NETWORK ADMINISTRATION

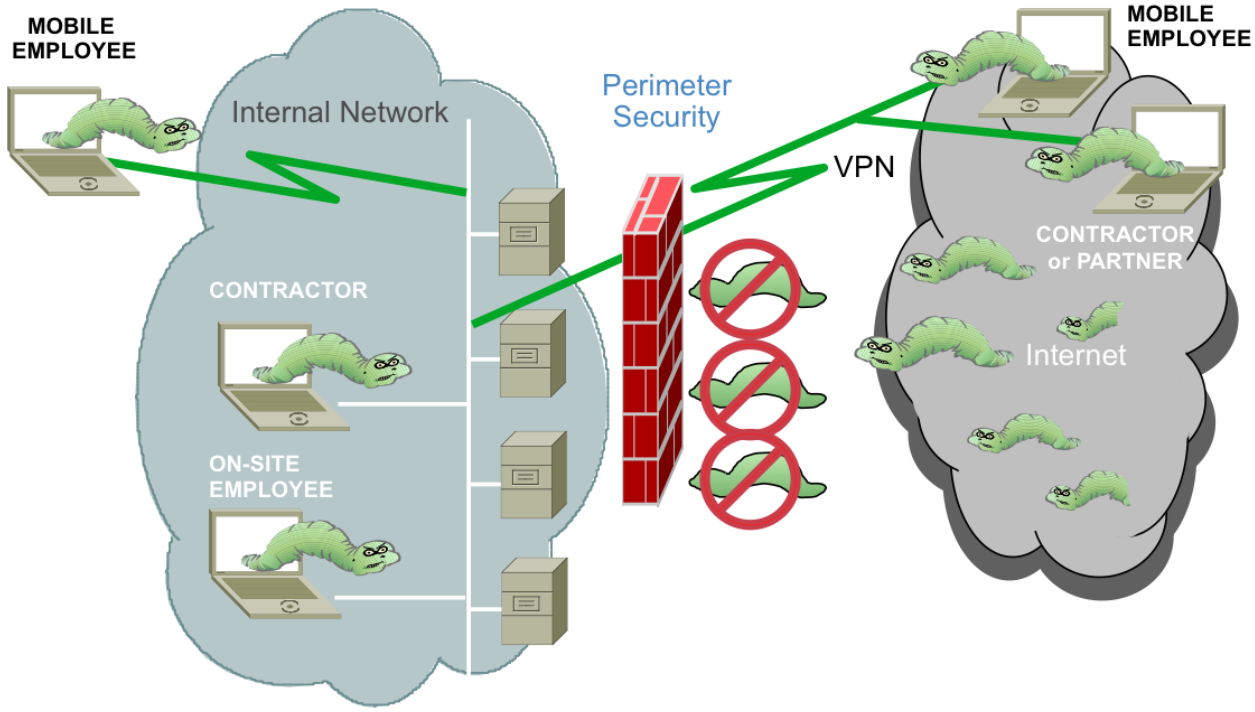
Lecture 11

Network traffic access control systems

Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

Problem - How to protect the computer network from our own users?

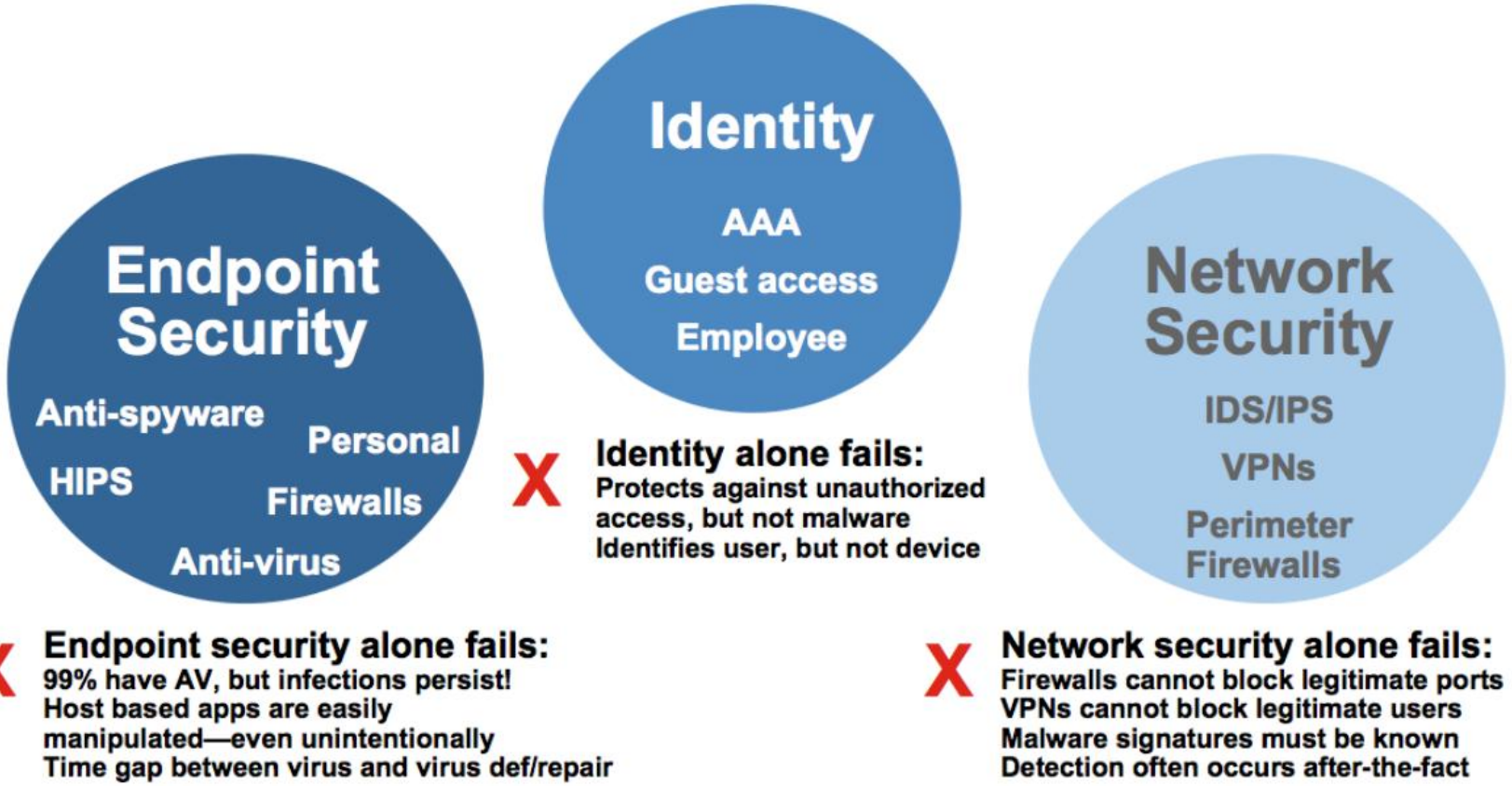


Viruses, worms and botnets are often spread by unknowing victims. These victims may be their own computer network users.

Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

Problem - How to protect the computer network from our own users?



NETWORK ADMINISTRATION

Advantages and disadvantages of Endpoint security systems

Advantages:

- According to Gartner, they are products that combine antivirus and anti-spyware protection, personal firewall, application control and intrusion prevention elements.
- Centralized management and enforcement of terminal device policies.
- Identify devices that do not have updated definitions or versions of system and application software
- Imposed policies cannot be banned by consumers

Disadvantages:

- Software agents reduce device performance, and sometimes users can stop scanning

NETWORK ADMINISTRATION

Advantages and disadvantages of Identity management systems

Advantages:

- Reduce the risk of an account being compromised
- Provide centralized management
- They are applicable for medium and large business

Disadvantages:

- They require perfect adherence to the security policy
- In an Ad Hoc environment, they cannot guarantee that employees only get access to the applications they need

NETWORK ADMINISTRATION

Advantages and disadvantages of Network security systems

Advantages:

- VLANs separate trusted devices and non-trusted devices in separate networks and create separate broadcast domains for them.
- The ability to spread viruses and attack trusted devices is limited

Disadvantages:

- There is no way to restrict the connection of untrusted devices to switch ports that are connected to the trusted network
- Device configuration errors can cause access to important resources
- The use of different subnets leads to inefficient use of IP addresses
- Switches can be vulnerable to MAC flooding, tagging, multicast brute force, etc.

Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

What is the solution?

- **The goal is to build a comprehensive solution for Network Access Control (NAC)**

- NAC is a computer network connection management solution that uses a set of protocols to define and implement a policy that describes how to provide access to network resources to devices at the time they first try to access the network.;

- NAC is an approach to computer network security that seeks to combine endpoint security technologies (such as antivirus protection, intrusion prevention, and vulnerability assessment), authentication of users or systems, and implementation of network security.;

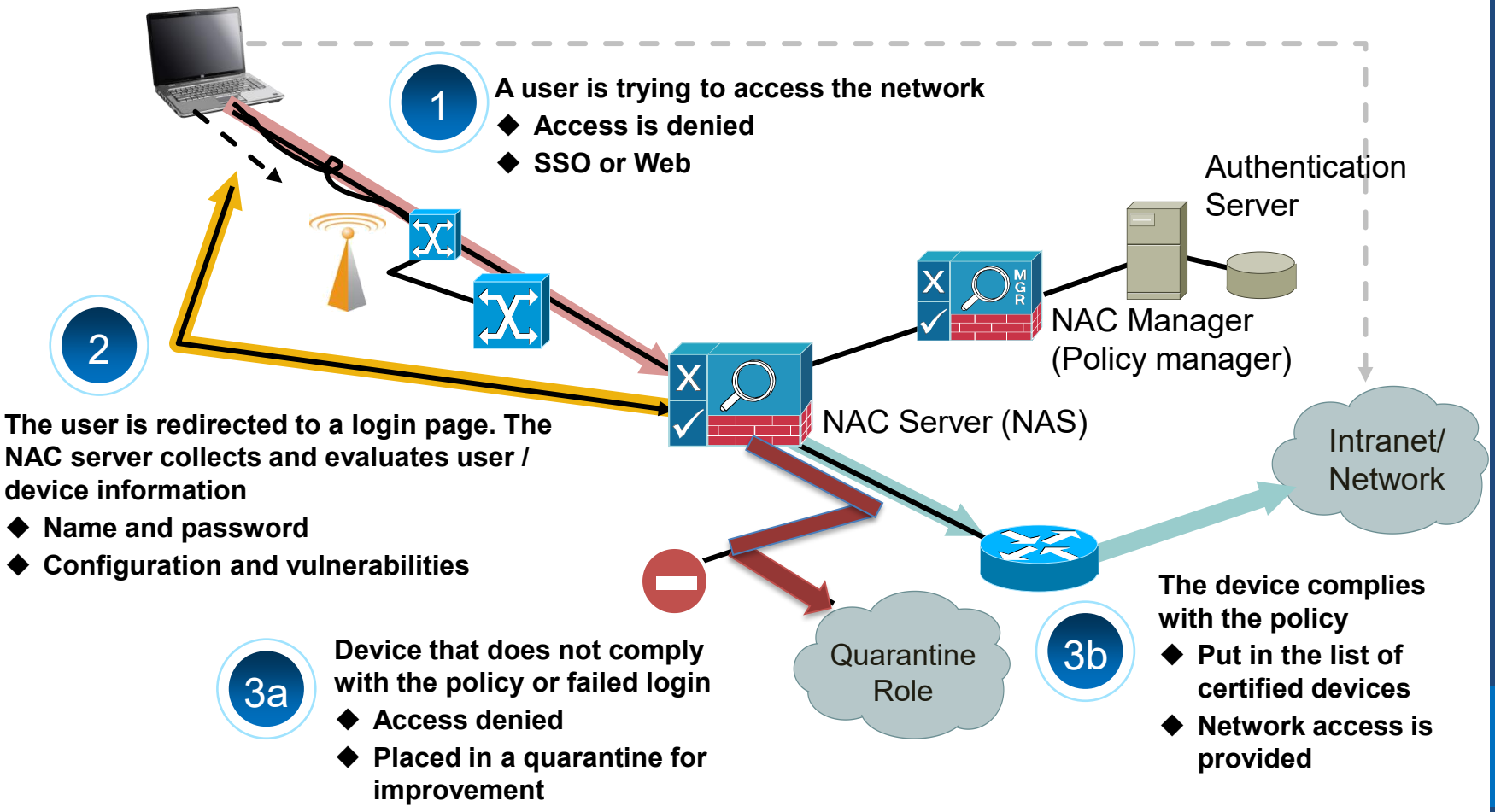
- NAC certifies users entering the network and determines which resources to access and what actions they can perform;

- NAC checks the status of the user 's computer or mobile device (endpoints);

NETWORK ADMINISTRATION

What is the solution?

The goal is to build a comprehensive solution for NAC



Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

What is the solution?

➢ **NAC components**

- **Access Requestor (AR) –** a client (requester) who is trying to access the network. This is any device that is controlled by NAC;
- **Policy server -** based on the policy defined by the organization, the policy server determines which access should be granted;
- **Network Access Server (NAS) -** also called a *media gateway*, a remote access server (RAS), or a policy enforcement server. The NAS functions as an access control point for users in remote locations who connect to the organization's internal network.

NETWORK ADMINISTRATION

Methods for providing network access

➢ Enforcement methods are actions that are applied to ARs in order to regulate access to the corporate network.

- **IEEE802.1X** – requires authorization before the AR is assigned an IP address. IEEE 802.1X uses the Extensible Authentication Protocol (EAP) for the authentication process).

- **Virtual local area networks (VLANs)** - the corporate network, consisting of an interconnected set of physical local area networks, is logically divided into a set of virtual local area networks. The NAC decides which of the VLANs the AR should join;

- **Firewall**: allows or denies network traffic between the organization's host and external users;

- **DHCP management:** DHCP allows dynamic allocation of IP addresses to hosts. The DHCP server manages and determines the IP addresses. Thus, NAC implementation is performed on an IP layer based on subnet affiliation and IP address assignment.

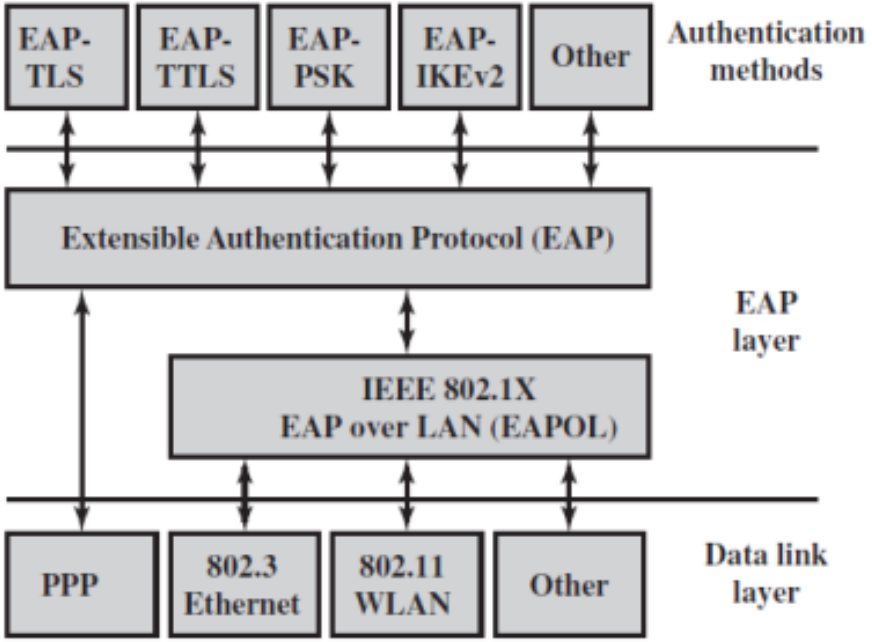
NETWORK ADMINISTRATION

Methods for providing network access

- **Extensible Authentication Protocol (EAP) RFC 3748 –** acts as a framework for network access management and authentication.

- EAP provides a set of protocol messages encapsulating different authentication methods that are used between a client and an authentication server.

- EAP can work in a variety of devices at the channel and network levels, including point-to-point connections, LAN, and other networks, and can meet authentication requirements for the various connections and networks.;



NETWORK ADMINISTRATION

Methods for providing network access

- **EAP-TLS (EAP Transport Layer Security) RFC 5216 :** determines how the TLS protocol can be encapsulated in EAP messages. The TLS handshake protocol is used. The client and server authenticate each other using digital certificates. The client generates a key that it encrypts with the server's public key and sends it to the server. This keyis used to generates the session key;

- **EAP-TTLS (EAP Tunneled TLS):** like EAP-TLS, except only the server has a certificate to authenticate itself to the client first. In EAP-TLS, a secure connection (the “tunnel”) is established with secret keys

NETWORK ADMINISTRATION

Methods for providing network access

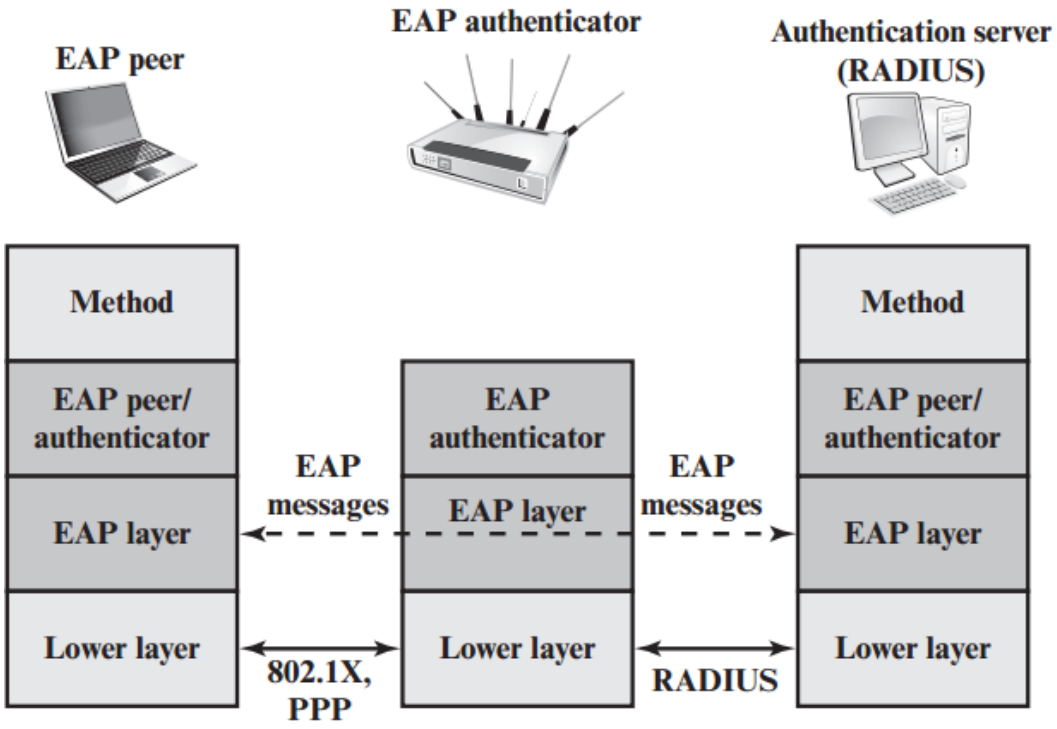
- **EAP-GPSK (EAP Generalized Pre-Shared Key) RFC 5433:** is an EAP method for mutual authentication and key exchange for a session using a pre-shared key (PSK). Therefore, this method is efficient in terms of message flows and computational costs, but requires the existence of pre-shared keys between each partner and the EAP server. Identifying these secret key pairs is part of partner registration. The method provides a secure communication channel for mutual authentication to be successful for both parties, and is intended for authentication when communicating on insecure networks such as IEEE 802.11. EAP-GPSK does not require public key encryption. The exchange of messages according to the EAP protocol method is carried out with a minimum of four messages.;

- **EAP-IKEv2 (RFC 5106):** based on version 2 of the Internet Key Exchange Protocol (IKEv2). It supports mutual authentication and session key generation through various methods;

NETWORK ADMINISTRATION

Methods for providing network access

- **EAP messaging (RFC 3748)**

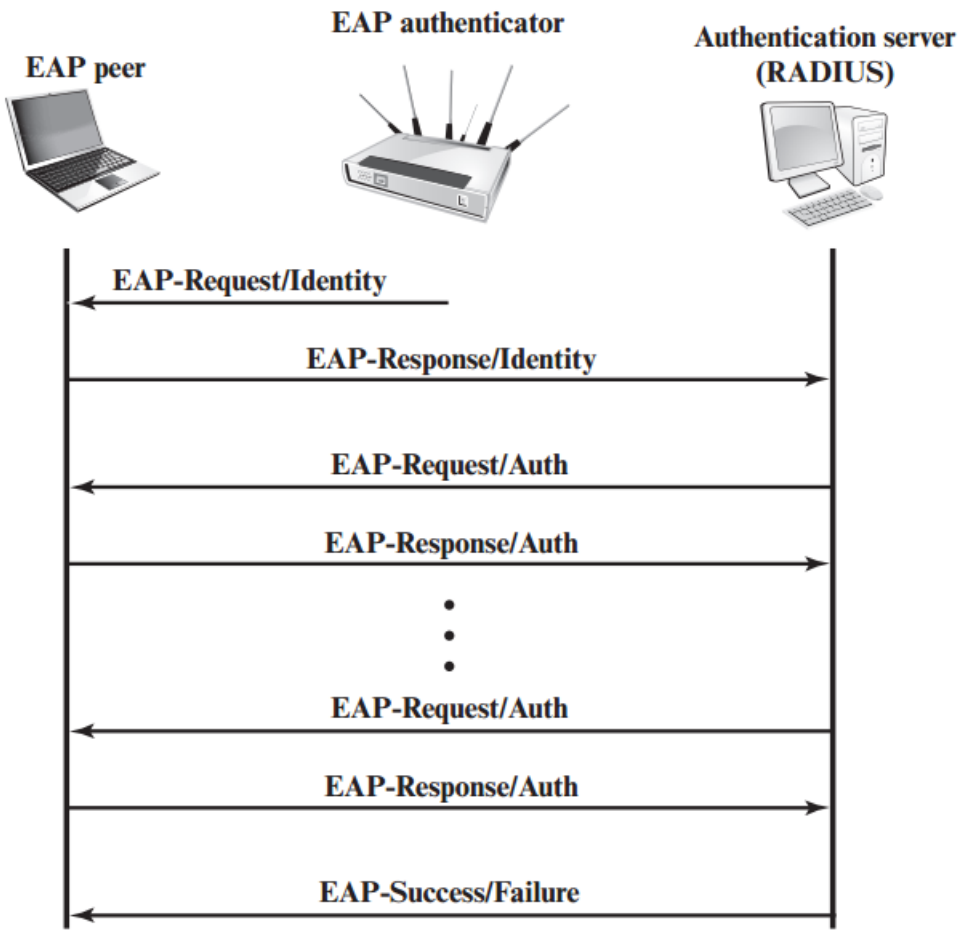


- **EAP peer:** client device trying to access the network
- **EAP authenticator:** an access point or NAS that requires EAP authentication before allowing network access;
- **Authentication server:** A server that validates client authentication data and authorizes network access. This is usually a RADIUS server.

NETWORK ADMINISTRATION

Methods for providing network access

- **EAP messaging (RFC 3748)**



- **EAP messages have the following fields:**

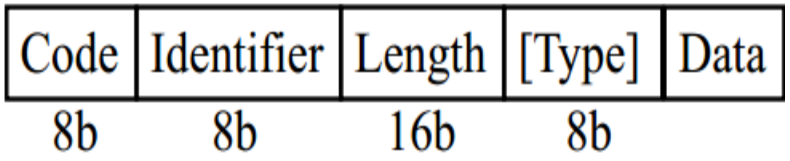
- ✓ **Code:** determines the type of message: Request (1); Response (2); Success (3); Failure (4)

- ✓ **Identifier:** used to match responses to requests. Its value increases with each subsequent message. The identifier in the response is equal to the identifier in the request.

NETWORK ADMINISTRATION

Methods for providing network access

- **EAP message format**



- ✓ **Lenght:** in octets, the length of the EAP message, including the Code, Identifier, Length, Type, Data fields

- ✓ **Type:** indicates the authentication method, according to the IANA definition.

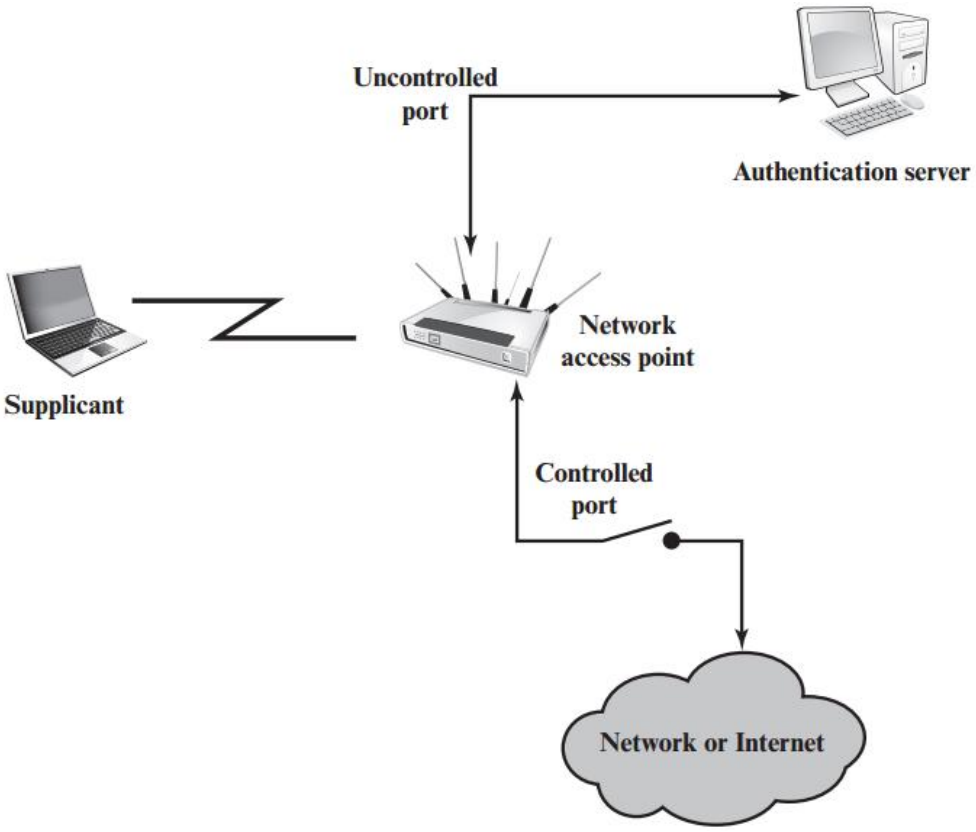
1 = Identity
2 = Notification
3 = NAK, valid only for responses
4 = MD5 Challenge (CHAP)
5 = One time password
6 = Generic Token card (GTC)
254 = Expanded types

- ✓ **Data:** Contains information related to authentication

NETWORK ADMINISTRATION

Methods for providing network access

- **Port-based authentication via IEEE 802.1X**



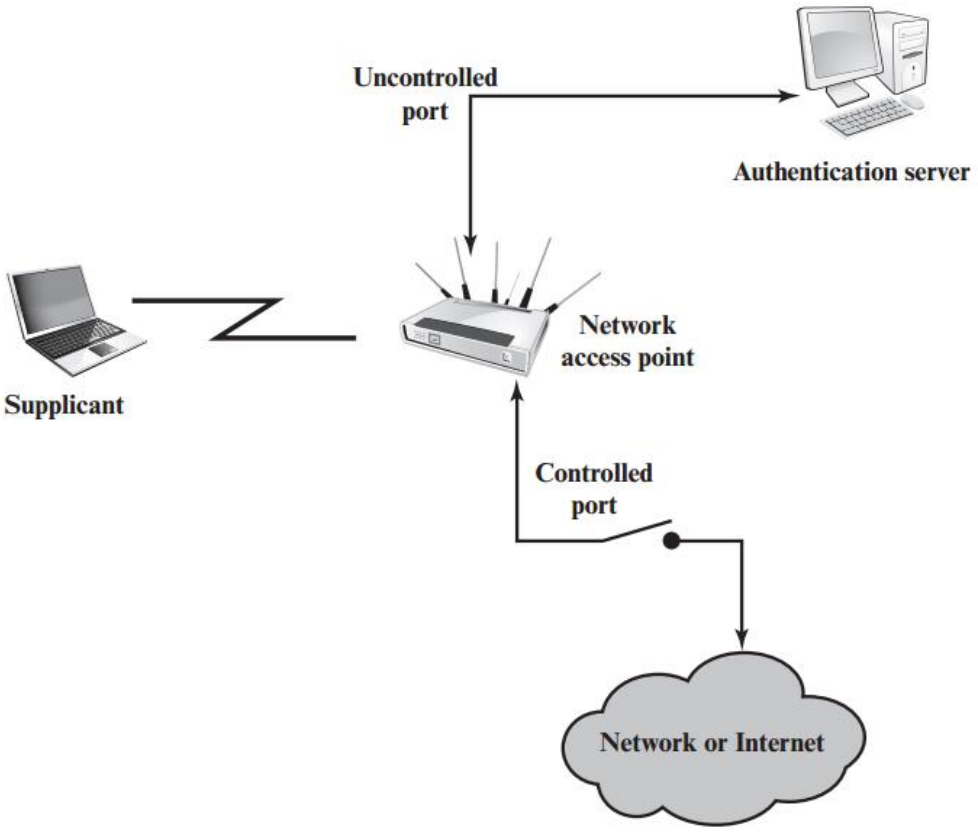
- **Terminology**

- ✓ Supplicant (EAP peer)
- ✓ Authenticator
- ✓ Authentication exchange
- ✓ Authentication process
- ✓ Authentication server (EAP AS)
- ✓ Authentication transport
- ✓ Bridge port
- ✓ Edge port
- ✓ Network access port (EAP authenticator)
- ✓ Port access entity (PAE)

NETWORK ADMINISTRATION

Methods for providing network access

- **Port-based authentication via IEEE 802.1X**



- **EAPOL (EAP over LAN)**

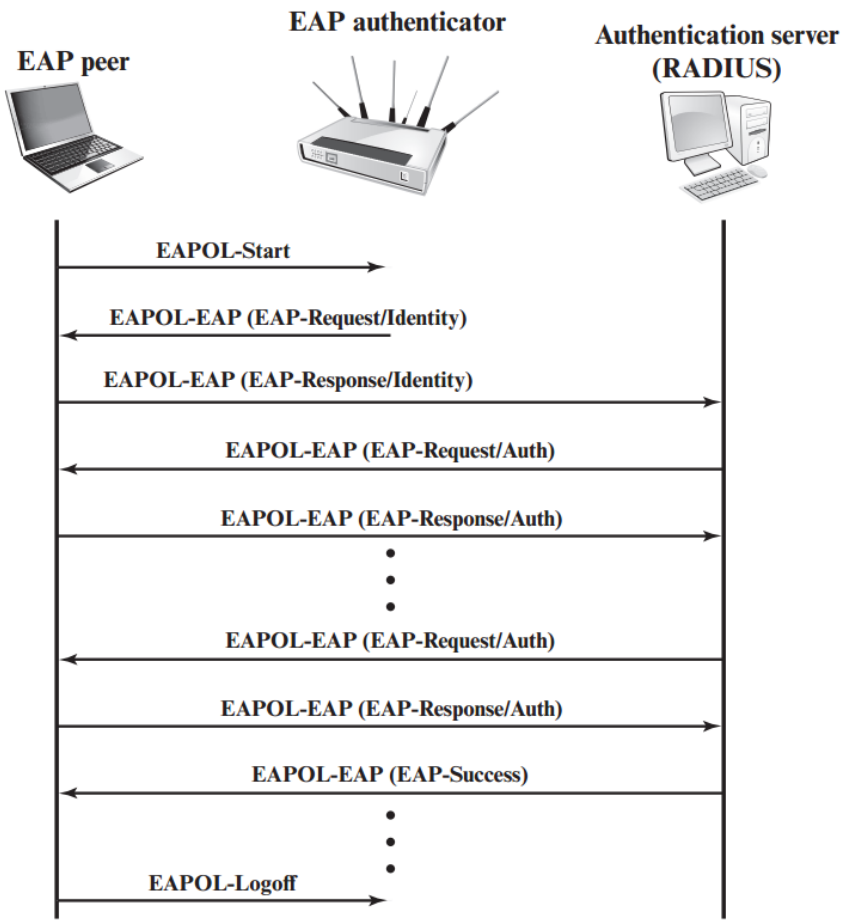
Frame types:

- ✓ EAPOL-EAP – contains an encapsulated EAP package
- ✓ EAPOL-Start – a package with which the client searches for an authenticator
- ✓ EAPOL-Logoff – a package with which the customer declares a wish to be disconnected from the network
- ✓ EAPOL-Key – a package that sends the session keys to the client when it is decided to give the client access

NETWORK ADMINISTRATION

Methods for providing network access

- **Example of IEEE 802.1X authentication with RADIUS**

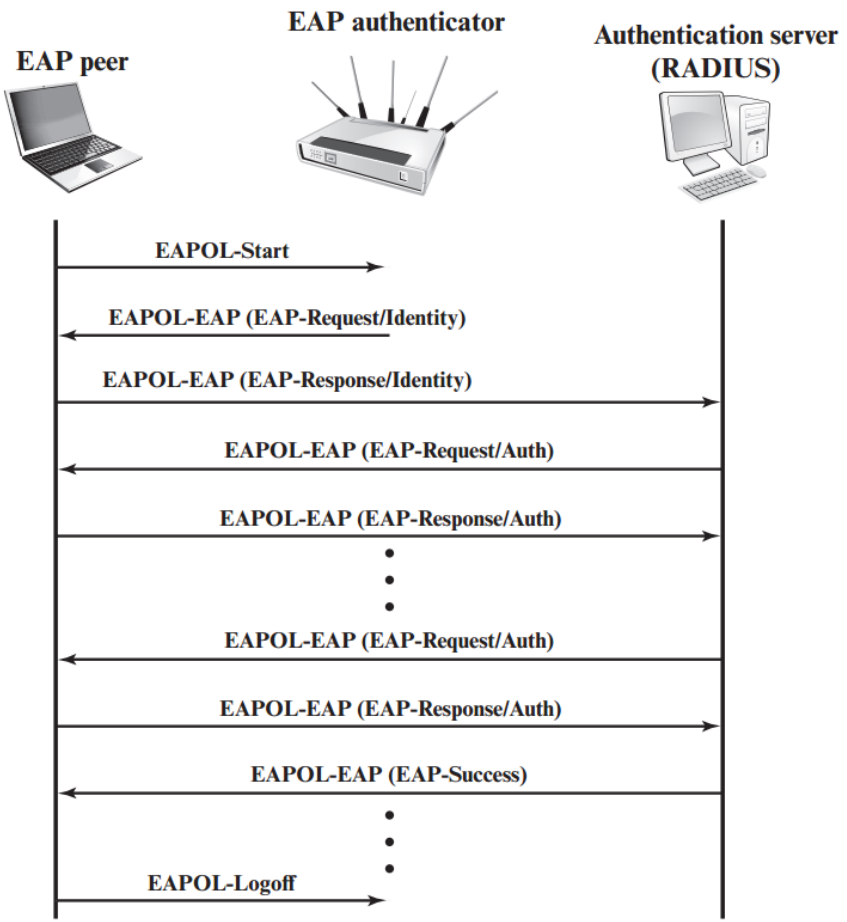


1. EAPOL-Start sent as a multicast to 01:80:c2:00:00:03
2. EAP-Request/Identity a frame sent by the authenticator requesting identification information, such as a name. The authenticator sends such a message periodically even before it has received EAPOL-Start;
3. The client sends the requested data in response with an EAP-Response / Identity frame that the authenticator receives via an uncontrolled port. It is encapsulated in a RADIUS over EAP packet and sent to the RADIUS server as a Radius-Access-Request packet.;
4. The RADIUS (AAA) server responds with a Radius-Access-Challenge packet, which is sent via the authenticator to the client as a EAP-Request and contains challenge information, e.g. password, and information for the authentication method that will be used in further communication. If the client does not support the proposed authentication method, it requests another method by sending an EAP-Response Auth NAK specifying the desired authentication method. The authenticator forwards the message to the AS;

NETWORK ADMINISTRATION

Methods for providing network access

- **Example of IEEE 802.1X authentication with RADIUS**

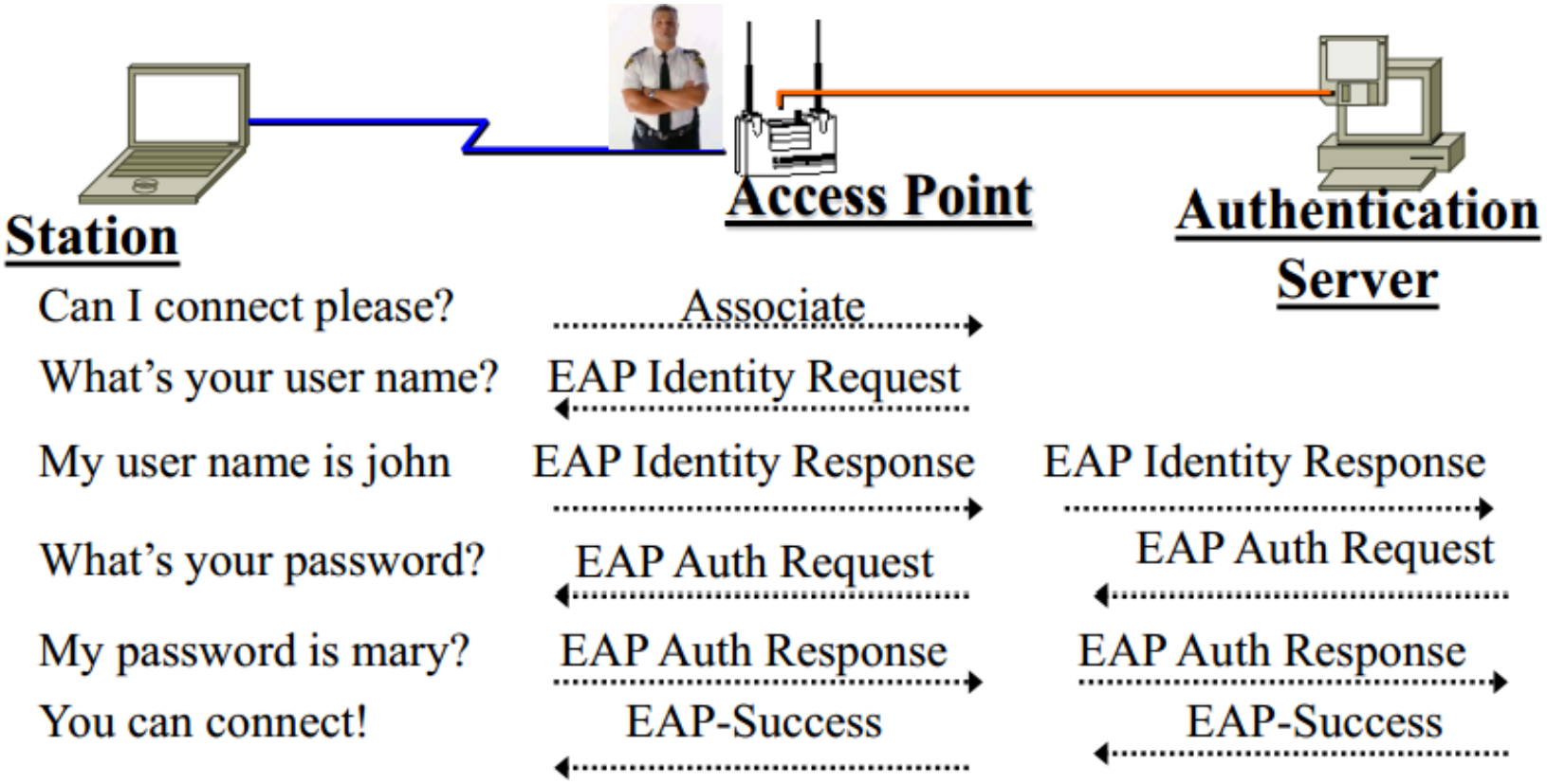


5. AS resends the Radius-Access-Challenge based on the EAP authentication method requested by the customer.;
6. The client forms an EAP-Response, and a Radius-Access-Request is formed in the authenticator with a response to the challenge. Once the authentication method is confirmed, several messages are exchanged;
7. The RADIUS (AAA) server provides access with a Radius-Access-Accept message. The authenticator issues an EAP-Success packet. The controlled port is authorized and the client can access the network. If the authentication data provided by the client is incorrect, the AS sends a radius-Access-Reject message;

NETWORK ADMINISTRATION

Methods for providing network access

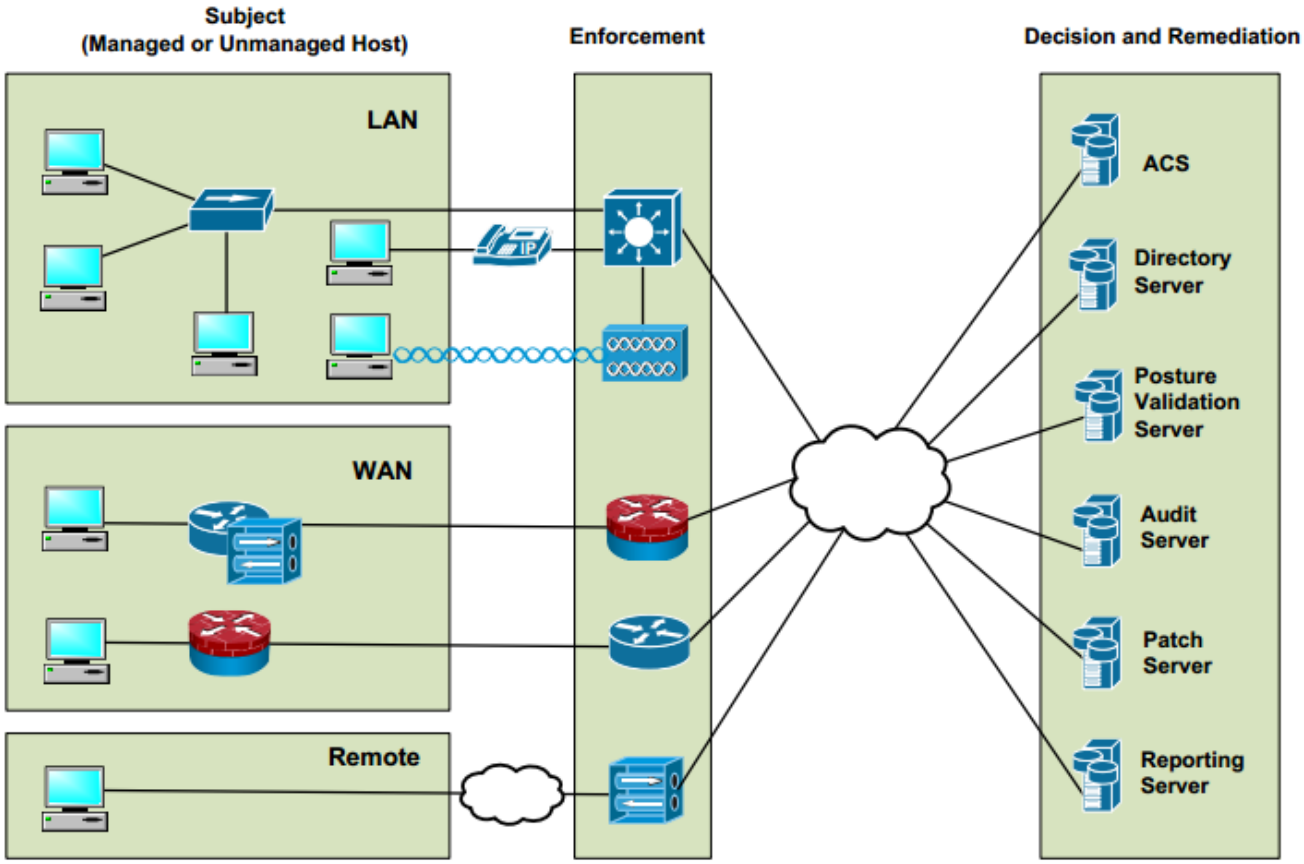
- **Example of IEEE 802.1X authentication**



NETWORK ADMINISTRATION

An example of a Cisco NAC Framework

- The NAC Framework assesses the state of hosts in order to prevent unauthorized or vulnerable endpoints from accessing the network.



Subjects: These are managed or unmanaged hosts that have access to the network on which the NAC is running.

Enforcement devices: These are network devices acting as points for enforcing NAC rules.

Decision and remediation devices: In this group, many different network devices support the NAC framework architecture:

NETWORK ADMINISTRATION

An example of a Cisco NAC Framework

- **Authentication, authorization, and accounting (AAA) server:** This is the central policy server that summarizes one or more credentials and permissions into a single solution, which it writes to the network profiler for execution by network access devices. Cisco's AAA server that supports NAC is called the Cisco Secure Access Control Server (ACS);

- **Directory server:** This is the central directory server that authenticates the user or machine. Examples here are Microsoft Active Directory, Novell Directory Services (NDS), and one-time password servers;

- **Posture validation server - PVS:** This server acts as a decision point depending on the specific policy in the NAC.

NETWORK ADMINISTRATION

An example of a Cisco NAC Framework

Depending on the policy adopted, it determines the set of necessary identification data. Examples include antivirus servers and secure application servers.

- **Remediation server**: It implements management decisions with the idea to bring non-compliant hosts into compliance. This can be done with specialized patch management applications or simply a software distribution website.;

- **Audit server**: It is a server or software that evaluates a host's vulnerability to determine its level of compliance or risk before it is allowed on the network.;

NETWORK ADMINISTRATION

An example of a Cisco NAC Framework

➢ **Support for NAC Framework of routers**

- The IP NAC mechanism in layer 3 uses the EAP and UDP protocols. Routers that support this mechanism are considered NAC Release 1.0 devices. They can act as a network intrusion prevention system (NIPS). Such devices first appeared in mid-2004 and were included in the Cisco IOS Software Release 12.3(8)T operating system. Firewalls, NIPS, and cryptographic support were then introduced.

- NAC Agentless Host is another NAC mechanism that allows access to a network of hosts that cannot be NAC compliant. This category includes printers, scanners, copiers, cameras, sensors and specialized equipment. This also includes computers with unsupported operating systems, embedded operating systems, and personal firewalls. For them, static exceptions can be configured to bypass the state validation process for individual MAC and IP addresses.

NETWORK ADMINISTRATION

An example of a Cisco NAC Framework

- **Support for NAC Framework of routers**

- Devices that support either the Layer 2 IP NAC mechanism (EAP and UDP protocols) or Layer 2 NAC 802.1X (EAP and 802.1X protocols) are considered NAC Release 2.0 devices. The IP NAC mechanism in layer 2 is triggered by the appearance of ARP or possibly DHCP traffic in the switch interface.

NETWORK ADMINISTRATION

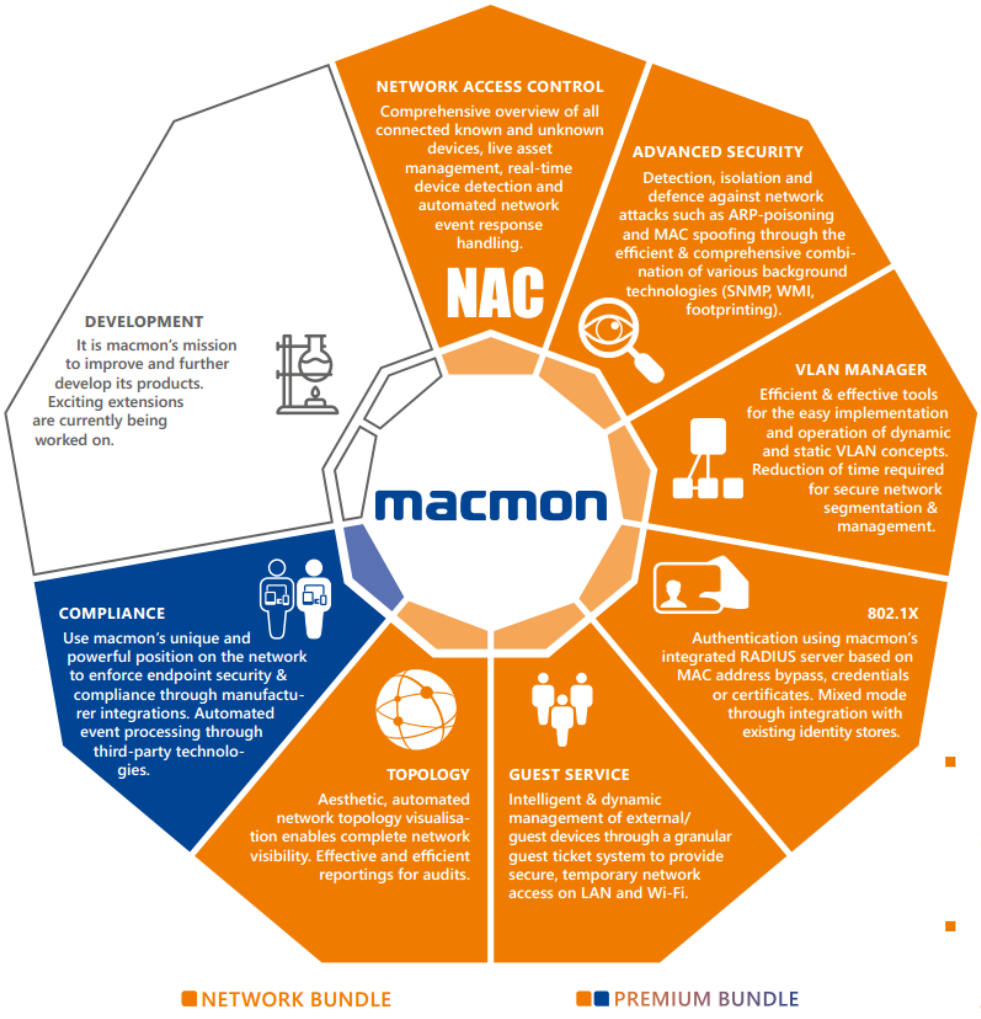
An example of a Cisco NAC Framework

➢ **Support for NAC Framework of switches**

- The NAC performs layer 2 state validation for hosts with or without 802.1X enabled. Vulnerable and non-compliant hosts can be isolated by gaining incomplete, reduced network access, or redirected to recovery servers depending on organizational policy..

NETWORK ADMINISTRATION

An example of a Macmon NAC Framework



- **Network Bundle**
  macmon NAC, Advanced Security, VLAN Manager, Guest Service, 802.1X, Topology
- **Premium Bundle**
  Modules of Network Bundle + extensive mechanisms to proof the compliance/security status of end devices

Assoc. Prof. Rosen Radkov PhD

NETWORK ADMINISTRATION

THANK YOU FOR THE ATTENTION!

Assoc. Prof. Rosen Radkov PhD