



Troubleshooting Guest Access

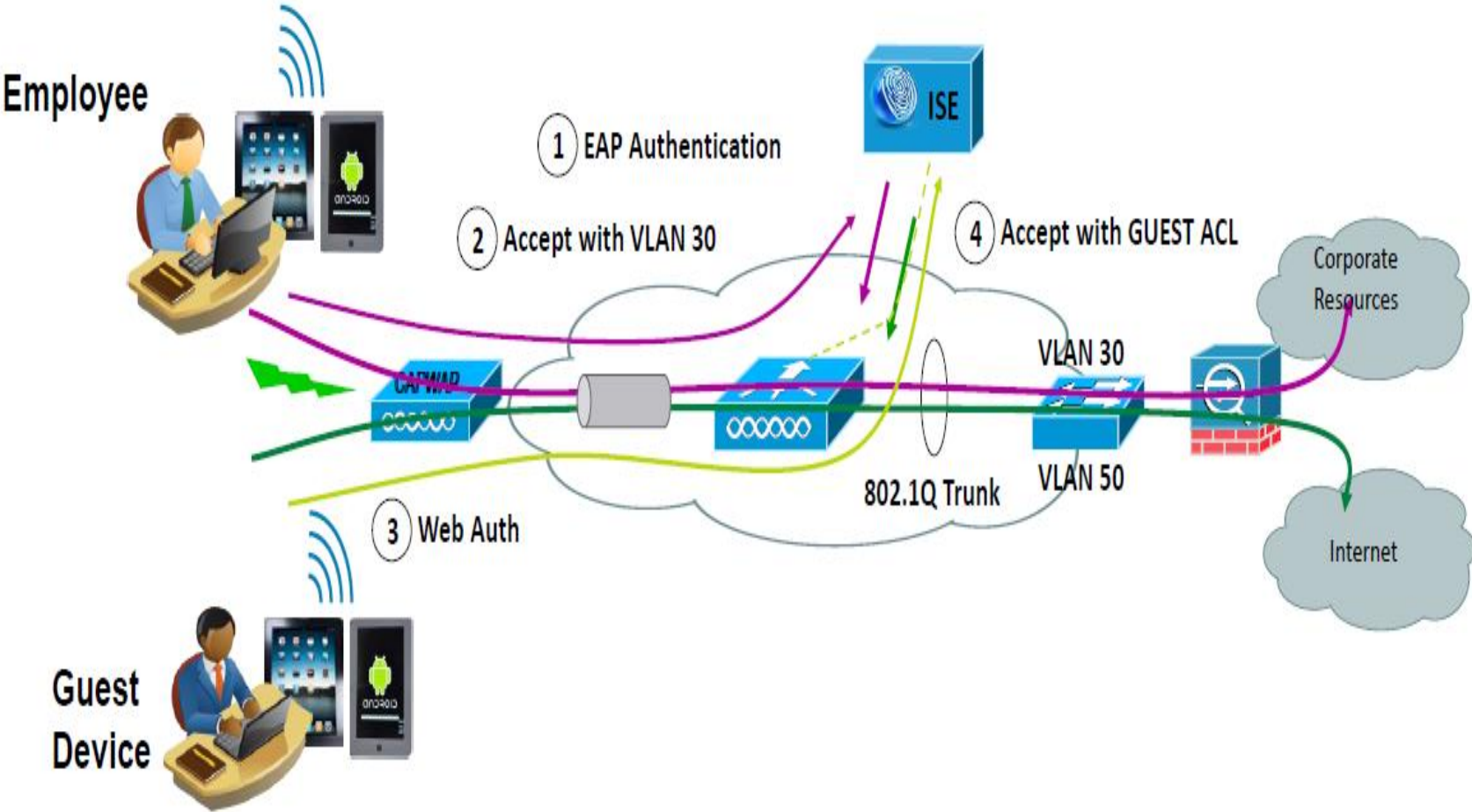
Debashree Barat

TAC Engineer - Wireless

Agenda

- Path Isolation in Guest Network
- Web-authentication – steps involved
- Troubleshooting web-authentication issues

Corporate vs Guests



Guest Access Control and Path isolation

To achieve end-to-end wireless guest traffic isolation, allowing internet access but preventing any other communications.

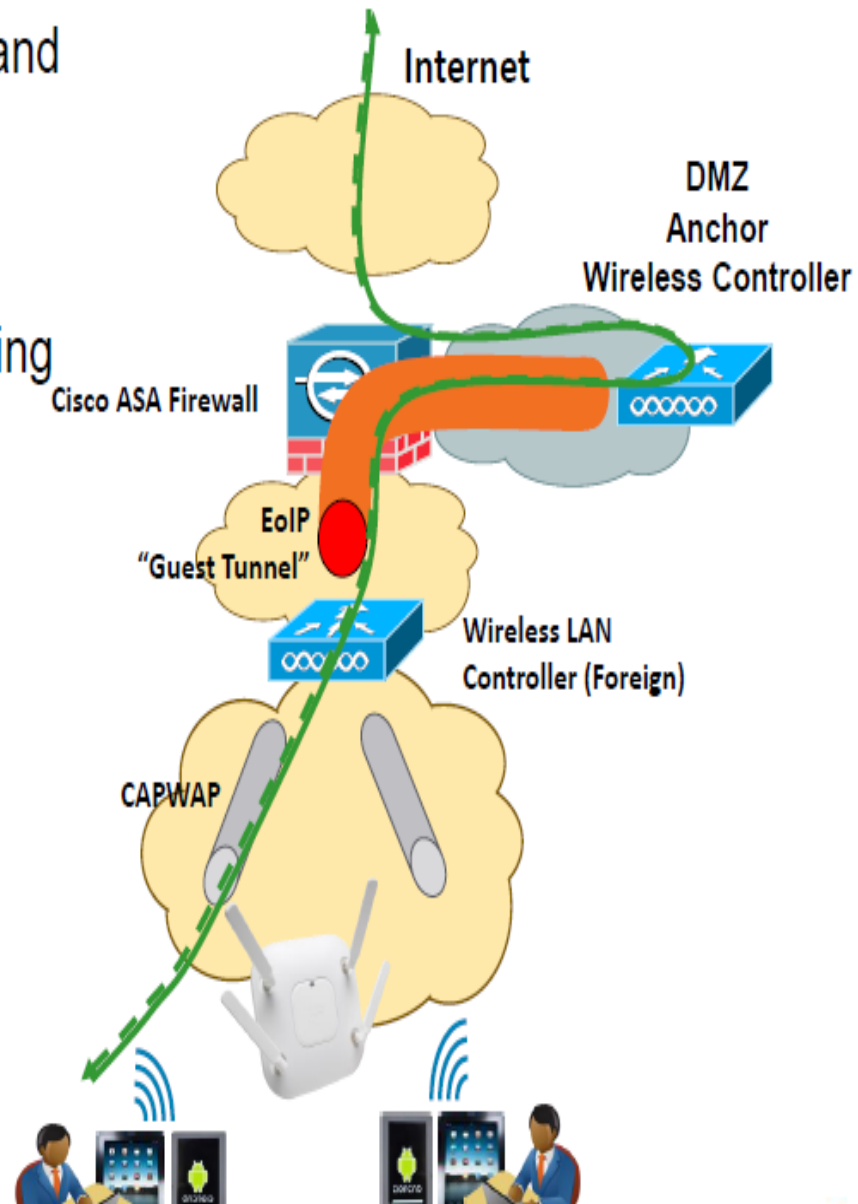
How can this be achieved as there is a single LWAPP/CAPWAP tunnel through which all the wireless traffic is sent?

Different methods to achieve this:

1. **Guest Path isolation using EOIP**: EoIP tunnels to logically segment and transport the guest traffic between remote and anchor controllers.
2. **Guest Path isolation using VRF** : Virtual Routing / Forwarding (VRF) or VRF- lite is the L3 virtualization used in Enterprise Campus networks and guest isolation will be done by VRF instances.

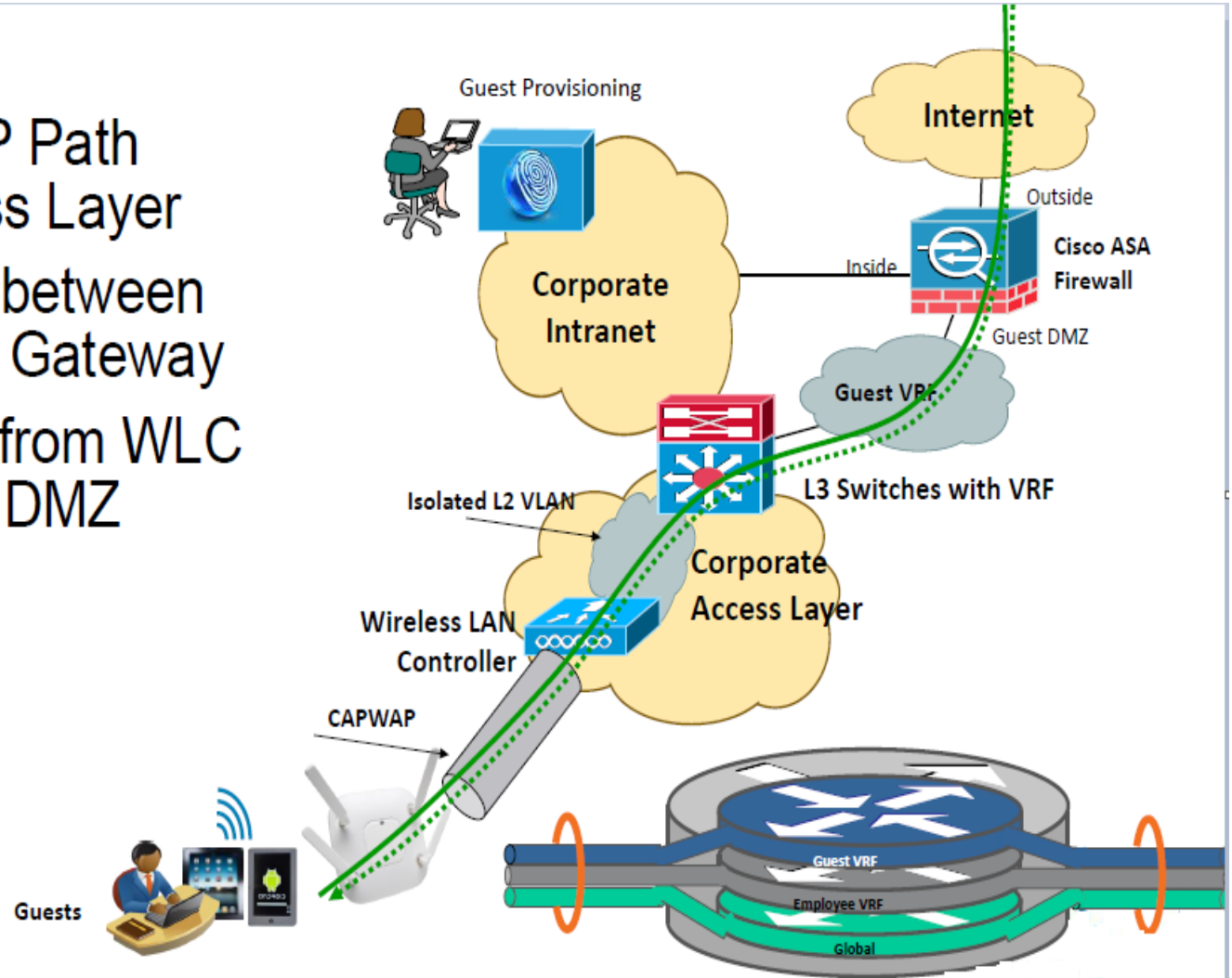
Path Isolation using EOIP

- Use of up to 71 EoIP tunnels to logically segment and transport the guest traffic between remote and anchor controllers
- Other traffic (employee for example) still locally bridged at the remote controller on the corresponding VLAN
- No need to define the guest VLANs on the switches connected to the remote controllers
- Original guest's Ethernet frame maintained across LWAPP/CAPWAP and EoIP tunnels
- Redundant EoIP tunnels to the Anchor WLC
- 2504/5508 are typical Anchor WLC's



Guest Path Isolation Using VRF

- LWAPP/CAPWAP Path Isolation at Access Layer
- L2 Path Isolation between WLC and Default Gateway
- L3 VRF Isolation from WLC to Firewall Guest DMZ interface



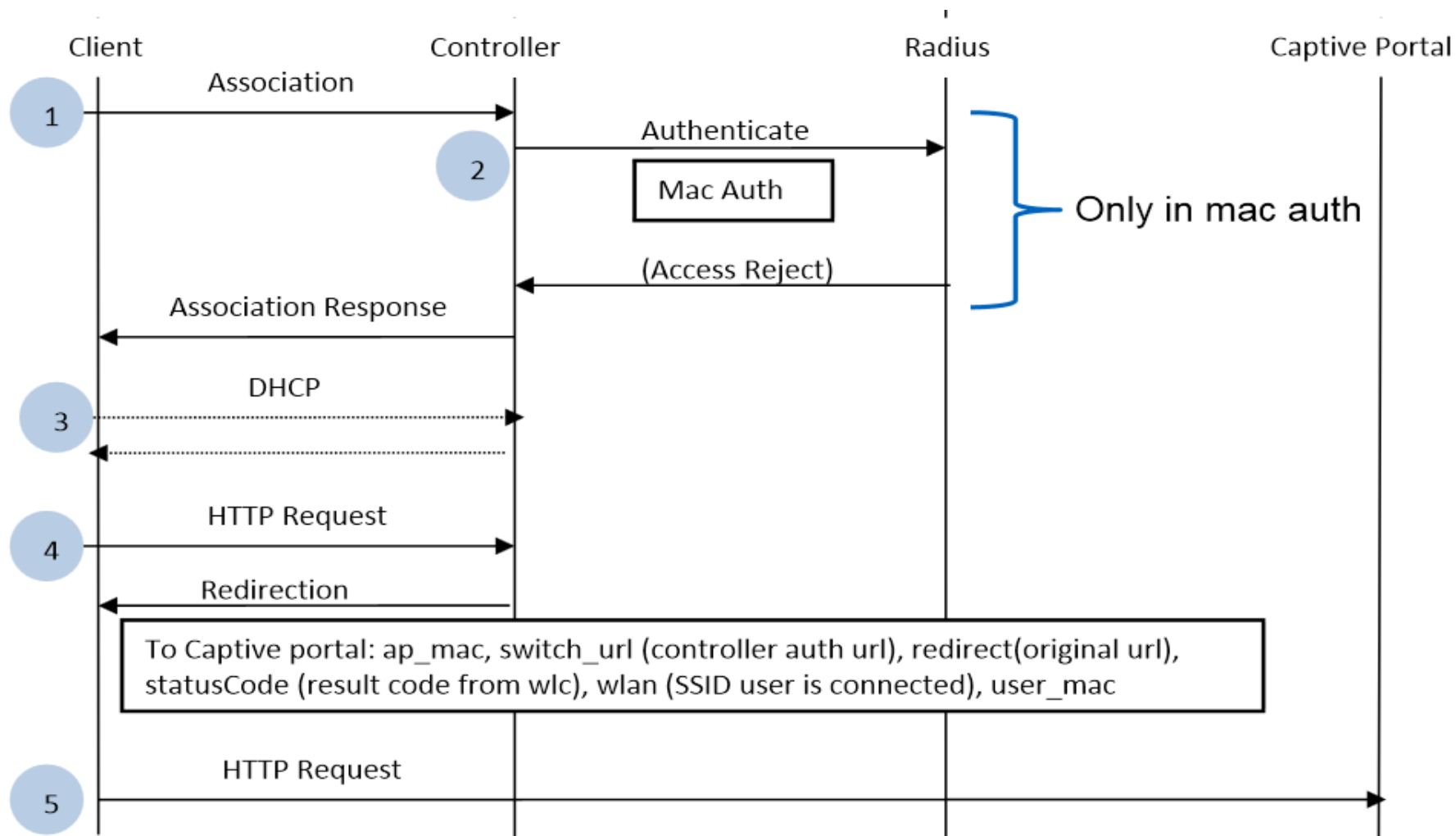
Web – Authentication (Captive Portal)

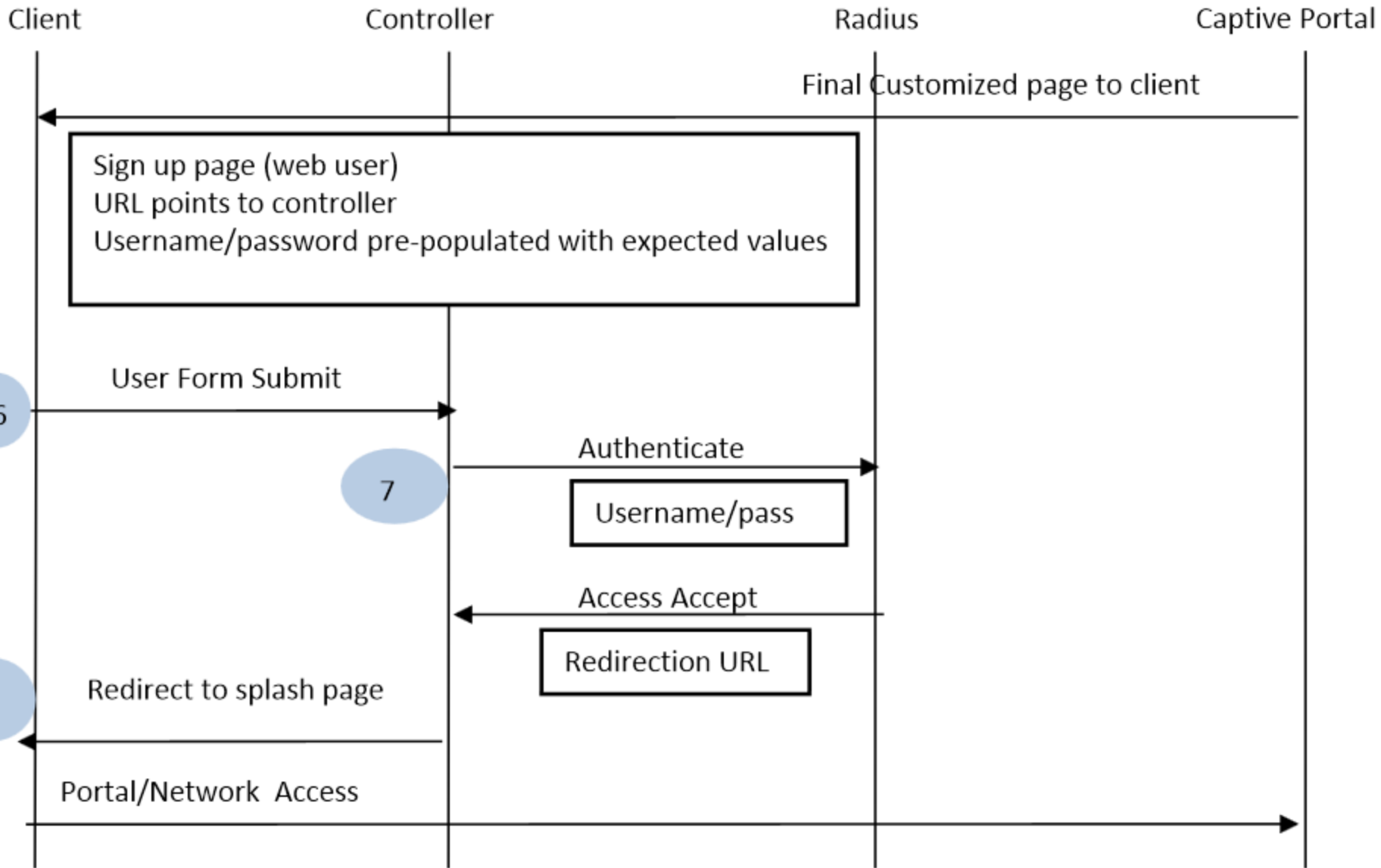
What is it and when to use it?

Web-Authentication is the Layer 3 authentication feature that causes the controller to not allow IP traffic (except DHCP and DNS -related packets) from a particular client until that client has correctly supplied a valid username and password.

It is used when users cant use 802.1X authentication and for the employees who need guest access.

Web-Authentication Process





Guest Authentication Portal

Available in 4 modes:

- Default internal web portal
- Customized (Downloaded Customised Web Pages) portal
- External Using ISE Guest Server
- External (Re-directed to external 3rd party server)

Wireless Guest Authentication Portal

Internal Web Portal

- Wireless guest user associates to the guest SSID
- Initiates a browser connection to any website
- Web login page will displayed

The screenshot shows the Cisco Web Management Interface (WMI) configuration page for the 'Web Login Page'. The 'Web Authentication Type' is set to 'Internal (Default)', and the 'Redirect URL after login' is 'www.cisco.com'. The 'Cisco Logo' is set to 'Show', the 'Headline' is 'Welcome to Cisco Live 2012!', and the 'Message' is 'THIS IS AVAILABLE TO ALL CISCO LIVE USERS...'. Below the configuration, a diagram illustrates the resulting login portal. The portal has a blue header with the Cisco logo and the word 'Login'. It features a yellow box for 'Fixed Welcome Text' containing the headline and message, and another yellow box for 'Login Credentials' containing the 'User Name' and 'Password' input fields and a 'Submit' button.

Wireless Guest Authentication Portal

Customisable Web Portal

- Create your own Guest Access Portal web pages
- Upload the customised web page to the WLC
- Configure the WLC to use “customisable web portal”
- Customised WebAuth bundle up to 5 Mb in size can contain
 - 22 login pages (16 WLANs , 5 Wired LANs and 1 Global)
 - 22 login failure pages (in WLC 5.0 and up)
 - 22 login successful pages (in WLC 5.0 and up)

GUEST PORTAL

Let Us Help

Call **877-604-1493** or [e-mail](#)
Locate [International Contacts](#)
Join a [Wireless Discussion](#)
Get [Technical Support](#)
Find a [Reseller in Your Area](#)
Manage [Your E-mail Preferences](#)

Live Discussions

can i bridge between a 12-12 :
Hi, can I make a wireless bridge between a 2142 AP and a 1131 AP?

Login

Guest Name :
Password :

Wireless Guest Authentication Portal

External Web Portal

The screenshot shows the Cisco WLC configuration interface for the 'Web Login Page'. The left sidebar shows the navigation menu with 'Security' selected. The main content area is titled 'Web Login Page' and includes a 'Preview...' button and an 'Apply' button. The configuration fields are:

- Web Authentication Type: External (Redirect to external server)
- Redirect URL after login: www.cisco.com
- External Webauth URL: https://ise-guest-server:8443/guestportal/Login.action

- Set in WLC > Security > WebAuth > Login
- Or override at Guest WLAN
 - Option to use Pre-Auth ACL

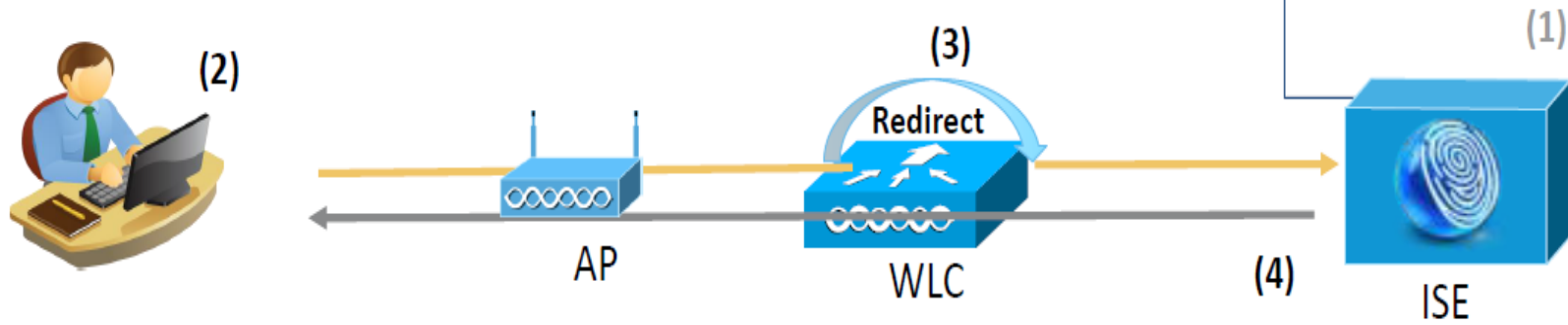
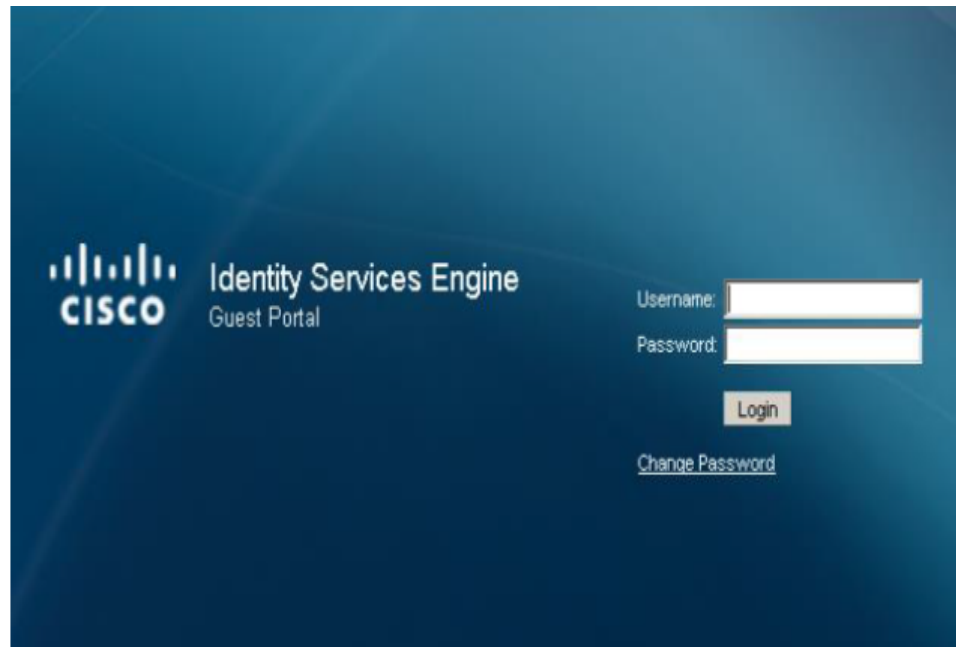
The screenshot shows the Cisco WLC configuration interface for the 'Guest WLAN'. The left sidebar shows the navigation menu with 'WLANs' selected. The main content area is titled 'WLANs > Edit 'Guest WLAN'' and includes a '< Back' button and an 'Apply' button. The configuration fields are:

- Layer 3 Security: None
- Web Policy: Web Policy
- Authentication: Authentication
- Preauthentication ACL: IPv4 ACL-REDIRECT
- Web Auth type: External(Re-redirect to external server)
- URL: https://10.10.10.60:8443/guestportal/portal.jsp

Wireless Guest

Centralised Login Page

- 1) Administrator Creates WLAN Login Page on ISE
- 2) Wireless Guest Opens Web browser
- 3) Web traffic is intercepted by Wireless LAN Controller and redirected to Guest Server.
- 4) Guest Server returns centralised login page



External Redirect Using ISE

Central Web-Authentication(CWA):

Steps Involved in this method are:

- User associate to the Web Auth SSID
- User starts its browser
- The WLC Redirect to the guest portal (ISE)
- The user authenticate on the portal
- The ISE send a Radius Change Of Authorization (CoA - UDP Port 3799) to indicate to the controller that the user is valid, and eventually push radius attributes (ACL for example).
- The User is prompted to retry his original URL

Troubleshooting Web-Authentication Issues

Webauth Redirect Logs

*pemReceiveTask: Jan 02 10:45:30.824: 68:7f:74:75:f1:cd 192.168.50.101 Added NPU entry of type 2, dtlFlags

captive-bypass detection disabled, Not checking for wispr in HTTP GET, client mac=68:7f:74:75:f1:cd

Preparing redirect URL according to configured Web-Auth type

Checking custom-web config for WLAN ID:2

unable to get the hostName for virtual IP, using virtual IP =1.1.1.1

Global status is enabled, checking on web-auth type

Web-auth type **Internal**, no further redirection needed. Presenting default login page to user

http_response_msg_body1 is <HTML><HEAD><TITLE> Web Authentication Redirect</TITLE><META http-equiv="Cache-control" content="no-cache"><META http-equiv="Pragma" content="

http_response_msg_body2 is "></HEAD></HTML>

parser host is 192.168.0.45

- parser path is /

added redirect=, URL is now https://1.1.1.1/login.html?

str1 is now https://1.1.1.1/login.html?redirect=192.168.0.45/

clen string is Content-Length: 302

Message to be sent is

HTTP/1.1 200 OK

Location: https://1.1.1.1/login.html?redirect=192.168.0.45/

Content-Type: text/html

Content-Length: 302

<HTML><HEAD><TITLE>

Webauth Redirect – IPv6

```
webauthRedirect: Jan 02 14:57:23.734: 28:37:37:7f:5c:7- str1 is now  
https://[::FFFF:1.1.1.1]/login.html?redirect=www.apple.com/library/test/success.html  
*webauthRedirect: Jan 02 14:57:23.734: 28:37:37:7f:5c:7- clen string is Content-Length: 337
```

```
*webauthRedirect: Jan 02 14:57:23.734: 28:37:37:7f:5c:7- Message to be sent is  
HTTP/1.1 200 OK  
Location: https://[::FFFF:1.1.1.1]/login.html?redirect=www.apple.com/library/test/success.html  
Content-Type: text/html  
Content-L  
*webauthRedirect: Jan 02 14:57:23.734: 28:37:37:7f:5c:7- send data length=498
```

Webauth Redirect

- Login page requested over https

```
*emWeb: Jan 02 10:45:53.334:
```

```
ewaURLHook: Entering:url=/login.html, virtIp = 1.1.1.1, ssl_connection=1, secureweb=1
```

```
*emWeb: Jan 02 10:45:53.334: WLC received client 68:7f:74:75:f1:cd request for Web-Auth page /login.html
```

```
*emWeb: Jan 02 10:45:53.335: WLC received client 68:7f:74:75:f1:cd request for Web-Auth page /login.html
```

```
...
```

```
*emWeb: Jan 02 10:45:53.335: WLC received client 68:7f:74:75:f1:cd request for Web-Auth page /login.html
```

Webauth Success

*emWeb: Jan 02 10:46:42.904:

ewaURLHook: Entering:url=/login.html, virtIp = 1.1.1.1, ssl_connection=1, secureweb=1

*ewmwebWebauth1: Jan 02 10:46:42.905: 68:7f:74:75:f1:cd Username entry (cisco) created for mobile, length = 5

*ewmwebWebauth1: Jan 02 10:46:42.905: 68:7f:74:75:f1:cd Username entry (cisco) created in mscb for mobile, length = 5

*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd 192.168.50.101 WEBAUTH_REQD (8) Change state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)

*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd apfMsRunStateInc

*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd 192.168.50.101 WEBAUTH_NOL3SEC (14) Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)

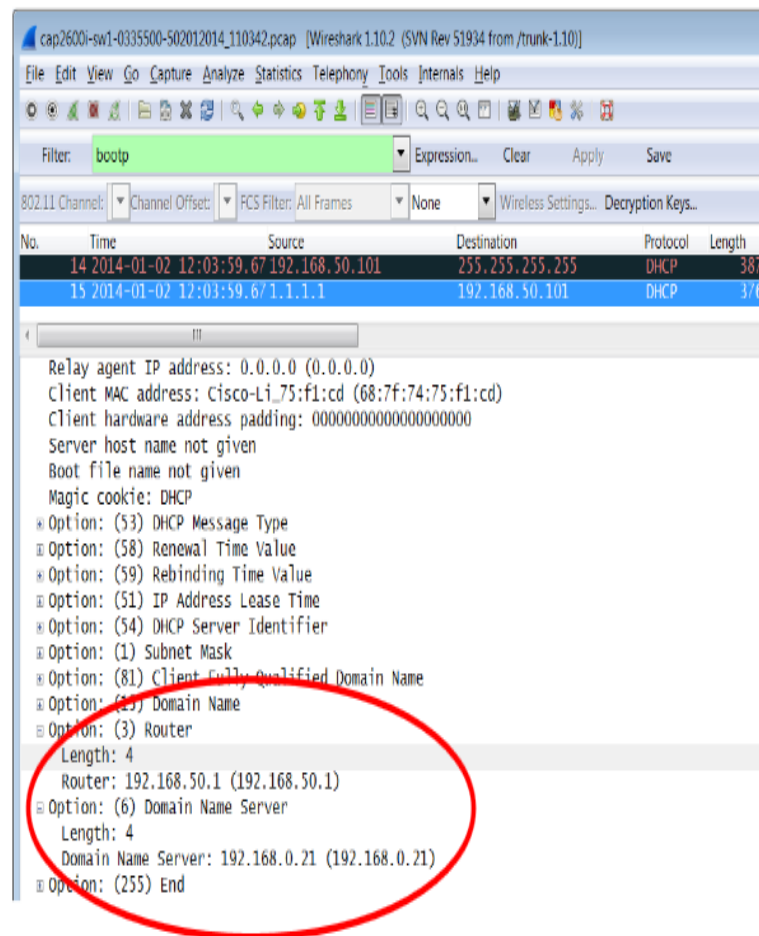
*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd Session Timeout is 1800 - starting session timer for the mobile

*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd 192.168.50.101 **RUN (20)** Reached PLUMBFASPATH: from line 6550

*ewmwebWebauth1: Jan 02 10:46:42.906: 68:7f:74:75:f1:cd 192.168.50.101 RUN (20) Replacing Fast Path rule

Web-auth Issues

- No DNS resolution
- No default GW
- Client doing request on different port
 - No HTTPS, or using 8000, etc.



Web-auth Issues

- No Preauth-ACL

- Server IP must be allowed on the preauth ACL... otherwise, loop!

```
*webauthRedirect: Jan 02 12:27:08.254: 68:7f:74:75:f1:cd- Web-auth type External, using  
URL:http://192.168.0.21/login.htm
```

```
..
```

```
*webauthRedirect: Jan 02 12:27:08.255: 68:7f:74:75:f1:cd- parser host is 192.168.0.21
```

```
*webauthRedirect: Jan 02 12:27:08.255: 68:7f:74:75:f1:cd- parser path is /
```

```
*webauthRedirect: Jan 02 12:27:08.255: 68:7f:74:75:f1:cd- added redirect=, URL is now
```

```
http://192.168.0.21/login.htm?switch\_url=https://1.1.1.1/login.html&ap\_mac=04:da:d2:4f:f0:50&client\_mac=68:7f:74:75:f1:cd&wlan=webauth&
```

NEXT:

```
*webauthRedirect: Jan 02 12:27:08.332: 68:7f:74:75:f1:cd- parser host is 192.168.0.21
```

```
*webauthRedirect: Jan 02 12:27:08.255: 68:7f:74:75:f1:cd- parser path is /
```

```
*webauthRedirect: Jan 02 12:27:08.332: 68:7f:74:75:f1:cd- added redirect=, URL is now
```

```
...
```

```
*webauthRedirect: Jan 02 12:27:08.332: 68:7f:74:75:f1:cd- str1 is now
```

```
http://192.168.0.21/login.htm?switch\_url=https://1.1.1.1/login.html&ap\_mac=04:da:d2:4f:f0:50&client\_mac=68:7f:74:75:f1:cd&wlan=webauth&redirect=192.168.0.21/
```

Web-auth Issues

- Untrusted Cert
 - Specially important when using ISE or any other external web server
 - Depending on client type/version:
 - External server not displayed
 - Authentication form not posted -> wlc sends internal page
 - Nothing is sent -> “client hangs”

Web-auth Takeaways

- If using external webauth
 - Certificate trust is critical (both WLC and external server). If suspected test with https disabled
 - Preauth ACL
- ARP/DNS must work before you can do anything
- Additional debug needed
 - debug web-auth redirect enable mac XX
- Client side capture/logs may be needed

Measures to take while Central webauth

- It is important to note that the client moves into RUN state on the foreign WLC. However, the correct status of the client can be seen only on the anchor. Below is a snippet of the **show client detail** output collected from the foreign at this point of time (only relevant information is shown):

```
Client MAC Address..... 00:17:7c:2f:b8:6e
Client Username ..... 00-17-7C-2F-B8-6E
AP MAC Address..... dc:a5:f4:ec:df:30
BSSID..... dc:a5:f4:ec:df:34
IP Address..... Unknown
Gateway Address..... Unknown
Netmask..... Unknown
Mobility State..... Export Foreign
Mobility Anchor IP Address..... 10.105.132.141
Policy Manager State..... RUN
Policy Manager Rule Created..... Yes
AAA Override ACL Name..... REDIRECT
AAA URL
redirect.....https://10.106.73.98:8443/guestportal/gatewayse
ssionId=0a6984a00000004c536bac7b&action=cwa
```

Authentication logs after Web Redirect

- It is important to note that the authentication part in the webauth process is handled at the foreign WLC and not at the anchor in a CWA setup. We can see the same in the **debug aaa** outputs on the foreign:
 - *aaaQueueReader: May 08 12:11:11.537: AuthenticationRequest: 0x2b6c0a78
 - *aaaQueueReader: May 08 12:11:11.537: Callback.....0x10166e78
 - *aaaQueueReader: May 08 12:11:11.537: protocolType.....0x40000001
 - *aaaQueueReader: May 08 12:11:11.537: proxyState.....00:17:7C:2F:B8:6E-00:00
 - *aaaQueueReader: May 08 12:11:11.537: Packet contains 12 AVPs (not shown)

Authorization response from ISE:

```
*radiusTransportThread: May 08 12:11:11.552: AuthorizationResponse: 0x14c47c58
*radiusTransportThread: May 08 12:11:11.552: structureSize.....252
*radiusTransportThread: May 08 12:11:11.552: resultCode.....0
*radiusTransportThread: May 08 12:11:11.552: protocolUsed.....0x00000001
*radiusTransportThread: May 08 12:11:11.552: proxyState.....00:17:7C:2F:B8:6E-00:00
*radiusTransportThread: May 08 12:11:11.552: Packet contains 6 AVPs:
*radiusTransportThread: May 08 12:11:11.552: AVP[01] User-Name.....deb0001 (8 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[02]
State.....ReauthSession:0a6984a00000004c536bac7b (38 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[03]
Class.....CACs:0a6984a00000004c536bac7b:sid-ise-1-2/188796966/40 (54 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[04] Session-Timeout.....0x00006e28 (28200) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[05] Termination-Action.....0x00000000 (0) (4 bytes)
*radiusTransportThread: May 08 12:11:11.552: AVP[06] Message-Authenticator.....DATA (16 bytes)
```

Authentication Verification for CWA

- Verify that authentication is complete is by verifying the passed logs on ISE and by collecting the output of show client detail on the controller which should show the client in 'RUN' state as shown below:

```
Client MAC Address..... 00:17:7c:2f:b8:6e
Client State..... Associated
Client NAC OOB State..... Access
Wireless LAN Id..... 5
IP Address..... 10.105.132.254
Mobility State..... Export Anchor
Mobility Foreign IP Address..... 10.105.132.160
Policy Manager State..... RUN
```

- Another important check is the fact that the anchor sends a gratuitous ARP after successful authentication for webauth and moving the client into 'RUN' state:
***pemReceiveTask: May 08 05:53:23.343: 00:17:7c:2f:b8:6e Sending a gratuitous ARP for 10.105.132.254, VLAN Id 20480**

Thank you.

