Network Access Control

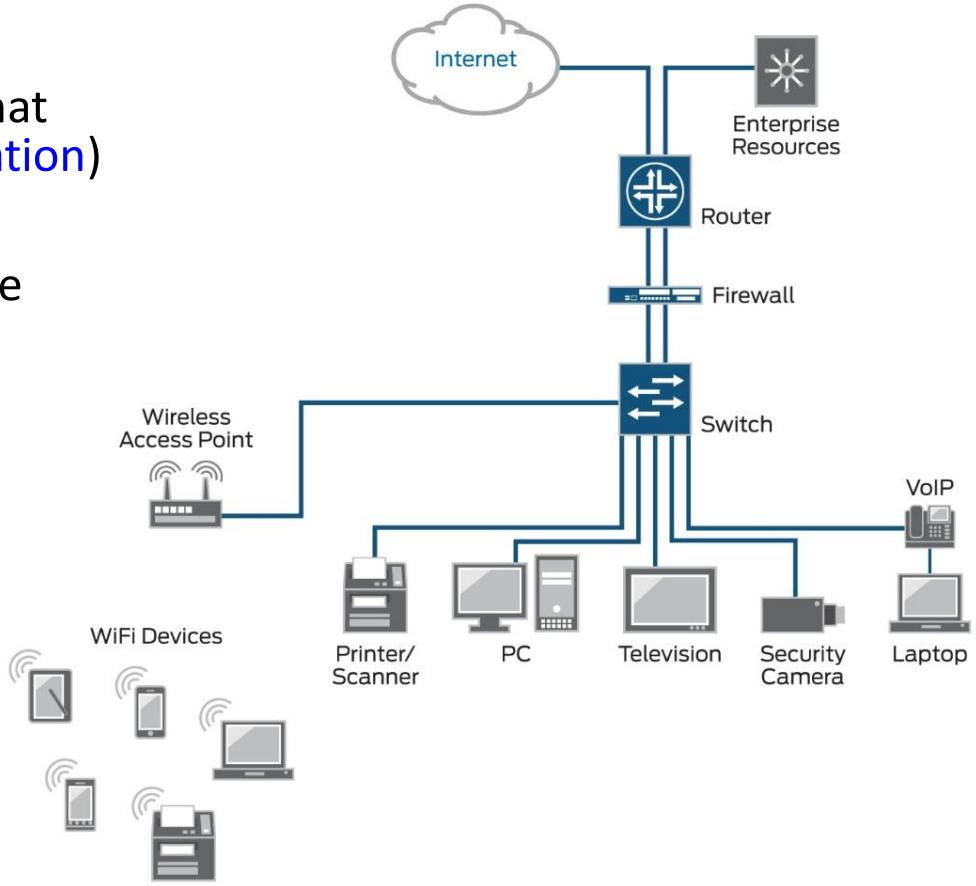
Dr. Mana Khatua
Assistant Professor
Dept. of CSE, IIT Guwahati
Email: manaskhatua@iitg.ac.in

Network Access Control (NAC)

- **An umbrella term** for managing access to a network
- Authenticates users logging into the network and determines what data they can access and actions they can perform (i.e. authorization)
- Also examines the health of the user's computer or mobile device

In other terms:

- ❖ Network access control (NAC) solutions support network visibility and access management through policy enforcement on devices and users of enterprise networks.
- ❖ A NAC system can deny network access to noncompliant devices, place them in a quarantined area, or give them only restricted access to computing resources, thus keeping insecure nodes from infecting the network.



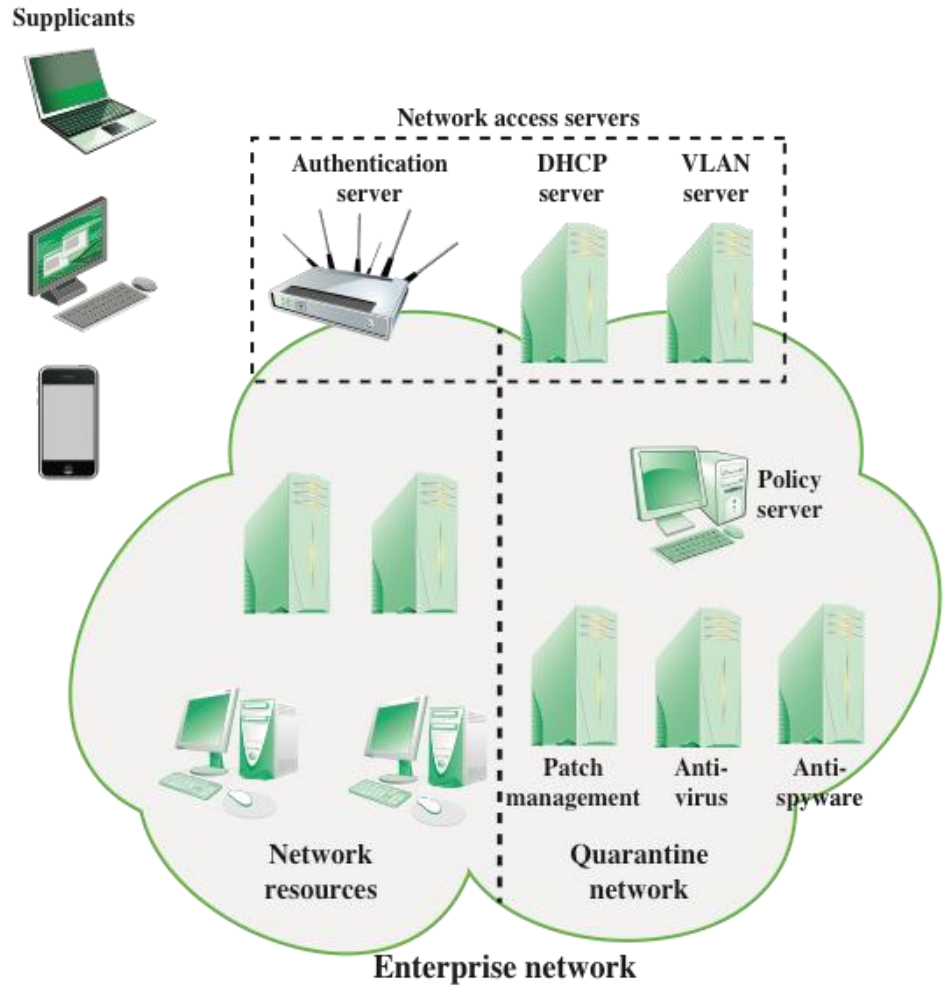
Source: https://www.cisco.com/c/en_in/products/security/what-is-network-access-control-nac.html

Source: https://www.juniper.net/us/en/research-topics/what-is-802-1x-network-access-control.html

Elements of a NAC System

NAC systems deal with three categories of components.

- Access Requester (AR)
  - Node that is attempting to access the network and may be any device that is managed by the NAC system, including workstations, servers, printers, cameras, and other IP-enabled devices
  - Also referred to as supplicants, or clients
- Policy Server
  - Determines what access should be granted
  - Often relies on backend systems
- Network Access Server (NAS)
  - Functions as an access control point for users in remote locations connecting to an enterprise's internal network
  - Also called a media gateway, remote access server (RAS), or policy server
  - May include its own authentication services or rely on a separate authentication service from the policy server

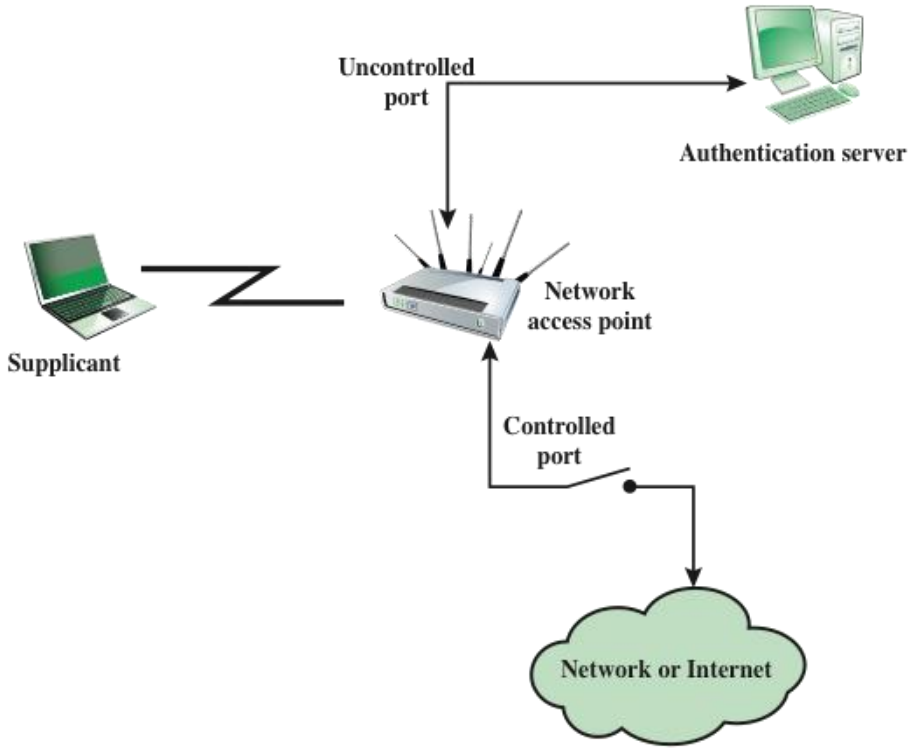


Network Access Enforcement Methods

- The actions that are applied to ARs to regulate access to the enterprise network
  - Many vendors support multiple enforcement methods simultaneously, allowing the customer to tailor the configuration by using one or a combination of methods

Common NAC enforcement methods:

- IEEE 802.1X
- Virtual local area networks (VLANs)
- Firewall
- DHCP management



IEEE 802.1X Port-based Access Control

What is 802.1X NAC?

802.1X network access control (NAC) enables administrators to provide uniform access control across wired and wireless networks.

It is widely deployed on campus and branch enterprise networks.

It is comprised of two major elements:

- 802.1X protocol – An IEEE standard for port-based network access control (PNAC).
  - ✓ 802.1X defines authentication controls for any user or device trying to access a LAN or WLAN.
- NAC - It identifies users and devices, and imposes control to access the network.
  - ✓ NAC controls access to enterprise resources using authorization and policy enforcement

What Can You Do with 802.1X NAC?

There are many ways to deploy a NAC, but the essentials are:

- ✓Pre-admission control—Blocks unauthenticated messages.
- ✓Device and user detection—Identifies users and devices with pre-defined credentials or machine IDs.
- ✓Authentication and authorization—Verifies and provides access.
- ✓Onboarding—Provisions a device with security, management, or host-checking software.
- ✓Profiling—Scans endpoint devices.
- ✓Policy enforcement—Applies role and permission-based access.
- ✓Post-admission control—Enforces session termination and cleanup.

How does 802.1X NAC works?

The 802.1X NAC operation sequence is as follows:

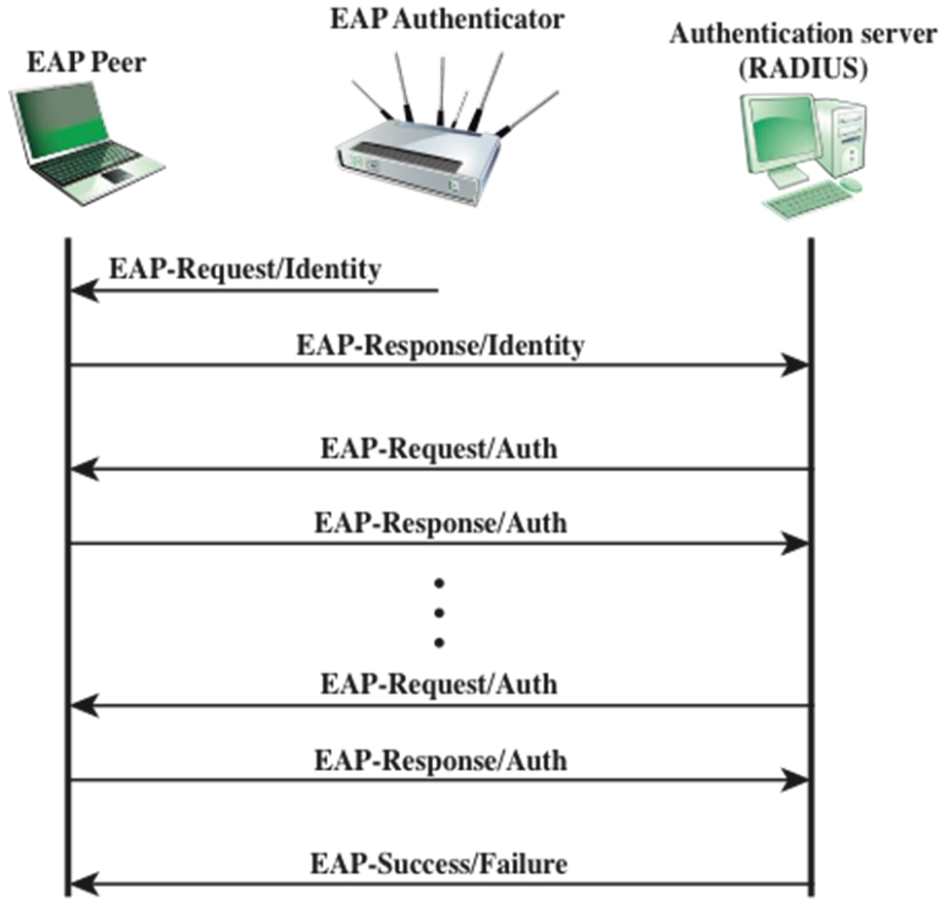
1) Initiation—The authenticator (typically a switch or an AP) or supplicant (client device) sends a session initiation request. A supplicant sends an EAP-response message to the authenticator, which encapsulates the message and forwards it to the authentication server (AS).

2) Authentication—Messages pass between the AS and the supplicant via the authenticator to validate several pieces of information.

3) Authorization—If the credentials are valid, the AS notifies the authenticator to give the supplicant access to the port.

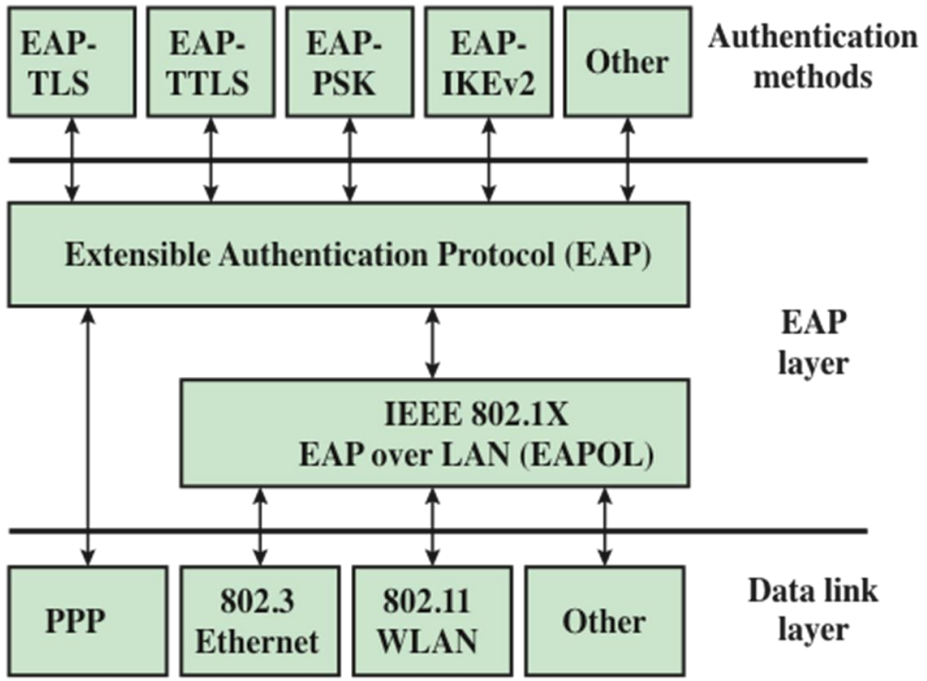
4) Accounting—RADIUS accounting keeps session records including user and device details, session types, and service details.

5) Termination—Sessions are terminated by disconnecting the endpoint device, or by using management software.



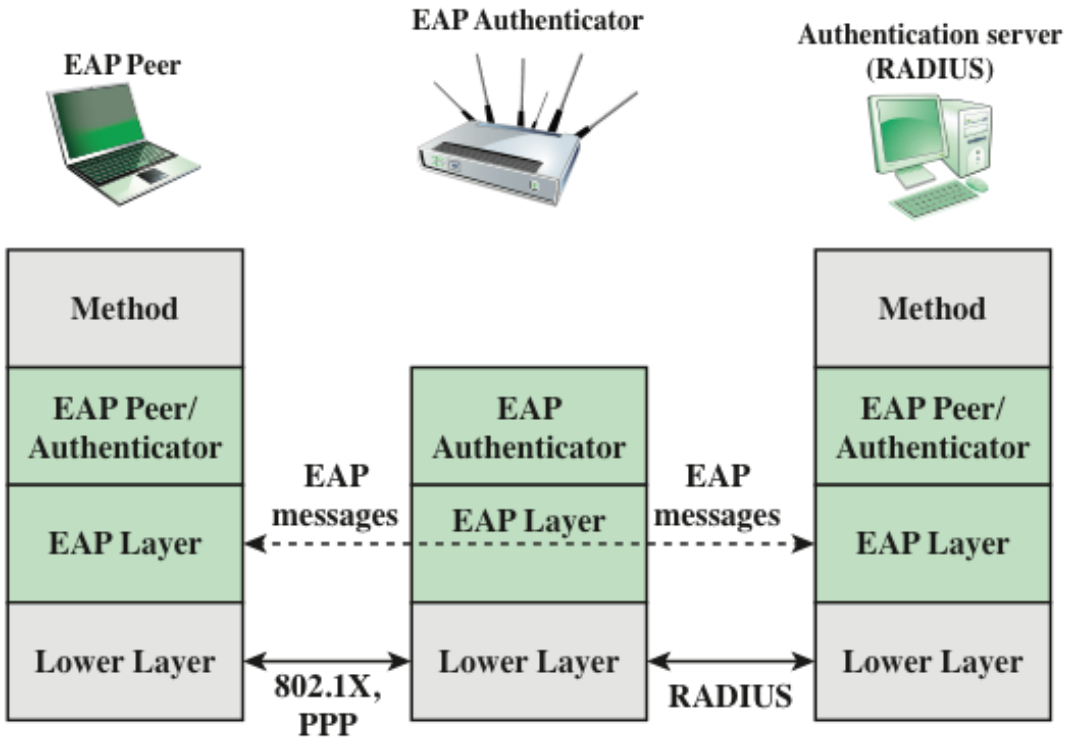
Extensible Authentication Protocol (EAP)

- ✓Defined in RFC 3748
- ✓EAP acts as a framework for network access and authentication protocols.
- ✓EAP supports multiple authentication methods. This is what is meant by extensible in EAP.
- ✓ EAP provides a set of protocol messages that can encapsulate various authentication methods
- ✓ EAP provides a generic transport service for the exchange of authentication information between a client system and an AS
- ✓The basic EAP transport service is extended by using a specific authentication protocol
  - ✓ EAP Transport Layer Security
  - ✓ EAP Tunneled TLS
  - ✓ EAP Generalized Pre-Shared Key
  - ✓ EAP Internet Key Exchange v2



EAP Layer Context

EAP Protocol Exchanges



Authentication server:

- negotiates the use of a specific EAP method with an EAP peer,
- validates the EAP peer's credentials, and
- authorizes access to the network.

Typically, the authentication server is a Remote Authentication Dial-In User Service (RADIUS) server.


Thank
You