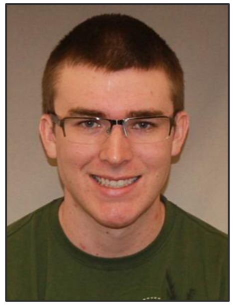
SNEAK PEEK

Cisco Support Community Expert Series Webcast

Identity Services Engine (ISE)

Guest & Posture Flow Troubleshooting



Aug 30th, 2016
with Sam Hertica and Maciej Podolski

Register Now : http://bit.ly/EN_aug16-ENWebcast

Agenda

- Guest Portal URL’s Anatomy
- Troubleshooting redirection
  - On ISE
  - Load Balancing
  - WLC and on Switch
- Certificate Issues
- Common ISE deployment bugs/Issues

Authentication Flow

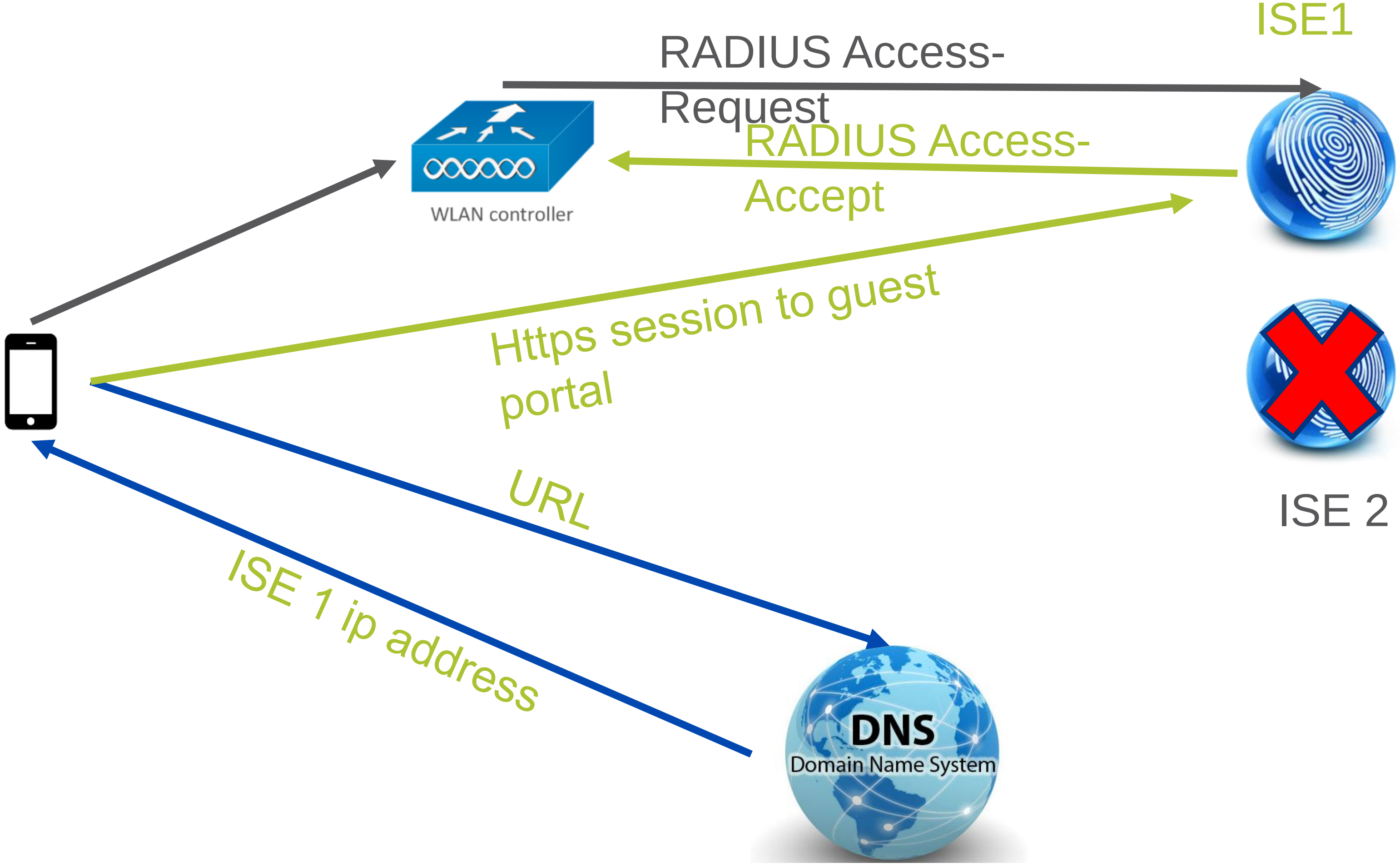
1. The endpoint connects to the SSID via MAB/dot1x

2. Radius session starts

3. ISE sends the RADIUS Access-Accept with redirect ACL + redirect URL POINTING TO ISE 1

4. Endpoint resolves the URL on the DNS

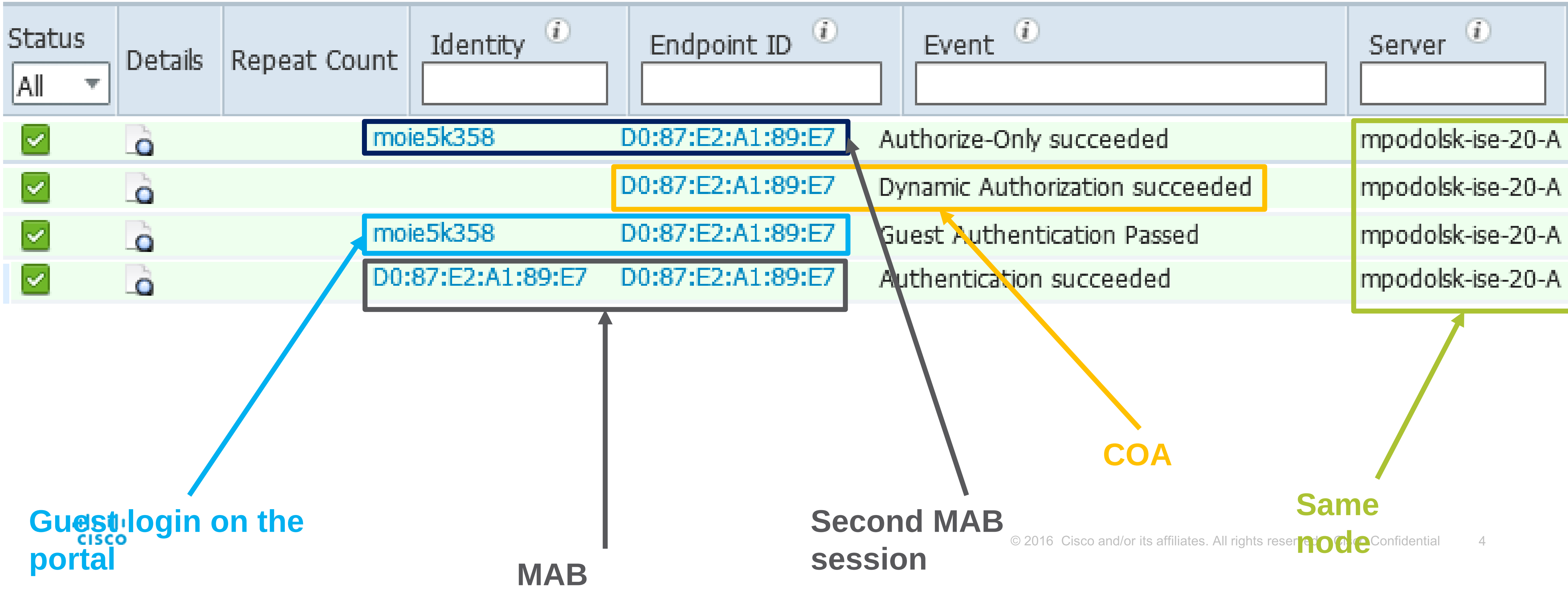
5. Https session to the guest portal



Make sure that the RADIUS session and the GUEST portal will be on the SAME NODE.

Guest user to MAC mapping

- When guest user is able to login on the Guest portal ISE is mapping the MAC address of that user with his guest account based on the RADIUS session ID in the URL. That is why portals are created per RADIUS session
- The session is valid on one and only one ISE node. (the one who returned the RADIUS



Status All	Details	Repeat Count	Identity	Endpoint ID	Event	Server
✓	🔍		moie5k358	D0:87:E2:A1:89:E7	Authorize-Only succeeded	mpodolsk-ise-20-A
✓	🔍			D0:87:E2:A1:89:E7	Dynamic Authorization succeeded	mpodolsk-ise-20-A
✓	🔍		moie5k358	D0:87:E2:A1:89:E7	Guest Authentication Passed	mpodolsk-ise-20-A
✓	🔍		D0:87:E2:A1:89:E7	D0:87:E2:A1:89:E7	Authentication succeeded	mpodolsk-ise-20-A

Guest login on the portal

MAB

Second MAB session

COA

Same node

The Golden Rule of Redirect ACLs

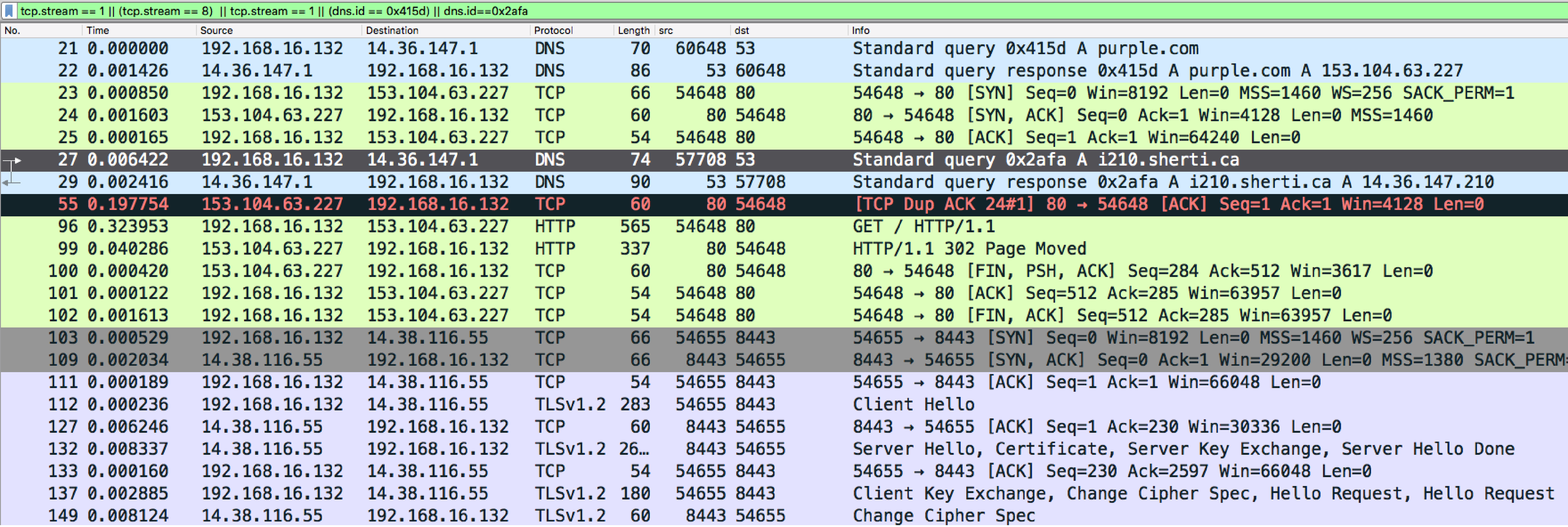
A redirect ACL is about identifying traffic you want to send to ISE.

Deny is bypassing the redirect, Permit is enforcing *

- You need an IP address (deny udp any any eq bootps)
- DNS has to function (deny udp any any eq domain)
- To send traffic to ISE, you need to not redirect traffic destined for your PSNs
- If you want to access other resources during the captive portal phase, deny it in the ACL.
- Everything else is redirected (permit ip any any)

*AirOS is special. Everything is backwards.

Detailed Capture Analysis



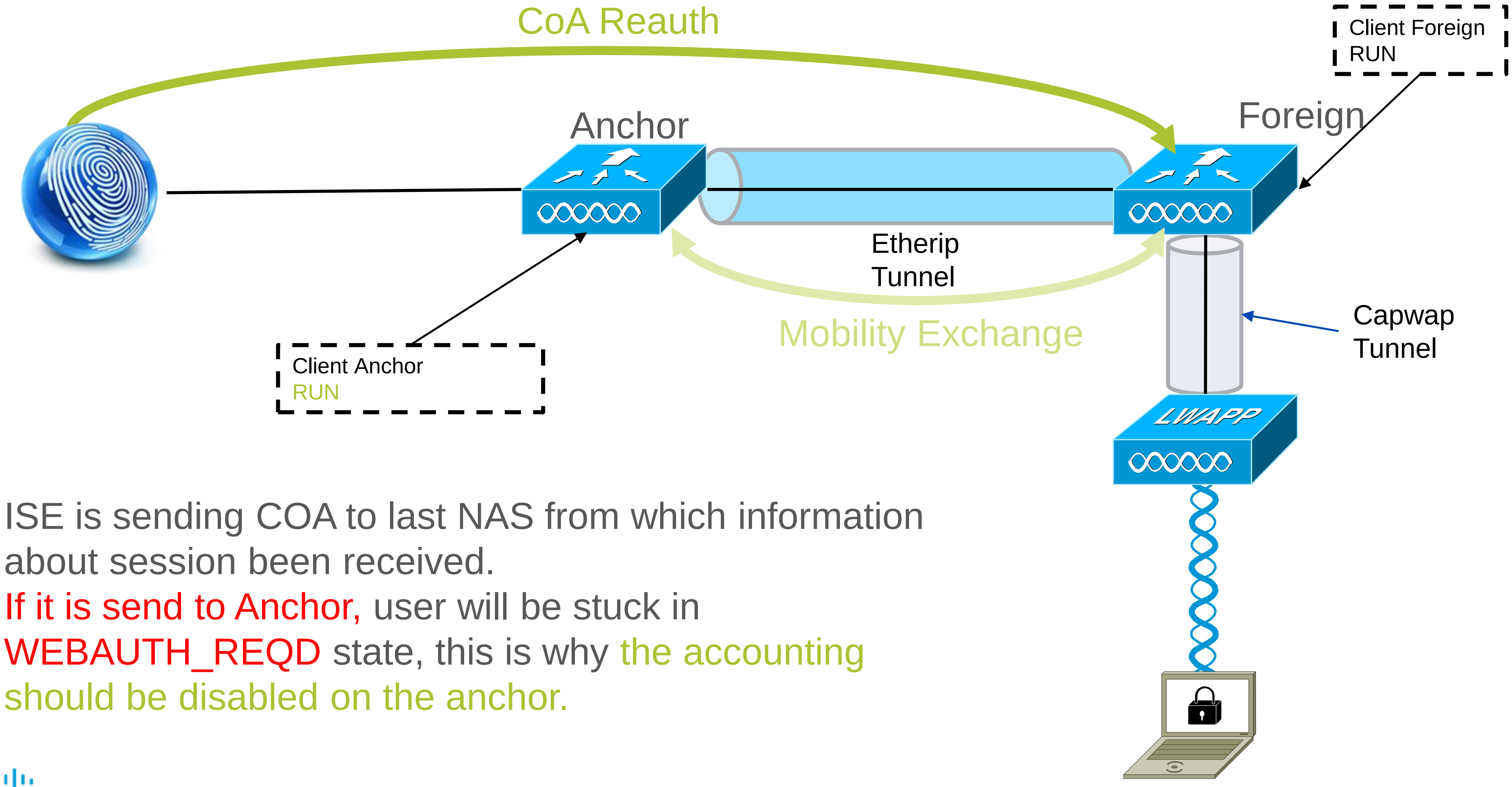
tcp.stream == 1 || (tcp.stream == 8) || tcp.stream == 1 || (dns.id == 0x415d) || dns.id==0x2afa

No.	Time	Source	Destination	Protocol	Length	src	dst	Info
21	0.000000	192.168.16.132	14.36.147.1	DNS	70	60648	53	Standard query 0x415d A purple.com
22	0.001426	14.36.147.1	192.168.16.132	DNS	86	53	60648	Standard query response 0x415d A purple.com A 153.104.63.227
23	0.000850	192.168.16.132	153.104.63.227	TCP	66	54648	80	54648 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
24	0.001603	153.104.63.227	192.168.16.132	TCP	60	80	54648	80 → 54648 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
25	0.000165	192.168.16.132	153.104.63.227	TCP	54	54648	80	54648 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
27	0.006422	192.168.16.132	14.36.147.1	DNS	74	57708	53	Standard query 0x2afa A i210.sherti.ca
29	0.002416	14.36.147.1	192.168.16.132	DNS	90	53	57708	Standard query response 0x2afa A i210.sherti.ca A 14.36.147.210
55	0.197754	153.104.63.227	192.168.16.132	TCP	60	80	54648	[TCP Dup ACK 24#1] 80 → 54648 [ACK] Seq=1 Ack=1 Win=4128 Len=0
96	0.323953	192.168.16.132	153.104.63.227	HTTP	565	54648	80	GET / HTTP/1.1
99	0.040286	153.104.63.227	192.168.16.132	HTTP	337	80	54648	HTTP/1.1 302 Page Moved
100	0.000420	153.104.63.227	192.168.16.132	TCP	60	80	54648	80 → 54648 [FIN, PSH, ACK] Seq=284 Ack=512 Win=3617 Len=0
101	0.000122	192.168.16.132	153.104.63.227	TCP	54	54648	80	54648 → 80 [ACK] Seq=512 Ack=285 Win=63957 Len=0
102	0.001613	192.168.16.132	153.104.63.227	TCP	54	54648	80	54648 → 80 [FIN, ACK] Seq=512 Ack=285 Win=63957 Len=0
103	0.000529	192.168.16.132	14.38.116.55	TCP	66	54655	8443	54655 → 8443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
109	0.002034	14.38.116.55	192.168.16.132	TCP	66	8443	54655	8443 → 54655 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1380 SACK_PERM
111	0.000189	192.168.16.132	14.38.116.55	TCP	54	54655	8443	54655 → 8443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
112	0.000236	192.168.16.132	14.38.116.55	TLSv1.2	283	54655	8443	Client Hello
127	0.006246	14.38.116.55	192.168.16.132	TCP	60	8443	54655	8443 → 54655 [ACK] Seq=1 Ack=230 Win=30336 Len=0
132	0.008337	14.38.116.55	192.168.16.132	TLSv1.2	26…	8443	54655	Server Hello, Certificate, Server Key Exchange, Server Hello Done
133	0.000160	192.168.16.132	14.38.116.55	TCP	54	54655	8443	54655 → 8443 [ACK] Seq=230 Ack=2597 Win=66048 Len=0
137	0.002885	192.168.16.132	14.38.116.55	TLSv1.2	180	54655	8443	Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request
149	0.008124	14.38.116.55	192.168.16.132	TLSv1.2	60	8443	54655	Change Cipher Spec

Walking through the capture, there's really four steps when it comes to redirection.

Initial DNS   NAD Spoofing TCP   DNS for ISE   ISE Portal Traffic

WLC Mobility and ISE – CWA and Auto Anchor



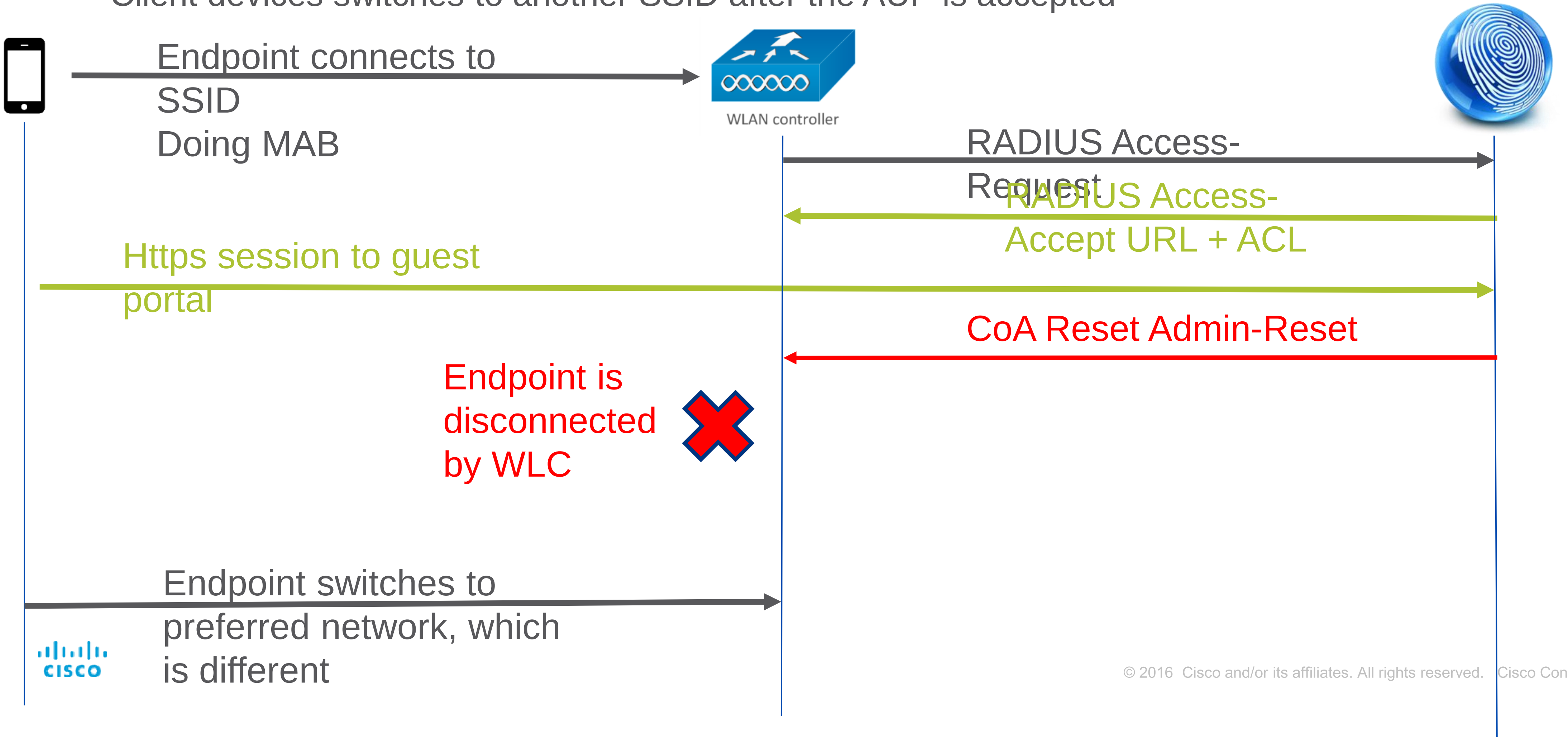
ISE is sending COA to last NAS from which information about session been received.

If it is send to Anchor, user will be stuck in WEBAUTH_REQD state, this is why the accounting should be disabled on the anchor.

Hotspot guest portal

Symptoms:

- Clients complain that is takes a long time after they accept AUP to get internet access
- Client devices switches to another SSID after the AUP is accepted



Endpoint connects to SSID
Doing MAB

RADIUS Access-Request

RADIUS Access-Accept URL + ACL

Https session to guest portal

CoA Reset Admin-Reset

Endpoint is disconnected by WLC

Endpoint switches to preferred network, which is different

Hope you enjoyed this little peek into the webcast.

Remember it was just a peek. Aug 30th, you get a chance to see the whole thing.

Register Now

http://bit.ly/EN_aug16-ENWebcast

At the webcast you will be able to learn so much more and get a chance to submit questions for the expert to answer during the broadcast.
We'll see you there!