CCNP Security – SISAS
Phased Deployment

Default Supplicant Network Access

- » When authentication is enabled on a switch port facing a supplicant
  - By default all network access is restricted before authentication
    - Only EAPOL traffic is allowed
  - After authentication network access is granted per the authorzation received from ISE
- » Default network access creates implementations issues
  - If something is miss-configured (can easily happen), users loose network access

The image cannot be displayed. Your computer may not

Phased Deployment

- Created by Cisco to easily implement MAB/ 802.1x
  - Minimizes network impact when EAP/802.1x is enabled
  - From users point of view, implementation is transparent
- Three-phase model
  - Monitor mode
  - Low impact mode
  - Closed mode

The image cannot be displayed. Your computer may not

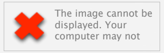
Monitor Mode

» Monitor mode

- Scope is to test authentication functionality
- Allows for transparent troubleshooting, without affecting users
- EAP and MAB is enabled on switch ports facing supplicants
- Supplicants are granted full network access
  - Before authentication
  - After authentication (requires no authorization received from ISE)
  - After authentication, even if it fails
- Enabled through **`authentication open`** command on switch port facing supplicant

Low Impact Mode

- Enabled once all users/supplicants have passed authentication
  - Scope is to test authorization functionality
- Keep the same configuration as in monitor mode
- Restrict network access before authentication
  - Apply a static pre-authentication ACL on switch port facing supplicants
  - Optionally can use the default ACL named **`auth-default-acl`**
- Authorization is received from ISE
  - ACL in order to override the static pre-configured one



The image cannot be displayed. Your computer may not

Closed Mode

- Enabled once all users/supplicants have passes authorization
- Disable monitor/low impact mode
  - Remove **`authentication open`**
  - Default network access behaviour
  - Prior to authentication only EAPOL traffic is allowed
- Authorization is received from ISE
  - ACL in order to override the static pre-configured one
- For users/supplicants to be granted network access
  - Supplicants need to pass authentication
  - Switch needs to successfully apply authorization received from ISE

The image cannot be displayed. Your computer may not

Q&A