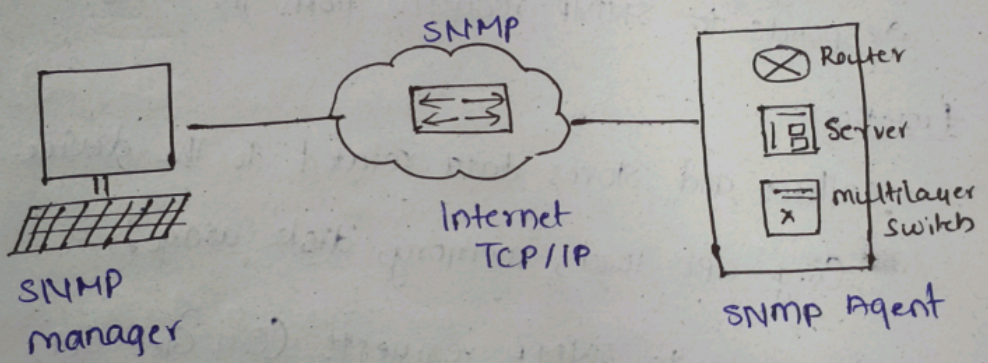
SIMPLE NETWORK MANAGEMENT PROTOCAL

⇒ SNMP is an Internet standard protocal used for Managing and Monitoring network-connected devices in IP networks.

⇒ SNMP is an application layer protocal That uses UDP port number 161/162. SNMP is used to monitor The network, detect network faults,

Architecture



⇒ The manager is a host That controls and monitors a set of agents such as routers

⇒ This protocal is used in a heterogeneous network made of different LANs and WANs connected by routers (or) gateways.

⇒ A manager is a host That runs The SNMP client program while The agent is a router That runs The SNMP server program.

Introduction (SNMP defn)

purpose

- To monitor the performance of devices like routers, switches, servers, and printers
- to detect and troubleshoot network issues
- to configure network devices remotely

ex:→ updating IP Addresses
→ Upgrades
→ Enable / Disable ports

Components of SNMP

1. Managed Devices: Network devices (eg routers, switches, servers, printers) that are being monitored or controlled via SNMP.

2. SNMP Agent: An SNMP Agent is software running on the managed device.

→ It acts as interface between the managed device and the Network Management System (NMS).

→ The agent collects and stores device data and responds to SNMP requests from the NMS.

Function

- collects and stores data related to the device (e.g CPU load, memory, disk usage).
- Responds to SNMP requests (e.g Get Set) from NMS to retrieve or modify information.
- Sends Traps to the NMS to notify about significant events (e.g device failure,)

3. Network Management System (NMS)

The Network Management System (NMS) is a central software platform that communicates with SNMP agents to manage and monitor

devices across the network.

→ The NMS sends request to Agents, receives responses,

→ Receives Traps and Inform messages from agents to detect events like failures or alarms.

4. Management Information Base (MIB)

MIB is a virtual database that defines the objects.

→ objects organized in a tree-like structure with Object Identifiers (OIDs) used to access and reference them.

→ Acts as blueprint

defines data available for monitoring and configuration)

SNMP Message types

- Get: Used by NMS to request information from agent
- Set: Used by NMS to modify the configuration of the managed device.
- GetNext: to Request the next object in MIB hierarchy

→ extention of Get, & primarily used when NMS wants to iterate over a list of objects.

• Get Bulk: A more efficient way to retrieve large datasets in SNMPV2

• Trap: An unsolicited message sent by the agent to the NMS to report an event (e.g: an error (or) status change)

• Inform: Similar to a Trap, but requires acknowledgment from the NMS. (whereas Traap do not)

• Response: Sent by the agent in reply to a request from the NMS (Get, Set, etc)

• GET WALK: Retrieve an entire table (or) structured data. (ex: get all devices connected to switch)

Applications i) fault management

① When a device experience an error (e.g interface down, power failure) SNMP traps or Informs are sent to the Network Management System to alert administrators of the problem

ii) Configuration management

Using SNMP set requests, administrators can configure devices, change parameters like IP addresses, modify routing tables.

iii) Security Mana

Security

and responding

network usi

→ It prot

ex:- If som

Clike a

alert (t

iv) Data

Data

and con

data co

ex:- SN

CPU

Usecase:- En

→ Take

iii) Security management :

Security management involves monitoring, detecting and responding to security-related events within a network using SNMP.

→ It protects from unauthorized access.

ex:- If someone repeatedly tries to log in to a device (like a router, switch) and fails, SNMP can send an alert (trap) to the administrator.

iv) Data center management :

Data center management involves monitoring and controlling the devices and infracture within a data center.

ex:- SNMP tracks the status of servers, such as CPU usage, memory utilization and disk space.

usecase :- Ensure server don't overload or run out of resources

→ Take actions before equipment overheats.

SNMPV1

→ first and simplest version

→ sends and receives data but has no strong security

SNMPV2

→ Improved version with better performance and error reporting

→ security still weak

SNMPV3

→ The most secure and advanced version.

Conclusion

* Its goal is to ensure the efficient operation of networked systems

~~* without any obstacles~~