Simple Network Management Protocol (SNMP)

- Simple Network Management Protocol (SNMP) is an open standard for network monitoring.
- An **SNMP Manager** (the SNMP server) can collect and organize information from an **SNMP Agent**, which is SNMP software which runs on managed devices such as routers and switches.
- The SNMP Manager is commonly called an SNMP Server or NMS (Network Management System).

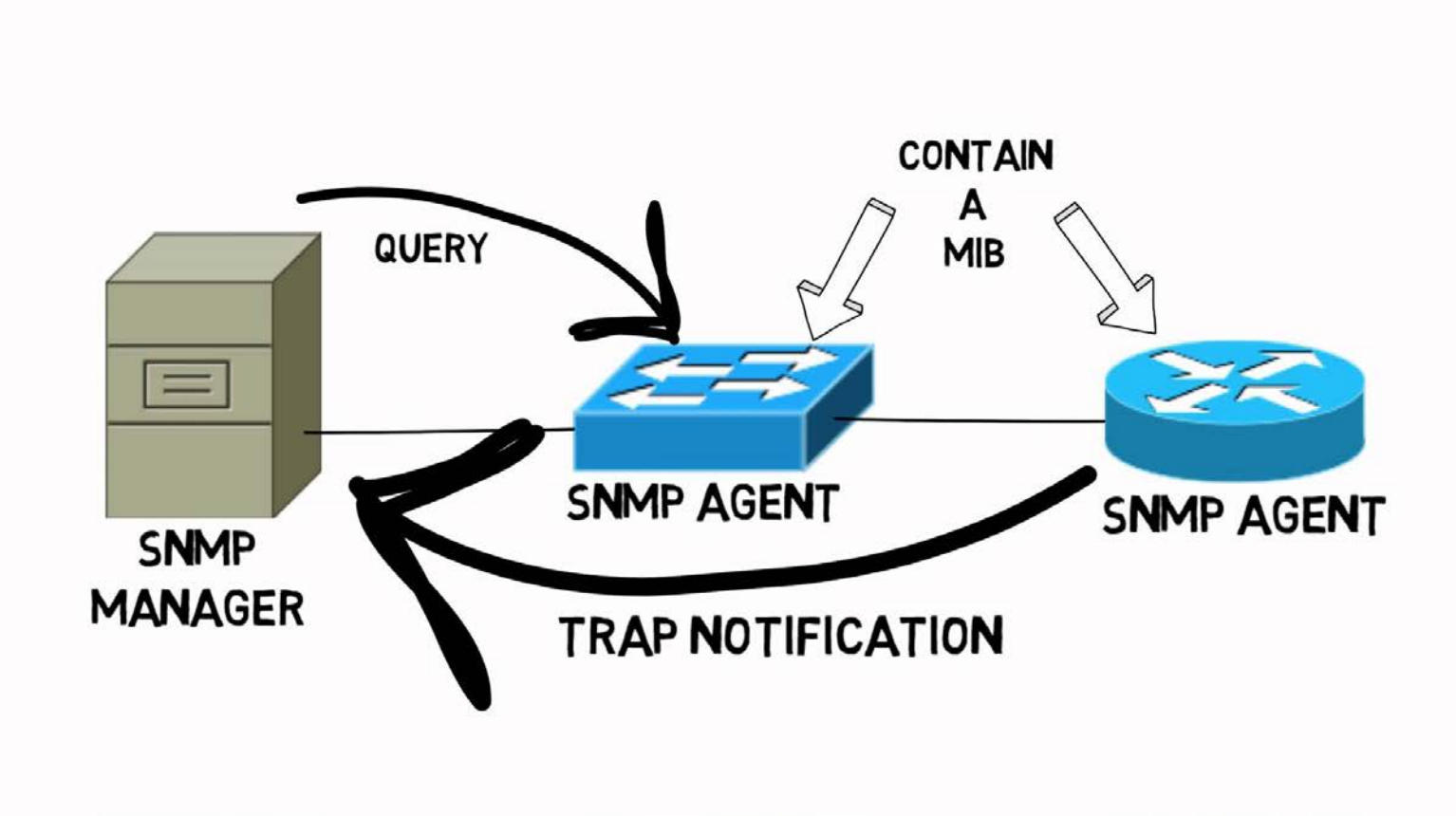
Simple Network Management Protocol (SNMP)

- The SNMP Manager can pull information from the device ('Get') or the device can push it to the server ('Trap').
- For example the Manager could query traffic statistics from the device or the device could report an HSRP state change.
- The standard also includes support for modifying Agent information from the SNMP Manager to change device behaviour.

MIB Management Information Base

- Data variables on SNMP managed systems are organized in a Management Information Base (MIB).
- The SNMP Manager and Agent need to share the MIB so they know which variables can be reported on.

Simple Network Management Protocol (SNMP)



SNMP Versions

- Three significant versions of SNMP have been developed and deployed.
- SNMPv1 uses plain text authentication between the Manager and Agent using matching Community strings.
- SNMPv2c also uses plain text Community strings. It supports bulk retrieval.
- SNMPv3 supports strong authentication and encryption. It is the preferred version but is not supported on all devices.

SNMPv2c Community Strings

- SNMPv2c uses Community strings rather than a username and password to authenticate the SNMP Manager and Agent to each other
- Matching community strings need to be set on both sides for the Manager and Agent to communicate
- The read only (ro) community is used by the Manager to read information
- The read write (rw) community is used by the Manager to set information

SNMPv2c Configuration Example

```
R1(config)#snmp-server contact neil@flackbox.com
R1(config)#snmp-server location Flackbox Lab
```

(Optional, identifies the Agent to the Manager)

```
R1(config)#snmp-server community Flackbox1 ro
R1(config)#snmp-server community Flackbox2 rw
```

```
R1(config)#snmp-server host 10.0.0.100 Flackbox1
R1(config)#snmp-server enable traps config
```

(When a configuration change is made a trap will be sent to the NMS system at 10.0.0.100 using the ro Community string)

SNMP Security Best Practice

- Most devices use a default ro Community string of ‘public’ and a default rw Community string of ‘private’
- Attackers can use this to read or set information on your devices
- Best practice is to disable SNMP on devices where it is not used
- Use SNMPv3 with secure passwords on devices where it is used
- If SNMPv3 is not supported, use non-default Community strings