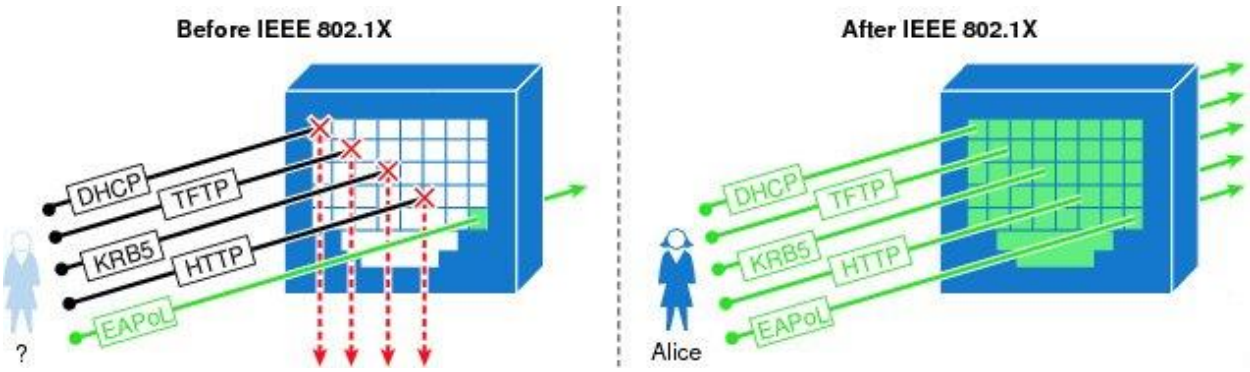
Implement 802.1X:

- IEEE 802.1x is a standard set by the IEEE 802.1 working group.
- IEEE 802.1X commonly referred or called Dot1x.
- IEEE 802.1X authentication is a Data Link Layer (Layer 2) protocol.
- IEEE 802.1X provide port-based network access control using authentication.
- IEEE 802.1X authentication method service is called port-level authentication.
- IEEE 802.1x is defined as a standard for “Port-Based Network Access Control”.
- The protocol in 802.1X is called EAP Encapsulation over LANs (EAPOL).
- IEEE 802.1X method is used mainly for port-based authentication.
- Dot1x can be used to prevent unauthorized devices from gaining access to network.
- Dot1x standards provide authentication & authorization services at network port level.
- Dot1x provide real security for wired and wireless networks at layer two.
- IEEE 802.1x authentication is a Client and Server based authentication protocol.



802.1X Components:

The IEEE 802.1x framework defines three roles in the authentication process:

Supplicant (Client or Host):

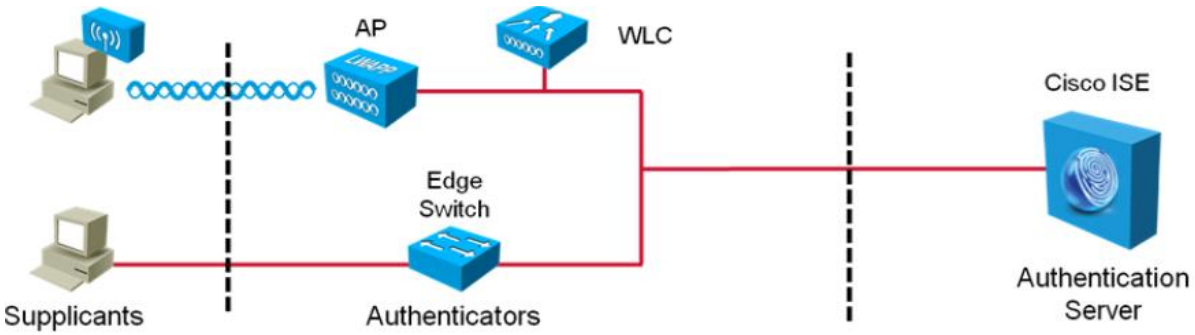
- Supplicant is the user or device that wants access the wireless or wire network.
- Supplicant, client or host is the device or user requiring authentication.
- Supplicant is also known Client, as 802.1x Port-Based Authentication.
- Supplicant is the Workstation that is connected through Network Access Switch.
- Supplicant is the workstation request for accessing the network resources.
- Supplicant is the Workstation or Client must be using 802.1x Client software.
- Supplicant could be an end-user device, a printer, or an IP phone.
- The supplicant is the 802.1x software that runs on the endpoint.
- Windows has own common native supplicant for wired networks.

Authentication Server:

- Authentication Server is a device that processes authentication such as RADIUS.
- Authentication Server is the device that authenticates the Supplicant or client.
- The entity that validates the identity of the supplicant and notifies the authenticator.
- Authentication Server notifies authenticator to allow or deny the client request.
- For example, RADIUS server, such as ACS, can provide authentication server services.

Authenticator (Switch, AP):

- Device between supplicant & authentication server that facilitates authentication.
- The client or supplicant is normally directly connected to the authenticator.
- For example, switch or wireless access point provide authenticator services to clients.
- Authenticator is the network device that is acting as a "gatekeeper" to the network.
- Authenticator is typically a switch or Wireless LAN Controller (WLC).



802.1X Port States:

- When using 802.1x, there are three defined port states:
- Port state determines whether client will get the network access.

Auto:

- Enables 802.1X port-based authentication & causes the port to begin in unauthorized state.
- Auto port state allowing only EAPOL frames, CDP, and STP traffic to be sent and received.
- After the supplicant is authenticated, the port transitions to the authorized state.

Forced-Authorized:

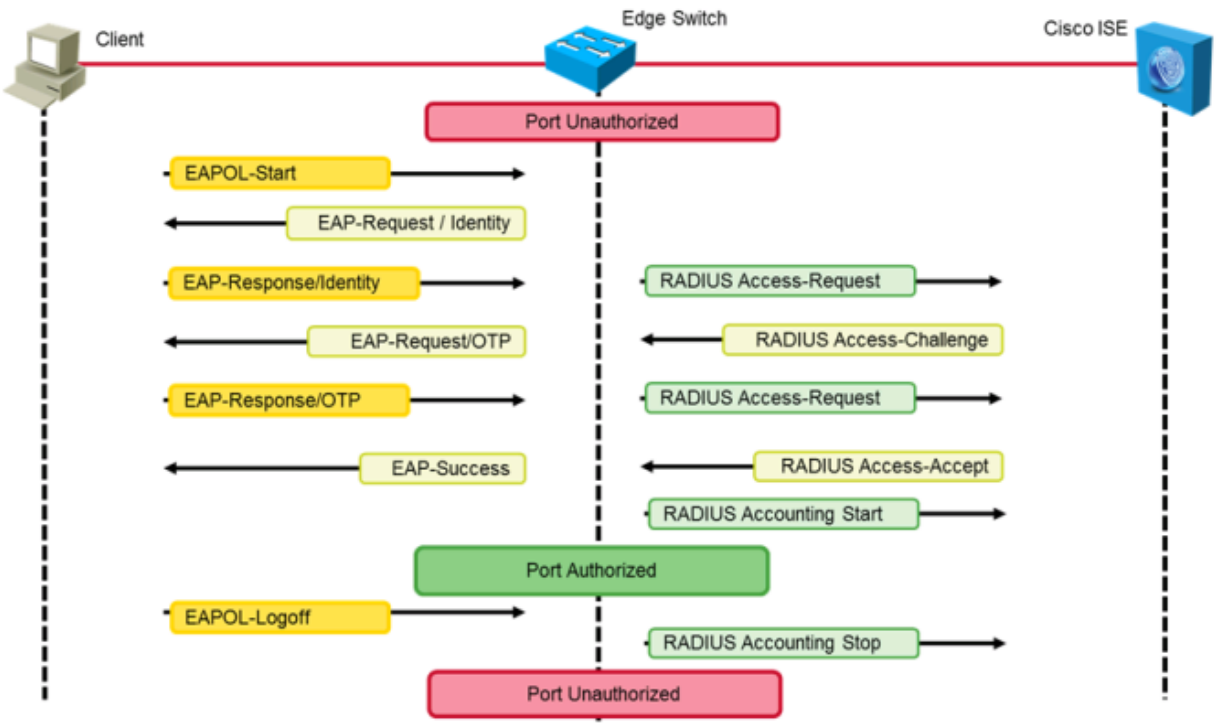
- Forced Authorized state disables 802.1x port-based authentication.
- Disables 802.1x and causes the port to transition to the authorized state.
- In this state, all traffic is allowed as normal without restriction.
- The port transmits & receives normal traffic without 802.1x-based authentication.

Forced-Unauthorized:

- In this state, the port ignores all traffic, including any attempts to authenticate.
- The port is forced to never authorize any connected client.
- Port remain in the unauthorized state, ignoring all attempts by client to authenticate.
- The authenticator cannot provide authentication services to the supplicants.

802.1X Port State	
802.1X Port State	**Description**
Force-Authorized	Client is always authorized to send traffic (Default)
Force-Unauthorized	Client is never authorized to send traffic (Even after authentication)
Auto	802.1x decides whether client is authorized or not to send traffic

Host Modes	Description	MAC
Single-host	Only one client can connected to the 802.1X enabled port	1
Multi-host	Allow multiple hosts useful for Access Point	*
Multi-domain	Allow both a host & VOIP Phone to be connected	2
Multi-auth	Allow one client Voice & multiple client data	*



802.1X Phasing:

- There are three mode of IEEE 8021.X mention below.

Monitor Mode:

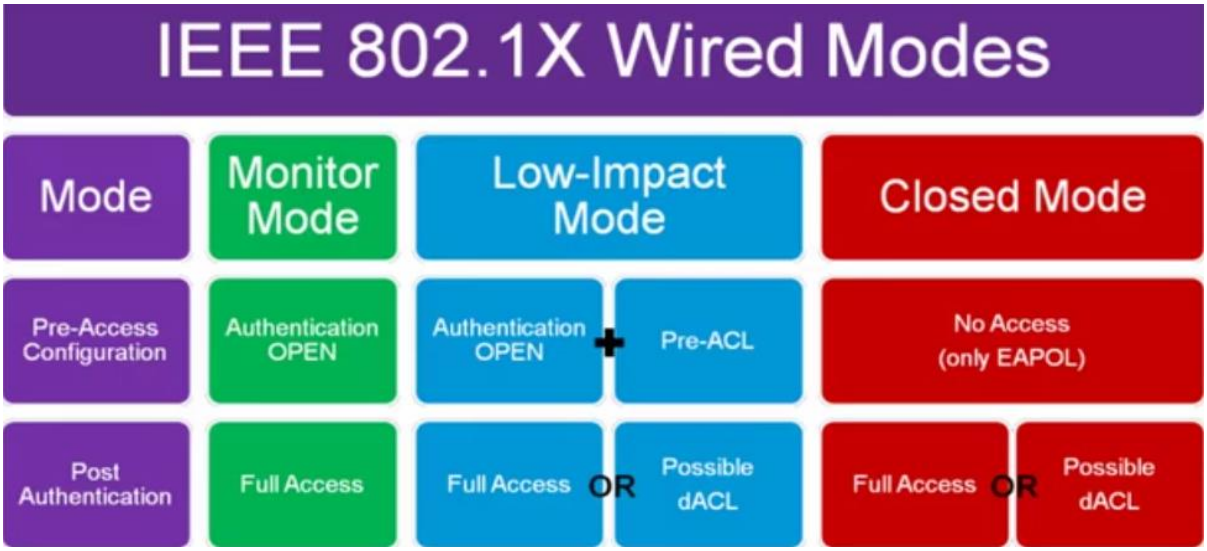
- Monitor mode is the Phase 1 of 802.1x phasing.
- Monitor Mode works like an audit mode.
- Even failed authentication will allow access to network.
- Administrator uses this mode to verify that all devices are authenticating.
- Administrator uses this mode by using Logging data for verification.
- Administrator get info, which users are, getting successful or failure authentications.
- Failure authentications can be solved without affecting end user access to the network.
- Authentication may be 802.1x or MAC Authentication Bypass (MAB).
- Monitor mode uses RADIUS accounting packets and Open Authentication.
- Monitor mode also uses RADIUS Multi Authentication feature to provide visibility.
- Monitor Mode is address any possible authentication issues to moving to next phases.
- Monitor Mode is that it is applicable to wired environments only.

Low Impact Mode:

- Low Impact Mode, Security is added over the framework built in Monitor mode.
- Low Impact mode is also same as monitor mode with prebuilt ACL on switch port.
- Low Impact Mode, Limited, basic access prior to authentication.
- ACL restricts the port to very limited network access prior the authentication.
- When user is authenticated successfully, additional resources may have granted.
- Low Impact Mode, grant specific access after successful authentication.
- In Low impact mode, host connected to the port may be allowed to use DHCP & DNS.
- Low impact mode to route to the Internet and blocked to use internal resources.
- In Low impact mode after authentication, a downloadable ACL may allow all traffic.

Closed Mode:

- Closed mode is also lies in the 2nd phase.
- Closed mode is formerly called High Security mode.
- Closed mode, only EAPOL traffic is allowed before authentication.
- Closed Mode, specific access after successful authentication.
- Closed Mode is default 802.1X behavior & most restrictive method.
- Any traffic before authentication will be dropped including DHCP, DNS, ARP etc.



IEEE 802.1X Wired Modes
Open Mode
SW(config)#interface e0/0 SW(config-if)#authentication host-mode multi-auth SW(config-if)#authentication open SW(config-if)#authentication port-control auto SW(config-if)#mab SW(config-if)#dot1x pae authenticator
Low Impact Mode
SW(config)#interface e0/0 SW(config-if)#authentication host-mode multi-auth SW(config-if)#authentication open SW(config-if)#authentication port-control auto SW(config-if)#mab SW(config-if)#dot1x ape authenticator SW(config-if)#ip access-group default-ACL in
Closed Mode
SW(config)#interface e0/0 SW(config-if)#authentication host-mode multi-auth SW(config-if)#authentication port-control auto SW(config-if)#mab SW(config-if)#dot1x pae authenticator

Monitor Mode Authentication Open	**Low Impact Mode** Authentication Open + ACL
Closed Mode Remove Authentication Open and ACL	