent. A master system sends an enquiry message to the agents and requests data, this can be done using special applications or using Telnet.

Using SNMP you can:

- Monitor trends.
- Monitor events for analysis.
- Monitor devices in the network and their status.
- Monitor an especially important connection.
- With the intention of prevention, check the traffic on one or more network devices.
- Configuration of devices.

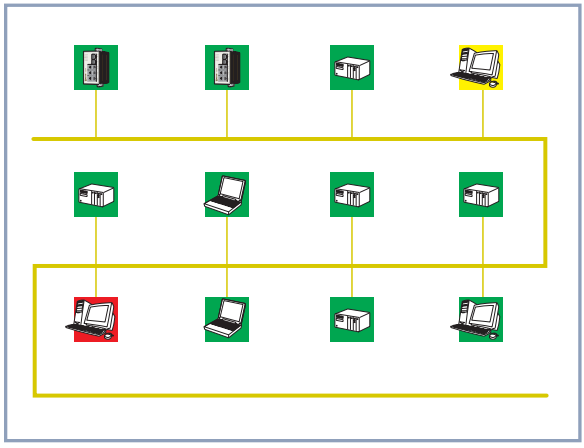


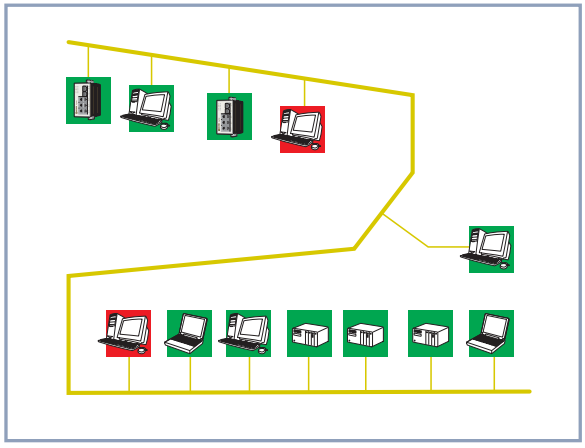
**SNMP software**

Software used to communicate with the agent is called **N**etwork **M**anagement **S**olution (NMS). The exchange of data with the agents is similar to communication between a master and slaves, i.e. communication with the underlying devices takes place through polling. The manager can request information from or perform an action on the agent, this responds to the enquiries or actions requested. Another option is for the agent to set a "trap" i.e. an event controlled function that is activated by a predetermined condition. When this occurs the agent sends data back to the manager.

**Let us show an example:**

In a large network there is critical equipment that uses UPS for its standby power. In the event of a power failure, the UPS units are automatically connected and the devices continue to work. This error condition must in some way be transferred to the network administrator; this can be done through a trap detecting that the UPS unit has been connected. The information is transferred to a SCADA system (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition) where the network administrator receives an alarm, through a flashing icon (activated by the SNMP trap) on the UPS unit.





**SNMP, SNMPv2 and SNMPv3**

There are three versions of SNMP. The original version of SNMPv1 has a multi security mechanism, which is a password. In version 1 you can not identify the sender of a message with all certainty. This makes SNMP open, which allows the reconfiguration of devices in the network. As a consequence of this many equipment manufacturers have chosen not to implement all the functions in the standard. These deficiencies were identified from the offset and a significantly improved version, SNMPv2, was planned. This uses an encryption algorithm for authentication of transfers between the SNMP servers and agents. SNMPv2 can also encrypt the transfer. SNMPv2, which was intended as the follow-up was never accepted as a standard. A contributing factor was the inability to reach agreement about how security should be implemented. However, SNMPv2 is an important link in the development of the next version, SNMPv3.

The SNMPv3 work group was formed in March 1997 with the task to examine the submitted security and administration proposals and from this find a common solution to the problem. The focus of the work was, as far as possible, to complete the submitted proposals and not put forward any new ideas. The proposal for SNMPv3 was finished in 1998. This was based on version 2 as well as a security and administration concept that centred on different modules which could be switched depending on the level of security to be attained.

SNMPv3, the current standard, provides many more opportunities to make network devices secure, yet introduction is slow. Most installed devices still follow SNMPv1.