Aruba Wireless Guest Access

Troubleshooting Captive Portal Problems

Ayman Mukaddam

Nov 18, 2020
Version 1.0

Posted on Airheads Community and on my blog https://whyfiplusplus.com

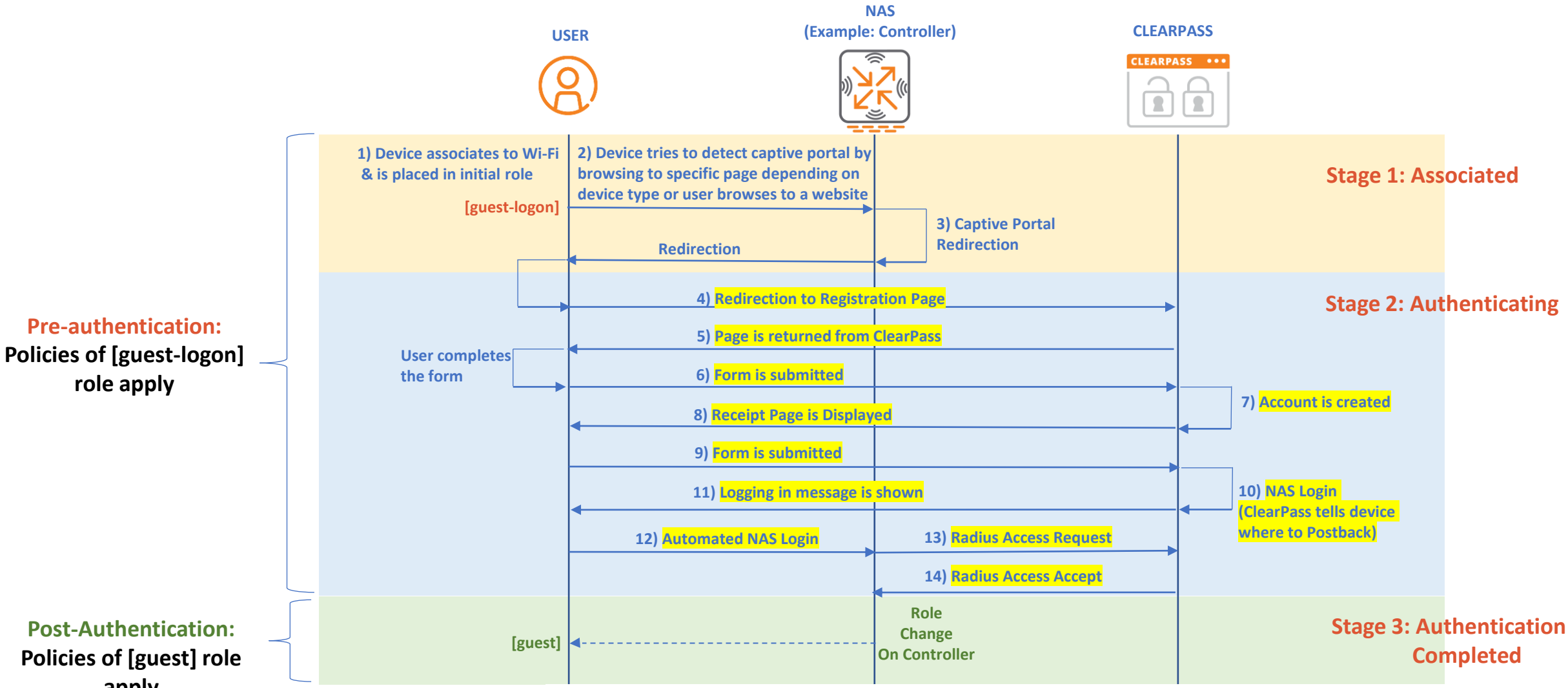
Overview

- Many of the calls I get from my partners and customers are related to guest captive portal issues
- I decided to document / clarify some of the issues I see frequently
- Hopefully, this document can be used to help you resolve such issues

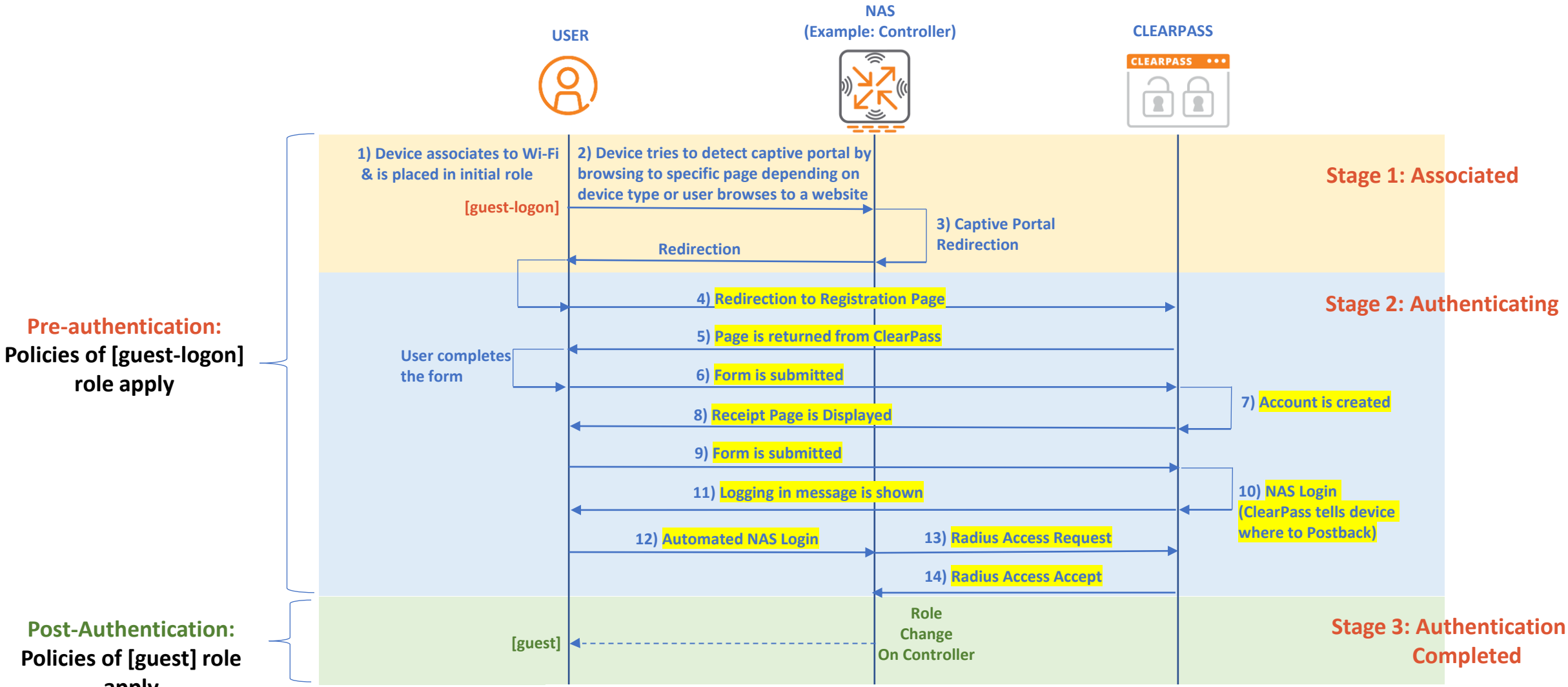
Overview

- Let’s start with Basic Guest Workflow without MAC Caching
  - To simplify troubleshooting, I think of it as
    - 2 roles (one before authenticating and one after authenticating)
    - 3 stages
      - Associated
      - Authenticating
      - Authentication Completed
  - The next slides show the workflow and the minimal policies needed in each role followed by common problems
  - Workflow is based on ClearPass self-registration (Steps 4 to 8) but the same logic applies even if these steps are skipped (direct redirection to login page instead)

Controller Initiated Login (No Mac-caching)



Note: The guest-logon and guest role names are just used as an example. You can use any role name with similar policies.



Note: The guest-logon and guest role names are just used as an example. You can use any role name with similar policies.

Pre-authentication Role - Minimal Policies

guest-logon (Pre-authentication)	Comments
Block device from acting as DHCP server	user any udp 68 deny
Allow device to act as DHCP client	any any svc-dhcp permit
Allow DNS to specific DNS servers	any alias ALLOWED_DNS_SERVERS svc-dns permit
Allow http to ClearPass	Can be removed - Better to only enable https though
Allow https to ClearPass	ClearPass must have a valid trusted certificate
Allow needed whitelisted traffic (if any)	Only needed if you need to allow access to certain destinations from unauthenticated users (For example if you are using social login, you need to whitelist the social login provider FQDNs)
Block unneeded traffic	any network 169.254.0.0 255.255.0.0 any deny any network 240.0.0.0 240.0.0.0 any deny
Built-in captiveportal policy (redirect http to ClearPass)	
Built-in captiveportal policy (redirect https to ClearPass)	This causes SSL certificate warnings (expected)
BLOCK ALL	Explicit Deny (optional)

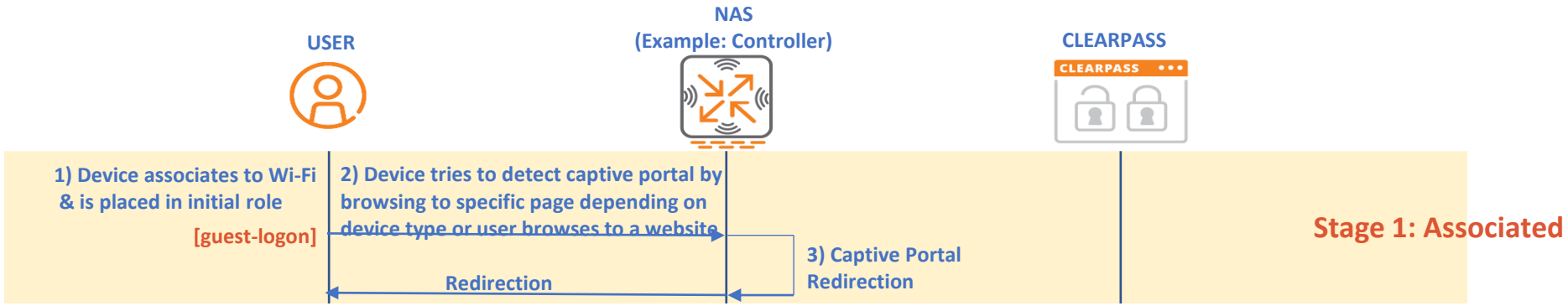
Post-authentication Role - Minimal Policies

guest (Post-authentication)	**Comments**
Block device from acting as DHCP server	user any udp 68 deny
Allow device to act as DHCP client	any any svc-dhcp permit
Allow DNS to specific DNS servers	any alias ALLOWED_DNS_SERVERS svc-dns permit
Block unneeded traffic	any network 169.254.0.0 255.255.0.0 any deny any network 240.0.0.0 240.0.0.0 any deny
Allow http to ClearPass	Better to only enable https though
Allow https to ClearPass	ClearPass must have a valid trusted certificate
BLOCK INTERNAL ACCESS	Logging can be enabled as well
ALLOW INTERNET ACCESS	Depending on your policy

Common Problems

- Below are some of the common encountered problems grouped by stage

Problems in Stage 1

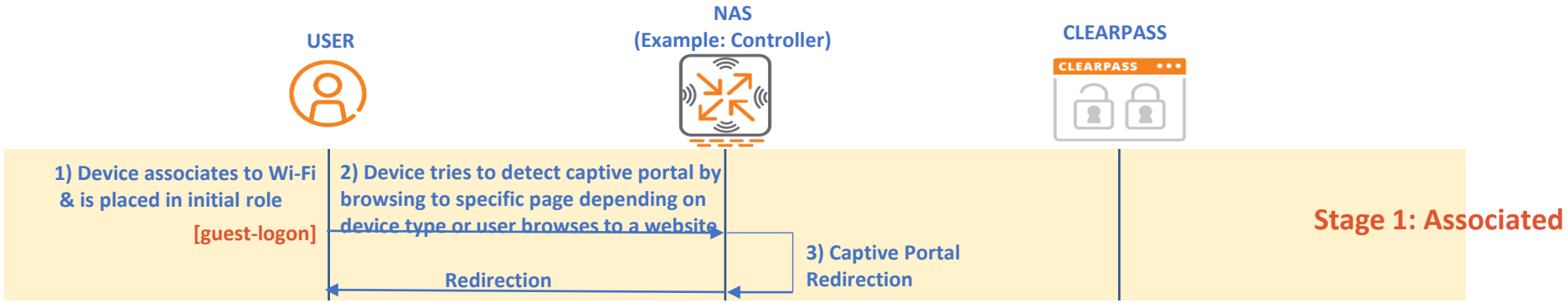


Step 1 - Common Problems

1. Device Connected to the right SSID? If not, check your client
2. Device got IP from the right subnet? If not, check your VAP profile & check if client has static IP configured
3. Device was assigned the right initial role? If not, check your initial role in AAA profile

Useful commands to check: show user-table mac <mac>
show aaa state user <IP>

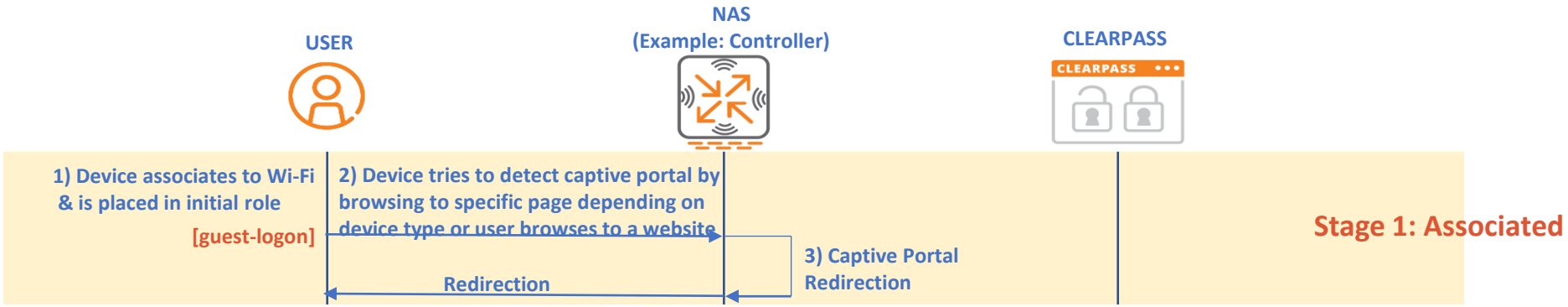
Problems in Stage 1



Steps 2/3/4 - Common Problems

1. Device didn't detect captive portal automatically –
   a) If your workflow requires direct verification (Example SMS OTP) or Onboarding, then this is normal as you need to disable the pop-up browser to avoid issues with Apple devices (Pop-up browser closes when you try to check the SMS)

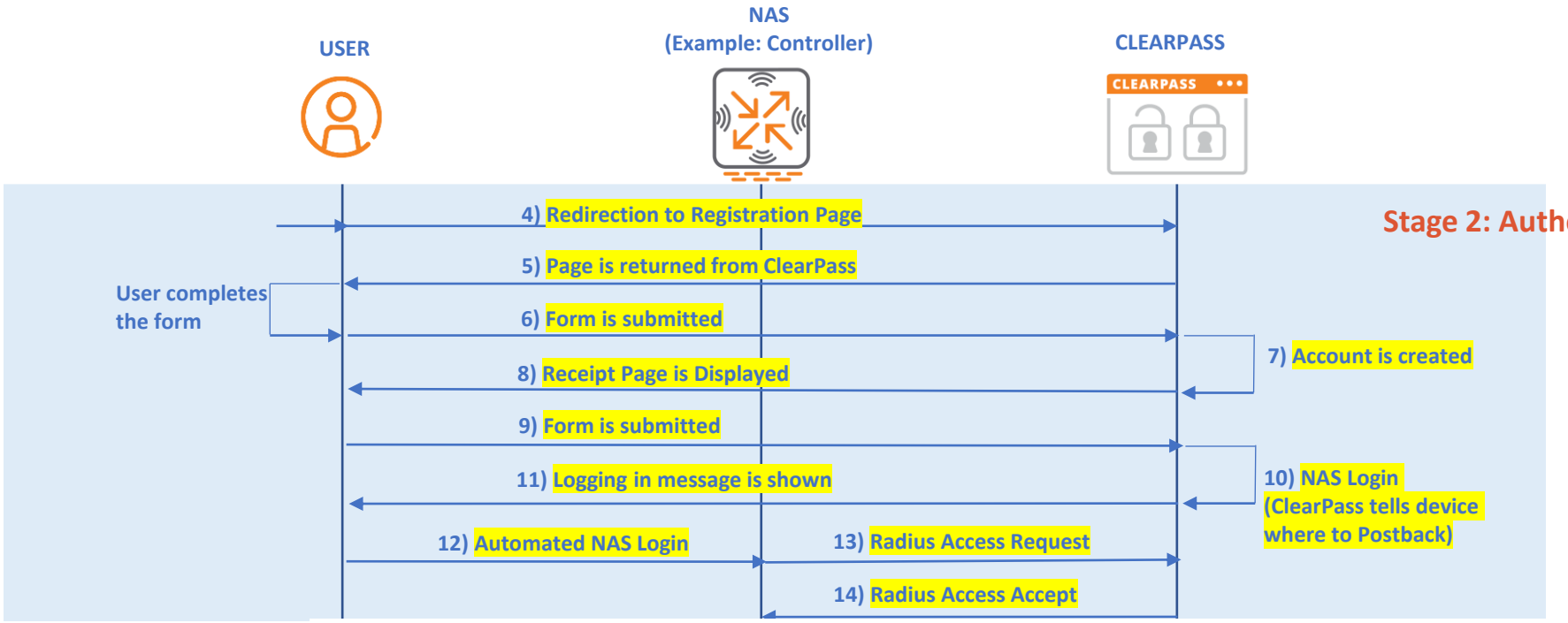
Problems in Stage 1



Steps 2/3/4 - Common Problems

1. Device didn't detect captive portal automatically (continued)
   b) If your workflow doesn't require verification nor onboarding, then
      - Does the controller have a Layer 3 interface in the Guest user vlan?
        - If no, then you need to use "firewall allow-tri-session" as described here https://community.arubanetworks.com/browse/articles/blogviewer?blogkey=afaa9b60-8087-47d6-b20a-5e355f16dbc0
        - If yes, try to open http://1.2.3.4 or any IP? Does it get redirected?
          - If yes, check your DNS?
            - Can the clients in the guest-logon role access the DNS server? Can they resolve any domain (For example www.nba.com) Can they resolve ClearPass FQDN name?
          - If no, try to access http://YOUR_CLEARPASS_IP/guest/YOUR_PAGE_NAME.php?
            - Check your initial role and confirm captive portal profile is associated with this role
            - Check your initial role policies (ClearPass whitelisted? captiveportal policy added in right place **after** ClearPass whitelist?)
            - Check your routing/NAT/firewall policies between client subnet and ClearPass. Enable ping in initial role if needed to check connectivity
            - Check your page name on ClearPass

Problems in Stage 2

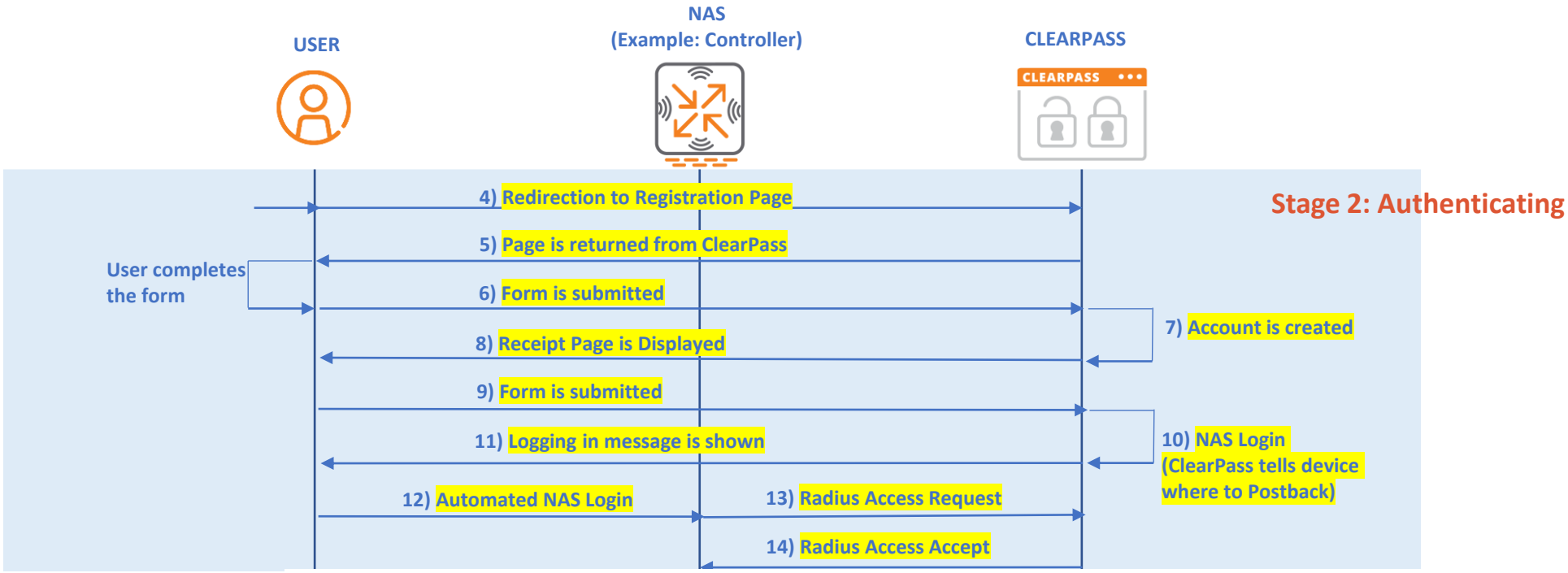


Step 5 - Common Problems

a) It is very important to note, that **<u>two certificates are needed</u>** in this workflow; one for ClearPass and one for controller.

- At step 5, ClearPass returns the guest webpage to the user → Here the client browser verifies the https certificate of ClearPass. It must be a trusted certificate to avoid warnings. **Make sure certificate is properly installed (full chain)**
- Later on, at Step 12, the client will post back to the controller so the second certificate will be used
- Many times the issues are related to certificates so check the recommendations section for certificates

Problems in Stage 2



Steps 6-9

a) These are usually ClearPass related steps

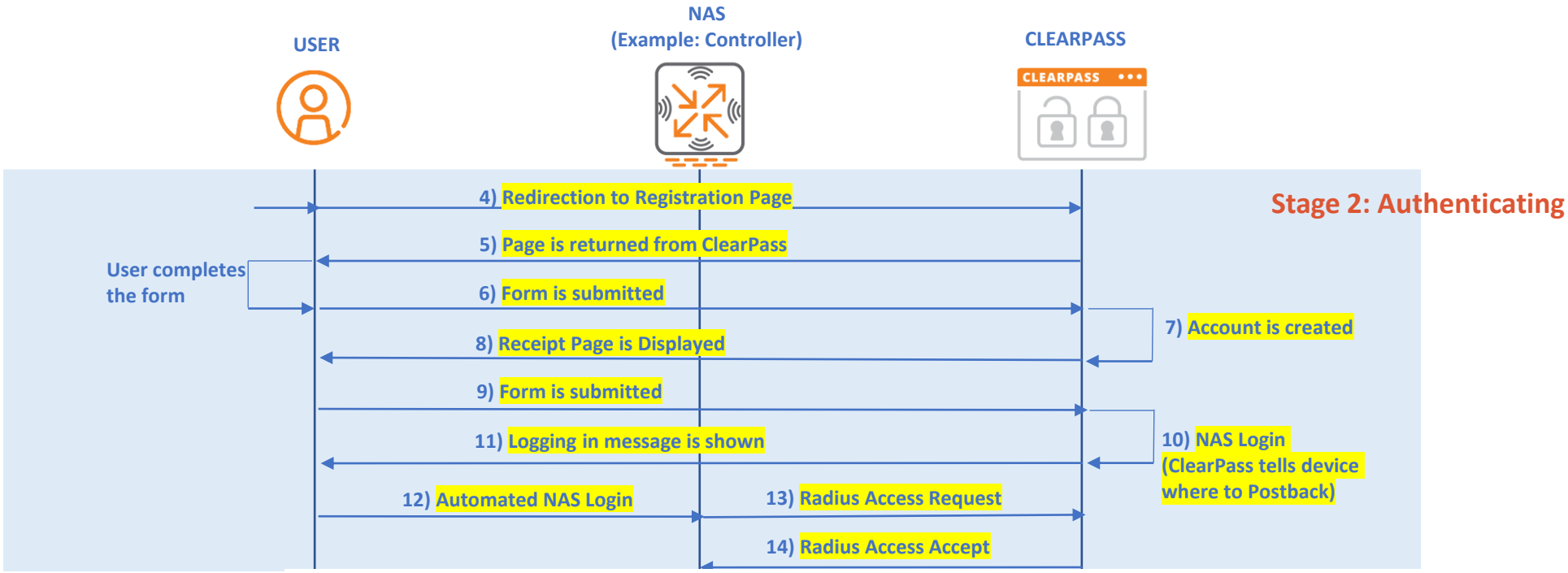
Problems in Stage 2 (Certificates Related)

1. With ClearPass Guest make sure you have 2 trusted certificates:
   - ClearPass HTTPS certificate should be trusted by the clients (issued by well known CA)
   - Domain validation certificate is enough
   - Https Certificate can be a wildcard or multi-SAN certificate but this is not a requirement
   - ClearPass **should have a DNS entry resolvable** by the clients pointing the ClearPass server
     - In many cases, Guest users use public DNS servers so you can publish a DNS A Record for your ClearPass FQDN pointing to a private IP. This will be resolved by public DNS servers
       - For example cppm.example.com → 10.10.50.100
       - Clients should have IP connectivity from the guest subnet to the IP resolved by DNS

2. Controller or Instant cluster certificate
   - **No need for FQDN to be in DNS**, controller or IAP will handle the DNS requests for the domain
   - Use the same certificate even in a multi-controller deployment (Each controller will DNS snoop the traffic and reply with its IP)
   - If using a wildcard certificate, set the Postback URL to captiveportal-login.your domain.com

     *.example.com → captiveportal-login.example.com
   - Can be a multi-SAN: however the first name must be used by the controller/IAP (DNS Snooping)
   - In case you use the same multi-SAN certificate for both controller and ClearPass then **you can't use the first name for ClearPass**

Problems in Stage 2



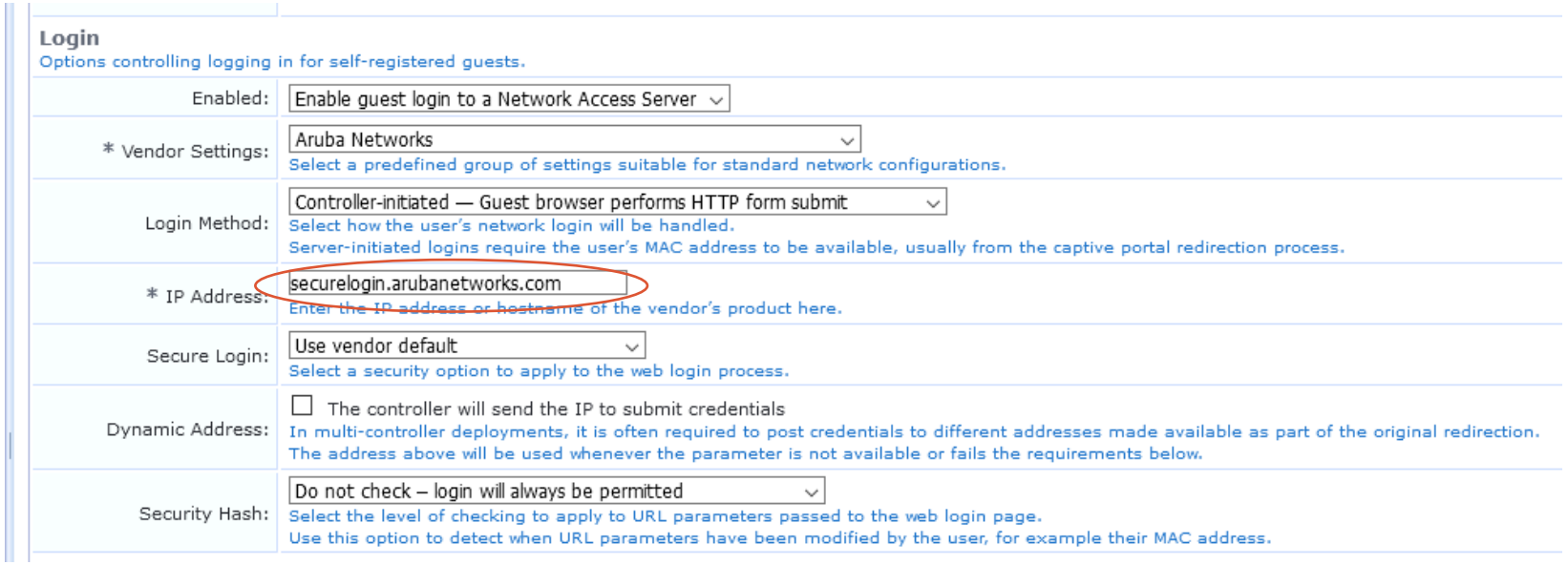
Steps 10

a) The most common problem in Step 10 is setting an incorrect post-back URL in ClearPass
b) It is recommended to use https for post-back and use a trusted certificate on the controllers as well.
c) Don't mix https to ClearPass and http PostBack to controller as some browsers might complain that the requested website is unsecure
d) For POC only, you can use http for both ClearPass and Controllers to avoid issues in certificates. Don't use this in any production network.

Problems in Stage 2

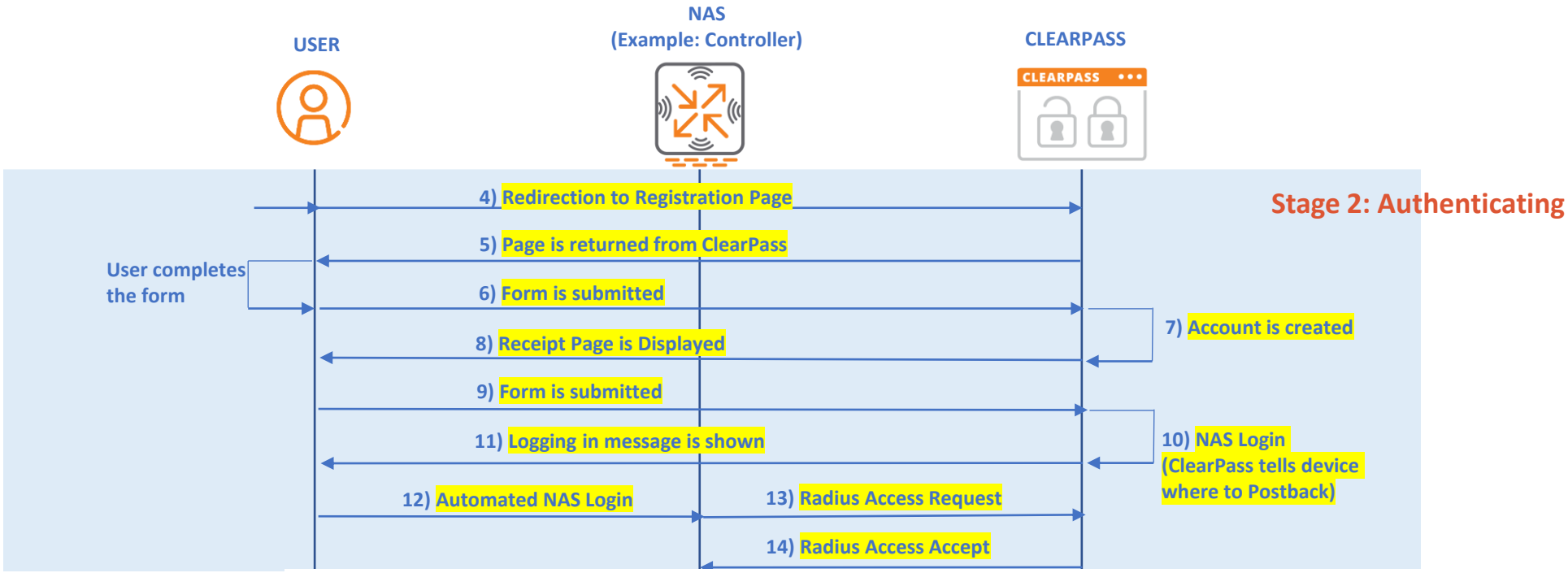
Steps 10

By default, ClearPass will post back to securelogin.arubanetworks.com (which is the default untrusted certificate of the controller)



This should be changed to point to the **common name** of your **trusted certificate** that is installed on **your controllers**

Problems in Stage 2

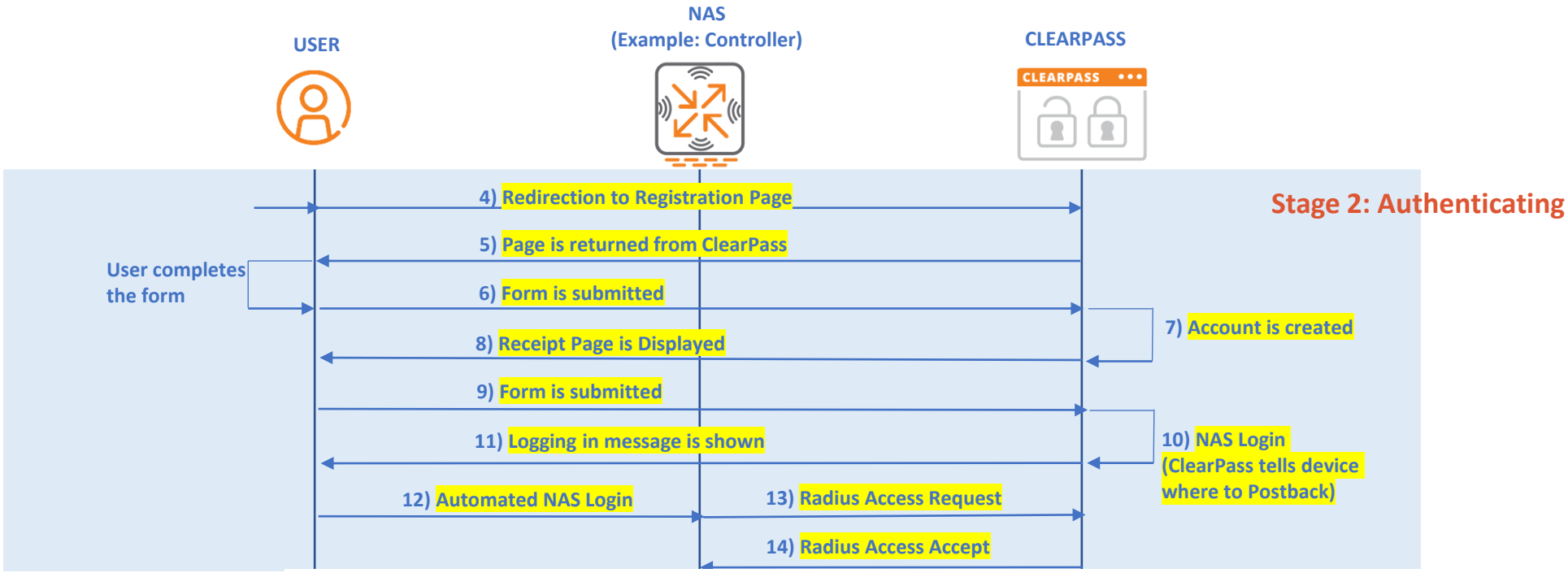


Steps 12-13

a) Many times the issues happen at step 12 where the user fills the form and presses submit but no request shows in Clearpass
   a) Check the captive portal profile and make sure the radius server group is set to ClearPass
   b) Check the radius server IP & key

Useful commands to check: show aaa authentication captive-portal < X >
encrypt disable
show aaa authentication-server radius <X >
encrypt enable

Problems in Stage 2



Steps 14

a) Many times the issues happen at step 14 where ClearPass returns Radius Reject instead of accept. Check your policy configuration on ClearPass in that case.

Problems in Stage 3

Steps 15

a) At this stage, device is authenticated and they should be placed in the post-authentication role
b) The problems in stage 3 are mostly related to the access permissions related to the guest role itself.
    a) Double check to confirm that the client got the post-authentication role
    b) Double check your role configuration to make sure the policies are correct.

Useful commands to check: show user-table mac <mac>
show aaa state user <IP>
show rights <Role>

Note: The guest-logon and guest role names are just used as an example. You can use any role name with similar policies.

Feedback & Comments

- Feel free to share your feedback / comments at ayman.mukaddam@hpe.com
- This is also posted on my blog https://whyfiplusplus.com