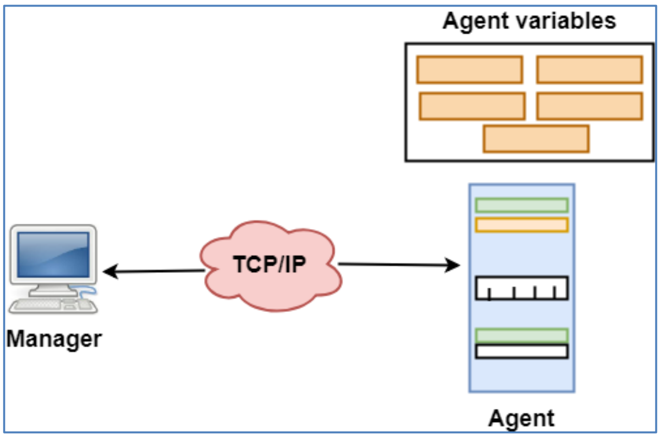
Network Management Security and Network Access Control

🔷SNMP

- SNMP stands for Simple Network Management Protocol.
- SNMP is a framework used for managing devices on the internet.
- It provides a set of operations for monitoring and managing the internet.
- It is mainly used for monitoring and organizing networking resources.
- It is a standard internet protocol which is to be followed by everyone. It sets a standard for everyone network management, database management, and organizing data objects.
- Administrator computers (managers) use SNMP for monitoring the clients in the network.
- This protocol allows for management activities using applications like Management Information Base (MIB).

🔷SNMP Concept



🔷Computer Network SNMP

- SNMP has two components Manager and agent.
- The manager is a host that controls and monitors a set of agents such as routers.
- It is an application layer protocol in which a few manager stations can handle a set of agents.
- The protocol designed at the application level can monitor the devices made by different manufacturers and installed on different physical networks.

🔷SNMP components –

There are 3 components of SNMP:

- **SNMP Manager –** It is a centralized system used to monitor network. It is also known as Network Management Station (NMS).
- **SNMP agent –** It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.
- **Management Information Base –** MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

🔷SNMP messages –

Different variables are:

- **GetRequest –** SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.
- **GetNextRequest –** This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.
- **GetBulkRequest –** This message is used to retrieve large data at once by the SNMP manager from the SNMP agent. It is introduced in SNMPv2c.
- **SetRequest –** It is used by the SNMP manager to set the value of an object instance on the SNMP agent.
- **Response –** It is a message sent from the agent upon a request from the manager. When sent in response to Get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.
- **Trap –** These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.
- **InformRequest –** It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn't provide.

🔷SNMP versions –

There are 3 versions of SNMP:

- SNMPv1 – It uses community strings for authentication and uses UDP only.
- SNMPv2c – It uses community strings for authentication. It uses UDP but can be configured to use TCP.
- SNMPv3 – It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, the conclusion is the higher the version of SNMP, the more secure it will be**.**

🔷Special Features about SNMPv3 :

- v3 is the latest version of SNMP which involves great management services with enhanced security.
- The SNMPv3 architecture makes the use of User-based Security Model (USM) for security of the messages & the View-based Access Control Model (VACM) for accessing the control over the services.
- SNMP v3 security models supports authentication and encrypting.
- SNMPv3 supports Engine ID Identifier, which uniquely identifies each SNMP identity. The Engine ID is used to generate a unique key for authenticating messages.
- v3 provides secure access to the devices that send traps by authenticating users & encrypting data packets which are sent across the network.
- It also introduces the ability to configure and modify the SNMP agent using SET for the MIB objects. These commands enable deletion, modification, configuration and addition of these entries remotely.
- USM – For facilitating remote configuration and management of the security module.
- VACM – For facilitating remote configuration & management for accessing the controlling module.

🔷SNMPv3 Architecture:

The architecture of the v3 consists of –

- **Data definition language,**
- **Definition of MIB**
- **Protocol definition**
- **Security and administration.**

🔷Strength of SNMP:

- It is simple to implement.
- Agents are widely implemented.
- Agent level overhead is minimal.
- It is robust and extensible.
- Polling approach is good for LAN based managed object.
- It offers the best direct manager agent interface.
- SNMP meet a critical need.

🔷Strength of SNMP:

- It is simple to implement.
- Agents are widely implemented.
- Agent level overhead is minimal.
- It is robust and extensible.
- Polling approach is good for LAN based managed object.
- It offers the best direct manager agent interface.
- SNMP meet a critical need.

🚩Network Access Control(NAC):

- Network Access Control is a security solution that uses a set of protocols to keep unauthorized users and devices out of a private network or give restricted access to the devices which are compliant with network security policies.
- It is also known as Network Admission Control.
- It handles network management and security that implements security policy, compliance, and management of access control to a network.
- NAC works on wired and wireless networks by identifying different devices that are connected to the network.
- NAC network security solution, administrators will determine the protocols that will decide how devices and users are authorized for the right level of authorization.

🚩Components of Network Access Control Scheme:

Restricted Access: It restricts access to the network by user authentication and authorization control. For example, the user can’t access a protected network resource without permission to access it.

Network Boundary Protection: It monitors and controls the connectivity of networks with external networks. It includes tools such as controlled interfaces, intrusion detection, and anti-virus tools. It is also called perimeter defense. For example, the firewall can be used to prevent unauthorized access to network resources from outside of the network.

🚩 Types of Network Access Control:

Pre-admission: It happens **before** access to the network is granted on initialization of request by user or device to access the network.

It evaluates the access attempt and only allows the access if the user or device is compliant with organization security policies and authorized to access the network.

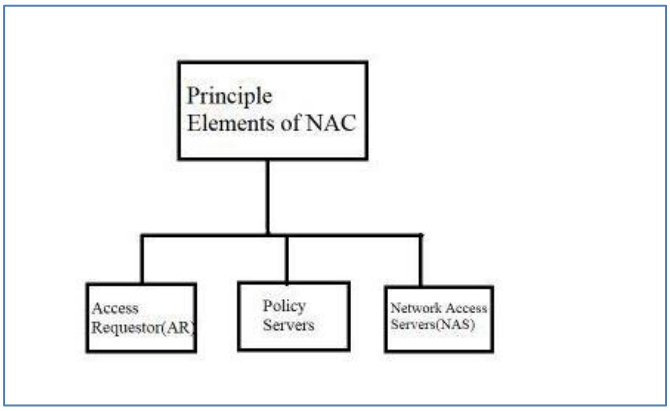
Post-admission: It happens within the network when the **user** or device attempts to access the different parts of the network.

It restricts the lateral movement of the device within the network by asking for re-authentication for each request to access a different part of the network.

🚩Principle Elements of NAC(Network Access Control):

There are mainly three principle elements of NAC which are:

1. Access Requestor(AR).
2. Policy Servers.
3. Network Access Servers(NAS)



Three Principle Elements of NAC(Network Access Control).

Let's look at them one by one now:

1.**Access Requestor(AR):** We may determine from the name that it is someone attempting to gain access by requesting it. This access can be granted to any entity, such as a device, person, or process.

- This entity attempts to get access to network resources. It might be any device handled by the NAC system, such as servers, cameras, printers, and other IP-enabled devices.
- ARs are also known as supplicants or clients at times. ARs ensures that no entity has illegal access to protected resources.
- To get access, these ARs must follow to the organization's specific guidelines or policies.

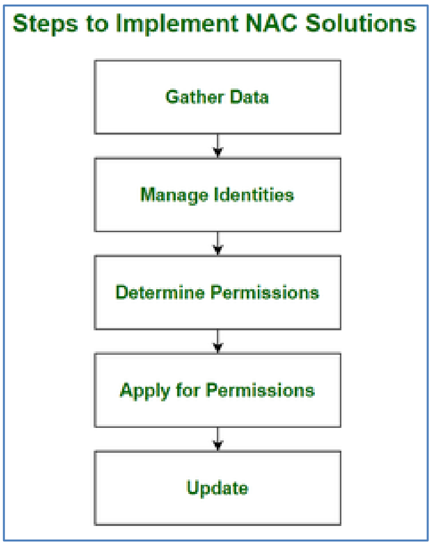
2.Policy Server: The policy server analyzes what access should be provided to AR based on the AR's identity, permission level, attempted request, and an organization's established access policy.

- The policy server frequently relies on backend services, such as antivirus, patch management, or a user directory, to function.

3.Network Access Server(NAS): Users connecting to an organization's internal network from distant locations utilize the NAS as an access control point. These often serve as VPNs and give users access to the company's internal network. These days, NAS functionality is frequently included in policy server systems.

🚩Steps to Implement NAC Solutions:

1. **Gather Data**: Perform an exhaustive survey and collect information about every device, user, and server that has to interface with the network resources.
2. **Manage Identities:** Verify user identities within the organization by authentication and authorization.
3. **Determine Permissions**: Create permission policies stating different access levels for identified user groups.
4. **Apply for Permissions:** Apply permission policies on identified user groups and register each user in the NAC system to trace their access level and activity within the network.
5. **Update**: Monitor security operations and make adjustments to permission policies based on changing requirements of the organization with time.



Responsibilities:

- It allows only compliant, authenticated devices to access network resources and infrastructure.
- It controls and monitors the activity of connected devices on the network.
- It restricts the availability of network resources of private organizations to devices that follow their security policy.
- It regulates the access of network resources to the users.
- It mitigates network threats by enforcing security policies that block, isolate, and repair non-compliant machines without administrator attention.

Common Use-Cases:

- Organizations that allow employees to use their own devices or take corporate devices home use NAC to ensure network security.
- Organizations use NAC to grant access to different network resources to people or devices that are outside of the organization and are subjected to different security controls.
- NAC protects from threats caused due to use of IoT devices by categorizing IoT devices into groups that have limited permission and constantly monitoring their activities.

Benefits:

- Users can be required to authenticate via multi-factor authentication, which is much more secure than identifying users based on IP addresses or username and password combinations.
- It provides additional levels of protection around individual parts of the network.

Limitations:

- It has low visibility in IoT devices and devices with no specific users associated with it.
- It does not protect from threats present inside the network.
- It may not work for organizations if it is not compatible with existing security controls.