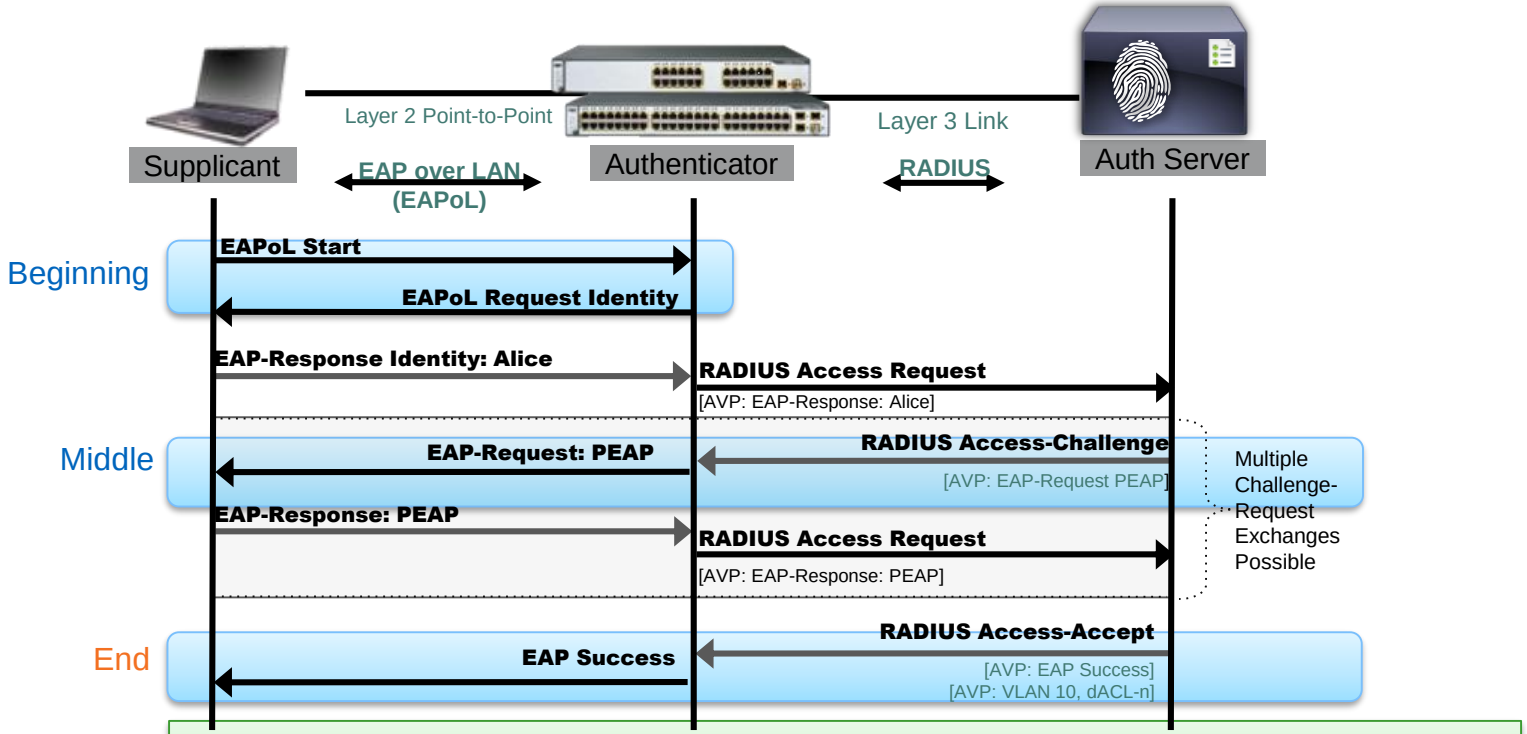
# Collection of ISE Auth and Service Flows

Craig Hyps, Principal Engineer

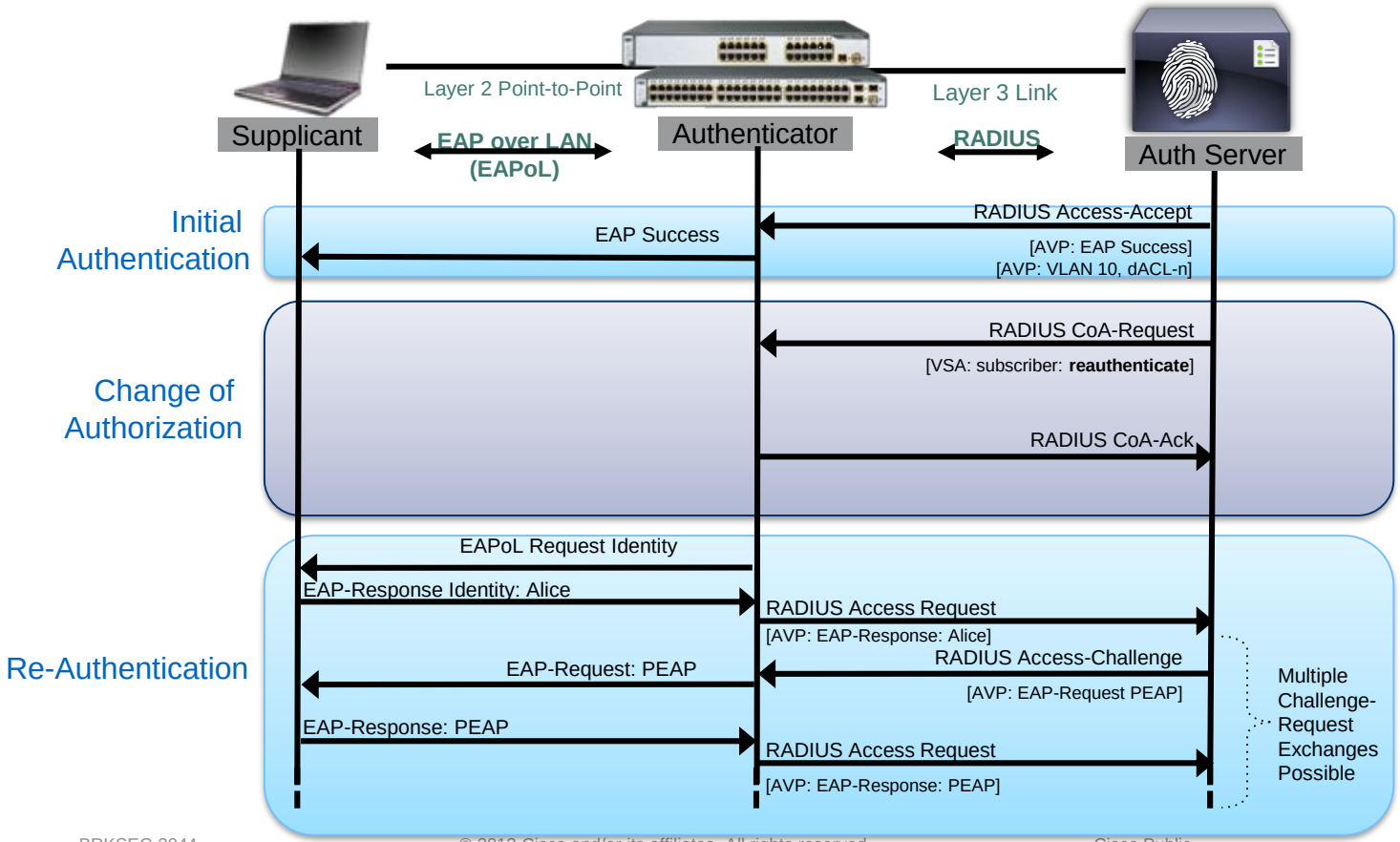
# IEEE 802.1X

## Port-based access control with authentication



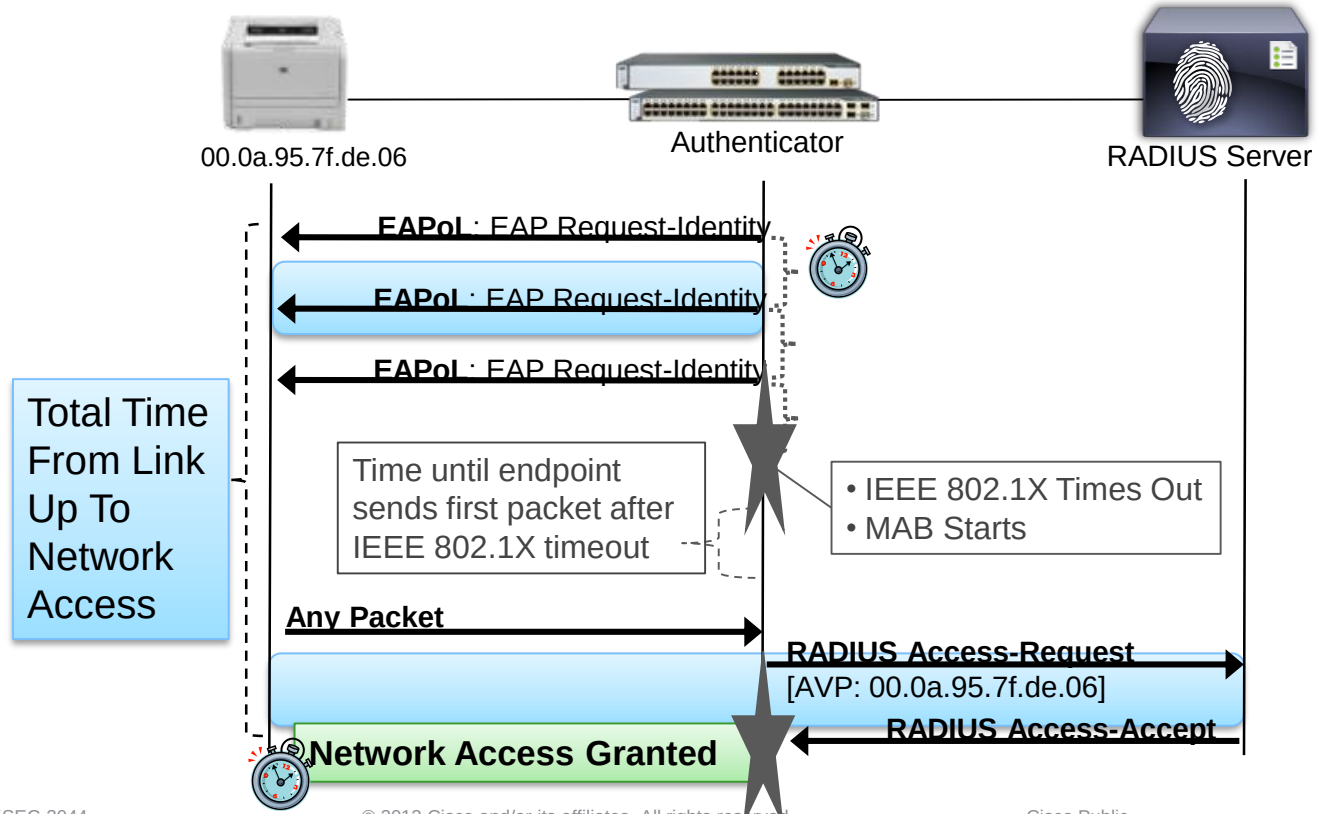

- 802.1X (EAPOL) is a **delivery mechanism** and it doesn't provide the actual authentication mechanisms.
- When utilizing 802.1X, you need to choose an **EAP type**, such as Transport Layer Security (EAP-TLS) or PEAP, which defines how the authentication takes place.

# IEEE 802.1X with Change of Authorization (CoA)

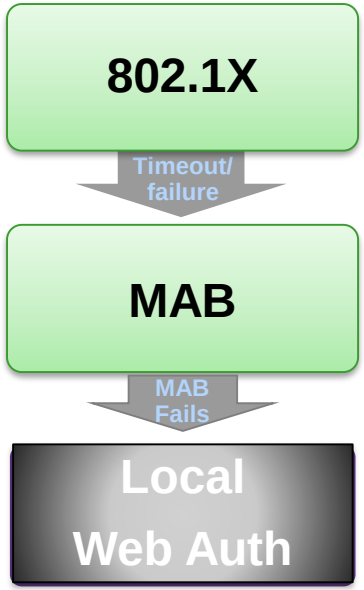


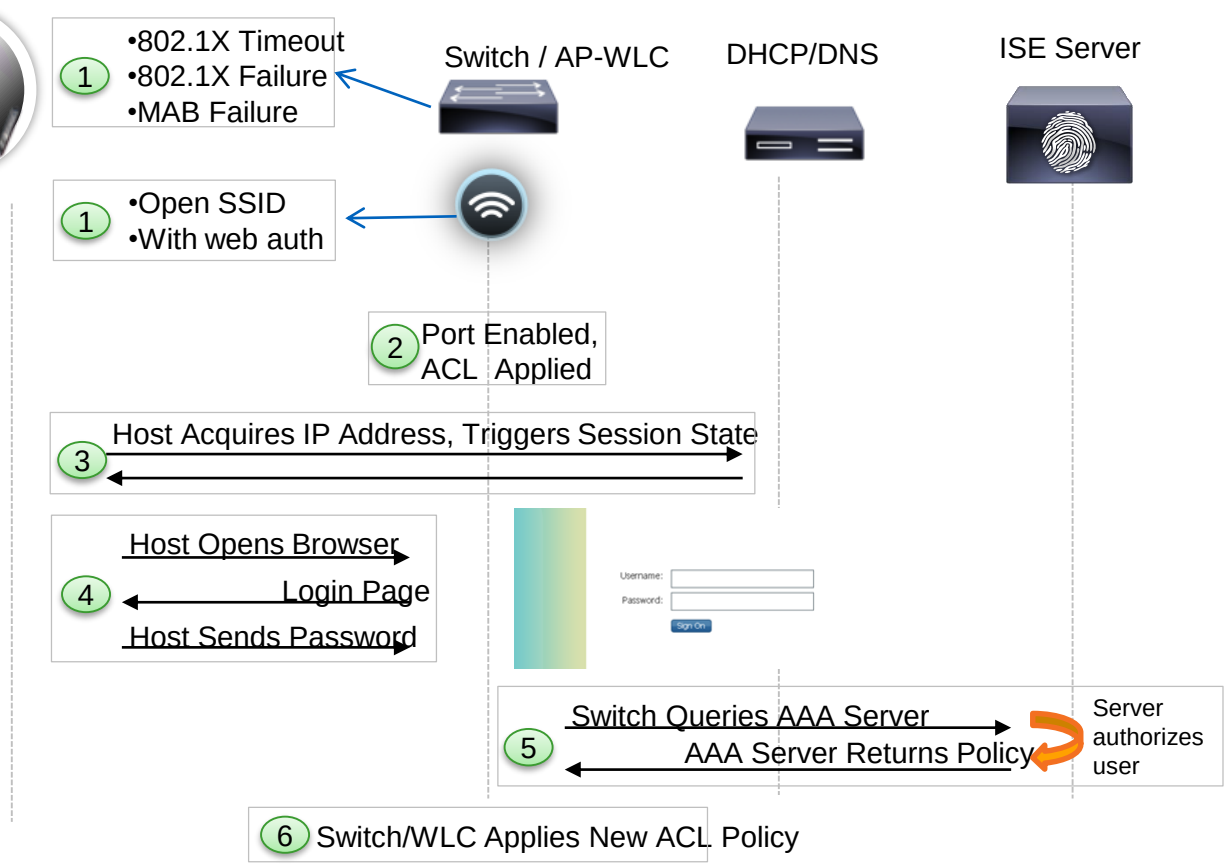
# MAC Authentication Bypass (MAB)

Non-802.1X capable devices and no “user intelligence” behind



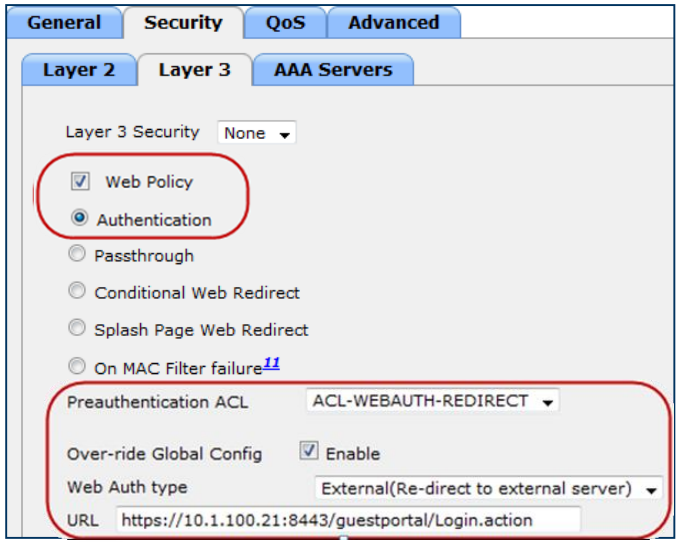
# LWA – Session Flow

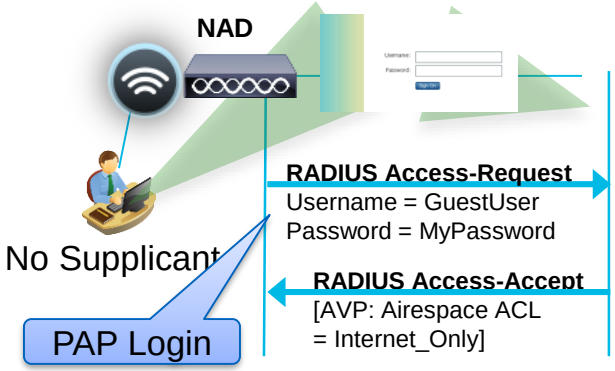



**Flex Auth**: After timeout or failure, port automatically tries “next-method” if another method configured.

# Wireless LWA Config




## Authentication Policy

| Status | Rule Name | | Conditions | | Identity Source |
|---|---|---|---|---|---|
| ✓ | MAB | if | Wired_MAB | then | Internal Endpoints |
| ✓ | Dot1X | If | Wired_802.1X | then | AD1 |
| ✓ | LWA | if | RADIUS:Service-Type = Login<br>RADIUS:NAS-Port-Type= Wireless – IEEE 802.11 | then | Internal Users |
| ✓ | Default | if | <no match> | then | AD1_Internal |

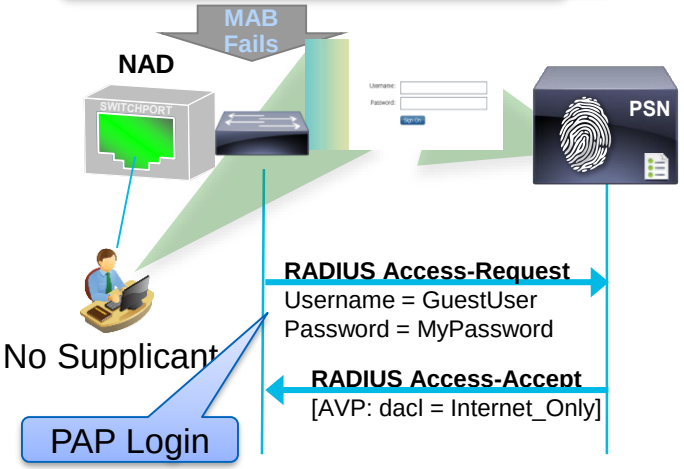
## Authorization Policy

| Status | Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|---|
| ✓ | IP Phones | if | Cisco-IP-Phone | then | Cisco_IP_Phone |
| ✓ | BYOD | if | BYOD and Employee | then | Employee |
| ✓ | Guest | if | Guest | then | Guest |
| ✓ | Contractor | if | Contractor | then | Contractor |
| ✓ | Employee | if | Employee | then | Employee |
| ✓ | Default | If no matches, then | | WEBAUTH | |

# Wired LWA Config

802.1X → Timeout/Failure → MAB → Failure → Local Web Auth

```
ip admission name WEBAUTH proxy http
ip access-list extended PRE_AUTH_POLICY
   permit udp any any eq bootps
   permit udp any any eq domain
fallback profile WEBAUTH_PROFILE
   ip access-group PRE_AUTH_POLICY in
   ip admission WEBAUTH
interface GigabitEthernet1/0/1
  authentication port-control auto
  authentication fallback WEBAUTH_PROFILE
  dot1x pae-authenticator
  mab
authentication event fail action next-method
```



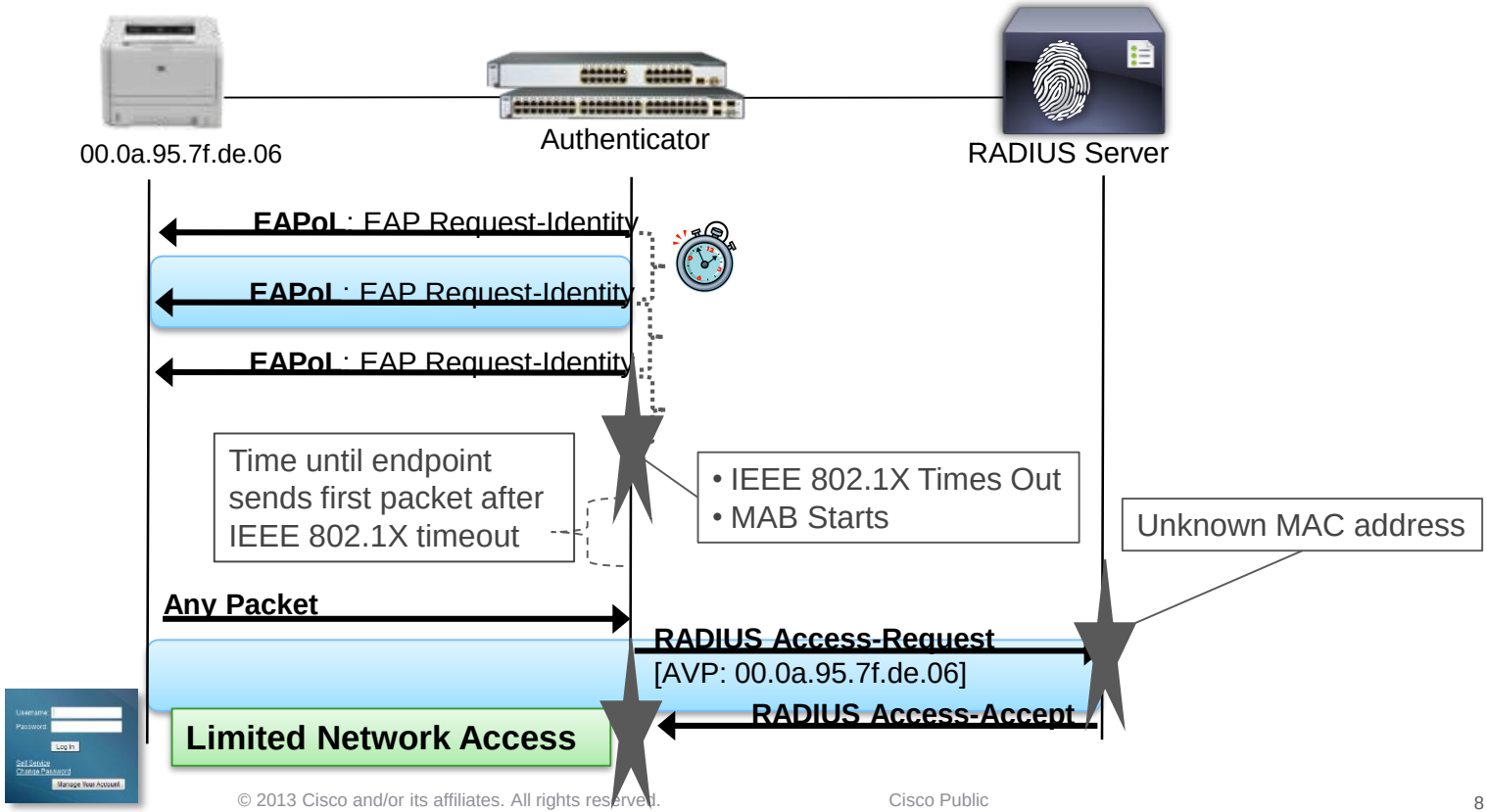

## Authentication Policy

| Status | Rule Name | | Conditions | | Identity Source |
|---|---|---|---|---|---|
| ✓ | MAB | if | Wired_MAB | then | Internal Endpoints |
| ✓ | Dot1X | If | Wired_802.1X | then | AD1 |
| ✓ | LWA | if | RADIUS:Service-Type = Outbound RADIUS:NAS-Port-Type= Ethernet | then | Internal Users |
| ✓ | Default | if | <no match> | then | AD1_Internal |

## Authorization Policy

| Status | Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|---|
| ✓ | IP Phones | if | Cisco-IP-Phone | then | Cisco_IP_Phone |
| ✓ | BYOD | if | BYOD and Employee | then | Employee |
| ✓ | Guest | if | Guest | then | Guest |
| ✓ | Contractor | if | Contractor | then | Contractor |
| ✓ | Employee | if | Employee | then | Employee |
| ✓ | Default | If no matches, then | | | WEBAUTH |

# Web Authentication



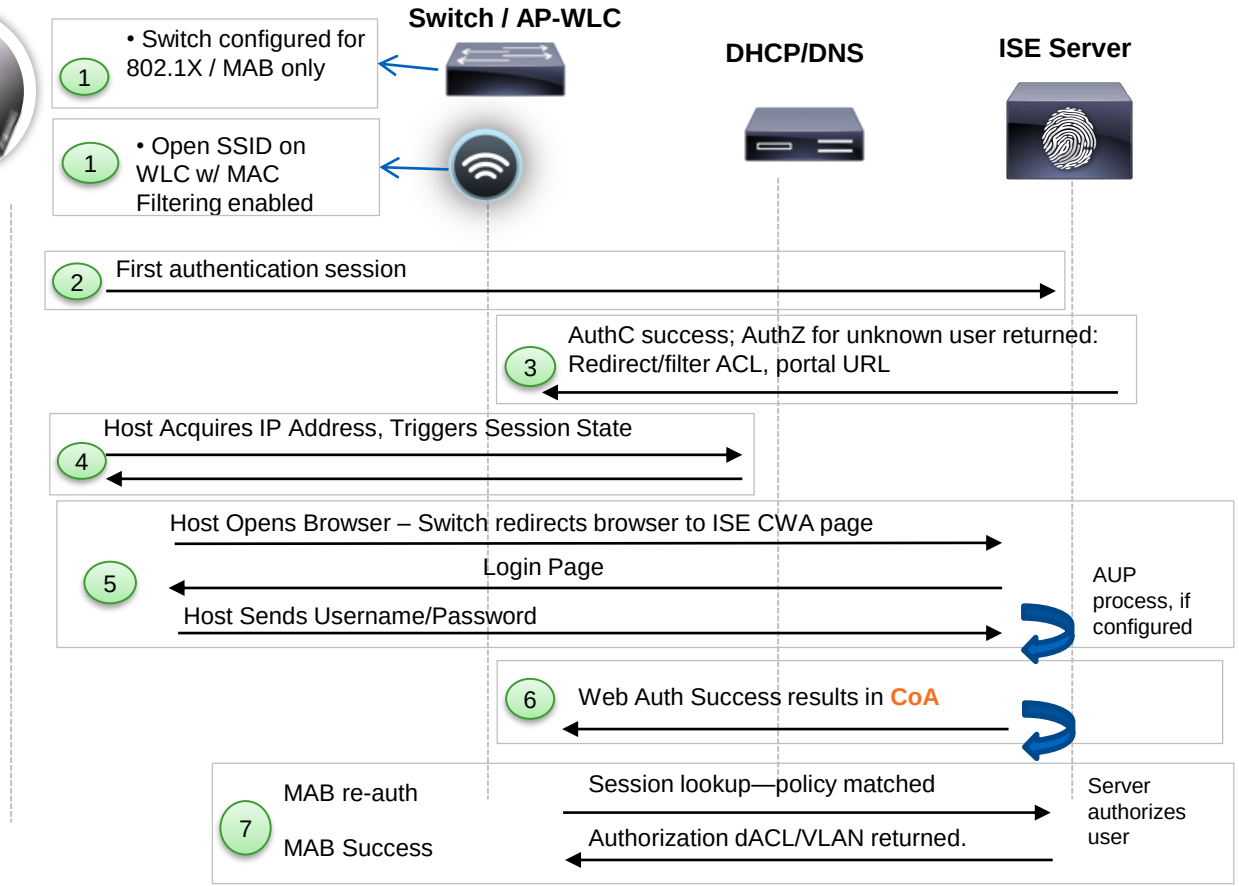
# CWA – Session Flow

**802.1X**

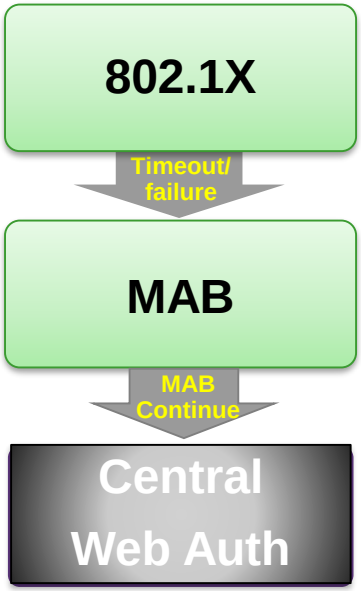
Timeout/ failure

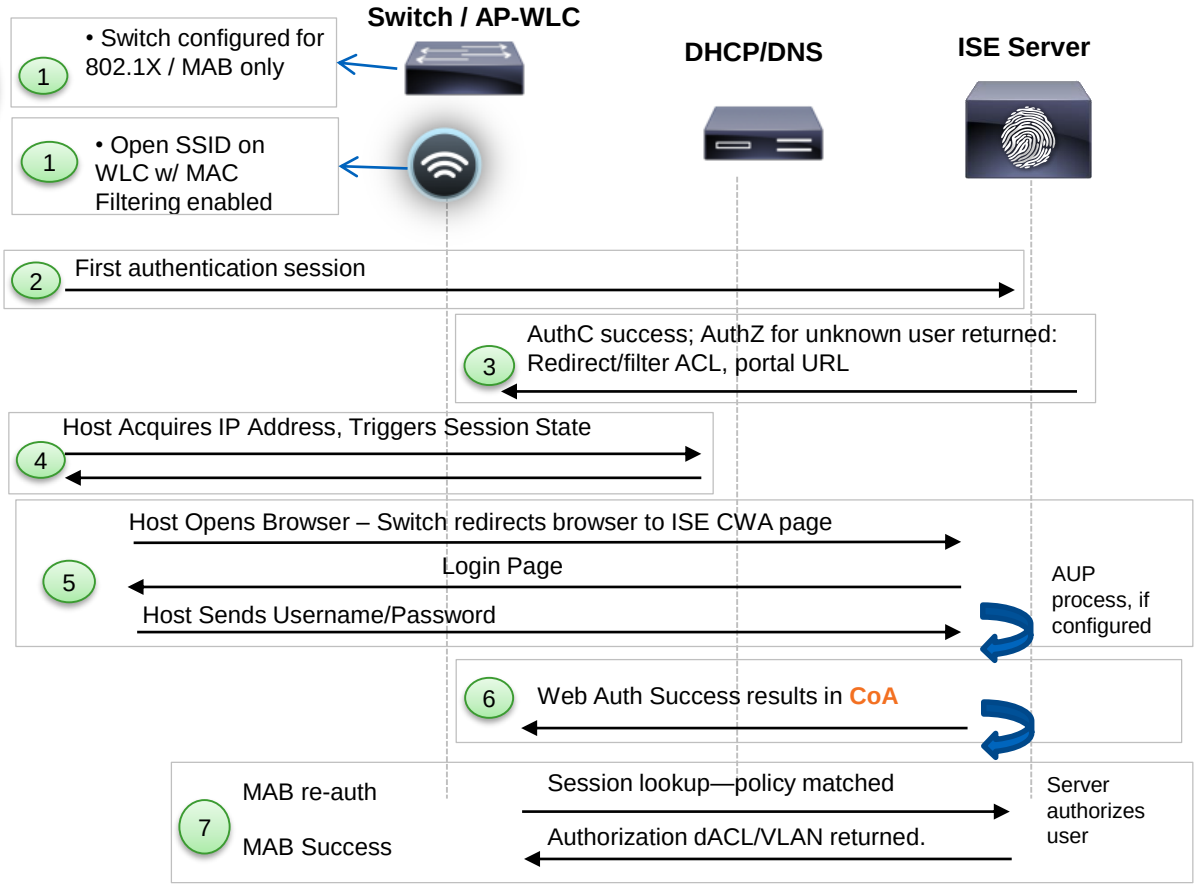
**MAB**

**Flex Auth**: If host not found (MAB lookup fails), then **Continue** to Authorization Policy processing



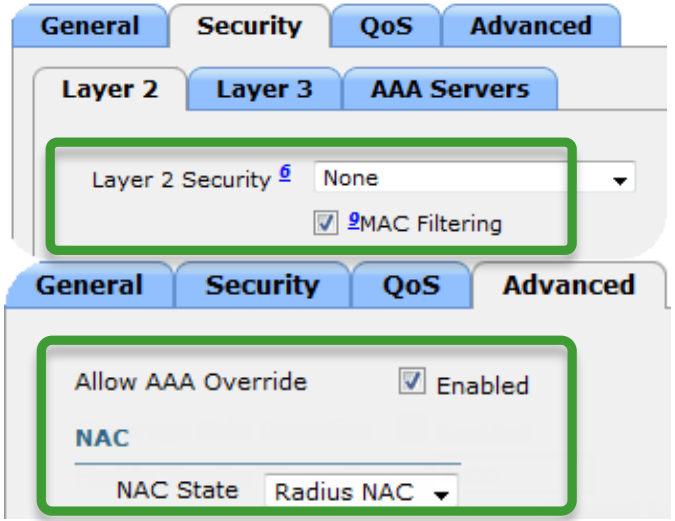
# CWA – Session Flow

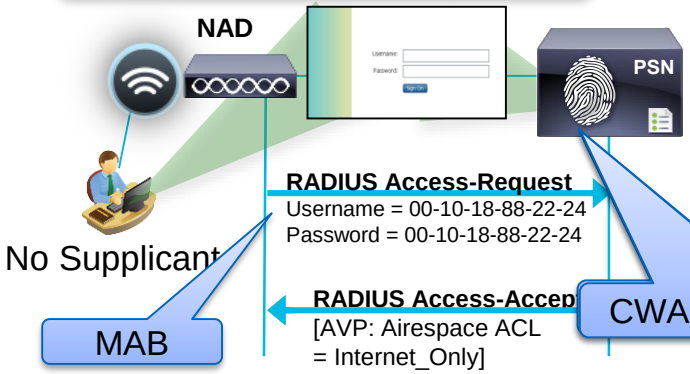



**Flex Auth**: If host not found (MAB lookup fails), then **Continue** to Authorization Policy processing

# Wireless CWA Config




## Authentication Policy

| Status | Rule Name | | Conditions | | Identity Source |
|---|---|---|---|---|---|
| | MAB | if | Wireless_MAB | then | Internal Endpoints |
| ✓ | Dot1X | If | Wireless_802.1X | then | AD1 |
| ✓ | Default | if | <no match> | then | AD1_Internal |

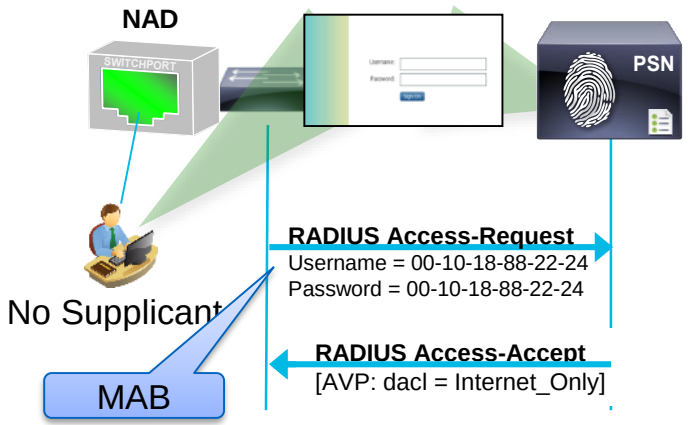
## Authorization Policy

| Status | Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|---|
| ✓ | IP Phones | if | Cisco-IP-Phone | then | Cisco_IP_Phone |
| ✓ | BYOD | if | BYOD and Employee | then | Employee |
| | Guest | if | Guest | then | Guest |
| ✓ | Contractor | if | Contractor | then | Contractor |
| ✓ | Employee | if | Employee | then | Employee |
| ✓ | Default | If no ma | | then | WEBAUTH |

# Wired CWA Config

For Your Reference

```
ip access-list extended PRE-AUTH-ACL
   permit udp any any eq bootps
   permit udp any any eq domain
   permit tcp any any eq http
   permit tcp andy any eq https
ip access-list extended ACL-WEBAUTH-REDIRECT
   deny udp any any eq domain
   deny tcp any host PSN eq 8443
   permit ip any any
interface GigabitEthernet1/0/1
   authentication port-control auto
   dot1x pae-authenticator
   mab
   authentication order dot1x mab
   authentication event fail action next-method
```



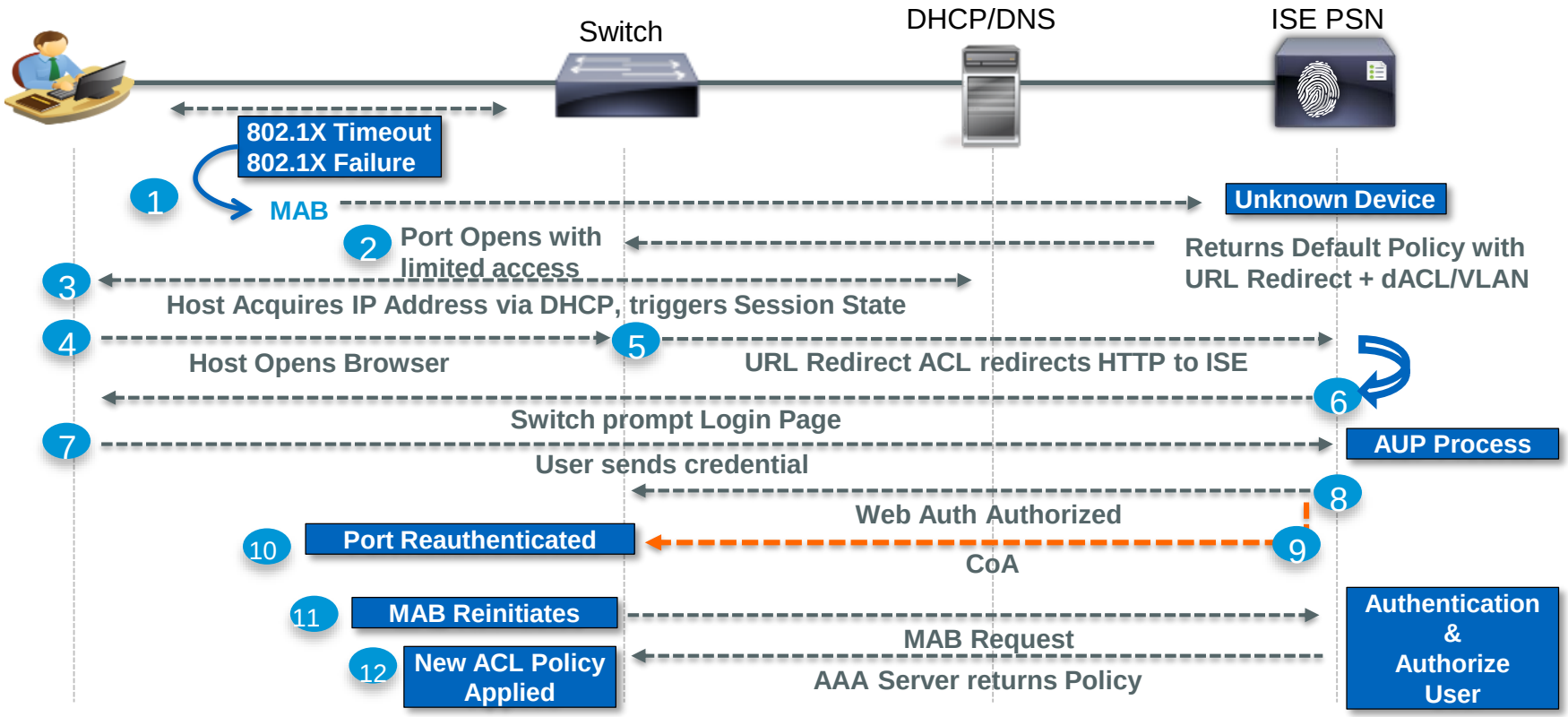

## Authentication Policy

| Status | Rule Name | | Conditions | | Identity Source |
|---|---|---|---|---|---|
| ✓ | MAB | if | Wired_MAB | then | Internal Endpoints |
| ✓ | Dot1X | If | Wired_802.1X | then | AD1 |
| ✓ | Default | if | <no match> | then | AD1_Internal |

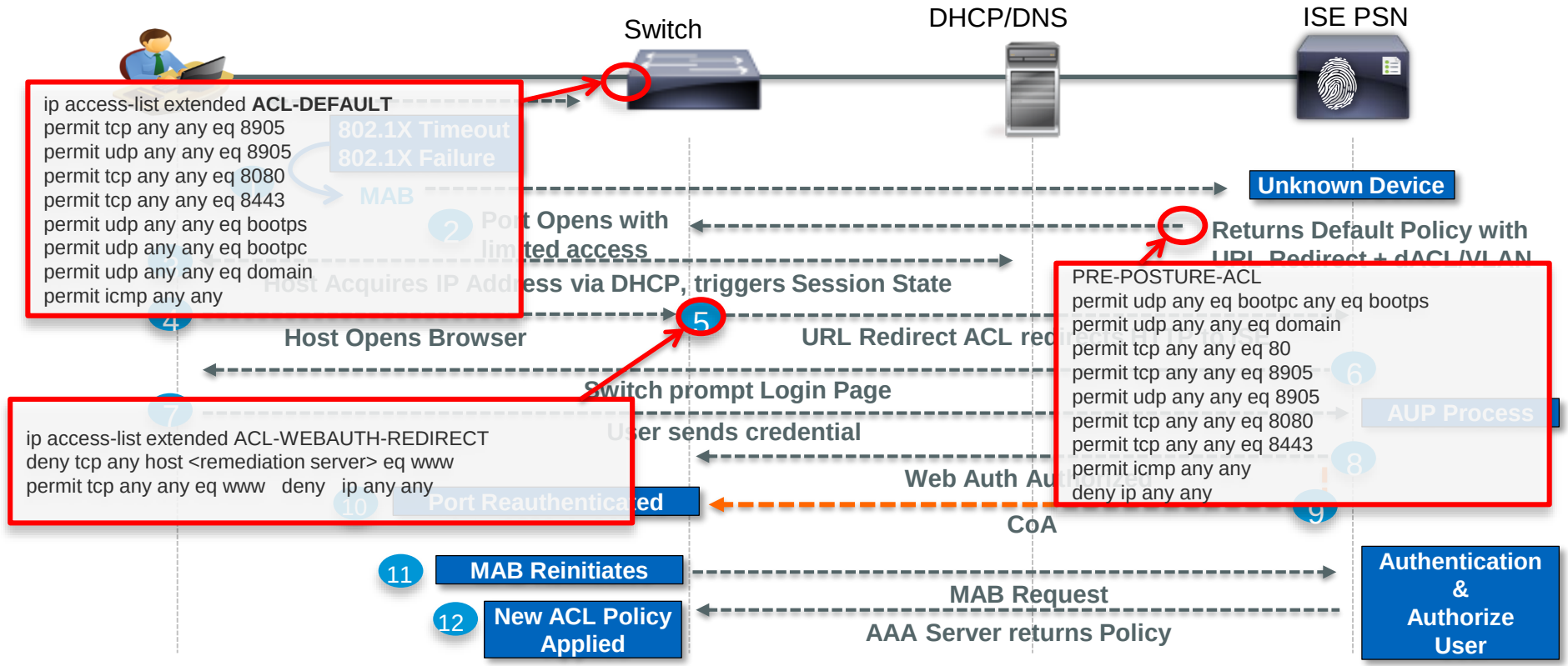
## Authorization Policy

| Status | Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|---|
| ✓ | IP Phones | if | Cisco-IP-Phone | then | Cisco_IP_Phone |
| ✓ | BYOD | if | BYOD and Employee | then | Employee |
| ✓ | Guest | if | Guest | then | Guest |
| ✓ | Contractor | if | Contractor | then | Contractor |
| ✓ | Employee | if | Employee | then | Employee |
| ✓ | Default | If no | | hen | WEBAUTH |

# Central Web Authentication (CWA) with ISE



# dACL + URL-Redirect for CWA



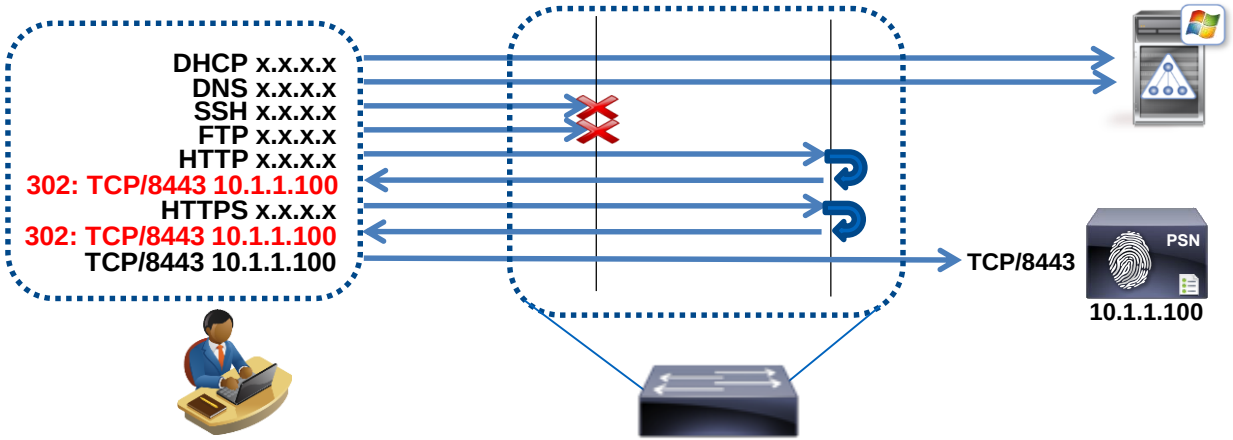
# Sample ACLs for CWA Redirection

```
ip access-list extended ACL-DEFAULT
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit tcp any any eq http
 permit tcp any any eq https
 permit tcp any host 10.1.1.100 eq 8080
 permit tcp any host 10.1.1.100 eq 8443
 (deny ip any any)
```

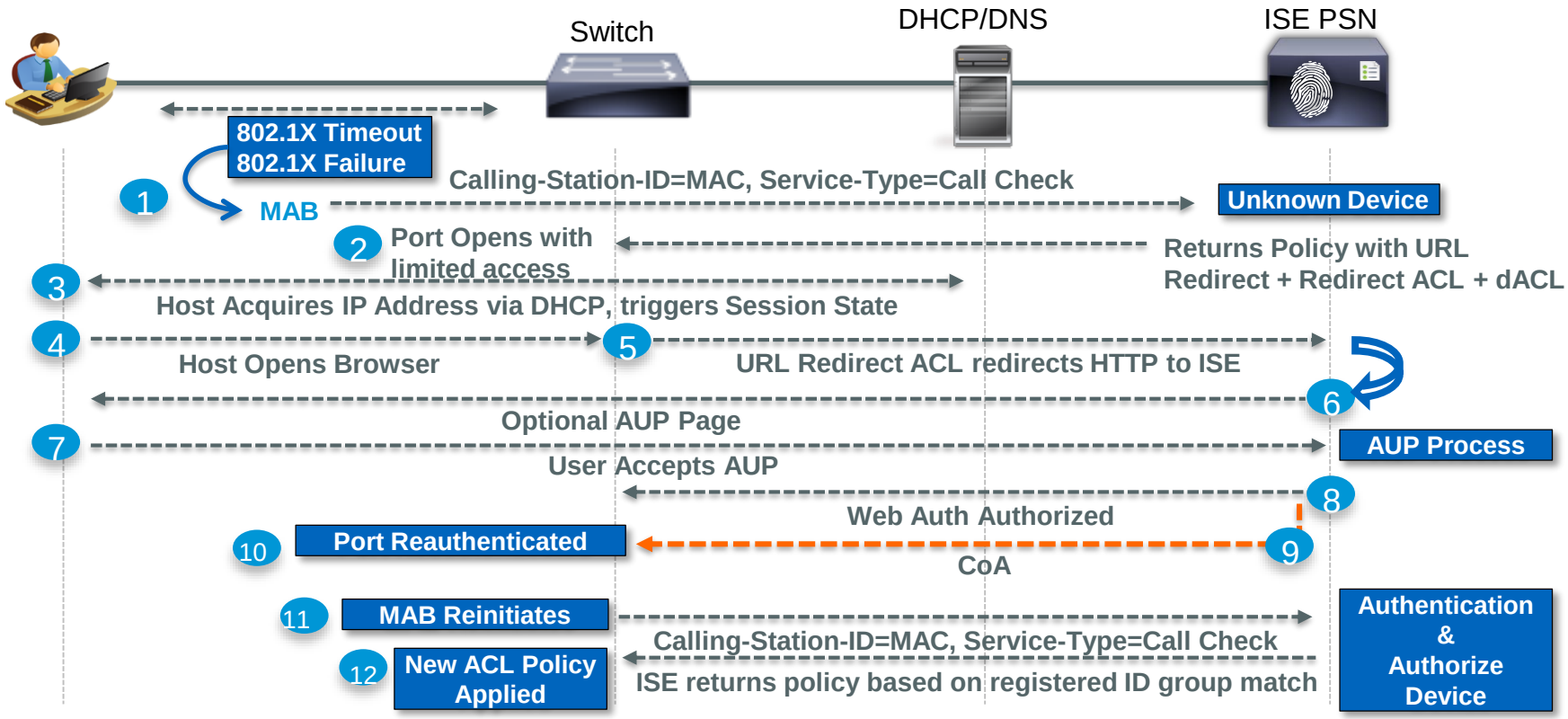
```
ip access-list extended ACL-WEBAUTH-REDIRECT
 deny   udp any eq bootpc any eq bootps
 deny   udp any any eq domain
 deny   tcp any host 10.1.1.100 eq 8080
 deny   tcp any host 10.1.1.100 eq 8443
 permit ip any any
```

Port ACL or dACL

Redirect ACL

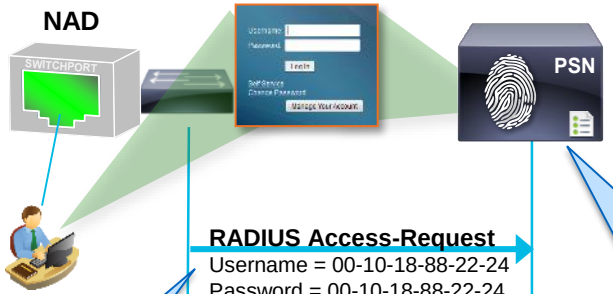


# Wired Device Registration Web Auth (DRW) Flow



# Wired CWA Config

```
ip access-list extended PRE-AUTH-ACL
   permit udp any any eq bootps
   permit udp any any eq domain
   permit tcp any any eq http
   permit tcp andy any eq https
ip access-list extended ACL-WEBAUTH-REDIRECT
   deny udp any any eq domain
   deny tcp any host PSN eq 8443
   permit ip any any
interface GigabitEthernet1/0/1
   authentication port-control auto
   dot1x pae-authenticator
   mab
   authentication order dot1x mab
   authentication event fail action next-method
```




Matched AuthC Rule = MAB

Authentication Policy

| Status | Rule Name | | Conditions | | Identity Source |
|---|---|---|---|---|---|
| | MAB | if | Wireless_MAB | then | Internal Endpoints |
| ✓ | Dot1X | If | Wireless_802.1X | then | AD1 |
| ✓ | Default | if | <no match> | then | AD1_Internal |

Authorization Policy

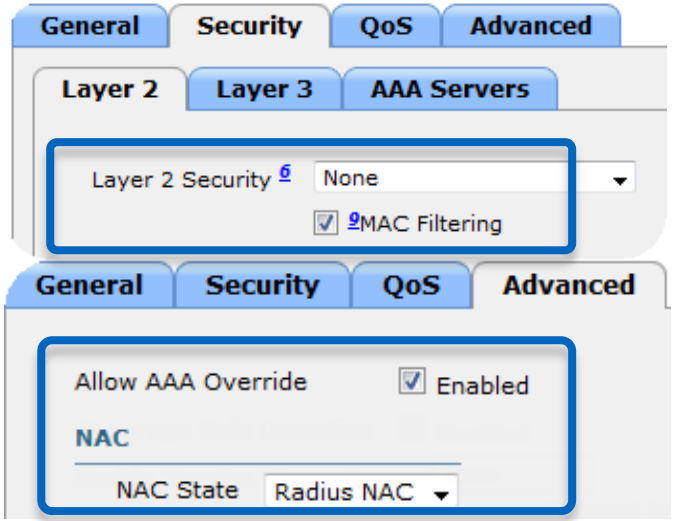
| Status | Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|---|
| ✓ | IP Phones | if | Cisco-IP-Phone | then | Cisco_IP_Phone |
| ✓ | BYOD | if | BYOD and Employee | then | Employee |
| | Guest | if | Guest | then | Guest |
| ✓ | Contractor | if | Contractor | then | Contractor |
| ✓ | Employee | if | Employee | then | Employee |
| ✓ | Default | If no match | | then | WEBAUTH |

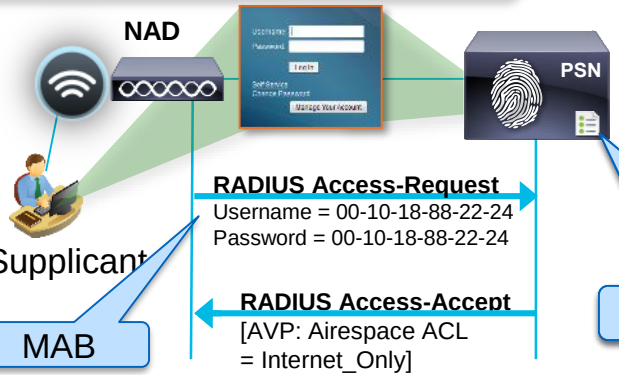
MAB

CWA username matches

Matched AuthZ Rule = Guest

# Wireless CWA Config




Matched AuthC Rule = MAB

Authentication Policy

| Status | Rule Name | | Conditions | | Identity Source |
|---|---|---|---|---|---|
| ✓ | MAB | if | Wireless_MAB | then | Internal Endpoints |
| ✓ | Dot1X | If | Wireless_802.1X | then | AD1 |
| ✓ | Default | if | <no match> | then | AD1_Internal |

Authorization Policy

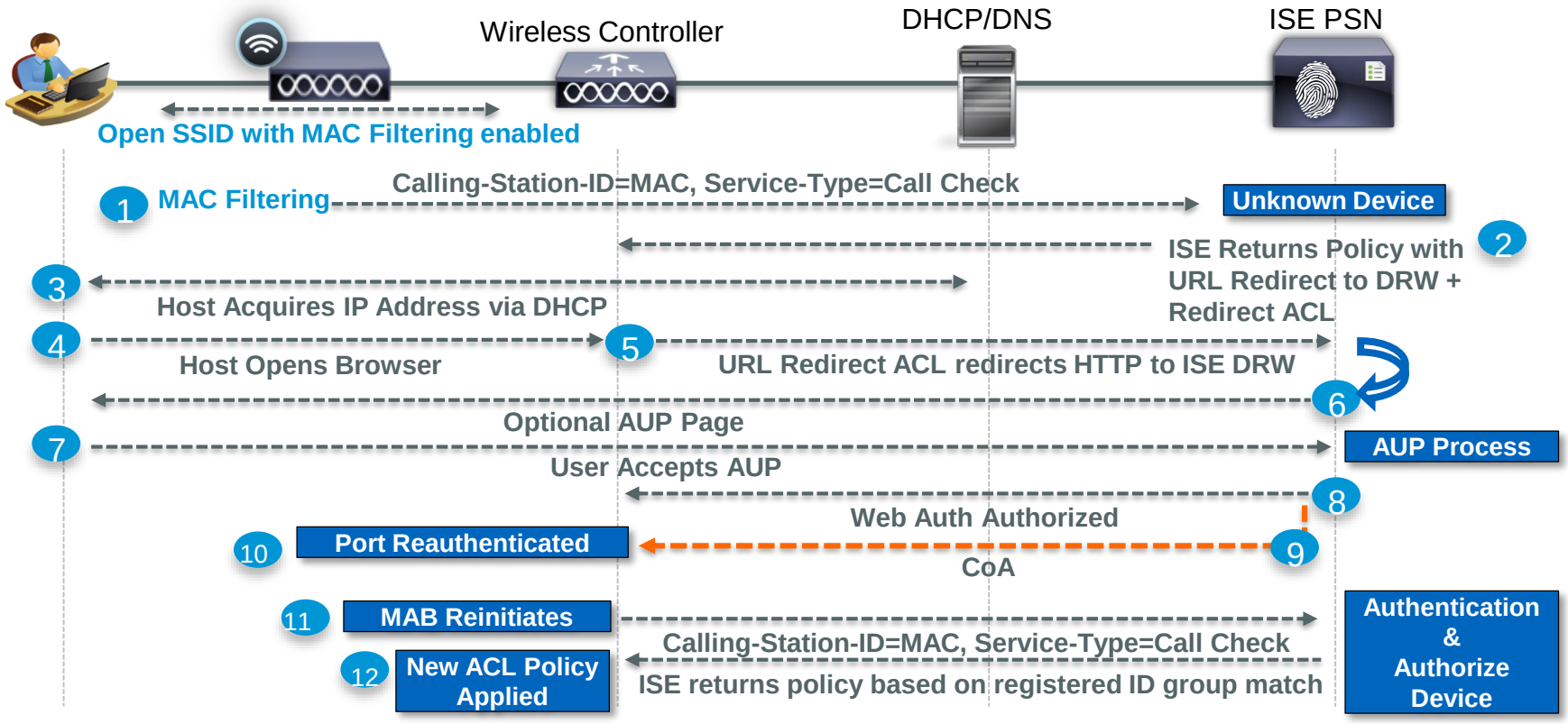
| Status | Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|---|
| ✓ | IP Phones | if | Cisco-IP-Phone | then | Cisco_IP_Phone |
| ✓ | BYOD | if | BYOD and Employee | then | Employee |
| ✓ | Guest | if | Guest | then | Guest |
| ✓ | Contractor | if | Contractor | then | Contractor |
| ✓ | Employee | if | Employee | then | Employee |
| ✓ | Default | If no match | | then | WEBAUTH |

MAB

CWA username matches

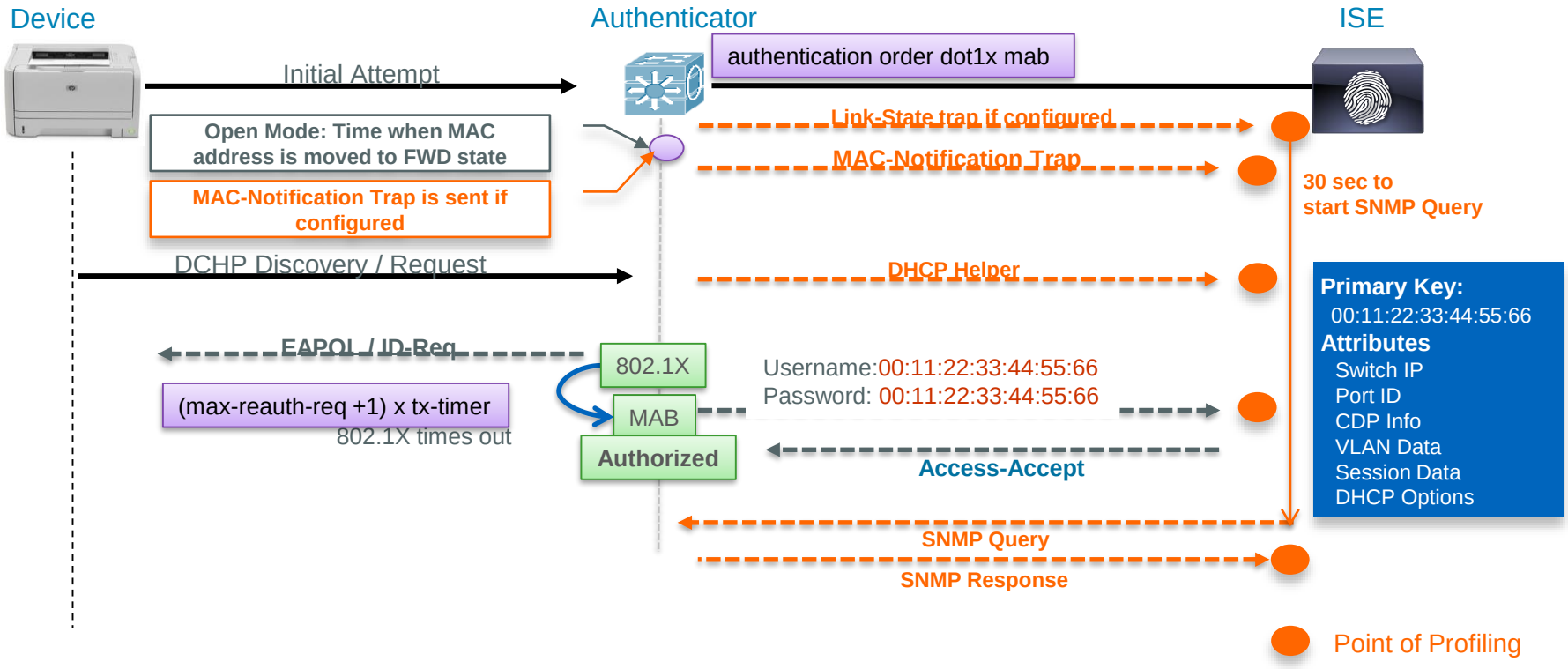
Matched AuthZ Rule = Guest

# Wireless DRW Flow



# Example of Profiling Flow with multiple probes

SNMP Query, SNMP Trap, RADIUS, DHCP Helper



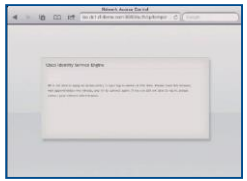
# Profiling without Probes

Direct Profiling using **Client Provisioning** (Posture Agent or NSP)


User authenticates and opens browser

HTTP GET http://www.google.com

RADIUS: URL Redirect=Client Provisioning / Posture



https://psn:8443/guestportal/gateway?sessionId=SessionIdValue&action=cpp

HTTP Response: “Please Reconnect”

RADIUS: CoA = Session Terminate

User re-auth

EAP Exchange

RADIUS: Access Accept: AVP=Permit Access


HTTP GET http://www.google.com

HTTP RESPONSE http://www.google.com

Client Provisioning captures user agent and MAC address from SessionID

# Probeless Profiling

## Wireless 802.1X with Posture Example

- Employee with iPad connects to corp SSID and logs in using AD account 'employee'
- Device type Unknown, so hit Emp_NonCompliant rule.
- Employee redirected to Client Provisioning/Posture
- OS detection performed to determine CP policy
- User agent captured—iPad not supported for posture agent so ISE send CoA w/session terminate.
- Endpoint user-agent and other data written to db using MAC address from Session ID lookup→Profile=iPad!
- On reconnect, match profile=iDevice and Employee.

Matched AuthC Rule = Dot1X

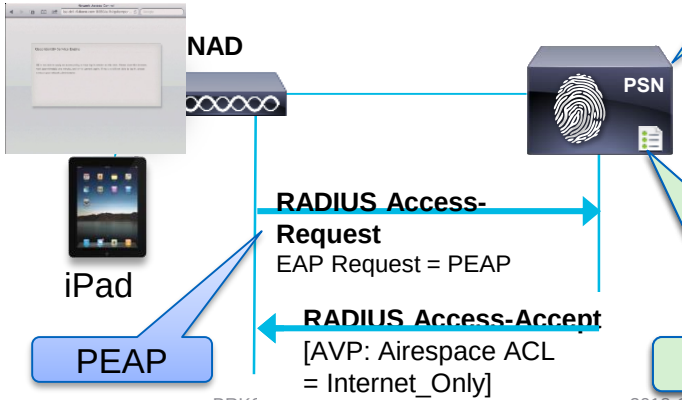
Authentication Policy

| Rule Name | | Conditions | | Identity Source |
|---|---|---|---|---|
| MAB | if | Wireless_MAB | then | Internal Endpoints |
| Dot1X | If | Wireless_802.1X | then | AD1 |
| Default | if | <no match> | then | AD1_Internal |

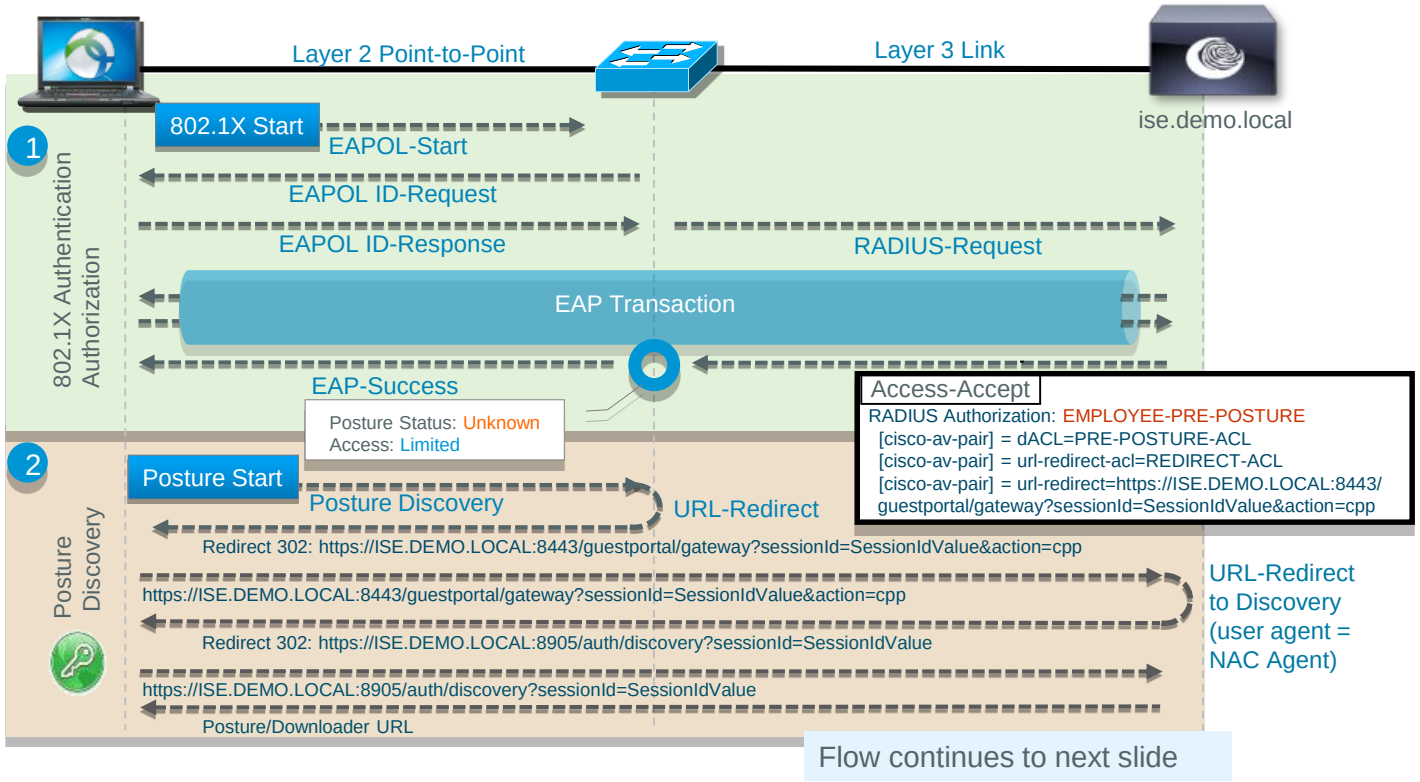
Endpoint Profile = iPad

Authorization Policy

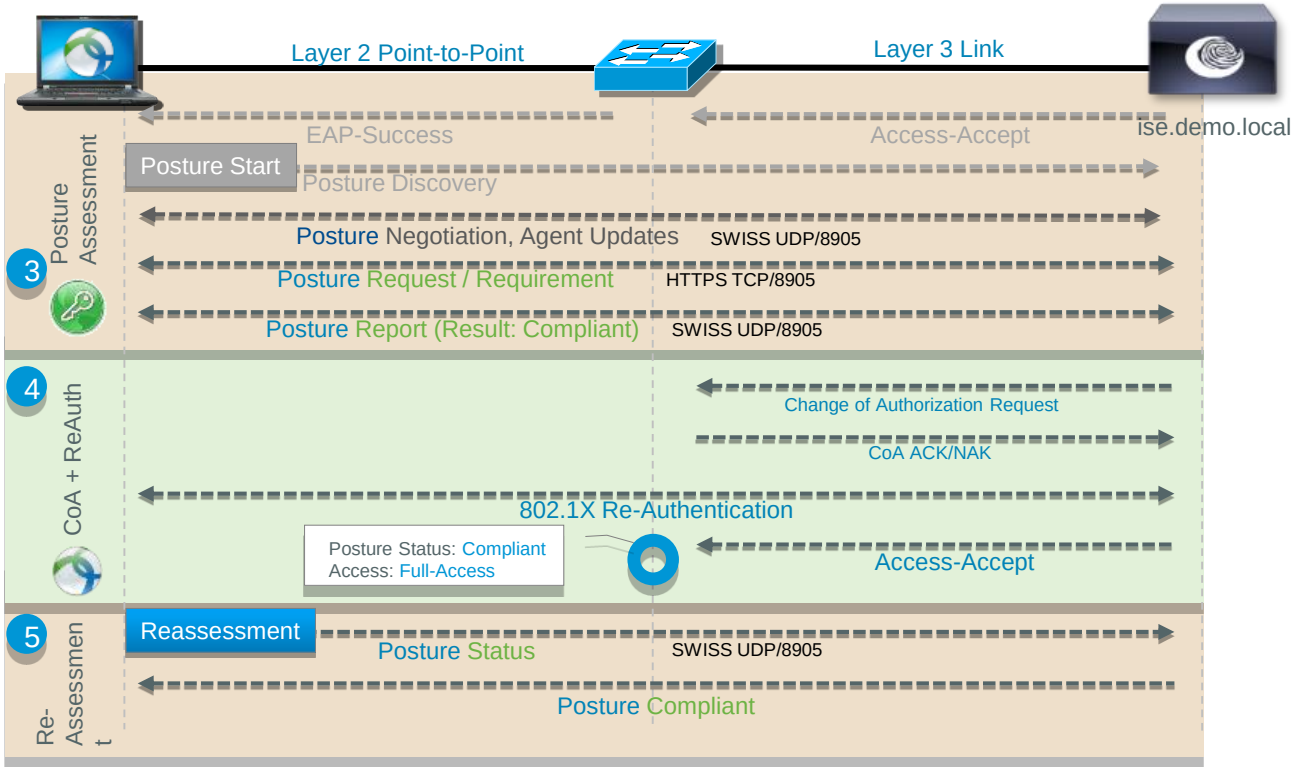
| Name | | Conditions | | Permissions |
|---|---|---|---|---|
| IP Phones | if | Cisco-IP-Phone | then | Cisco_IP_Phone |
| BYOD | if | iDevice and Employee | then | Internet |
| Employee | if | PC and Employee | then | Full_Access |
| Guest | if | Guest | then | Internet |
| Emp_NonCompliant | | Employee and Compliant | then | Posture |
| Default | If | <no | then | CWA_Posture |



# 802.1X End User Authentication with Posture



# 802.1X End User Authentication with Posture



# Adding Posture to the Authorization Policy

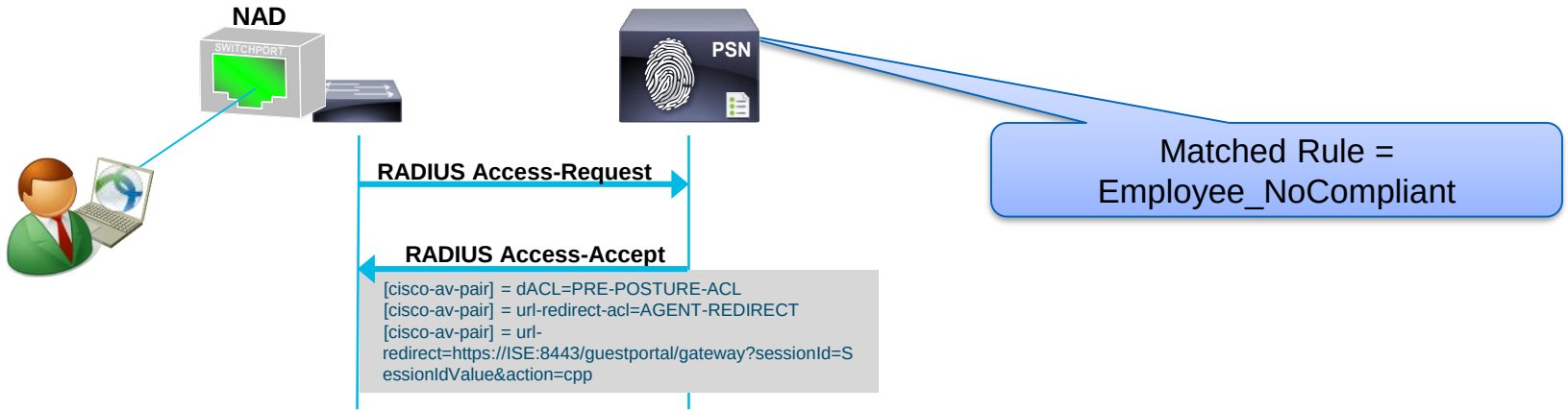
**AGENT-REDIRECT (local to Switch)**

```
ip access-list extended AGENT-REDIRECT
 deny   udp any any eq domain
 permit tcp any any eq www
```

**PRE-POSTURE-ACL (downloaded)**

```
permit udp any any eq domain
permit icmp any any
permit tcp any host 10.1.1.3 eq 8443
permit tcp any host 10.1.1.3 eq 8905
permit udp any host 10.1.1.3 eq 8905
permit tcp any any eq 80
permit tcp any any eq 443
```

| Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|
| IP Phones | if | Cisco-IP-Phone | then | Cisco_IP_Phone |
| Employee_ NoCompliant | if | Employee & Posture != Compliant | then | Posture |
| Employee | if | Employee & Posture = Compliant | then | Employee |
| GUEST | if | GUEST | then | GUEST |
| Default | If no matches, then | | WEBAUTH | |

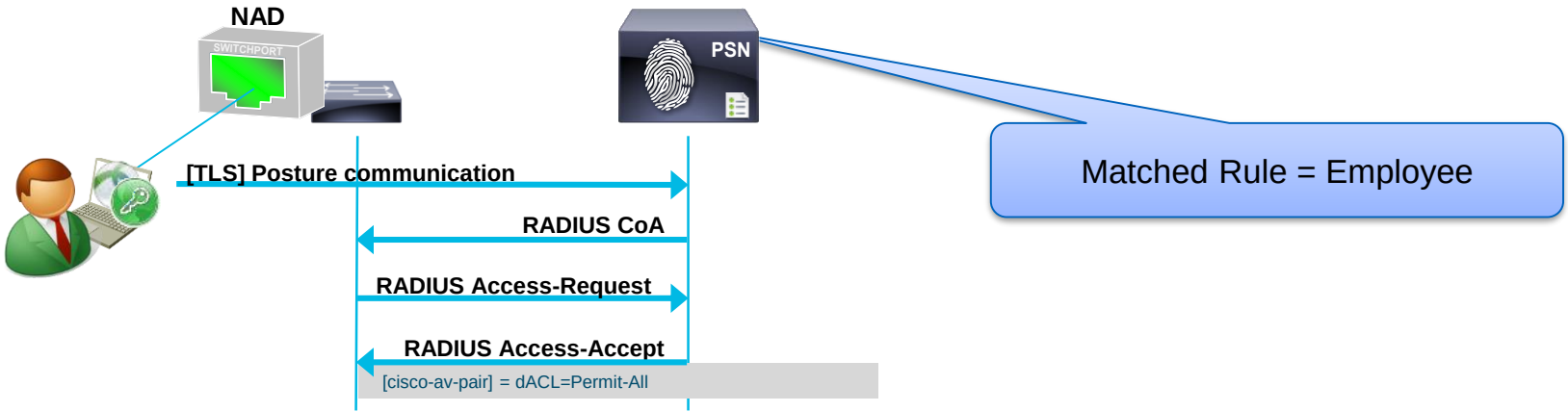


# Adding Posture to the Authorization Policy

**Permit-All (downloaded ACL)**

permit ip host any

| Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|
| IP Phones | if | Cisco-IP-Phone | then | Cisco_IP_Phone |
| Employee_ NoCompliant | if | Employee & Posture != Compliant | then | Posture |
| Employee | if | Employee & Posture = Compliant | then | Employee |
| GUEST | if | GUEST | then | GUEST |
| Default | If no matches, then | | WEBAUTH | |

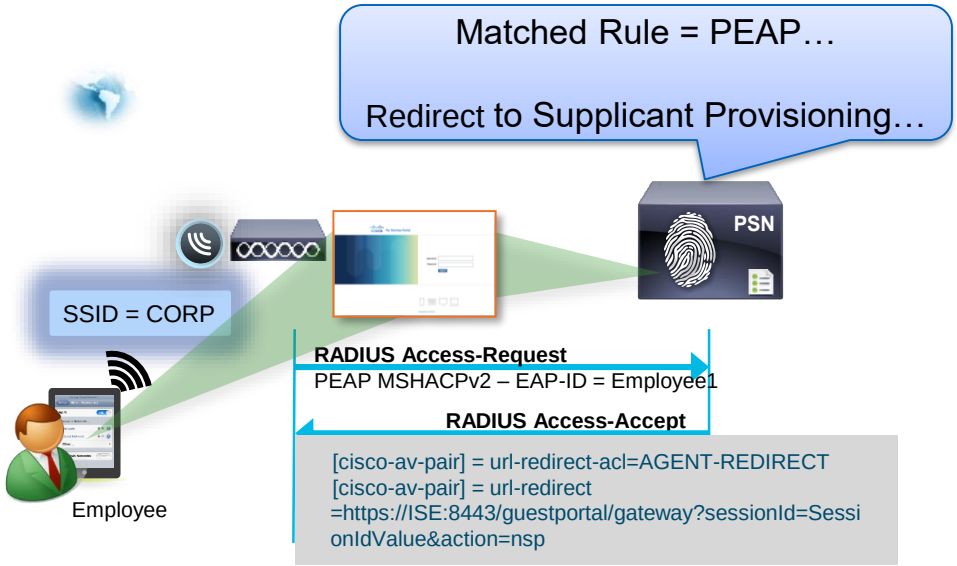


# BYOD AuthZ Policy

## Single SSID – Employee using PEAP

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

| Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|
| GUEST | if | GUEST | then | GUEST |
| Open Rule | if | Wireless_MAB | then | WEBAUTH |
| PEAP | if | Network Access:EapTunnel EQUALS PEAP | then | Supp-Provision |
| Employee | if | Employee & EAP-TLS & Certificate SAN = MAC_Addr | then | Employee |
| Default | If no matches, then | | Deny Access | |

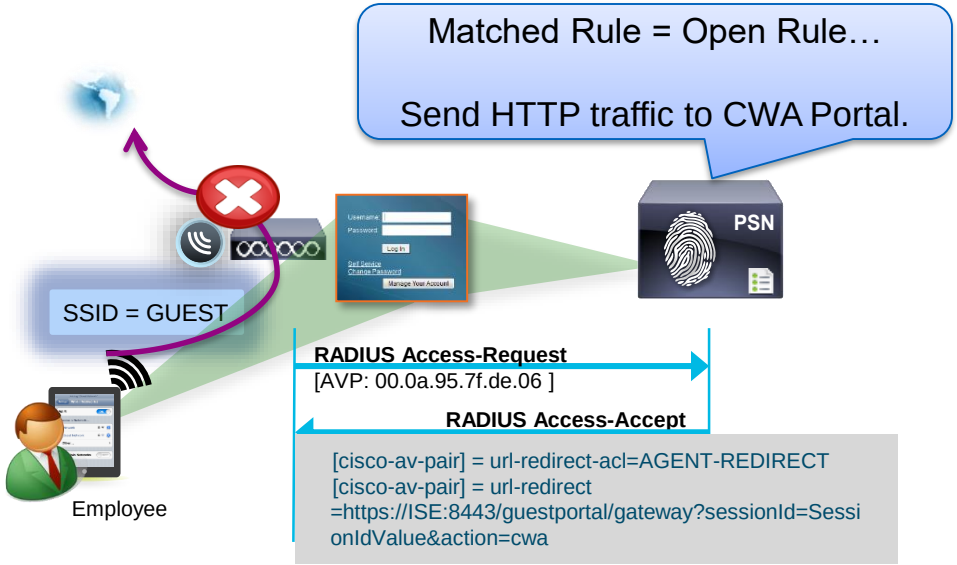


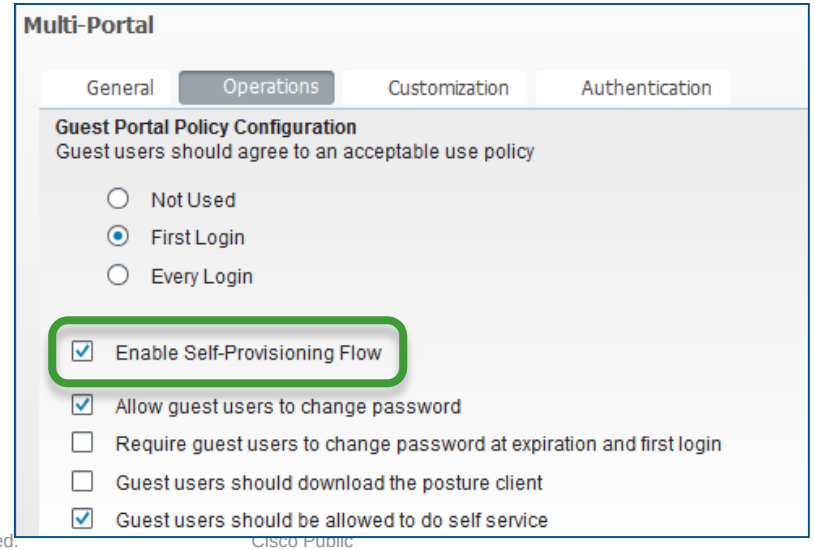
# BYOD AuthZ Policy

## Dual SSID – Employee using CWA

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

| Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|
| GUEST | if | GUEST | then | GUEST |
| Open Rule | if | Wireless_MAB | then | WEBAUTH |
| PEAP | if | Network Access:EapTunnel EQUALS PEAP | then | Supp-Provision |
| Employee | if | Employee & EAP-TLS & Certificate SAN = MAC_Addr | then | Employee |
| Default | If no matches, then | | Deny Access | |



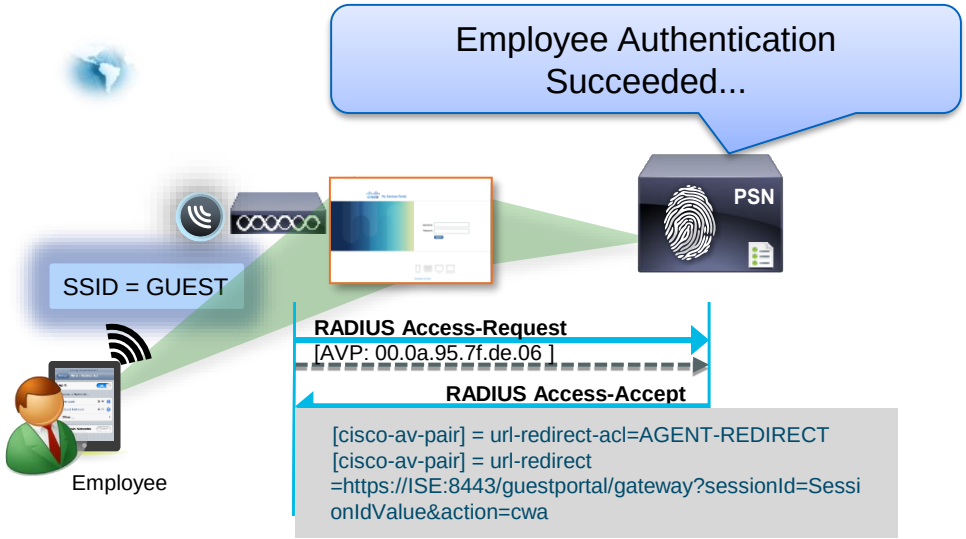



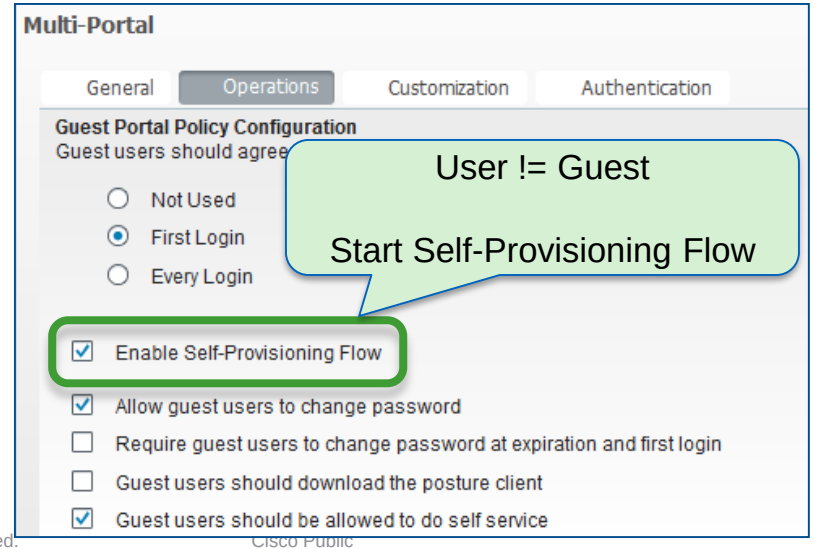
# BYOD AuthZ Policy

## Dual SSID – Employee using CWA

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

| Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|
| GUEST | if | GUEST | then | GUEST |
| Open Rule | if | Wireless_MAB | then | WEBAUTH |
| PEAP | if | Network Access:EapTunnel EQUALS PEAP | then | Supp-Provision |
| Employee | if | Employee & EAP-TLS & Certificate SAN = MAC_Addr | then | Employee |
| Default | If no matches, then | | Deny Access | |



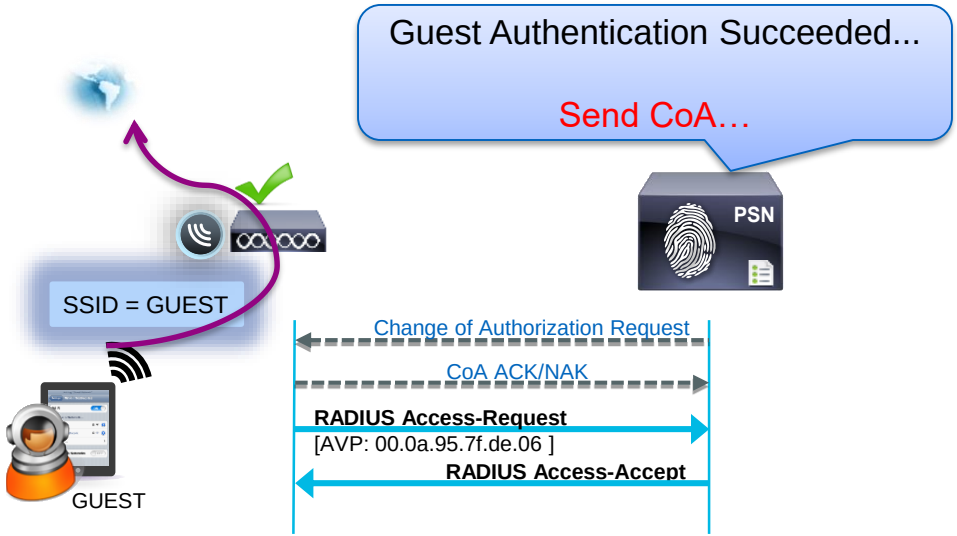



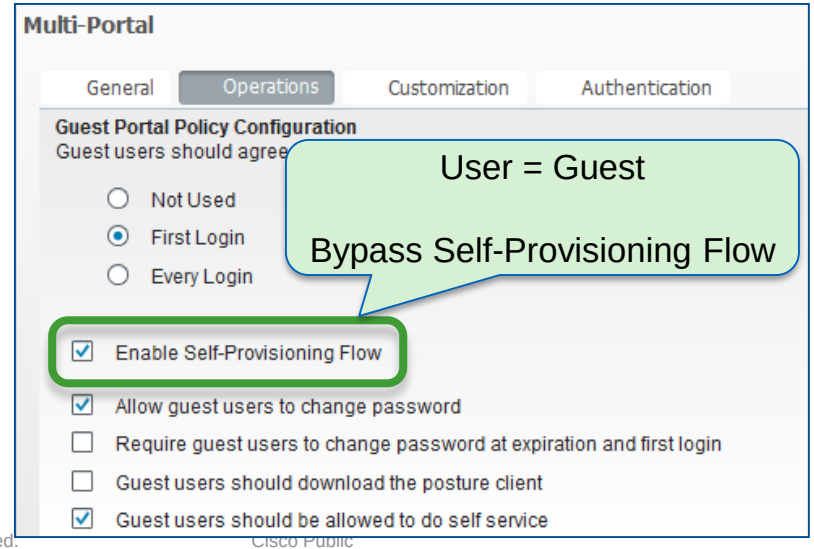
# BYOD AuthZ Policy

## Dual SSID – Guest using CWA

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

| Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|
| GUEST | if | GUEST | then | GUEST |
| Open Rule | if | Wireless_MAB | then | WEBAUTH |
| PEAP | if | Network Access:EapTunnel EQUALS PEAP | then | Supp-Provision |
| Employee | if | Employee & EAP-TLS & Certificate SAN = MAC_Addr | then | Employee |
| Default | If no matches, then | | Deny Access | |

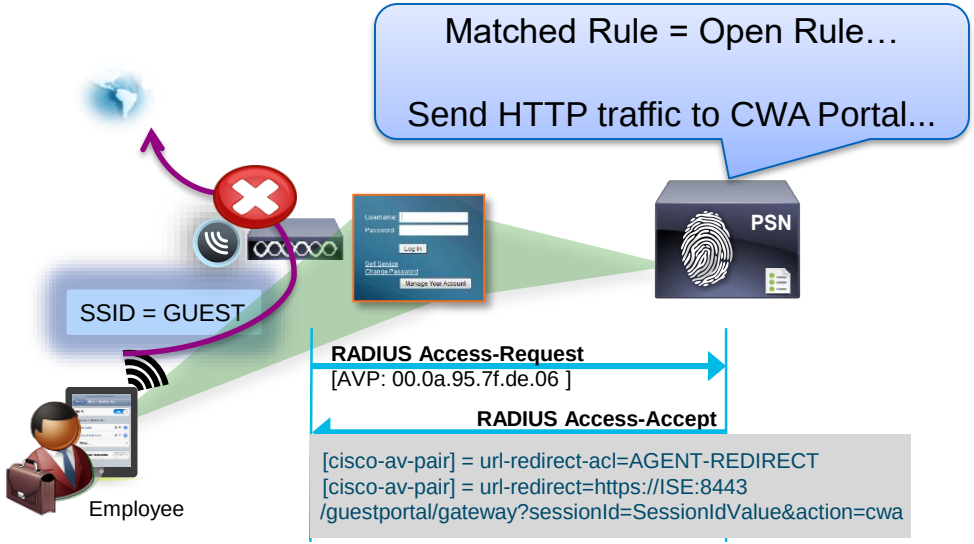


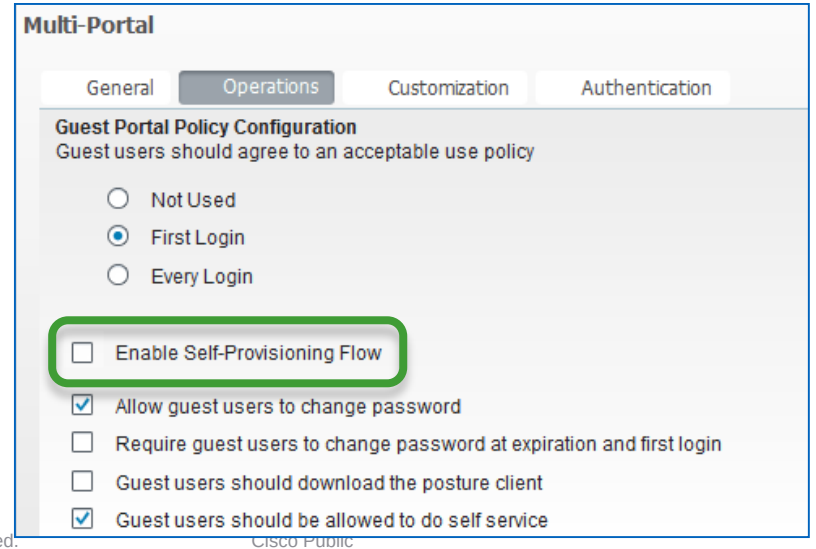
# BYOD AuthZ Policy

## Dual SSID – Select Employees using CWA

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.




| Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|
| GUEST | if | GUEST | then | GUEST |
| EmpWebAuth | if | Employee & Guest-Flow | then | Supp-Provision |
| Open Rule | if | Wireless_MAB | then | WEBAUTH |
| PEAP | if | Network Access:EapTunnel EQUALS PEAP | then | Supp-Provision |
| Employee | if | Employee & EAP-TLS & Certificate SAN = MAC_Addr | then | Employee |
| Default | If no matches, then | | Deny Access | |

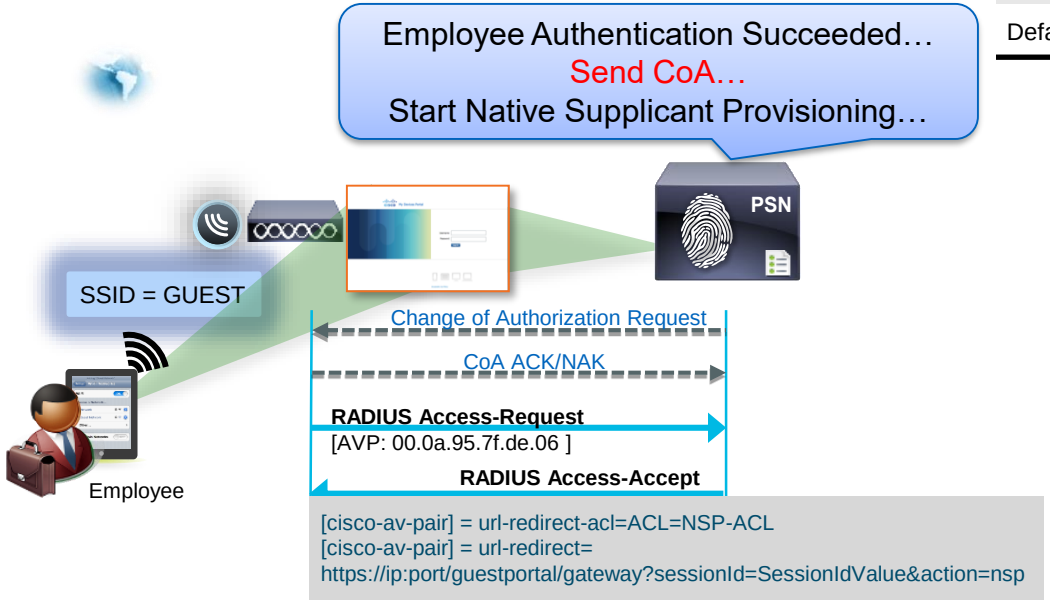


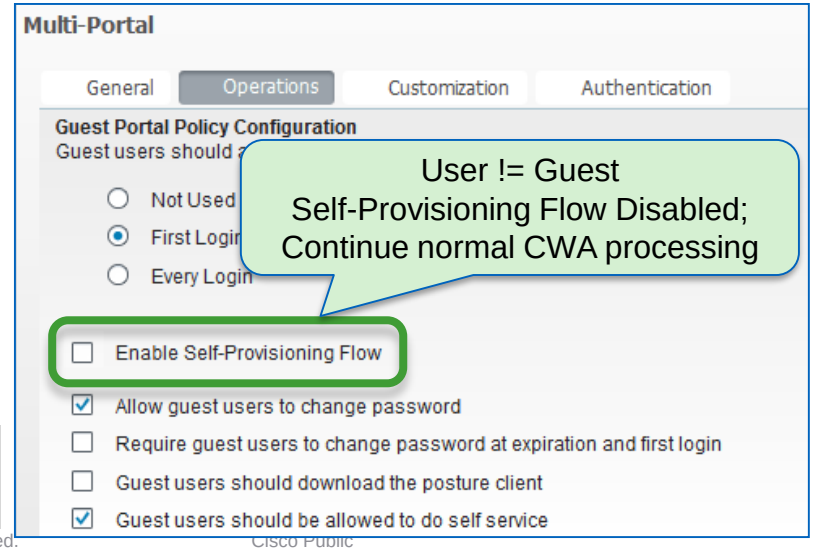
# BYOD AuthZ Policy

## Dual SSID – Select Employees using CWA

1. Any PEAP authentications:
   - Send directly to Native Supplicant Provisioning.
2. Add CWA to Open SSID
   - Need to know who they are, and IF we should provision them.

| Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|
| GUEST | if | GUEST | then | GUEST |
| EmpWebAuth | if | Employee & Guest-Flow | then | Supp-Provision |
| Open Rule | if | Wireless_MAB | then | WEBAUTH |
| PEAP | if | Network Access:EapTunnel EQUALS PEAP | then | Supp-Provision |
| Employee | if | Employee & EAP-TLS & Certificate SAN = MAC_Addr | then | Employee |
| Default | If no matches, then | | Deny Access | |



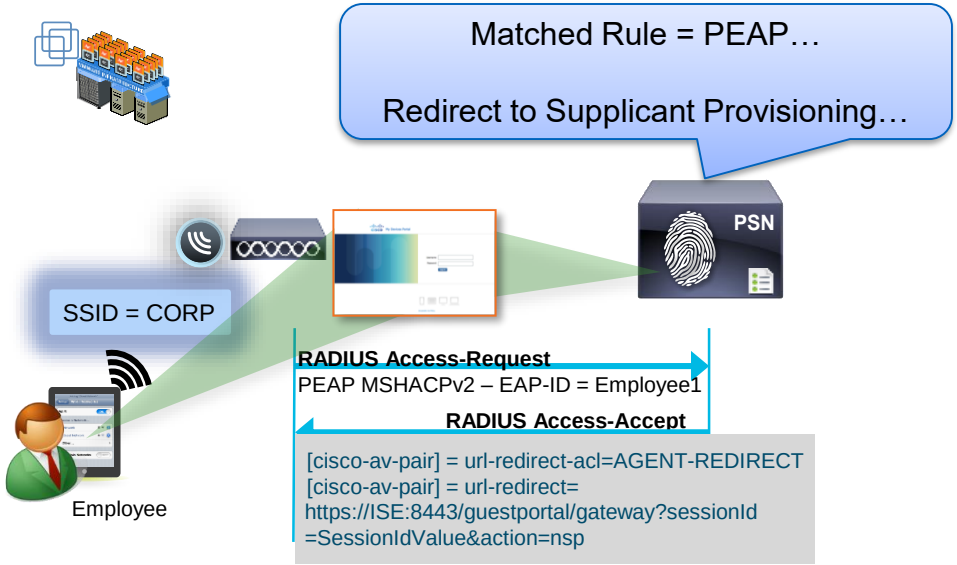



# BYOD AuthZ Policy

## Post-Supplicant Provisioning

1. Trigger Native Supplicant Provisioning
   - PEAP-MSCHAPv2 (Single SSID)
   - CWA to Open SSID (Dual SSID)
2. Reconnect using EAP-TLS

| Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|
| GUEST | if | GUEST | then | GUEST |
| Open Rule | if | Wireless_MAB | then | WEBAUTH |
| PEAP | if | Network Access:EapTunnel EQUALS PEAP | then | Supp-Provision |
| Employee | if | Employee & EAP-TLS & Certificate SAN = MAC_Addr | then | Employee |
| Default | If no matches, then | | Deny Access | |

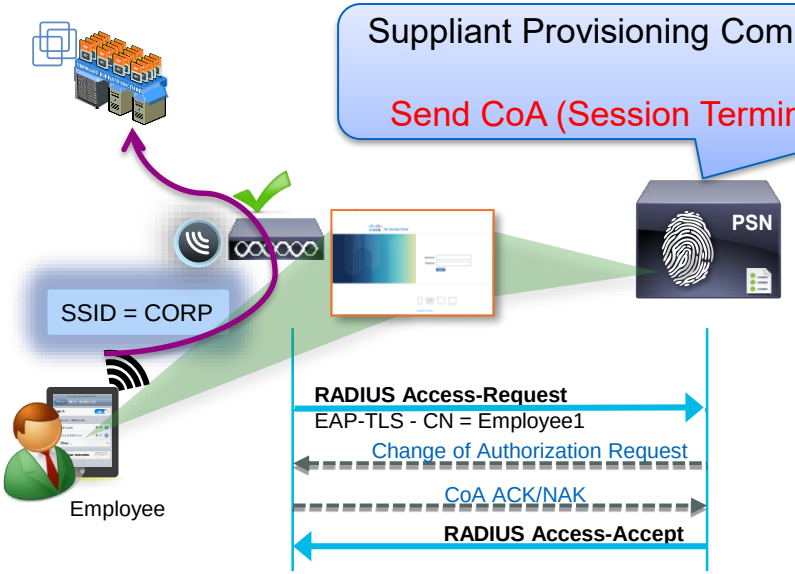


# BYOD AuthZ Policy

## Post-Supplicant Provisioning

1. Trigger Native Supplicant Provisioning
   - PEAP-MSCHAPv2 (Single SSID)
   - CWA to Open SSID (Dual SSID)
2. Reconnect using EAP-TLS

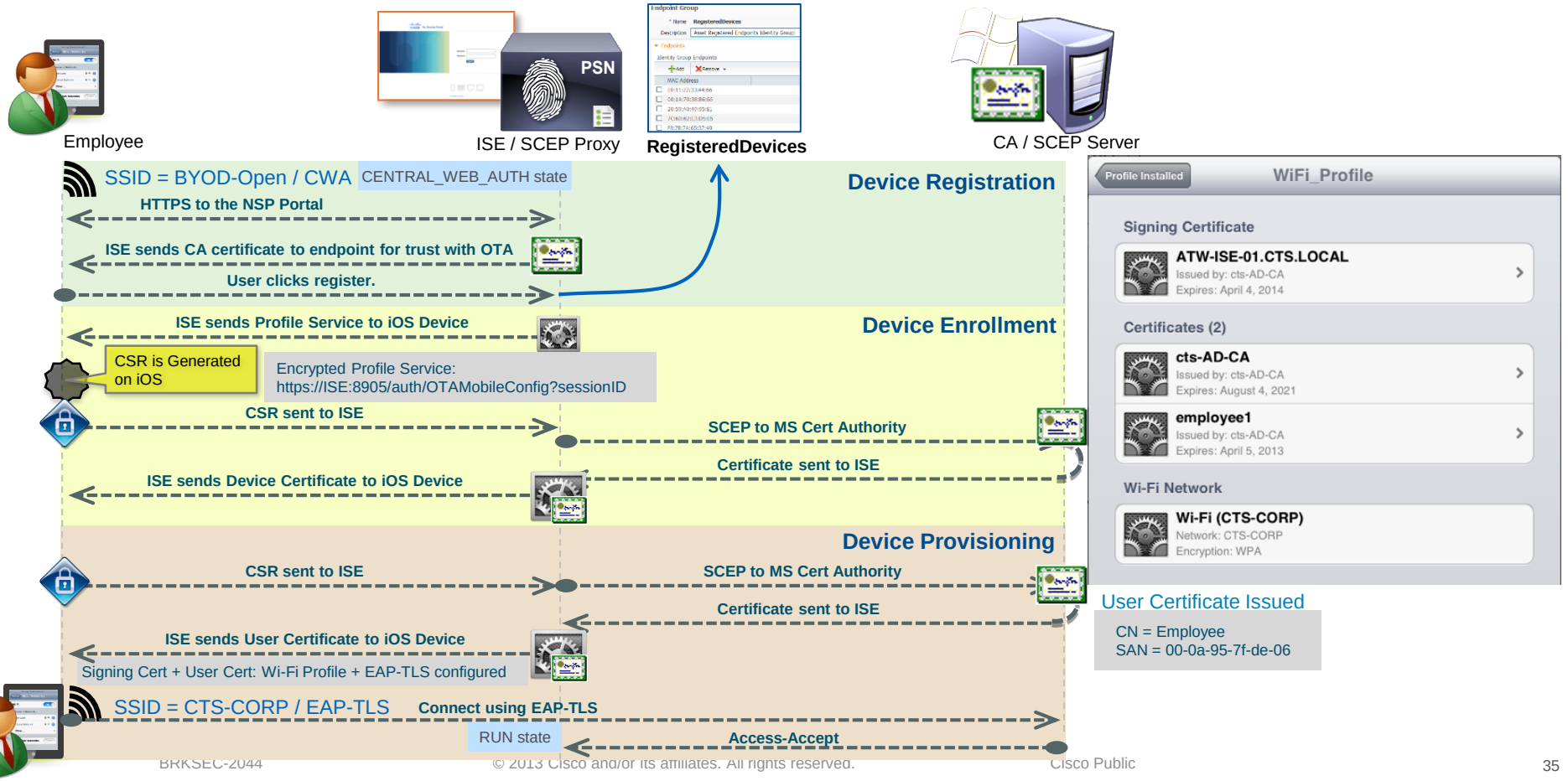
| Rule Name | | Conditions | | Permissions |
|---|---|---|---|---|
| GUEST | if | GUEST | then | GUEST |
| Open Rule | if | Wireless_MAB | then | WEBAUTH |
| PEAP | if | Network Access:EapTunnel EQUALS PEAP | then | Supp-Provision |
| Employee | if | Employee & EAP-TLS & Certificate SAN = MAC_Addr | then | Employee |
| Default | | | | ...cess |




(EndPoints:BYODRegistration EQUALS Yes AND
AD1:ExternalGroups EQUALS cts.local/Users/employees )AND
Network Access:EapAuthentication EQUALS EAP-TLS AND
Radius:Calling-Station-ID EQUALS CERTIFICATE:Subject Alternative Name )

Note: Once registered via NSP, ID group statically set to RegisteredDevices. Recommend use profile attribute, not ID groups, to match profile in Authorization Policy!

# Native Supplicant Provisioning (iOS Use-Case)



# NSP (Android Use-Case)