SNMP (Simple Network Management Protocol)

Can be used to monitor the status of devices, make configuration changes,.. etc.
It has two main types of devices: 1- Managed devices: network devices as routers and switches.
2- Network Management Station/System (NMS): the device/devices managing the managed devices (SNMP server).
There are three main operations:
1- Managed devices can notify the NMS of events.
2- The NMS can ask the managed devices for information about their current status.
3- the NMS tells the managed devices to change aspects of their configuration.

NMS Components: SNMP manager → the software on NMS which interacts with the managed devices, it receives notifications, sends requests for information, sends configuration changes,.. etc.
SNMP Application→ provides an interface for the network admin to interact with, displays alerts, statistics, charts,.. etc.

On a router/switch managed (devices): SNMP agent → the SNMP software running on the managed devices that interacts with SNMP
managers on NMS, sends notifications to/receives messages from NMS.
MIB (Management Information base) → the structure that contains the variables that are managed by SNMP, each variable is identified with an Object ID (OID).
Variables Examples: Interface Status – Traffic Throughput – CPU Usage - Temperature, .. etc.

SNMP OIDS are organized in a hierarchical structure.
SNMPv1 : the original version of SNMP.

SNMPv2c (c for community strings used as passwords): allows NMS to retreive large amounts of information in a single request, so it is more efficient.
SNMPv3 : a much more secure version of SNMP that supports encryption and authentication whenever possible this version should be used.

SNMP **Read**: sent by NMS to read info from managed devices as Get (request sent to an agent to retrieve the value of a variable (OID) or multiple variables and the agent sends a response with the current value of each variable.
GetNext: a request sent from the manager to the agent to discover the available variables in MIB.
GetBulk: a more efficient version of the GetNext message introduces in SNMPv2.
Write: sent by NMS to change info on managed devices as IP.
Set: a request from manager to agent to change value of 1 or more variables, the agent will send a response message with the new values.
Notification: messages sent by the manged devices to alert NMS of a particular event.
Trap: a notification from the agent to the manager with no response from manager to ack that it received the trap so not reliable.
Inform: a notification message that is acked with a response message, originally used for communication between mangers, but later updates allow agents to send inform messages to managers too.
Response: messages sent in response to a previous message/request.
SNMP Agent: UDP 161, SNMP Manager UDP 162.
Command: snmp-server contact <contact {email}>. Command: snmp-server location <location>.
Command : snmp-server community <password> ro/rw {read only/write} default strings are public for ro , private for rw.
Command: snmp-server host <NMS IP Address> version <version> <community string>.
Command: snmp-server enable traps {config/snmp linkdown linkup}.