07- Cisco Secure Network Access Solutions (Cisco ISE)

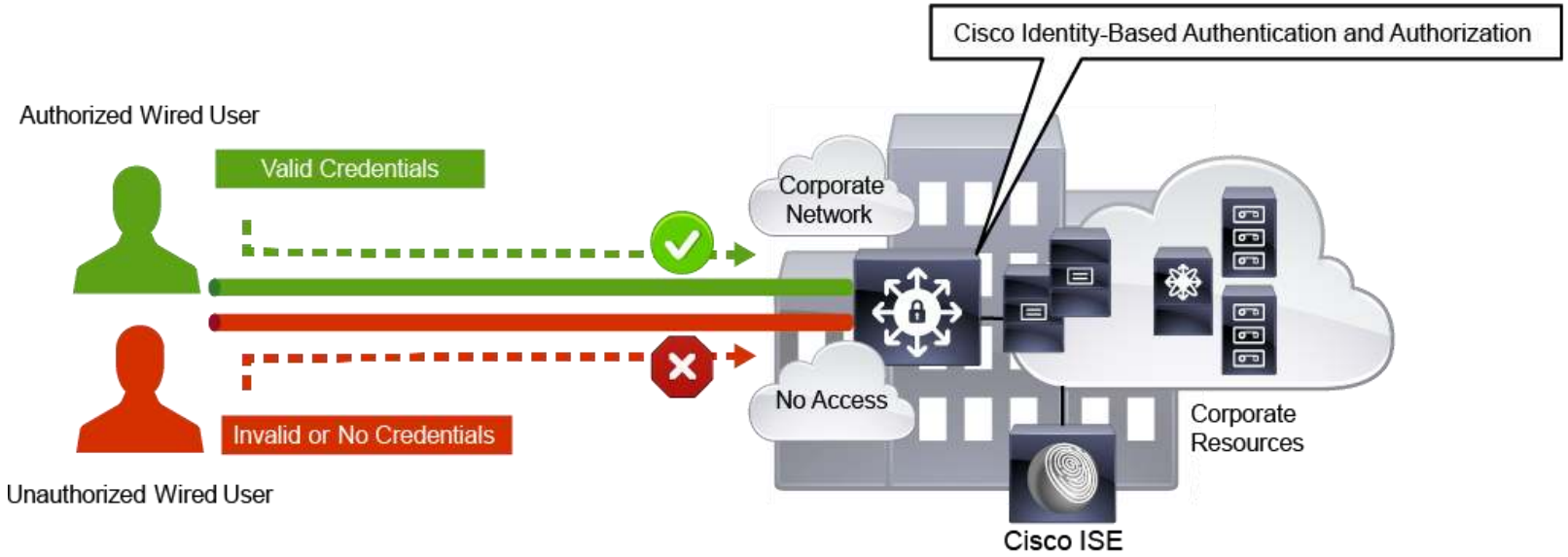
Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Cisco Secure Network Access

- Cisco secure network access is characterized by a suite of services that are embedded in Cisco Catalyst switches and Cisco WLCs.
- Cisco ISE uses infrastructure services provided by switches and WLCs to allow you to implement the following services:
  - Strong authentication using IEEE 802.1X, MAB, and Web Authentication
  - Policy-based authorization via downloadable ACLs, VLAN assignment, or SGTs.

Cisco Secure Network Access (cont.)

- The Cisco secure network access solution promotes authentication to access the network.
- Authentication serves as the basis for differentiating users and/or devices, providing varying levels of access to networked resources based on corporate access policy.



Cisco Secure Network Access (cont.)

- **The foundation for Cisco Secure Network Access is IEEE 802.1X**, a port-based authentication and access control protocol, which can be applied at a physical switch port on the wired network or on a wireless LAN (WLAN) on Cisco WLC.
- In both **wired** and **wireless** domains, clients will require the installation of a **Cisco 802.1X supplicant**, the configuration of a **native operating system supplicant** or, in the case of **Linux clients, the installation of an open-source supplicant**.
- Wireless users generally expect that they will need to authenticate before being granted access to the corporate network.
- As a result, populations of wireless users are good candidates for initial Cisco secure network access deployments.

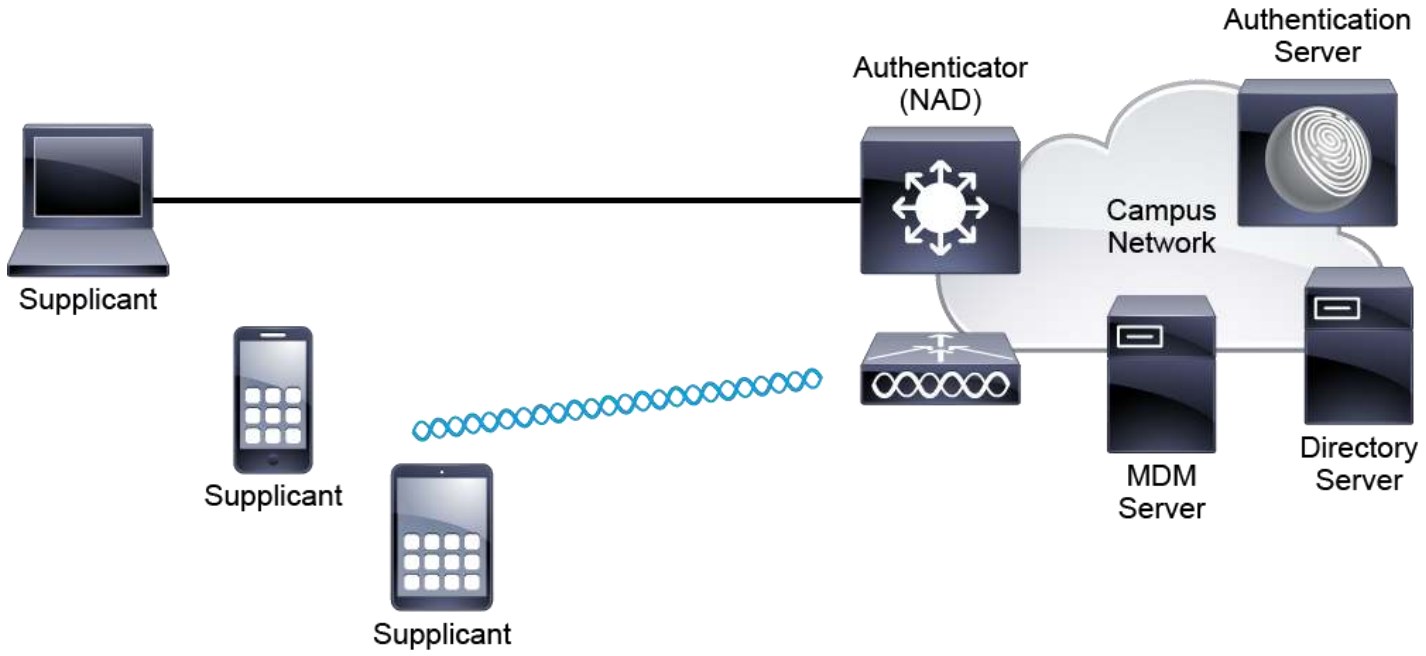
Cisco Secure Network Access Components

The main components and functions of secure network access using 802.1X are:

- **802.1X client supplicant software:** Each client that connects to a wired or wireless network under 802.1X control requires supplicant software. The supplicant is responsible for initiating an authentication session with the authenticator.
- **802.1X authenticator:** The 802.1X authenticator, or also called network access device (NAD), determines the pre-authorization traffic policy, forwards supplicant credentials to the authentication server, and enforces network access policy as prescribed by the authentication server.
- **802.1X authentication server:** The 802.1X authentication server is responsible for validating the access credentials forwarded by the authenticator and performs an identity-based policy lookup. Access restrictions are then pushed to the authenticator, or the NAD. The credentials that are supplied by the client can take the form of digital certificates, passwords, one-time passwords (OTPs) supplied by a token, or a client MAC address.

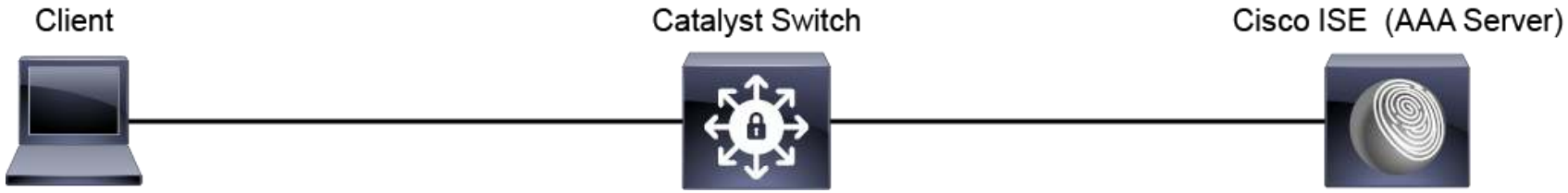
Cisco Secure Network Access Components (cont.)

The main components and functions of secure network access using 802.1X (cont.)



AAA Role in Cisco Secure Network Access Solution

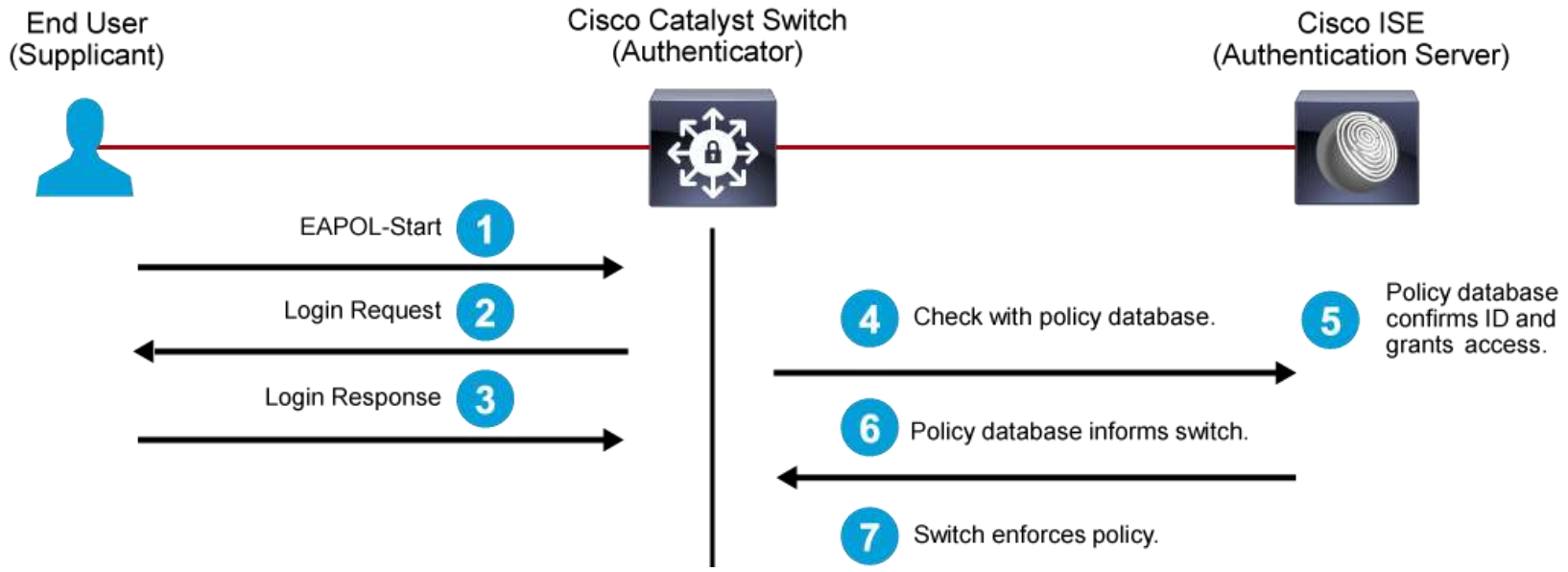
- To authenticate users and devices, the integration of authentication, authorization, and accounting (AAA) services are required.



- Authentication can be compared to being stopped at the office lobby by a security guard, After you provide a driver's license to validate that you are on the guest list, you are given an access badge.
- Authorization relates to which doors the access badge opens, Your access is restricted by the badge policy.
- Accounting is the system that tracks your movements through the building and records which doors you accessed with your badge and whether access was permitted or denied.

AAA Role in Cisco Secure Network Access Solution (cont.)

- Here, Cisco ISE acts as AAA server in Cisco Identity Based Networking Services (IBNS) deployments and provides authentication, authorization, and accounting services for controlled network access.



AAA Role in Cisco Secure Network Access Solution (cont.)

- The basic phases of Cisco secure network access wired port control are as follows:

1. The supplicant on the end user machine announces itself to the authenticator (switch).
2. The authenticator (switch) prompts the supplicant for authentication credentials.
3. The supplicant provides credentials to the authenticator (switch), The credentials are provided by the supplicant to the authenticator (switch) via the Extensible Authentication Protocol (EAP), EAP supports various authentication methods, Some of the most commonly deployed EAP authentication types include EAP-MD5, EAP-TLS, EAP-PEAP, EAP-TTLS, and EAP-FAST.

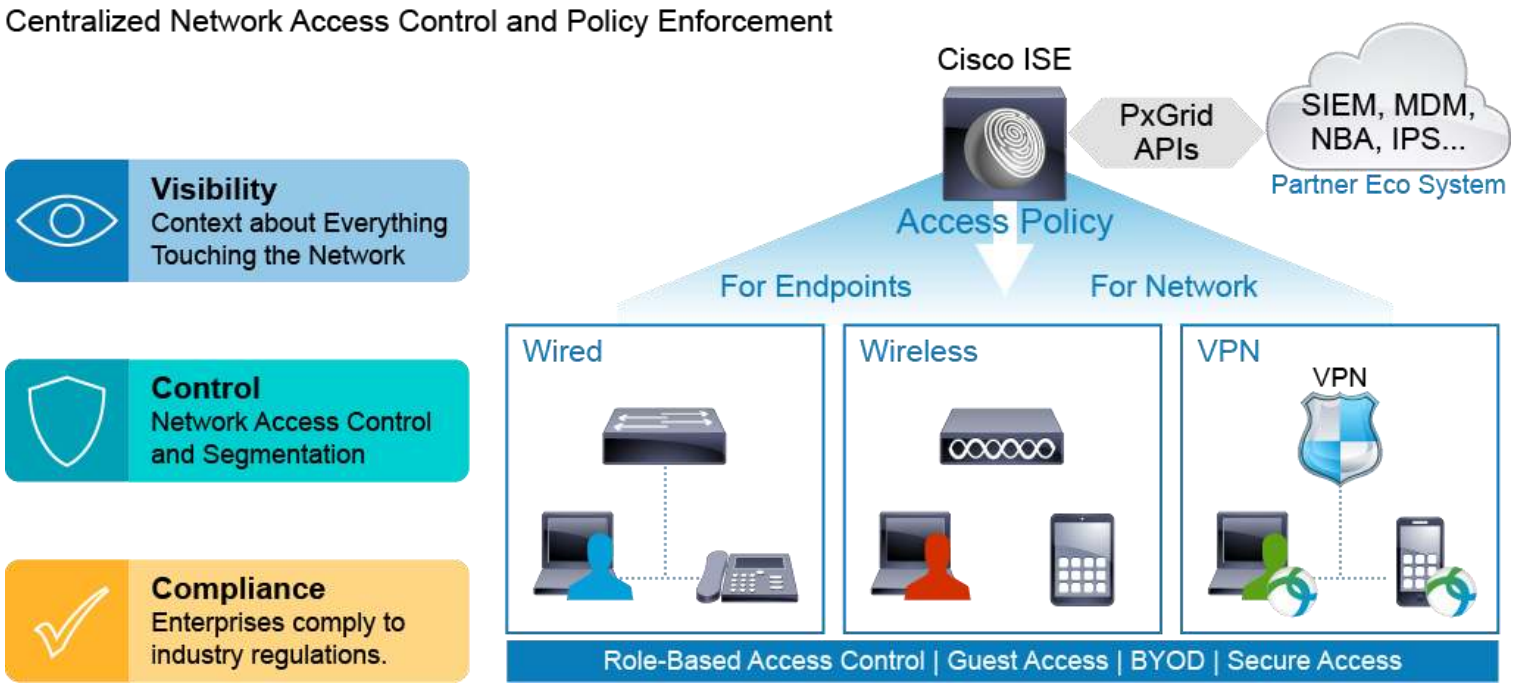
AAA Role in Cisco Secure Network Access Solution (cont.)

- The basic phases of Cisco secure network access wired port control are as follows (cont.)

4. The authenticator (switch) forwards the credentials to the authentication server (Cisco ISE), The authenticator (switch) proxy the EAP data from the supplicant to the authentication server (Cisco ISE) using RADIUS encapsulation.
5. The authentication server (Cisco ISE) validates the credentials and makes a policy decision that is based on the supplied identity.
6. The authentication server (Cisco ISE) instructs the authenticator (switch) to enforce policy on the switch port.
7. Authenticator (switch) enforces policy.

Cisco Identity Services Engine

- Cisco ISE is a centralized network access control and policy enforcement platform. With it you gain centralized policy management solution to control network access and usage policies from a single location.



Cisco Identity Services Engine (cont.)

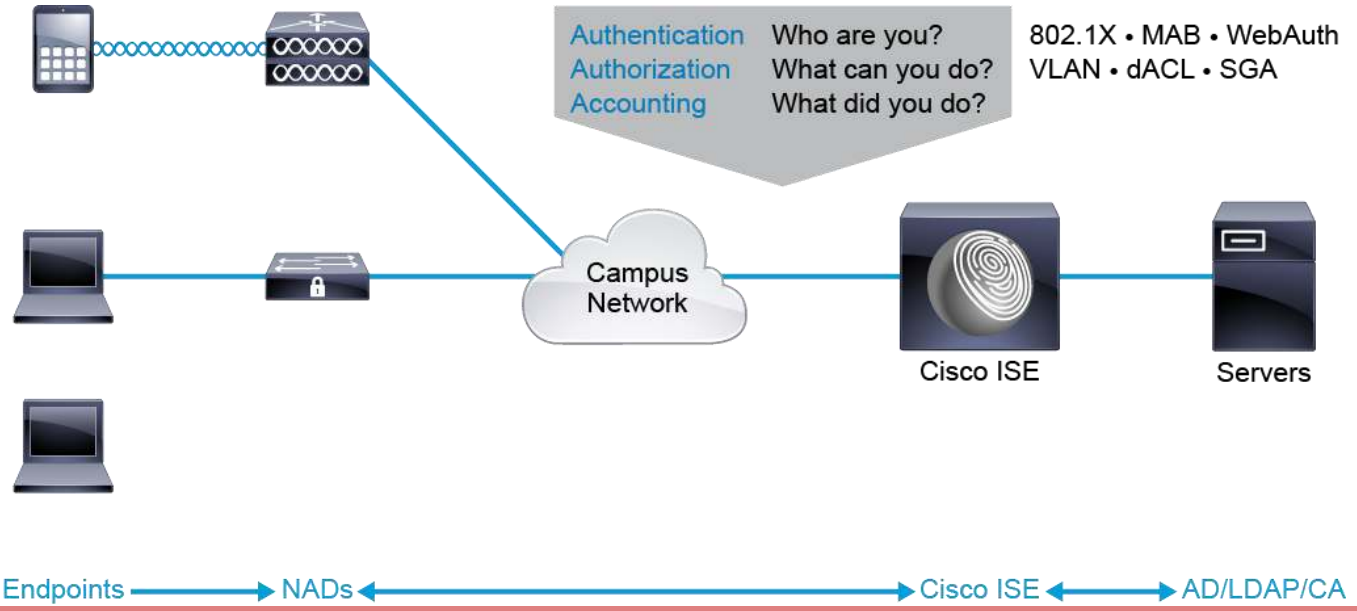
- Cisco ISE gathers key information about user and device access, and uses this information to control end user network access and administrative network device access, regardless of connection type.
- Wired, wireless, and remote users can connect directly or through VPNs.
- Whether connected remotely or directly to corporate resources, users can receive the same unified access and control.
- Cisco ISE also delivers guest and enterprise mobility management capabilities that regulate access to Internet, internal corporate network and resources.

Cisco Identity Services Engine (cont.)

- Cisco ISE can also use gathered information to ensure regulatory compliance to various government and industry standards.
- This information can also be shared among Cisco Eco system partner devices over pxGrid (Plaftorm Exchange Grid), to enhance the capabilities for services including Security Information and Event Management (SIEM), Mobile Device Management (MDM), Network Behavior Analysis (NBA), intrusion prevention systems (IPS), and much more.
- pxGrid is an open, scalable, and IETF standards-driven API platform helps automate security to get answers and contain threats faster.

Cisco Identity Services Engine (cont.)

- Integrated RADIUS services inside Cisco ISE, enable AAA, which is typically used for end user network access.
- User identities can be validated against an internal Cisco ISE database, back-end external Microsoft Active Directory, or LDAP servers.



Cisco Identity Services Engine (cont.)

Cisco ISE Posture Compliance

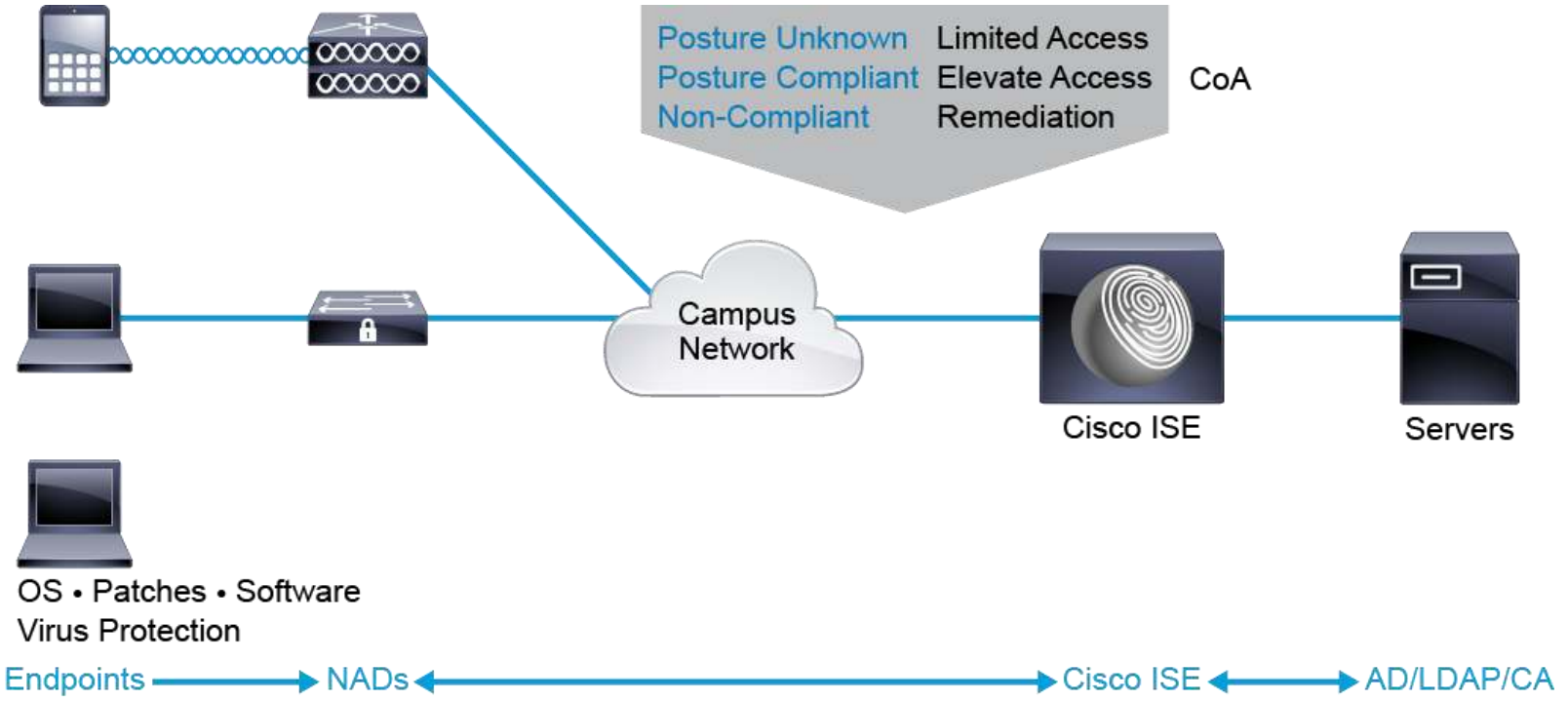
1. Authentication determines whether the user can access the network.
2. After the Cisco ISE RADIUS service verifies user identity and processes account attributes, it can apply an authorization profile to the session.
3. Cisco ISE sends this authorization policy to the NAD in a RADIUS Access-Accept reply.
4. This authorization policy controls what actions a user can perform.
5. Accounting tracks user actions, when and where they logged in, what they accessed, and more.

Cisco Identity Services Engine (cont.)

6. Posture assessment allows you to validate and maintain endpoint security capabilities.
7. You can configure initial RADIUS authentication to grant only limited client access.
8. After initial client access, posture assessment can validate endpoint operating system and patch versions, virus protection, and other compliance requirements.
9. If the device meets these criteria, elevated access can be granted by using RADIUS Change of Authorization (CoA) massaging.
10. If devices are noncompliant, you can engage remediation functions.

Cisco Identity Services Engine (cont.)

- This feature helps to ensure that endpoints conform defined security standards.



Cisco Identity Services Engine (cont.)

Cisco ISE Profiling Service

1. **Initial access:** Profiling services enable Cisco ISE to determine the endpoint device type and capabilities. After initial authentication, devices can be placed in an "unknown" category.

2. **Classification/profiling:** The profiling service will then probe key characteristics, such as interactions with HTTP, Domain Name System (DNS), DHCP, and RADIUS services. It can thus determine the device type and place it in a defined category such as Android, Apple, or iPad. An internal endpoint database stores the profiling results to streamline subsequent authorization and categorization.

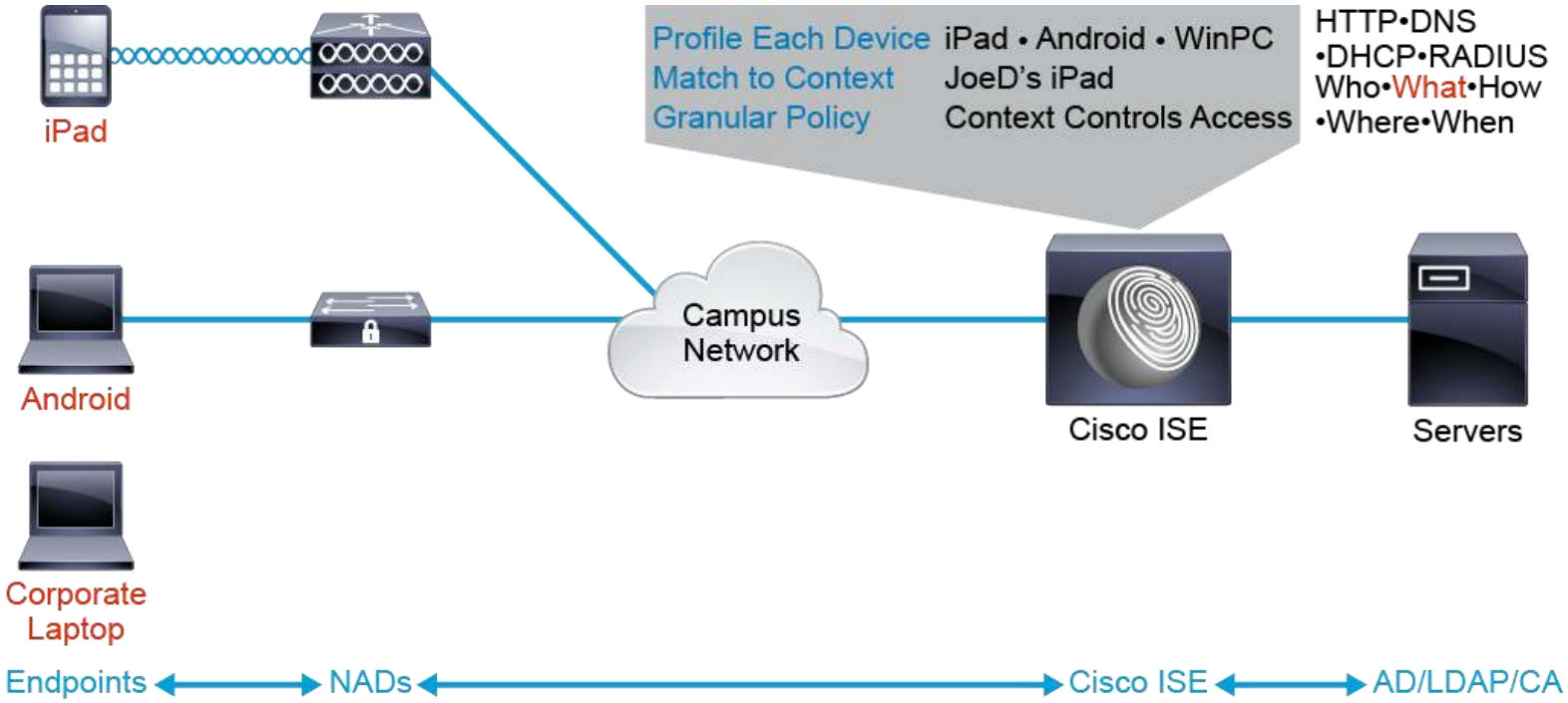
Cisco Identity Services Engine (cont.)

Cisco ISE Profiling Service (cont.)

3. **Match device type to other context:** Cisco ISE is now aware of the contextual what, and matches it with who, how, where, and when.
4. **Granular Policy:** You can now use this context to create very granular policy. When user "JoeD" logs in using his personal iPad from a public café, he may have limited access. But when he logs in using his corporate laptop from his desk at the office, he gains elevated levels of access.

Cisco Identity Services Engine (cont.)

Cisco ISE Profiling Service (cont.)



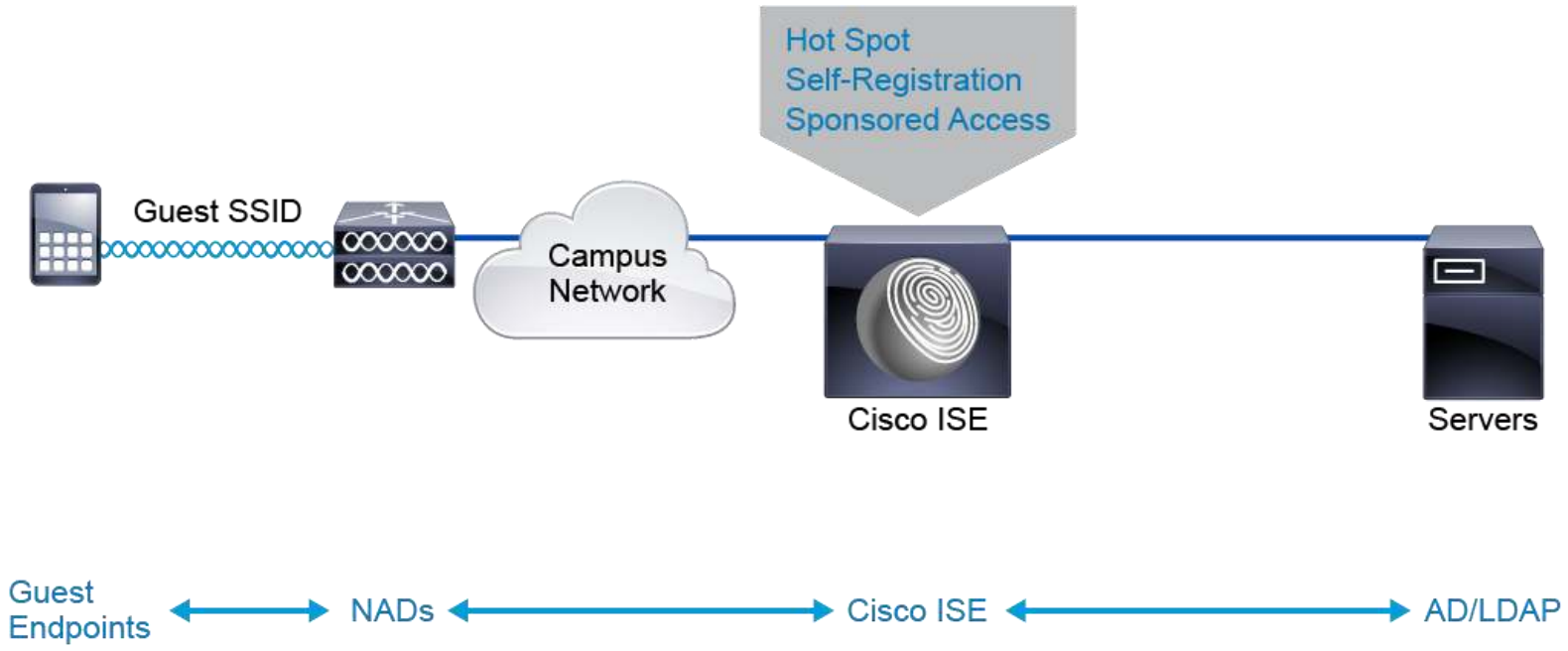
Cisco Identity Services Engine (cont.)

Cisco ISE Guest Management

- Cisco ISE provides a complete system for guest life-cycle management.
- Guest users can access the network for a limited time by using either the Sponsored Guest Portal, Self-Registered Guest Portal, or Hotspot Guest Portal.
- Administrators can customize the portals and policy based on the specific needs of the enterprise.

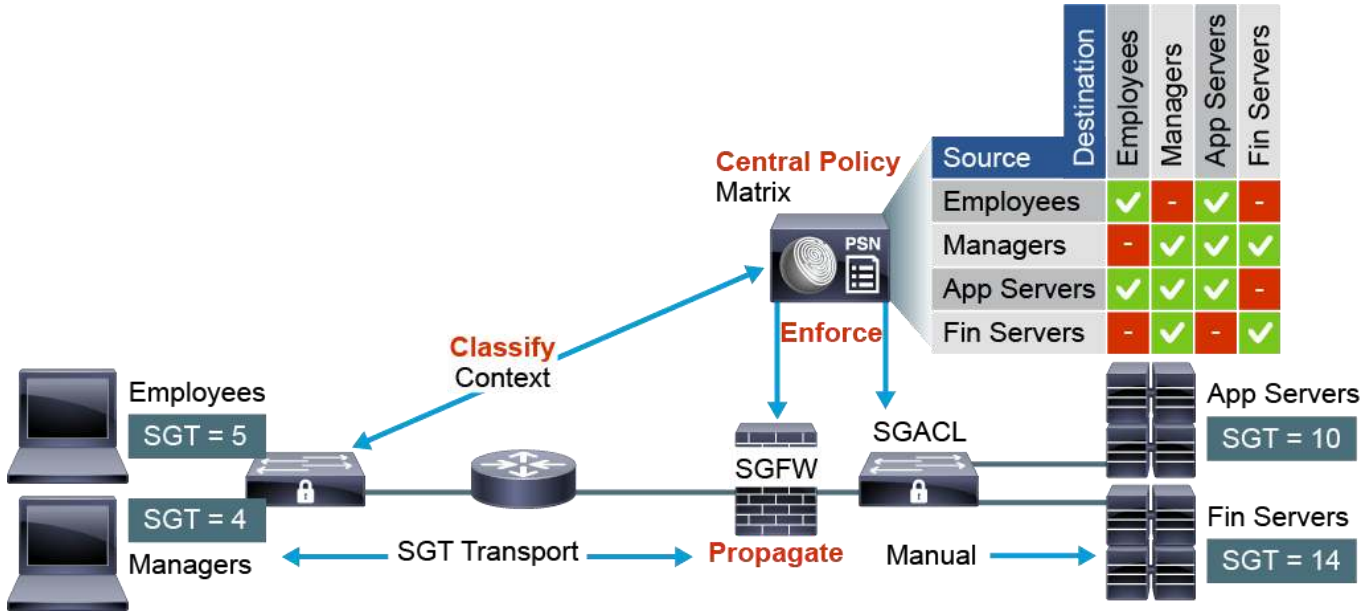
Cisco Identity Services Engine (cont.)

Cisco ISE Guest Management (cont.)



Cisco TrustSec

- Cisco TrustSec simplifies the provisioning and management of secure access to network services and applications.
- It defines policies using logical policy groupings, so secure access is consistently maintained even as resources are moved in mobile and virtualized networks.



Cisco TrustSec (cont.)

- Cisco TrustSec access control is implemented using ingress tagging and egress enforcement.
- At the ingress point to the Cisco TrustSec domain, traffic from the source is tagged with an Security Group Tag (SGT) containing the security group number of the source entity.
- At the egress point of the Cisco TrustSec domain, an egress device uses the source SGT and the security group number of the destination entity (the destination SG,or DGT) to determine which access policy to apply from the SGACL policy matrix.

Cisco TrustSec (cont.)

- The previous figure provides an example of using SGACL to control access:

1. Cisco ISE informs the NAD to assign an SGT of 5 for all packets from Employees and an SGT of 4 for all Managers.
2. Cisco ISE dynamically pushes these tags to the network access devices (NADs) via SGT transport.
3. The central policy indicates that Employees (SGT=5) may access Applications servers (SGT=10), but not financial servers (SGT=14), while Managers can access all servers.
4. To enforce this policy, Cisco ISE pushes SGACLs down to the switches and SGFW configuration to the firewalls.

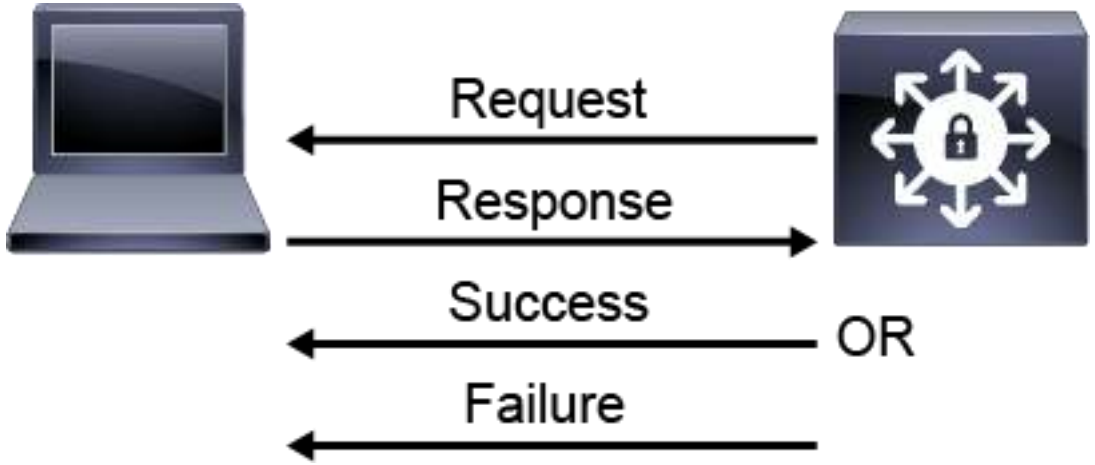
802.1X and EAP

- EAP is a flexible transport protocol used to carry arbitrary authentication information, and not the authentication method itself (EAP supports a wide selection of authentication methods).
- EAP is also media-independent, but typically runs over data link layers such as PPP, IEEE 802.3 wired, or 802.11 wireless media.
- There are four EAP packet types defined in RFC 3748 and listed by the number that is assigned to the code field of the EAP packet:

Code Field	EAP Packet Type
1	Request
2	Response
3	Success
4	Failure

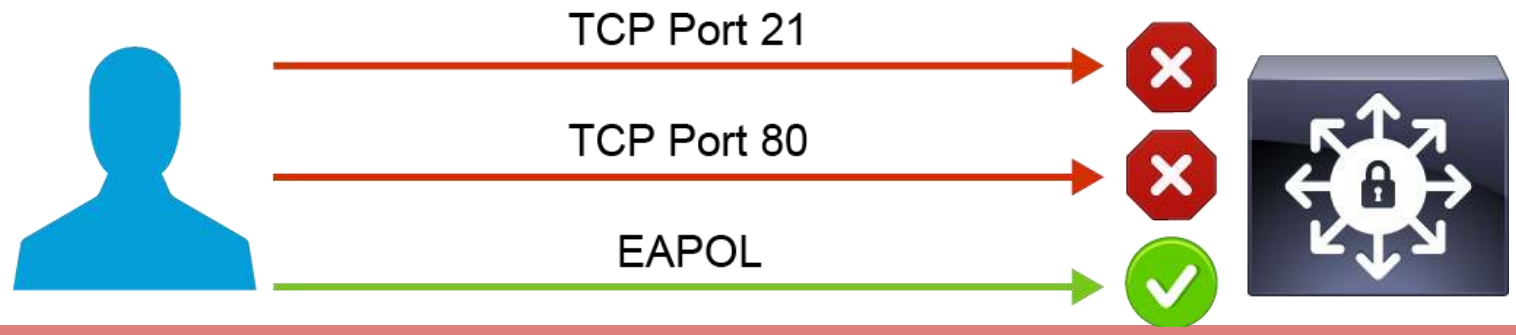
802.1X and EAP (cont.)

- It is important to understand that EAP itself is a specification for the *transport* of authentication and authorization mechanisms and not an authentication protocol.



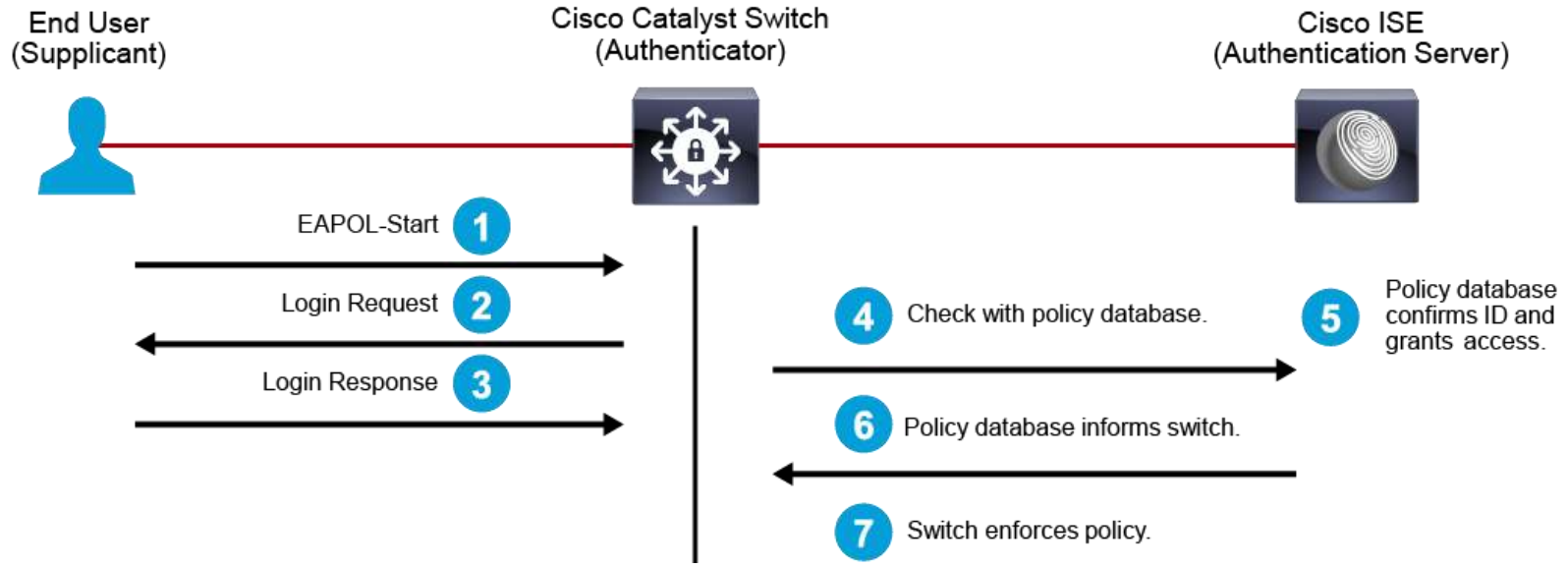
802.1X and EAP (cont.)

- 802.1X defines the encapsulation of EAP over IEEE 802, which is known as **EAPOL**.
- When a switch port is configured to require 802.1X authentication, it is called a controlled port.
- A controlled port, by default, does not allow any input on that port except for EAPOL.
- The supplicant can only access network services beyond the port after the supplicant authenticates.



802.1X and EAP (cont.)

- The role of the authenticator is to enforce policies that are provided by the authentication server, to serve as a translator between Layer 2 EAPOL messages from the supplicant, and to encapsulate EAP in Layer 3 RADIUS messages to the authentication server, **Cisco ISE** in this example.



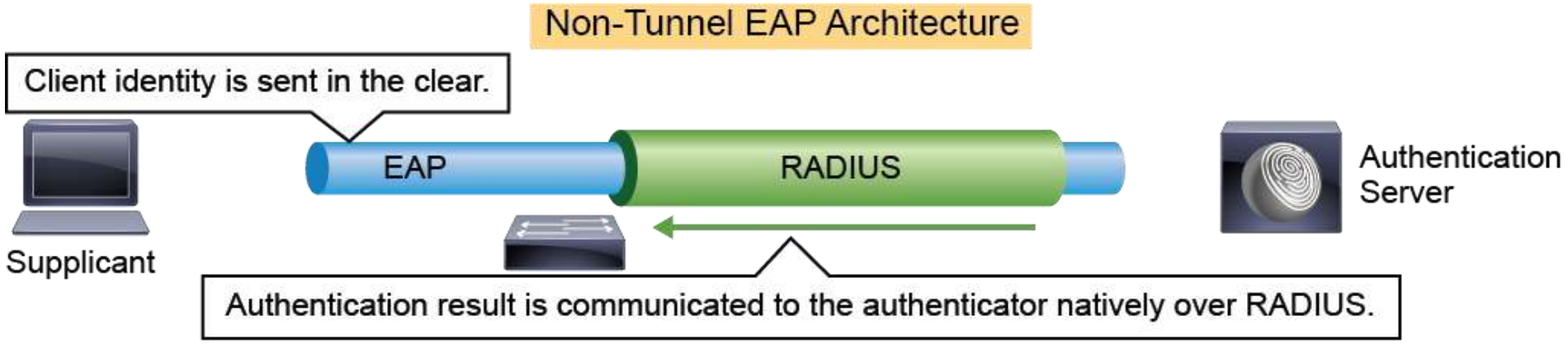
EAP Methods

- The authentication protocol that is used within EAP authentication and authorization mechanism is defined by the used EAP method.

- There are two types of EAP methods:
  1. Tunnel EAP
  2. Non-tunnel EAP.

EAP Methods (cont.)

- In the simple, Non-tunnel EAP architecture, a single EAP session exists between the supplicant and the authentication server.
- In this architecture, the supplicant sends its identity (name) in the clear to the authentication server.

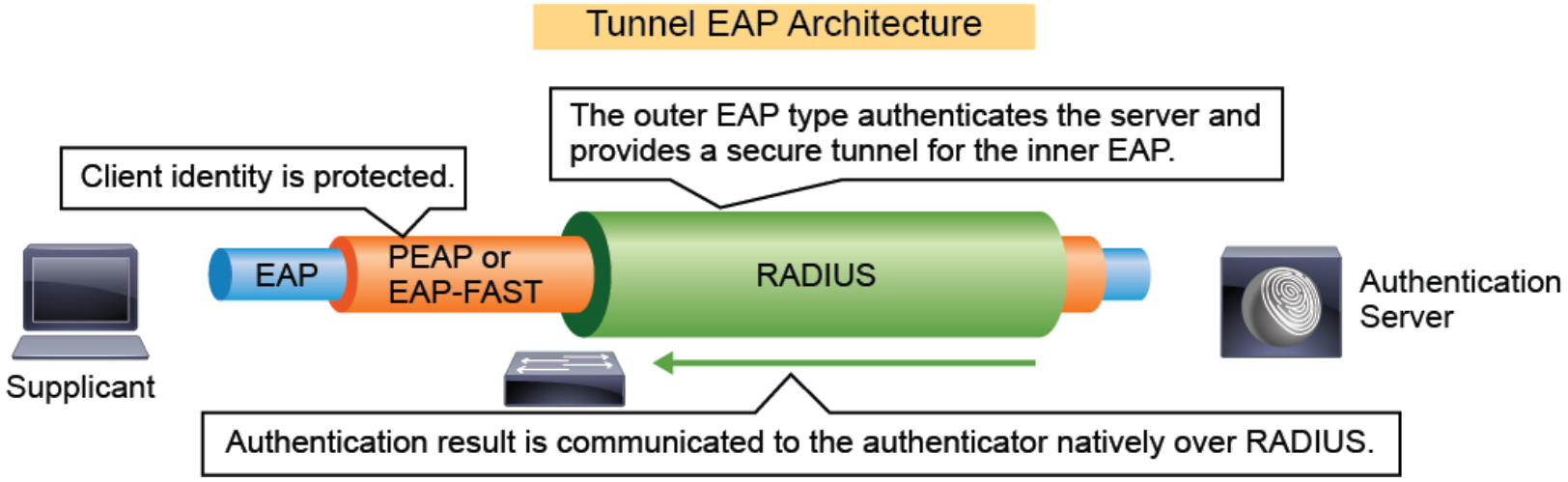


EAP Methods (cont.)

- This step is followed by an exchange that authenticates the authentication server to the user, and the user to the authentication server.
- If the user is successfully authenticated, the authentication server signals success to the authenticator via the RADIUS protocol.
- This mode is simple to understand, but has the limitation of transmitting the user identity (but not the credentials) in the clear.
- These EAP architectures cannot easily support one-time passwords, because these passwords do not support challenge-response methods that are typically used inside the EAP authentication exchange.

EAP Methods (cont.)

- To overcome these limitations, you can use a tunneled EAP architecture, in which an outer EAP encapsulates an inner EAP.
- The outer EAP provides server authentication, and a cryptographically secure tunnel for the inner EAP method to run in.



EAP Methods (cont.)

- Typical outer EAPs are Protected Extensible Authentication Protocol (PEAP),
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST).
- Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2 (EAP-MSCHAPv2),
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS),
- Extensible Authentication Protocol-Generic Token Card (EAP-GTC) are commonly used for the inner EAP.

EAP Methods (cont.)

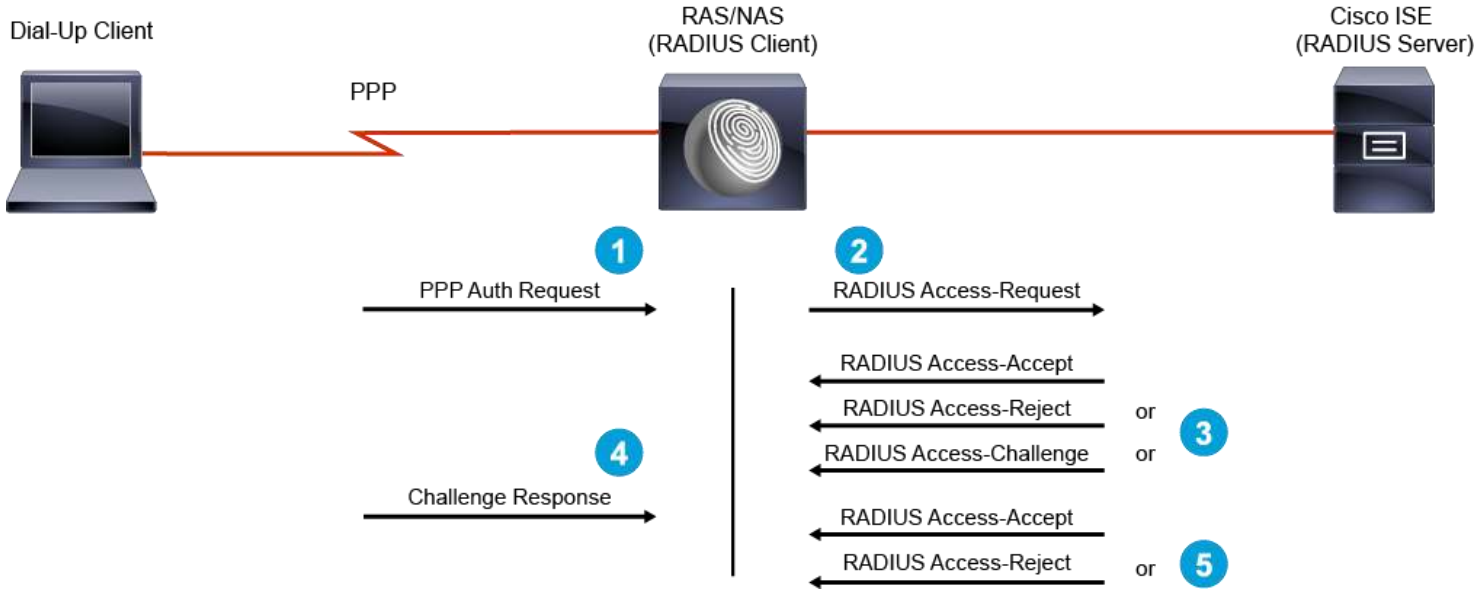
- **EAP-TLS** and **EAP-MSCHAPv2**, tunneled inside PEAP or EAP-FAST are the most widely used EAP methods to deploy secure network access.
- However, EAP functionality varies based on the EAP method selected and it is important to consider the capabilities of each EAP method when making a selection for a new implementation.
- For example, if there is a requirement to use digital certificates for client authentication, **EAP-TLS** is the only non-tunnel method that satisfies the requirement.

Describing 802.1X Authentication

- RADIUS Initially developed in 1991 by Livingston to provide authentication, authorization, and accounting (AAA) services for its line of remote access servers (RASs), RADIUS has been extended and expanded to service the AAA needs of a wide variety of devices and requirements.

Describing 802.1X Authentication (cont.)

- RADIUS defines four packet types that are used to authenticate and authorize user communications.
- In the context of 802.1X, these four packet types are used to carry EAP messages.

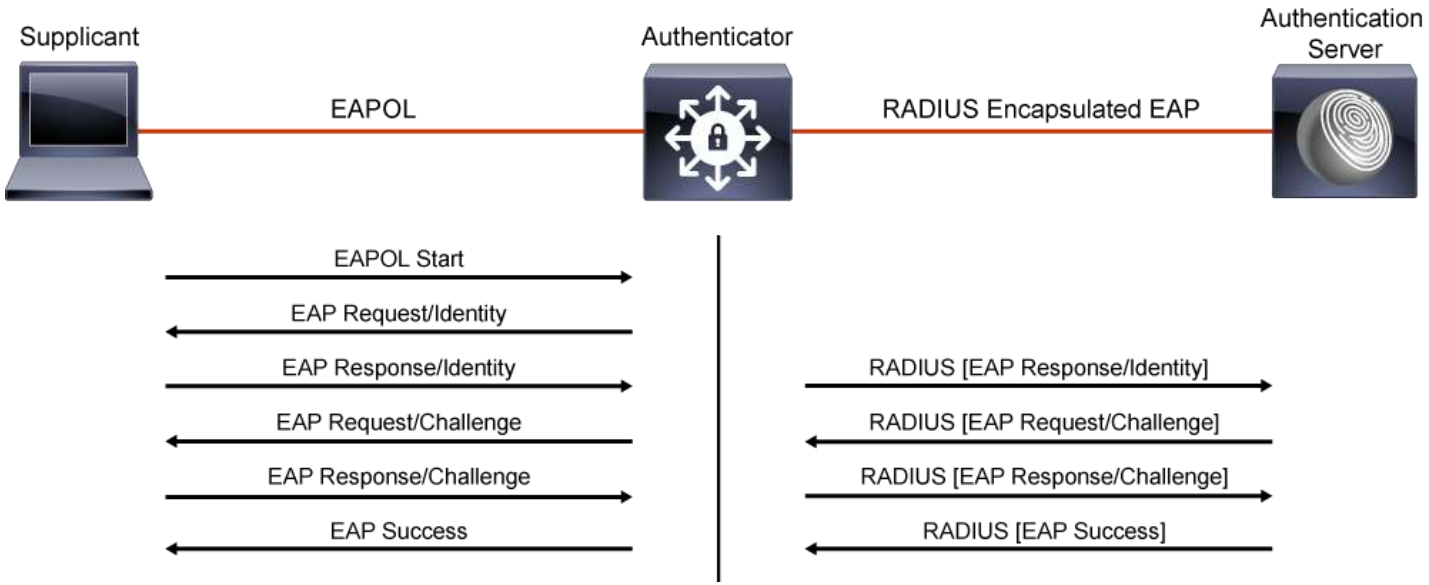


Describing 802.1X Authentication (cont.)

RADIUS Packet Types	Description
Access-Request	Every RADIUS session must begin with an Access-Request. The request usually includes a username, but must include information about the network access server (NAS) and some form of password. This packet type is always sent to the RADIUS server.
Access-Accept	This packet type is used to convey the configuration information to the NAS to provision services for the user. In the context of 802.1X, this could include a DACL, or VLAN assignment. This packet type is always sent from the RADIUS server.
Access-Reject	If any attribute received by the RADIUS server is not acceptable, an Access-Reject packet must be sent to the NAS. This packet type is always sent from the RADIUS server.
Access-Challenge	Upon receipt of an Access-Request, the RADIUS server may issue a challenge to the user. In an EAP-MD5 exchange, the RADIUS server will use this packet type to send the challenge string to the user. The proper response to an Access-Challenge packet is an Access-Request packet with the answer to the challenge. This packet type is always sent from the RADIUS server.

Describing 802.1X Authentication (cont.)

- In the context of 802.1X, RADIUS is used as a transport mechanism for EAP messages, sourced from 802.1X supplicant and sent to authentication server.
- Note that EAP messages are transported inside RADIUS only between an authentication and authentication server.



Describing 802.1X Authentication (cont.)

- EAP messages from the supplicant to the authenticator are exchanged as Layer 2 EAPOL packets.
- Because the authentication server speaks the RADIUS protocol and is likely Layer 3 adjacent to the authenticator, the authenticator encapsulates EAP messages in RADIUS.
- The authenticator acts as a translating transit point for EAP and RADIUS.
- Any EAP methods that are used by the client must be also be configured in the RADIUS authentication server.

Describing 802.1X Authentication (cont.)

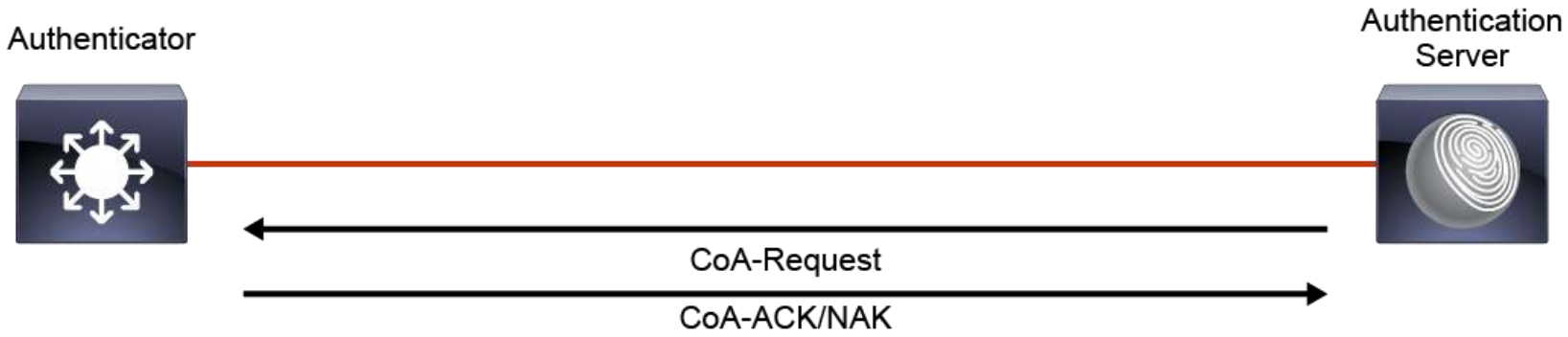
- The authentication can be initiated by **the supplicant** or **the authenticator**.
- The authenticator initiates authentication when the link state changes from down to up, or periodically as long as the port remains up and unauthenticated.
- The authenticator sends an EAP request or identity frame to the client to request its identity.
- Upon receipt of the frame, the supplicant responds with an EAP response or identity frame.
- However, if during bootup, the supplicant does not receive an EAP request or identity frame from the authenticator, the supplicant can initiate authentication by sending an EAPOL start frame, which prompts the authenticator to request the identity of the client.

Describing 802.1X Authentication (cont.)

- When the supplicant provides its identity, the authenticator begins its role as the intermediary and passes EAP frames between the supplicant and the authentication server until authentication succeeds or fails.
- If the authentication succeeds, the authenticator port is authorized.

RADIUS Change of Authorization

- The RADIUS CoA feature provides a mechanism to change the attributes of a AAA session after it is authenticated.
- When a policy changes for a user or user group on a AAA server, such as Cisco ISE, the server can send unsolicited RADIUS CoA request to reinitialize authentication and apply the new policy.

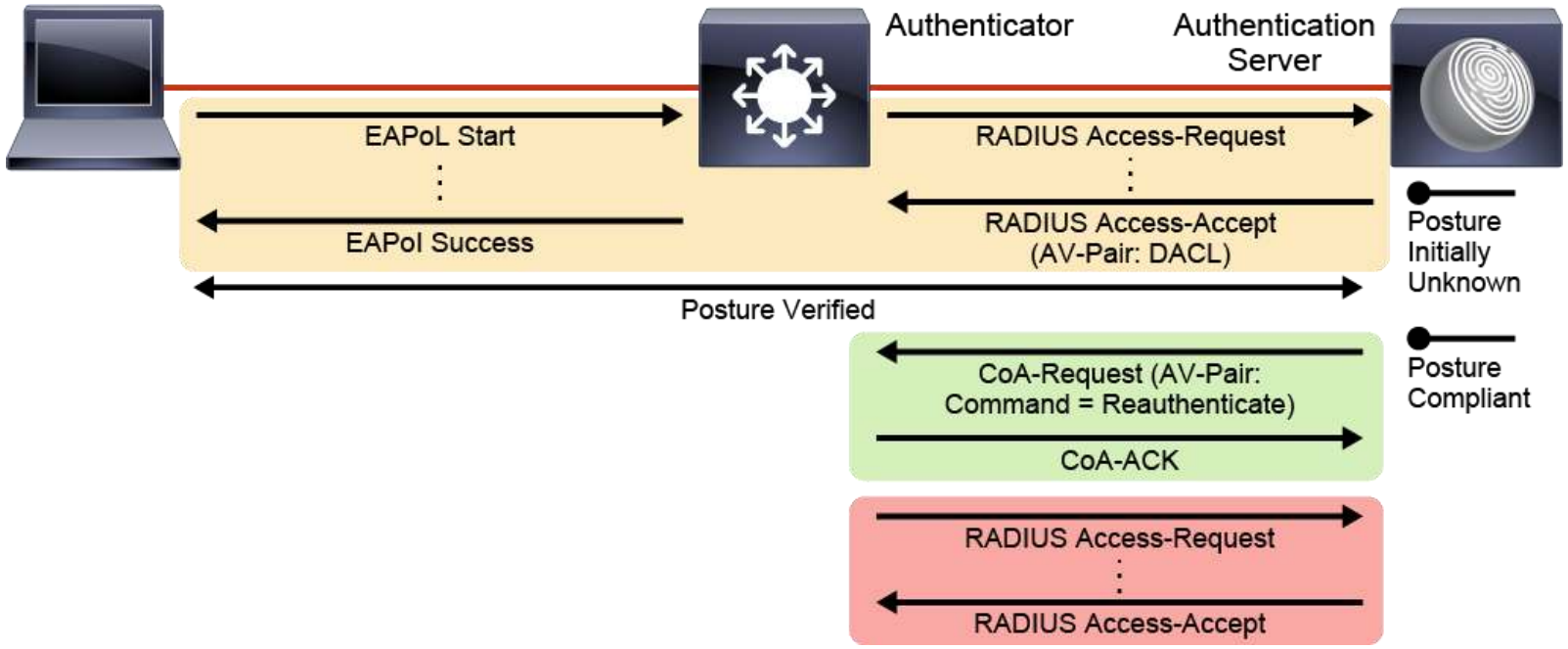


RADIUS Change of Authorization

- Cisco ISE server heavily relies on RADIUS CoA. Without support for CoA on ISE and Cisco IOS and IOS XE devices, and Cisco WLCs, the following services would not be available:
  - **Central web authentication:** CoA is used to change authorization session of a user after the user authenticates via a captive guest portal.
  - **Client posturing:** CoA is used to change authorization session of a user after Cisco ISE determines posture status of the client.
  - **Client profiling:** CoA is used to change authorization session of a device after Cisco ISE determines profile and classification of the device.
  - **Rapid threat containment:** CoA is used to change authorization session of a user if another Cisco devices, such as Cisco Stealthwatch, or Cisco FirePower Next-Generation Firewall, detects malicious event involving the user.

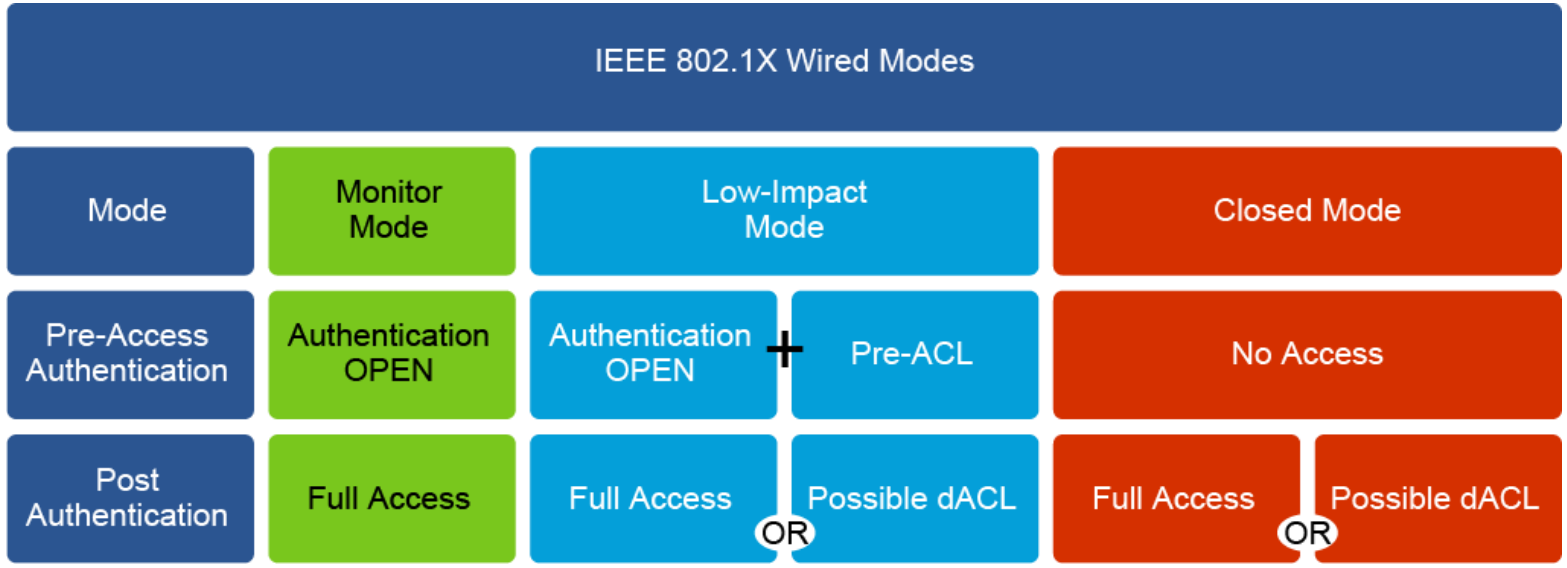
RADIUS Change of Authorization

- The following figure displays a sample flow of RADIUS CoA for the purposes of client posturing with Cisco ISE.



Cisco Catalyst Switch 802.1X Configuration

- You can use a phased approach when deploying 802.1X.
- This phased approach helps you to determine the potential impact to devices, adjust policy enforcement over time, and ensure a smooth transition to identity-based policy services.



Cisco Catalyst Switch 802.1X Configuration (cont.)

You can use these 802.1X deployment modes:

- **Monitor (open) mode:** Allows you to enable authentication across the wired infrastructure, without affecting wired users or devices. administrators use the monitor mode to help ensure that all devices are authenticating correctly, either with 802.1X or MAB. If a device is misconfigured or is missing an 802.1X supplicant, access will be allowed and logged. However, if authentication succeeds, authorization (for example, Dynamic VLAN, Downloadable access control list (DACL)) can still be applied.

- **Low-impact mode:** It allows selective transition from an open (nonfiltering) preauthorization method to selective preauthorization. This function is provided by static port ACLs (Pre-ACL as shown in the previous figure) that allow necessary services such as Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) while blocking all other network access. Users connected to controlled ports will receive additional access (based on policy) after successful authentication, based on DACL that will override the static ACL on the port.

- **High-security (closed) mode:** It provides the highest level of controls by configuring the closed pre-authorization port control. No traffic will be permitted on a port except EAPOL before authentication and authorization.

Cisco Catalyst Switch 802.1X Configuration (cont.)

802.1X Fallback Options

- IEEE 802.1X supplicant support on user's devices, there are always some devices that either do not have the supplicant installed or supported.
- Such non-supplicant devices can come in the form of wired or wireless devices, such as laptops, printers, IP cameras, tablets, and other mobile devices.

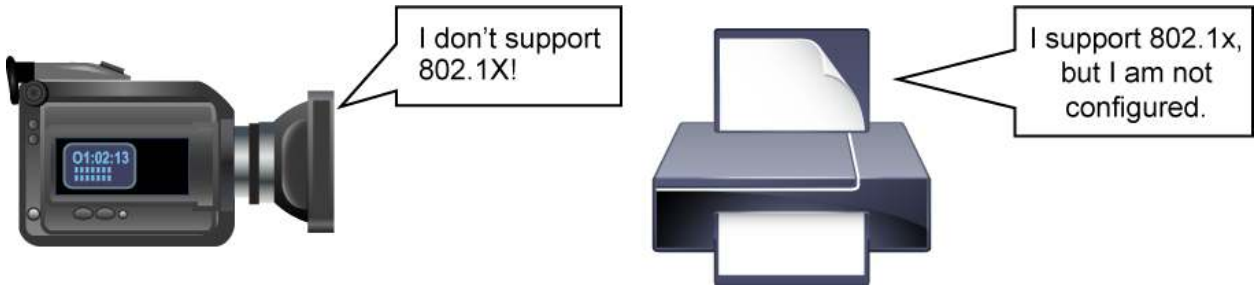
Cisco Catalyst Switch 802.1X Configuration (cont.)

802.1X Fallback Options (cont.)

- In that case, you need to configure some kind of a fallback mechanism in an 802.1X enabled network that will allow connectivity from such devices to the network.
- Here are the available mechanisms:
  - MAB (MAC Authentication Bypass)
  - Guest VLAN
  - Restricted VLAN (Authentication fail VLAN)
  - Central Web Authentication (CWA) with Cisco ISE

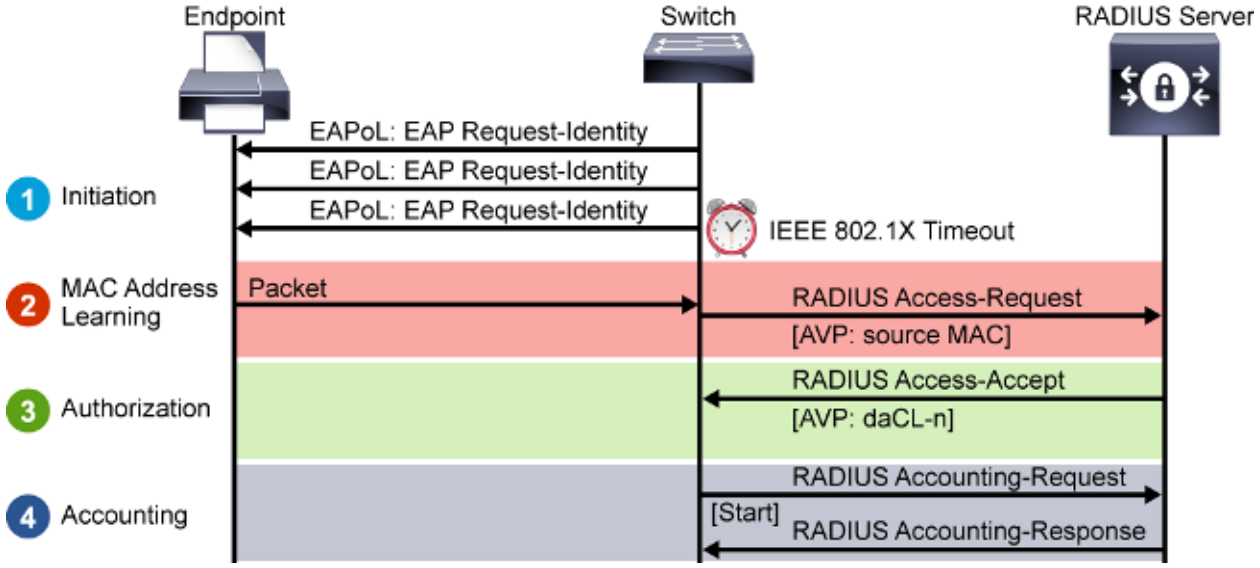
Cisco Catalyst Switch 802.1X Configuration (cont.)

- **MAC Authentication Bypass**
  - This authentication is the most basic form of authentication in deployments because many devices either do not, or cannot, support 802.1X.
  - Because MAC addresses are easily spoofed, they are a relatively weak form of authentication, but they are a good first step for device identification.
  - It is very common to use MAB as an 802.1X fallback mechanism to authenticate simple devices, such as printer, IP cameras, or physical access control mechanisms, such as card readers.



Cisco Catalyst Switch 802.1X Configuration (cont.)

- The figure illustrates a high-level functional sequence, when MAB is configured as a fallback mechanism to 802.1X.
- If 802.1X is not enabled, the sequence is the same except that MAB starts immediately after link-up, instead of waiting for IEEE 802.1X to time out.

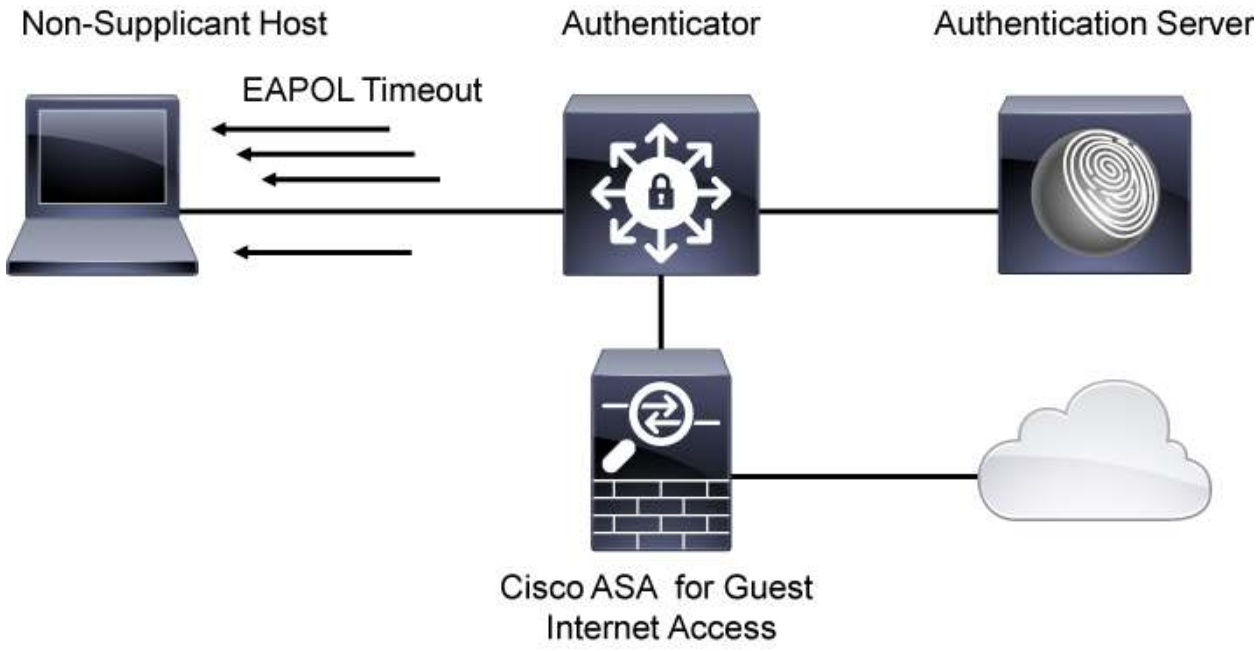


Cisco Catalyst Switch 802.1X Configuration (cont.)

- **Guest VLAN**
  - The guest VLAN feature is designed to support non-supplicant hosts that are attempting to access a wired switch port that is configured for the 802.1X port control.
  - After three EAP retries, the switch dynamically places that port on a guest VLAN that is configured on the switchport.
  - Guest VLAN is compatible with MAB.
  - If MAB is configured and MAB fails after 802.1X failure, the port can be moved to the guest VLAN.
  - The guest VLAN traffic is typically restricted by using an ACL on the termination point of the VLAN, for example, to allow access only to the Internet.

Cisco Catalyst Switch 802.1X Configuration (cont.)

- The example that is shown in the figure allows secure guest access to the internet through a Cisco Adaptive Security Appliance (ASA) firewall.

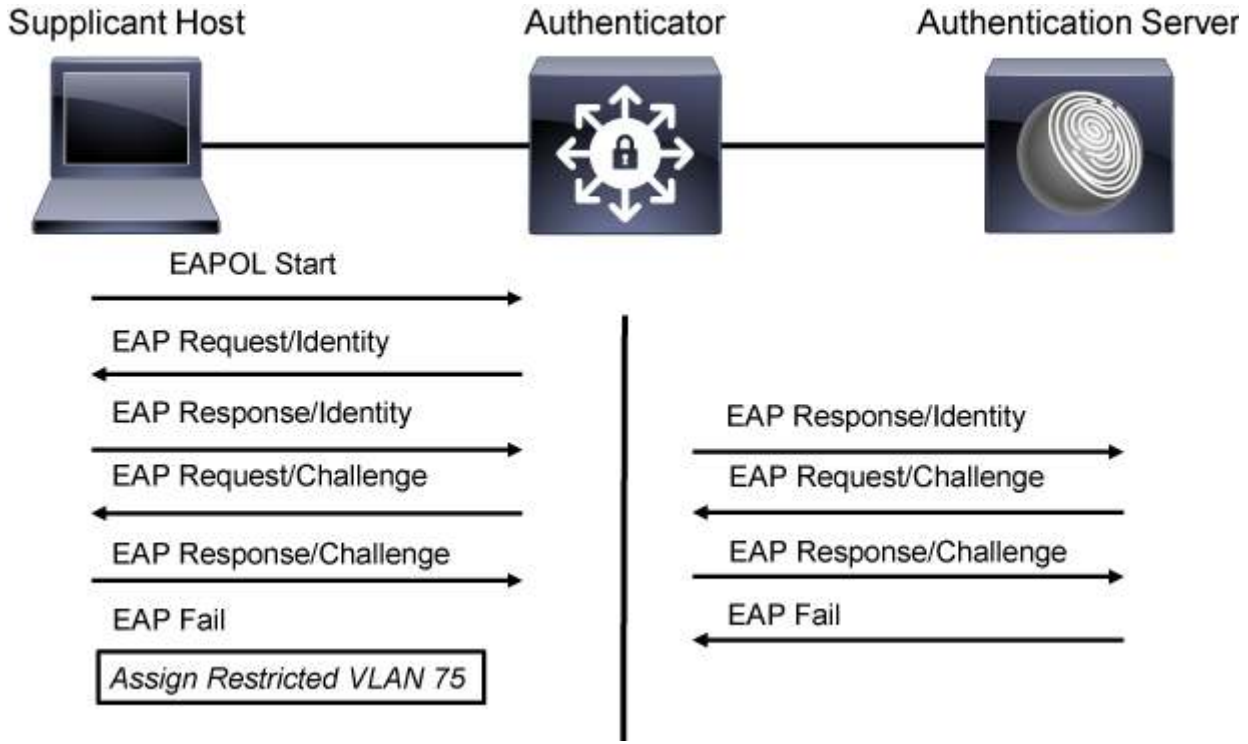


Cisco Catalyst Switch 802.1X Configuration (cont.)

- **Restricted VLAN**
  - Sometimes, a guest user will connect to the network of your organization with a host with 802.1X supplicant software.
  - When the host plugs in to the switch port, the supplicant will initiate an EAPOL connection with the switch.
  - However, because the user lacks local authentication credentials, authentication will fail.
  - By configuring a restricted VLAN, the user can be dynamically assigned to a VLAN for restricted access.

Cisco Catalyst Switch 802.1X Configuration (cont.)

- After 802.1X authentication failure, the switch can be configured either to deploy restricted VLAN or proceed to the next authentication method, which is usually MAB.



Cisco Catalyst Switch 802.1X Configuration (cont.)

802.1X Host Modes

- The host mode of the 802.1X port determines whether more than one client can be authenticated on the port and how authentication will be enforced.
- You can configure an 802.1X port to use any of four host modes.
- In addition, each mode may be modified to allow preauthentication open access.

Cisco Catalyst Switch 802.1X Configuration (cont.)

1- Single host mode:

- In the single host mode, only one client can be connected to the 802.1X-enabled port.
- When the port state changes to "up," the switch detects the client and sends an EAPOL frame.
- Client access is granted after authentication.
- Packets from other hosts are dropped.
- If the client leaves, or is replaced with another client, the switch changes the port link state to "down."
- The port is then returned to the unauthorized state.

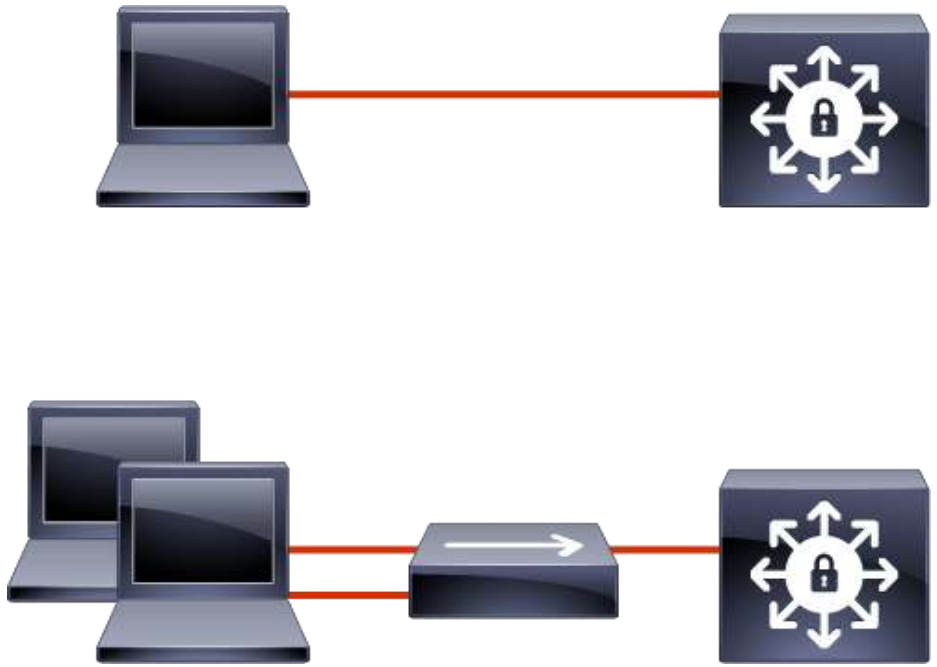
Cisco Catalyst Switch 802.1X Configuration (cont.)

2- Multiple host mode:

- In the multiple host mode (often called multi-host mode), you can attach multiple hosts to a single 802.1X-enabled port.
- In this mode, only the first client that attaches clients must be authorized.
- All subsequent clients are granted network access based on this authentication.
- If the port becomes unauthorized (reauthentication fails or an EAPOL logoff message is received), the authenticator denies network access to all attached clients.

Cisco Catalyst Switch 802.1X Configuration (cont.)

Single host mode and Multiple host mode



Cisco Catalyst Switch 802.1X Configuration (cont.)

3- Multiple Domain Authentication Mode:

- Multidomain Authentication (MDA) mode allows an IP phone, and a single host behind the IP phone, to authenticate independently via 802.1X, MAB, or (for the host only) web-based authentication.
- In this application, multidomain refers to two domains (data and voice VLAN).
- Only one MAC address is allowed per domain.
- The switch can place the host in the data VLAN and the IP phone in the voice VLAN, but they appear on the same switch port.
- The data and voice VLAN assignment can be obtained dynamically from the authentication, authorization, and accounting (AAA) server such as Cisco ISE.

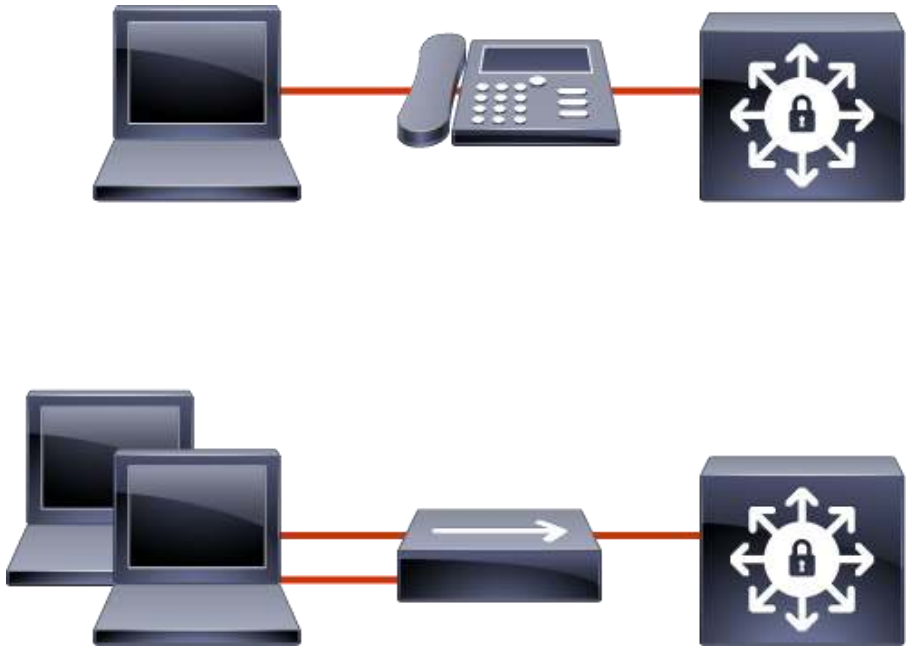
Cisco Catalyst Switch 802.1X Configuration (cont.)

4- Multiple Authentication Mode:

- Multiple Authentication mode (often called multi-auth mode) allows one 802.1X or MAB client on the voice VLAN.
- It also allows multiple authenticated 802.1X, MAB, or web authorization clients on the data VLAN.
- When a hub or access point is connected to an 802.1X port, multi-auth mode provides enhanced security over the multi-hosts mode by requiring authentication of each connected client.
- For non-802.1X devices, MAB, or web-based authentication, can be used as the fallback method for individual host authentications, which allows different hosts to be authenticated through different methods on a single port.

Cisco Catalyst Switch 802.1X Configuration (cont.)

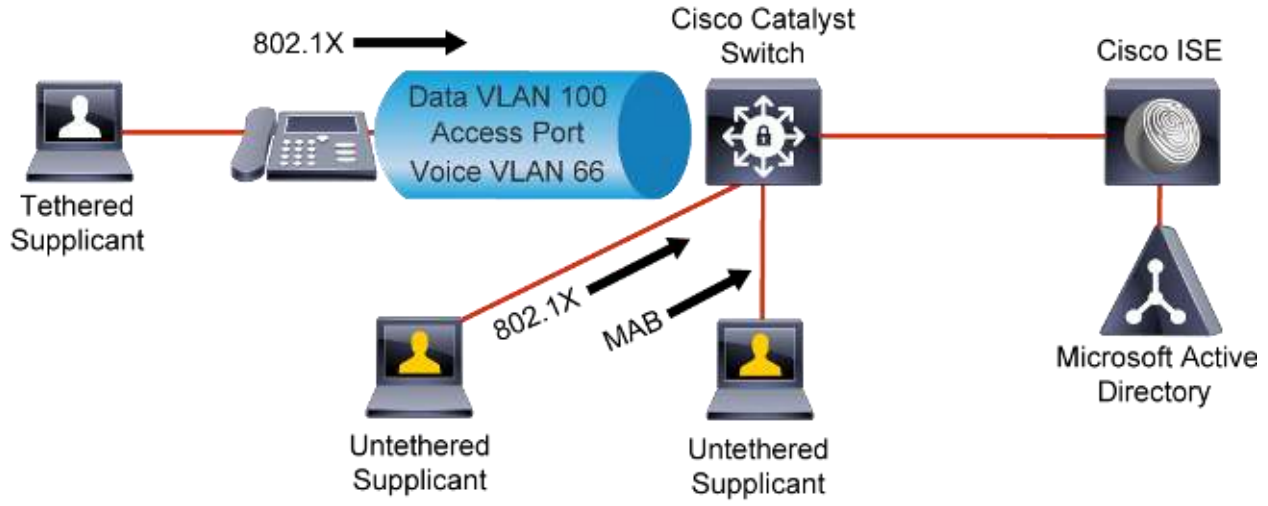
Multiple Domain Authentication Mode and Multiple Authentication Mode



Cisco Catalyst Switch 802.1X Configuration (cont.)

802.1X Flexible Authentication

- Flexible authentication provides a flexible timeout and fallback mechanism among 802.1X, MAB, and local web authentication methods.



Cisco Catalyst Switch 802.1X Configuration (cont.)

- On switch ports that are configured for 802.1X port control, Flexible Authentication, or FlexAuth, sets the order of methods that the switch attempts when trying to authenticate a new device that is connected to a port.
- If one method in the list is unsuccessful, the next method is attempted.
- This simplifies the identity configuration by providing a single set of configuration commands to manage different types of endpoints connecting to the switch ports.
- In addition, FlexAuth sequencing allows you to configure any authentication method on a standalone basis.
- In other words, MAB can be configured without requiring 802.1X configuration.

Cisco Catalyst Switch 802.1X Configuration (cont.)

- **By default**, the Cisco Catalyst switch will first perform 802.1X authentication.
- If it fails, and the switch is configured to proceed with the next method, such as MAB, the switch will then perform MAB.
- In environments where the majority of hosts authenticate using MAB, you may want a switch to perform MAB first and 802.1X second.
- This will prevent hosts being delayed when accessing the network and waiting for 802.1X to timeout.

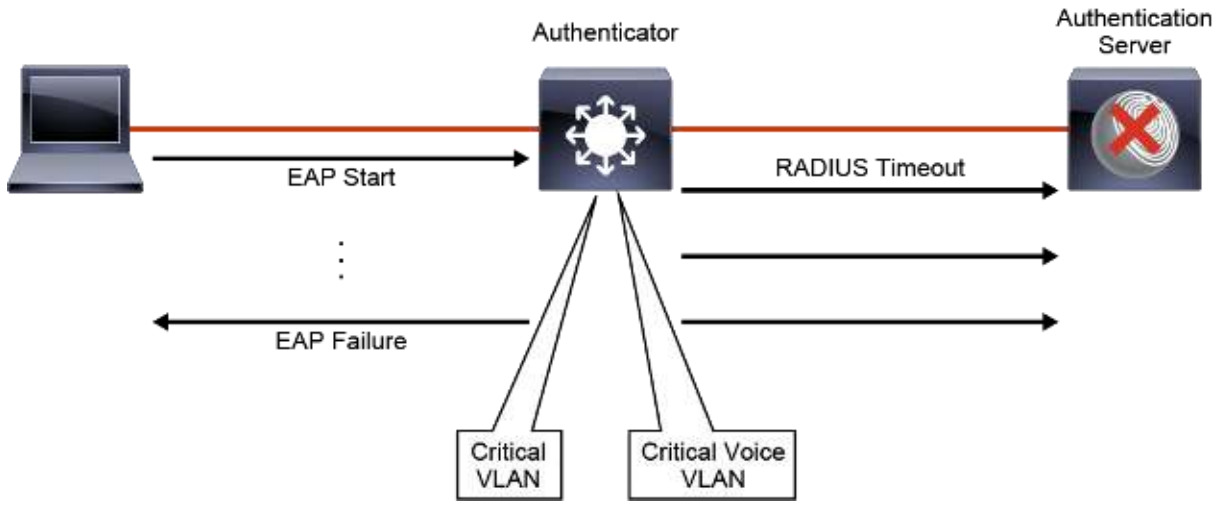
Cisco Catalyst Switch 802.1X Configuration (cont.)

- When the authentication order is set to initiate MAB first, the endpoint directory on the authentication server will be queried.
- If the host has an 802.1X supplicant, the supplicant will also initiate 802.1X authentication from its side.
- As a result, it may happen that both MAB and 802.1X authentication will succeed.
- In such case, you need to configure **FlexAuth priority** for 802.1X authentication to have priority over MAB.
- In such case, if the supplicant on the port begins an EAPOL session, MAB will be interrupted and normal authentication will proceed.

Cisco Catalyst Switch 802.1X Configuration (cont.)

Inaccessible Authentication Bypass

- When deploying 802.1X it is also recommended to deploy the inaccessible authentication bypass feature, also referred to as critical authentication or the AAA fail policy.
- If the feature is configured, when a new host tries to connect to the port and RADIUS server (ISE) is not reachable, that host is moved to a user-specified access VLAN, the critical VLAN.



Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure 802.1X on a Cisco Catalyst Switch

1. To configure 802.1X on a Cisco Catalyst switch you need to first configure global AAA settings, These settings include enabling AAA new-model and configure AAA lists for 802.1X.
2. Next, you need to configure global RADIUS settings, which include configuration of individual RADIUS servers (ISE), RADIUS server group, RADIUS attributes, and RADIUS Change of Authorization (CoA), The RADIUS CoA feature provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated, When there is a policy change for a user or user group in AAA, RADIUS CoA packets can be sent from the AAA server such as ISE to reinitialize the authentication and apply the new policy.

Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure 802.1X on a Cisco Catalyst Switch (cont.)

3. Then, enable the IP device tracking functionality. The purpose of IP device tracking is for the switch to obtain and maintain a list of devices that are connected to the switch via an IP address. This functionality is critical whenever DACLs are used with 802.1X in order to replace the "any" keyword as the source in the ACL with the IP address of the device connected to the switch.
4. Now you need to enable 802.1X authentication globally.
5. Finally, you enable 802.1X functionality and related features on every interface you would like to enable for secure network access. These settings include enabling 802.1X and MAB, configuring order of 802.1X and MAB using Flexible Authentication, tuning of 802.1X timers, setting deployment mode, setting host mode, enabling reauthentication, configuring guest and restricted VLAN, and enabling Inaccessible Authentication Bypass (IAB) or critical data VLAN and critical voice VLAN. Some of these settings are discussed below.

Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure Global AAA Settings

- Enter configuration mode and enable AAA and 802.1X:

```
aaa new-model
```

- Configure AAA for 802.1X:

```
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
```

Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure Global RADIUS Settings

- Configure the RADIUS server with a shared secret and automated test user:

```
radius server ISE
address ipv4 192.168.43.200 auth-port 1812 acct-port 1813
key cisco
```

Cisco Catalyst Switch 802.1X Configuration (cont.)

- Configure the RADIUS server group:

```
aaa group server radius ISE
server name ISE
```

- Configure RADIUS CoA:

```
aaa server radius dynamic-author
client 192.168.43.200 server-key cisco
```

Cisco Catalyst Switch 802.1X Configuration (cont.)

- Configure support to send RADIUS vendor-specific attributes (VSAs):

  radius-server vsa send authentication

  radius-server vsa send accounting

Cisco Catalyst Switch 802.1X Configuration (cont.)

- Enable IP device tracking:

```
ip device tracking
```

Cisco Catalyst Switch 802.1X Configuration (cont.)

- Enable 802.1X globally:

```
dot1x system-auth-control
```

Cisco Catalyst Switch 802.1X Configuration (cont.)

- Optionally, create an access list to define permitted traffic before the port is authenticated (used for low-impact mode):

```
ip access-list extended PRE-AUTH
  remark DHCP
  permit udp any eq bootpc any eq bootps
  remark DNS
  permit udp any any eq domain
  remark Ping
  permit icmp any any echo
  remark PXE / TFTP
  permit udp any any eq tftp
  remark Drop and log the rest
  deny ip any any log
```

Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure Interface Specific Settings

- Once you are done configuring global settings, you need to apply interface-specific 802.1X commands on all interfaces that will run the 802.1X authentication.
- The example shows how to configure a switch port for basic operations, which is required before you can apply an 802.1X configuration:
    1. First, enter the interface configuration mode.
    2. Set the port mode to access.
    3. Configure the access VLAN.
    4. Bind the preauthentication port ACL to the interface.
    5. Enable PortFast.

Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure Interface Specific Settings (cont.)

```
interface GigabitEthernet1/0/1
 description PC
 switchport mode access
 spanning-tree portfast
 ip access-group PRE-AUTH in
```

Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure Interface Specific Settings (cont.)

- The next example shows the minimum commands that are necessary to configure 802.1X on an interface:

1. Optionally, allow hosts to access the network before the port is authorized (low-impact mode)
2. Enable 802.1X support on the interface.
3. Enable periodic reauthentication of the supplicant.
4. Configure the reauthentication timeout.

Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure Interface Specific Settings (cont.)

```
interface GigabitEthernet1/0/1
 authentication open
 authentication port-control auto
 authentication periodic
```

Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure Interface Specific Settings (cont.)

- Generally, it is recommend to set the FlexAuth order to 802.1X authentication first and MAB second. The same applies for the priority.
- The next example shows how to configure support for an IP phone:
  1. Configure a voice VLAN.
  2. Configure MDA.
  3. Configure FlexAuth authentication order.
  4. Configure FlexAuth authentication priority.
  5. Enable MAB on the interface.

Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure Interface Specific Settings (cont.)

```
interface GigabitEthernet1/0/1
 description IP Phone + PC
 switchport voice vlan 40
 authentication open
 authentication host-mode multi-domain
 mab
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication event fail action next-method
```

Cisco Catalyst Switch 802.1X Configuration (cont.)

Configure Interface Specific Settings (cont.)

- The next example shows how to enable inaccessible authentication bypass (critical data VLAN and critical voice VLAN):
  1. Configure critical VLAN for data
  2. Configure critical voice VLAN
  3. Reinitialize port when AAA server comes back up

Cisco ISE 802.1X Configuration

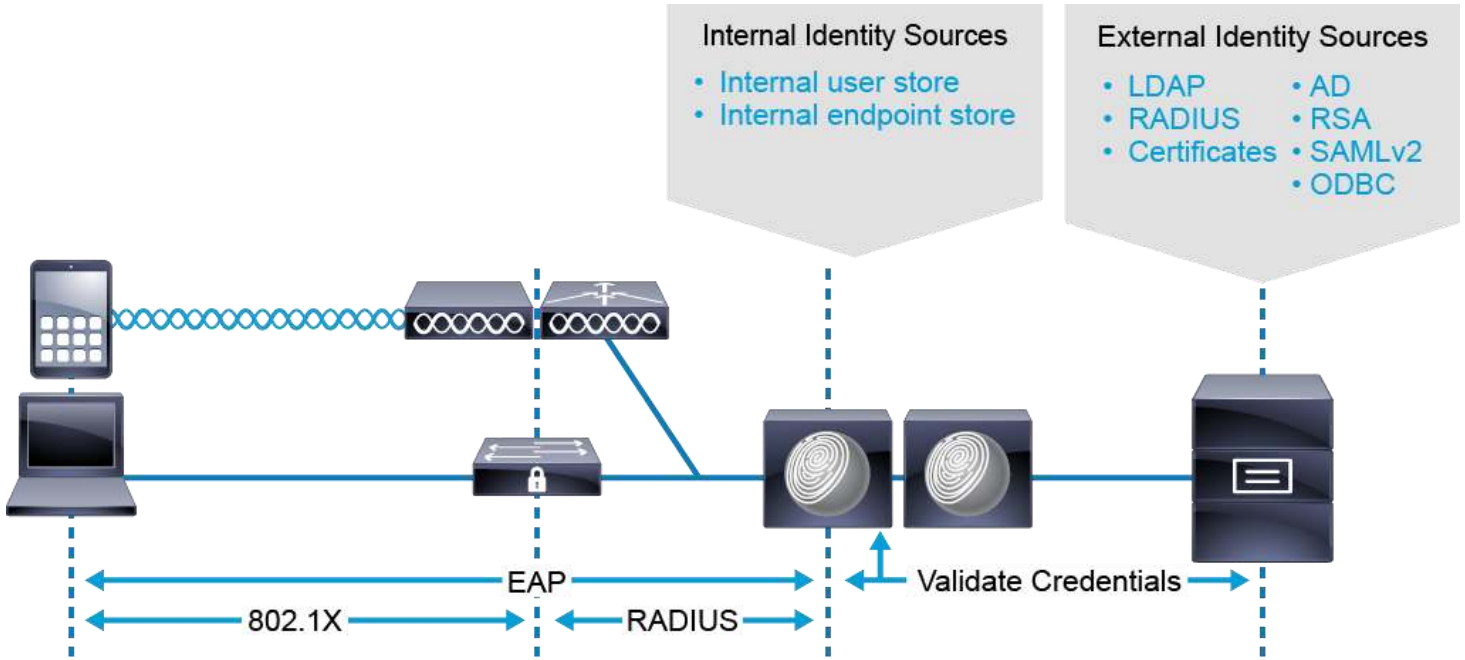
Cisco ISE configuration for 802.1X consists of the following overall tasks:

1. Configure identity sources, that are used to verify clients identity. This include configuration of local user and device accounts, and integrations with external identity sources, such as Microsoft Active Directory, or general Lightweight Directory Access Protocol (LDAP) server.
2. Configure network devices, which act as RADIUS clients. The settings include device name, IP address, and RADIUS settings.
3. Review authentication policy. Generally, no changes are needed in Cisco ISE default authentication policy.
4. Configure authorization policy. Authorization policy on Cisco ISE usually needs to be customized based on your requirements.

Cisco ISE 802.1X Configuration (cont.)

1. Configure Cisco ISE Identity Sources

- Cisco ISE relies on various identity sources to validate the user credentials and to check group information and other user or endpoint attributes.



Cisco ISE 802.1X Configuration (cont.)

- **Cisco ISE supports internal and external identity sources.**
- The internal identity source support the following entities:

  - **User:** User identity information can include a username, password, e-mail address, account description, associated administrative group, user group, and role.

  - **Endpoint:** Endpoint identity information is stored for wired, wireless, or VPN-connected devices. The endpoint identity store typically represents an endpoint by its MAC address. Stored endpoint attributes may also include various other attributes, such as platform and OS version.

Cisco ISE 802.1X Configuration (cont.)

- Cisco ISE supports the following external identity sources:

  - **LDAP:** LDAP is a standards-based networking protocol that is used to query and modify directory services. LDAP can be used to retrieve user identity from Active Directory servers, Sun Directory servers, and the Novell eDirectory.

  - **Active Directory (Multi-Active Directory):** Cisco ISE uses Microsoft Active Directory (AD) to access information about users, machines, groups, and attributes. Cisco ISE supports Multi-Active Directory: multiple joins to Active Directory domains, without need for specific trusts between them. Cisco ISE supports up to 50 Active Directory joins.

  - **RADIUS:** A RADIUS identity source is an external collection of subjects and their credentials and uses the RADIUS protocol for communication. Cisco ISE supports any RADIUS RFC 2865-compliant server.

Cisco ISE 802.1X Configuration (cont.)

- Cisco ISE supports the following external identity sources (cont.)

  - **RSA:** RSA SecurID is a two-factor authentication external authentication server, which provides a unique dynamic authentication code for user authentication.

  - **SAML:** Supports Security Assertion Markup Language Version 2.0 (SAMLv2), which enables the exchange of security authentication information between an Identity Provider (IdP) and a service provider (Cisco ISE).

  - **Certificate Authentication Profile:** Some authentication methods use certificates in addition to, or instead of, password or one-time password (OTP)-based authentication. For example, if you want to use the EAP-TLS certificate-based authentication method, it is necessary to create a certificate authentication profile.

Cisco ISE 802.1X Configuration (cont.)

- Cisco ISE supports the following external identity sources (cont.)
  - **ODBC:** As of Cisco ISE v2.2, you can use an Open Database Connectivity (ODBC)-compliant database as an external identity source to authenticate users and endpoints. ODBC identity sources can be used in an identity store sequence and for guest and sponsor authentications, as well as for Bring Your Own Device (BYOD) flow. The following database engines are supported:
    - MySQL
    - Oracle
    - PostgreSQL
    - Microsoft SQL Server
    - Sybase
  - **Social Login**: as of Cisco ISE v2.3 you can use social login, such as Facebook ,as an exernal identity source for guest users.

Cisco ISE 802.1X Configuration (Lab)

Lab1: Configure Cisco ISE 802.1x Internal Authentication and MAB

Lab2: Configure Cisco ISE 802.1x External Authentication with AD