March 2021

ENHANCED CENTRAL WEB AUTHENTICATION

Sachin D. Wakudkar

Sergio Barreto Andrade

Taha Hajar

ENHANCED CENTRAL WEB AUTHENTICATION

AUTHORS:
Sachin D Wakudkar
Sergio Barreto Andrade
Taha Hajar

ABSTRACT

Central web authentication (CWA) is widely deployed for guest user authentication in environments that include a Remote Authentication Dial-In User (RADIUS) server. The various CWA flows work well with existing security policy management platforms without any security concerns, but potentially there could be security issues while working with third-party RADIUS servers. To address these types of challenges, techniques are presented herein that support, among other things, enhanced CWA flows to work with untrusted RADIUS servers and selectively extending Layer 3 (L3) authentication timeouts for high-profile customers.

DETAILED DESCRIPTION

Central web Authentication (CWA) is widely deployed for guest user authentication purposes where a Remote Authentication Dial-In User Service (RADIUS) server maintains the client state, redirects a client to a guest portal, validates user credentials, and through change of authorization (CoA) provides a client full connectivity. CWA flows work well with existing security policy management platforms without any security concerns, but potentially there could be security issues while working with third-party RADIUS servers where, for example:

1. A client is not forced to re-authenticate when a session timeout happens.
2. A client is not re-authenticated when it rejoins the network.

A malicious user could potentially exploit this using Media Access Control (MAC) spoofing and, in many cases, a customer may not be even aware of the issues. It is important to note that there are many customers deploying CWA with a third-party RADIUS server.

To address the types of challenges that were described above, techniques are presented herein that support further flow extensions to address the security gap with third-party RADIUS servers while making sure that the original flow, that is designed to work with existing security policy management platforms, is actually enforced with any other third-party servers as well.

As will be described below, under aspects of the techniques presented herein additional extensions may be added to the existing CWA solutions to provide differential services to guest users which are requested by multiple customers. One requirement that may be called out is that vendors would like to give special treatment to their loyal and very important person (VIP) guest users, whereby once they are web authenticated they are not required to be re-authenticated over a longer period. The enhancements to the existing CWA flows that are presented herein accommodate, among other things, such a requirement.

In support of the discussion that is provided below of the techniques presented herein, it will be helpful to begin with a description of the existing CWA flows, as illustrated in Figure 1, below.

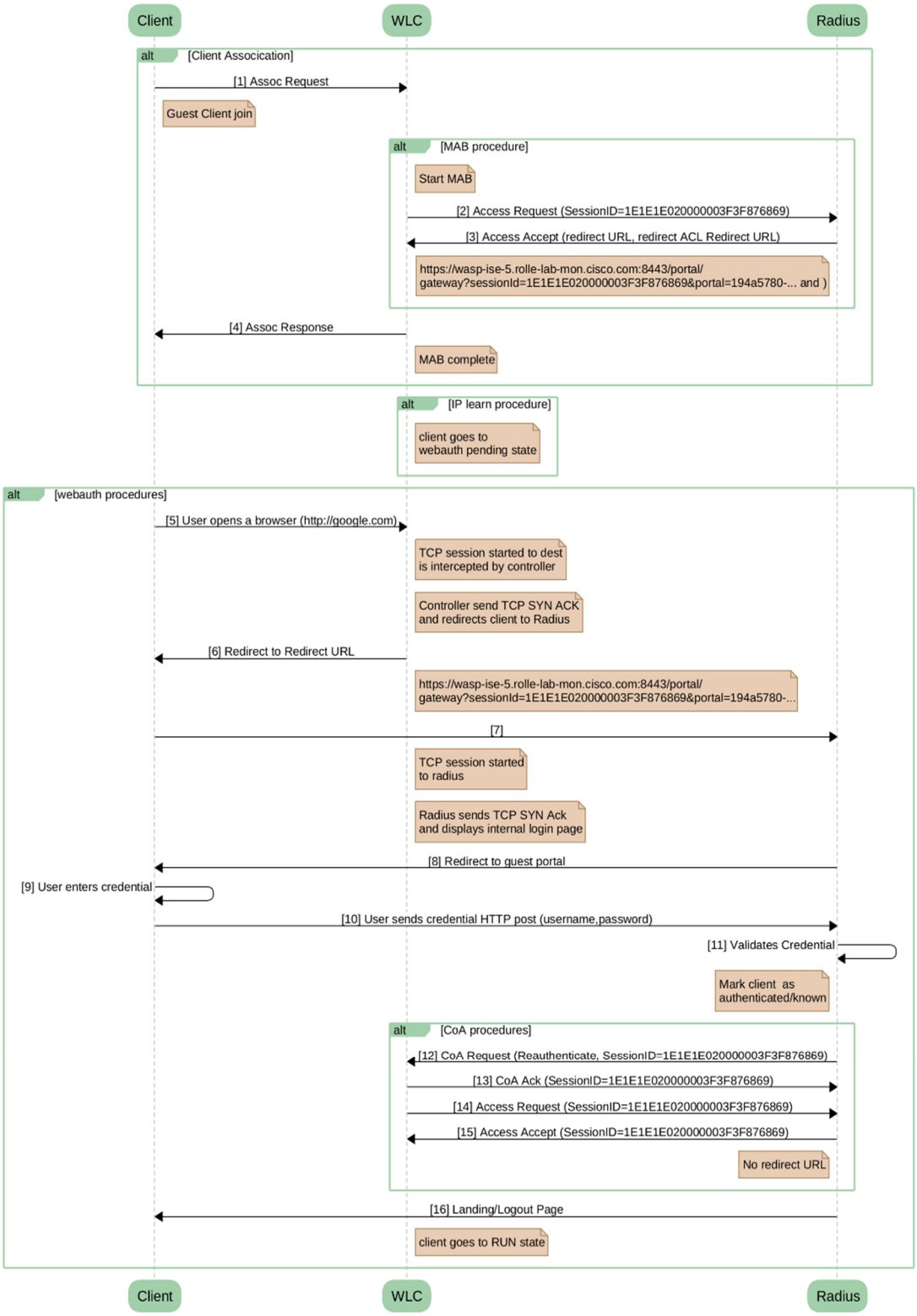

Figure 1: Example CWA Flow

As depicted in Figure 1, the existing CWA flows include the following steps:

1. A client (e.g., a STA) does an association with a Wireless Local Area Network (LAN) Controller (WLC).
2. The WLC initiates a MAC Address Bypass (MAB) authentication with a RADIUS server, creates an audit session identifier (ID) to uniquely identify a given session, and sends an Access Request to the RADIUS server.
3. The RADIUS server pushes a redirect access-control list (ACL) and redirect Uniform Resource Locator (URL) attribute to the STA in an Access Accept to allow the client to get to the portal on the RADIUS server for L3 authentication. The redirect URL and redirect ACL are plumbed in the data path for the STA.
4. After MAB is successful, the controller sends an Association Response to the STA and learns the Internet Protocol (IP) address and then moves the client to a web authentication pending state.
5. The STA opens a browser and tries to reach, for example, google.com. The Transmission Control Protocol (TCP) session from the client is intercepted by the controller.

6-10. The controller pushes the STA to a redirect portal and the STA initiates a TCP session with the RADIUS server. The STA gets redirected to a guest portal on the RADIUS server through which the STA user enters login credentials and the STA sends the credentials.

11. The RADIUS server validates the credentials and allows full access to the client.
12. The RADIUS Server sends a CoA Request of re-authenticate type with an audit session ID.
13. The WLC responds with a CoA Ack and initiates a re-authentication procedure.
14. The WLC initiates MAB authentication towards the RADIUS server and sends an Access Request.
15. The RADIUS server responds with an Access Accept and since the client is fully authorized it removes the redirect URL and ACL attribute for the STA.
16. The RADIUS server provides the STA with a landing page with logout portal after which the WLC gives the STA full access and moves the STA to a run state.

When validating and enforcing a CWA L3 authentication, it is expected that the entire flow is to be managed by a RADIUS server. A controller follows the RADIUS server and applies the policies that are pushed by the RADIUS server without revalidation, which could potentially leave security gaps when dealing with untrusted or misbehaving or third-party RADIUS servers.

Consequently, consistent with the techniques presented herein, various changes may be made to the existing flow. For example, a WLC may track if a client has gone through successful L3 authentication using CWA and also inform peers to allow seamless roaming. Further, when a session timeout happens, or when a STA leaves and joins back, a controller may assign a new session id for the client. The client will go through MAB authentication again. Since it is a new unauthenticated session, the controller expects the RADIUS server to push a redirect ACL and URL in the Access Accept in order to force the STA to complete L3 authentication. Finally, if a controller does not receive the redirect ACL and URL, it will redirect the client with the new session ID to a default portal.

An enhanced CWA flow, incorporating such changes or enhancements, is presented in Figure 2, below.

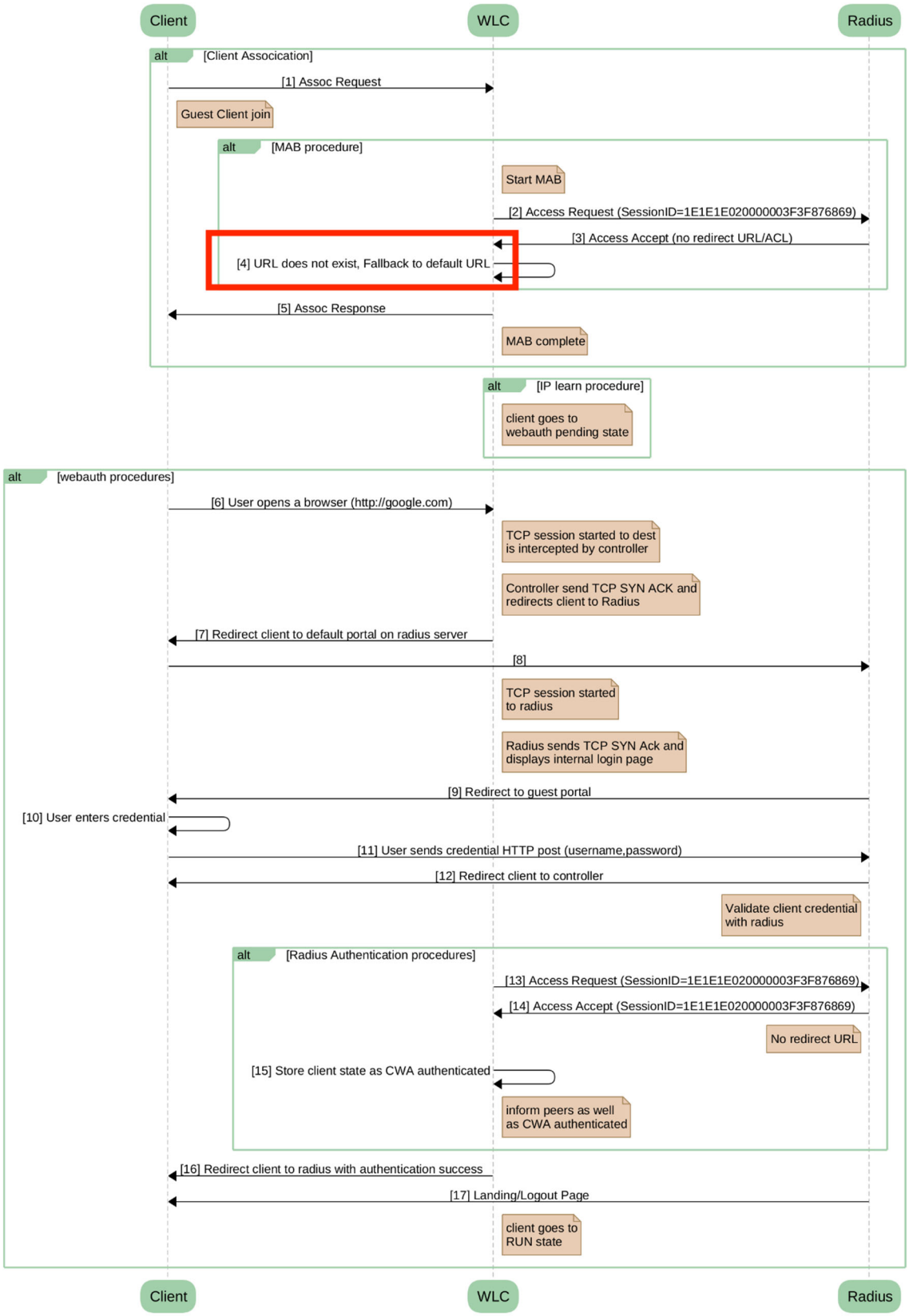

Figure 2: Enhanced CWA Flow

Under aspects of the techniques presented herein, it is possible to extend CWA authentication status for high-profile customers. As one possible example, a new attribute-value pair (AVP) may be added, post CoA, in an Access Accept which would indicate the duration over which the web authentication state may be extended. A controller may keep the audit session ID for a given client over that period so that when the client joins back before the expiry of the extended session the controller would relay the same audit session ID and a RADIUS server may skip the web authentication steps for the client. Aspects of such an approach are depicted in Figure 3, below.

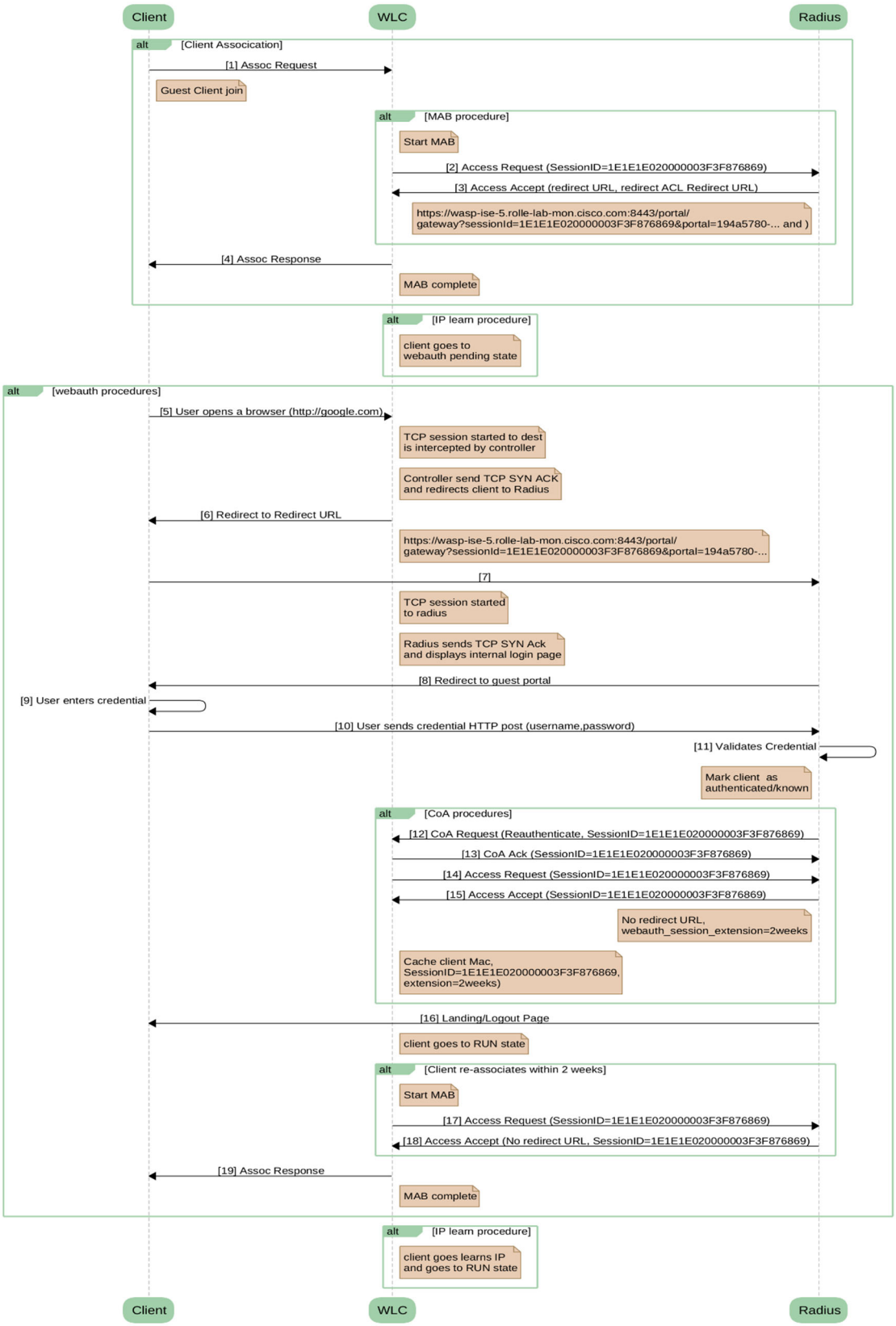

Figure 3: Extended CWA Authentication for High-Profile Customers

In summary, techniques have been presented that support, among other things, enhanced CWA flows to work with untrusted RADIUS servers and selectively extending L3 authentication timeouts for high-profile customers. Further, techniques herein may support implementations that may involve randomized MAC addresses as long as the identity towards the RADIUS server and the Dynamic Host Configuration Protocol (DHCP) server is not changed and a translation is provided between the randomized MAC and a fixed identity of the client.