802.1X Phasing:

- There are three modes or Phasing of IEEE 8021.X (Dot1x) mention below.

Monitor Mode:

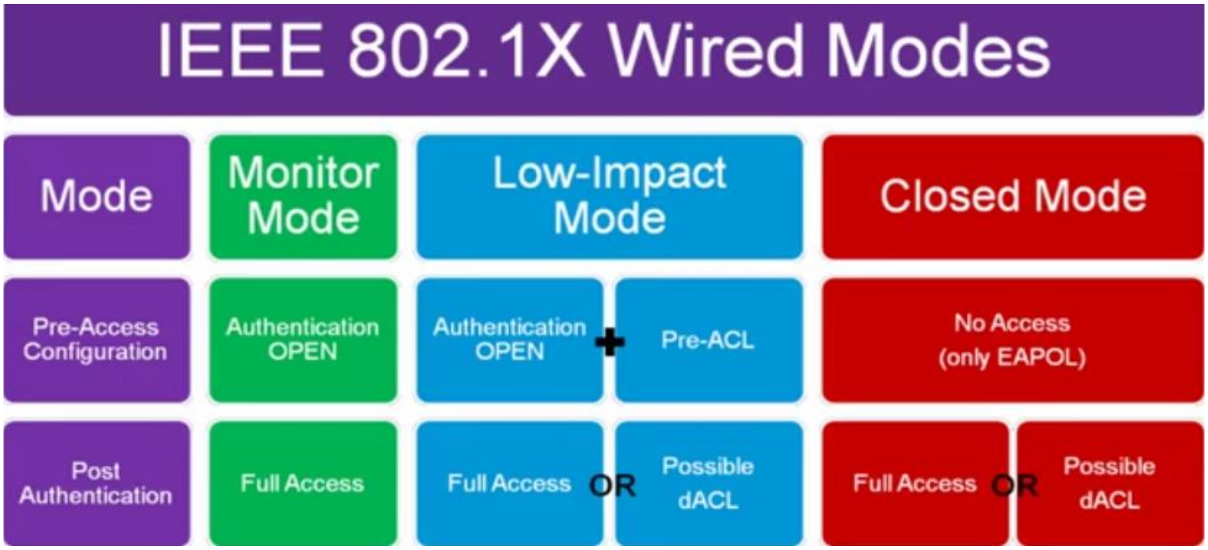
- Monitor mode (Open Mode or Audit Mode) is the Phase 1 of IEEE 802.1x phasing.
- Monitor Mode works like an audit or open mode and will not impact on production.
- In this mode audit logs can be used to understand what is going on the network.
- In Monitor or Open Mode, even failed authentication will allow access to network.
- Administrator uses Monitor mode, to verify that all the devices are authenticating.
- Administrator uses Monitor Mode by using Logging data for verification purposes.
- Administrator get info, which users are, getting successful or failure authentications.
- Failure authentications can be solved without affecting end user access to the network.
- In Monitor Mode, authentication may be 802.1x or MAC Authentication Bypass (MAB).
- Monitor or Audit Mode uses RADIUS accounting packets and Open Authentication.
- Monitor mode also uses RADIUS Multi Authentication feature to provide the visibility.
- Monitor Mode is address any possible authentication issues to moving to next phases.
- Monitor Mode (Open or Audit 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 ingress ACL applied.
- The ACL restricts the port to very limited network access prior the authentication.
- When user is authenticated successfully, additional resources may have granted.
- IEEE 8021.X 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:

- In IEEE 8021.X (Dot1x) Closed Mode is also lies in the Second (2nd) Phase.
- In IEEE 8021.X (Dot1x) Closed Mode is formerly called High Security mode.
- In Closed Mode, only EAPOL traffic is allowed before the authentication.
- In Dot1x only The EAPoL traffic is allowed until authentication takes place.
- In IEEE 8021.X Closed Mode, specific access after successful authentication.
- Closed Mode is the default 802.1X behavior and most restrictive method.
- Any traffic before authentication will be dropped including DHCP, DNS, ARP.

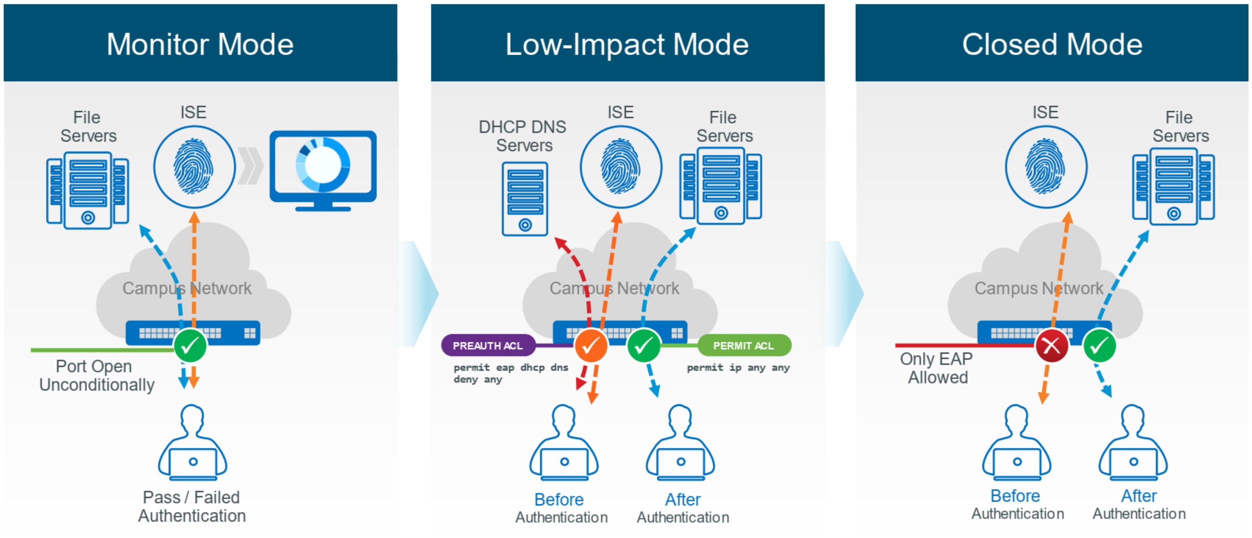


IEEE 802.1X Wired Modes

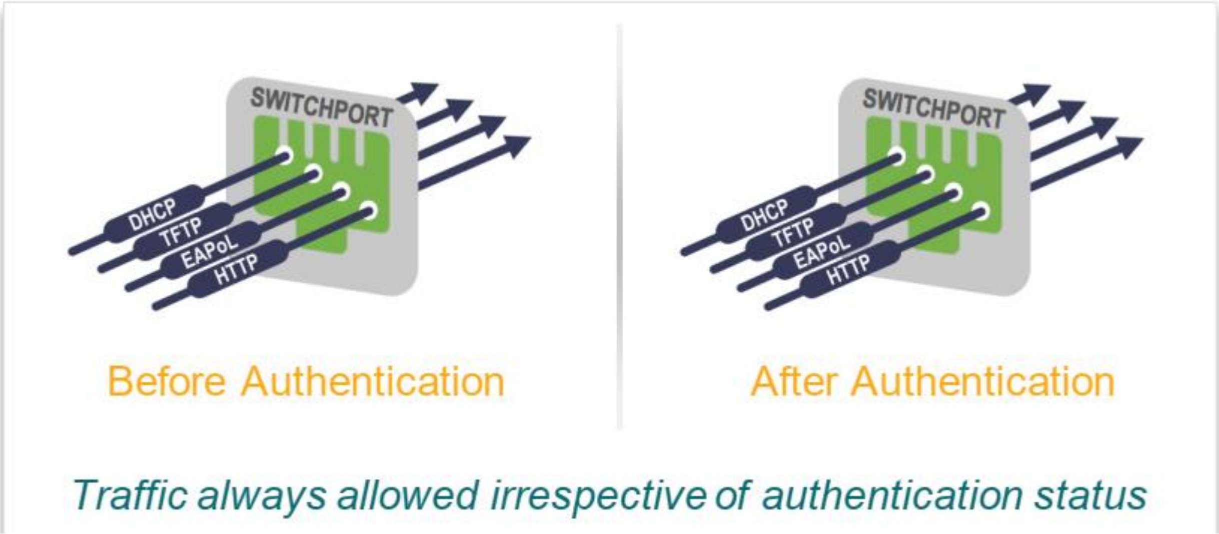
Mode	Monitor Mode	Low-Impact Mode	Closed Mode
Pre-Access Configuration	Authentication OPEN	Authentication OPEN + Pre-ACL	No Access (only EAPOL)
Post Authentication	Full Access	Full Access OR Possible dACL	Full Access OR Possible dACL

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	

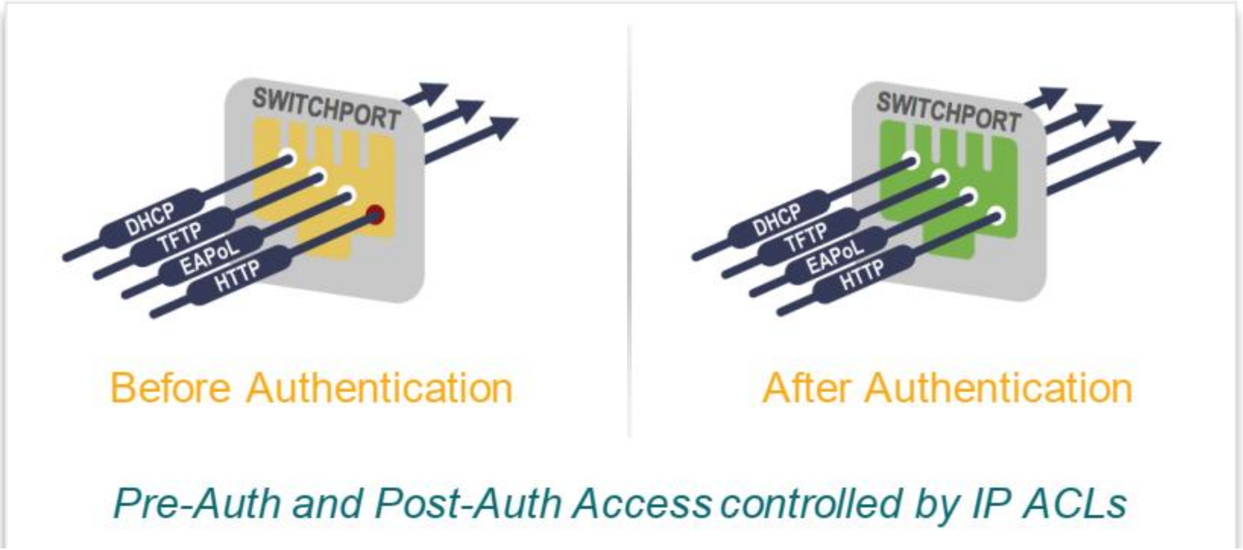


Monitor Mode:

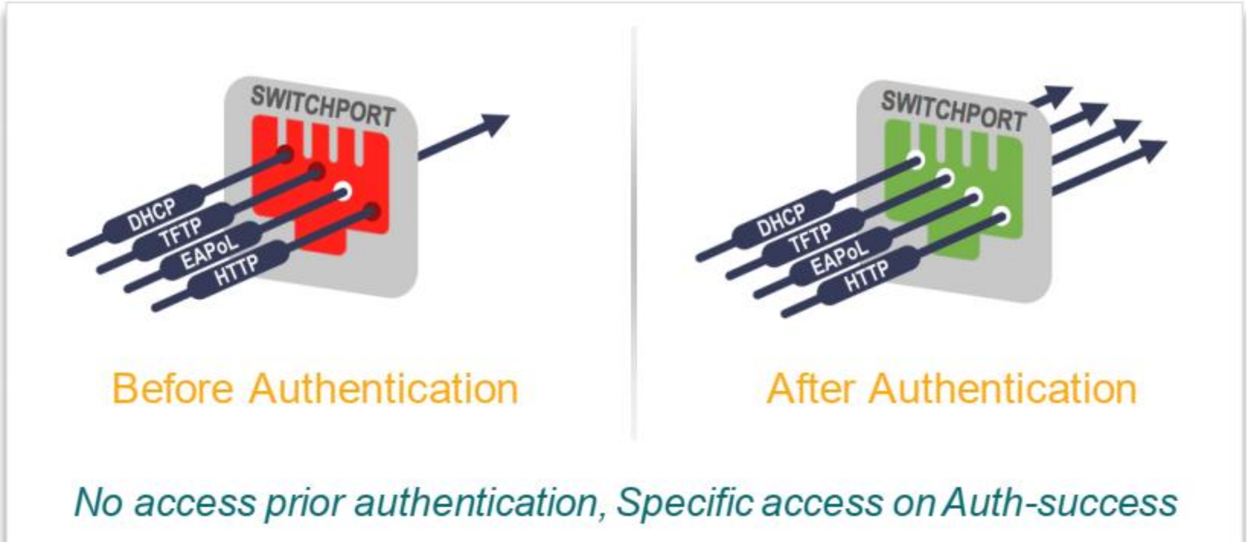


Traffic always allowed irrespective of authentication status

Low Impact Mode:



Closed Mode:


SWITCHPORT
DHCP
TFTP
EAPoL
HTTP
Before Authentication
SWITCHPORT
DHCP
TFTP
EAPoL
HTTP
After Authentication
No access prior authentication, Specific access on Auth-success