March 2022

METHOD TO OPTIMISE DISTRIBUTION OF AUTHENTICATION INFORMATION FOR CLIENT RE-CONNECTIVITY

Niranjan M M

Vijay Kothamasu

METHOD TO OPTIMISE DISTRIBUTION OF AUTHENTICATION INFORMATION FOR CLIENT RE-CONNECTIVITY

AUTHORS:
Niranjan M M
Vijay Kothamasu

ABSTRACT

There are many customer deployments wherein the switches and WLCs authenticates the clients using 802.1X authentication methods which uses EAP to exchange messages during the authentication process. Here, AAA servers acts as Authenticator. Typically, AAA servers are deployed remotely and connected to enterprise over the WAN link. In short, client authenticates with the AAA server through Switch/WLC. In the scenarios such as, if AAA server(s) is/are down OR the respective link between "Switch/WLC and AAA servers" is down and in-turn servers are not reachable, clients will fail to connect, and service will be impacted. There are techniques which caches the authentication credentials locally on the Switch/WLC when client connects first time. Further when client connects to the same Switch/WLC next time, this local cache can be used to authenticate the client even when AAA server is not available. But there is no guarantee the next time client will connect to the same Switch/WLC. In such cases client connectivity will fail, even though Authentication Cache is available with the other Switch. The techniques presented here is one such method for the clients to re-connect to any Switch/WLC of a particular deployment, even when the link is down, or AAA server(s) is/are not reachable. As per this method, when client connects first time, authentication credentials are stored on any one of the Switch/WLC by hashing the client MAC address. Further if client re-connects to a different Switch/WLC and if AAA servers are not available or reachable, then Switch/WLC will calculate the hash using the client MAC address and find the right Switch/WLC to fetch the authentication details to proceed with client authentication and connectivity.

DETAILED DESCRIPTION

There are many customer deployments wherein the switches (wired deployments) and WLCs (wireless deployments) authenticates the clients using 802.1X (dot1x) authentication methods which uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. Here, AAA servers acts as Authenticator. Typically, AAA servers are deployed remotely (on the branch office or on the cloud) and connected to enterprise (headquarters) over the WAN link. In short, client authenticates with the AAA server through Switch. In the scenarios such as, if AAA server(s) is/are down OR the respective link between "Switch and AAA servers" is down and in-turn servers are not reachable, clients will fail to connect, and service will be impacted.

There are techniques which caches the authentication credentials locally on the Switch when client connects first time. Further when client connects to the same Switch next time, this Local Cache can be used to authenticate the client even when AAA server is not available.

But there is no guarantee the next time client will connect to the same Switch. In such cases client connect will still fail, even though Authentication Cache is available with the first Switch

(Let's say, Source Switch). Since this is very common scenario, there is desperate need to address this problem as it can have serious impact on customer satisfaction.

Even if we want to distribute (replicate) the authentication caching information across Switches in the deployment, it is not an amicable solution to replicate the cache across all Switches. Same thing holds good for Wireless deployments where-in wireless clients authenticate with the AAA server through WLC (Wireless LAN Controller) instead of Switch. Replicating the authentication caching across WLCs is not at-all an amicable solution especially for Wi-Fi with the increase in number of clients supported with 11ax (Wi-Fi6/Wi-Fi7).

The techniques presented here is one such method for the clients to re-connect to any Switch/WLC of a particular deployment, even when the link is down, or AAA server(s) is/are not reachable. As per this method, when client connects first time, authentication credentials are stored on any one of the Switch by hashing the client MAC address. Further if client re-connects to a different Switch (at a later point in time) and if AAA servers are not available or reachable, the second Switch will calculate the hash using the client MAC address and find the right Switch (using the consistent hashing based on client's MAC address) to fetch the authentication details. Thus, using these details, client can still be authenticated and can connect successfully. This will drastically improve customer satisfaction as it avoids the service impact. This is the case when AAA servers are down or not reachable.

Additionally, this method of authenticating with Cached credentials can also be used by default or primary method of authentication. This will reduce the client joining time, as it avoids the overhead EAP operation and minimizes the load on AAA servers as well. Same things hold good for Wireless deployments where-in wireless clients authenticate with the AAA server through WLC (Wireless LAN Controller) instead of Switch.

For the wired deployments, Switches of a specific Site (Location) are grouped to reduce the number of switches participating in the hashing mechanism. Similarly, for the wireless deployments, WLCs of a particular Site (Location) are grouped as part of a Mobility Domain where same set of clients/subscribers can roam or re-join repeatedly.

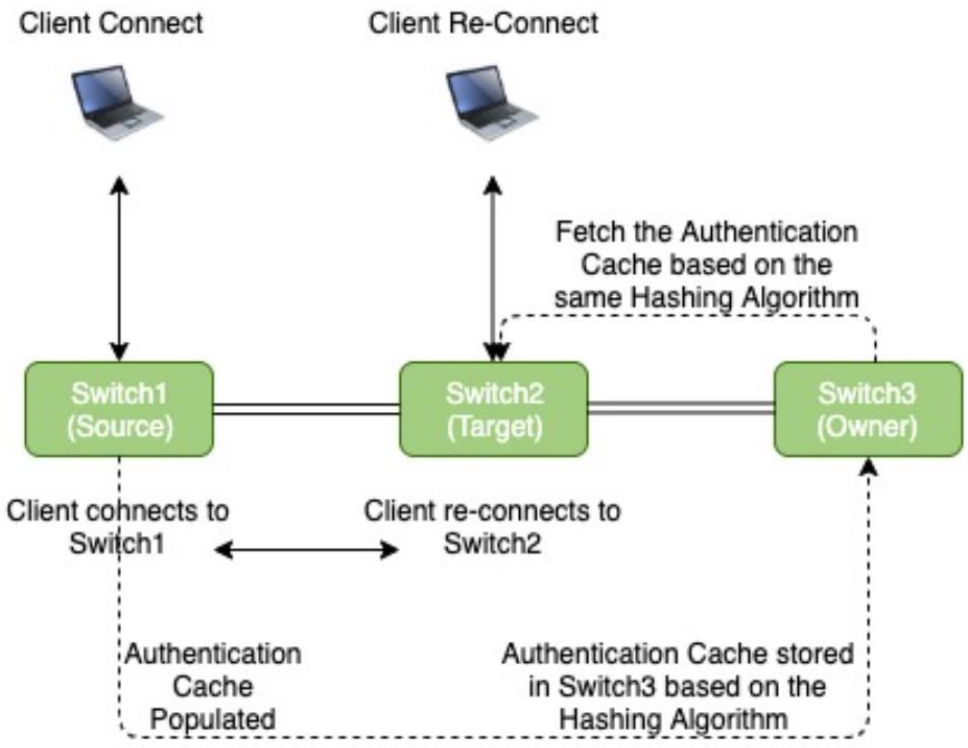
The techniques presented herein is explained in detail as below:

- A set of Switches (Here, Switch1, Switch2, Switch3) are configured with the same configurations in each Site (Location).
- First time when a client connects a Switch (let's say, Source Switch, here Switch1), it will get authenticated through AAA server.
- Switch1 (called Source Switch) will compute the consistent hash based on client MAC address and selects one or more of the Switches (let's say, Owner Switch, here Switch3) in the deployment to Cache the Authentication credentials.
- At a later point in time, when client re-connects to a different Switch (let's say, Target Switch, here Switch2) and AAA servers are down or not reachable.
- Switch2 (called Target Switch) computes the consistent hash based on the client MAC address to find the right Switch Switch3 (called Owner Switch) and fetches the Cache details of client with its MAC address from Switch3.
- Switch2 will use this Authentication Cache information to authenticate the client, apply the policies and client can connect successfully.

Admin can configure to use Cached details to authenticate client as primary method instead of using AAA server. This will enhance and speed up the client join process and reduce the load on

AAA servers. Same things hold good for Wireless deployments where-in wireless clients authenticate with the AAA server through WLC (Wireless LAN Controller) instead of Switch. This method is very much required with Wi-Fi6 in-place, as number of client support is multi-folded with 11ax, and we cannot afford to replicate whole Cache of Authentication Information across all WLCs in the deployment.

Figure-1 describe the above method with the help of flow diagram for Wired Deployments. Here, laptop (wired client) connected with Switch1 initially. Authentication Cache is populated on Switch1 and stored in Switch3 based on the Consistent Hashing. Later when client re-connected to Switch2. Switch2 runs the same hash algorithm to find the right Switch (Switch3) where Authentication Cache is available. Switch2 retrieve the Authentication Cache and authenticates that client. Let us assume, building having three floors and each floor having one switch each, initially user/client connects to Switch1 (Source Switch) and when user/client move from first floor to second floor, user/client no need to re-authenticate with the AAA server, instead Switch2 (Target Switch) of second floor do the re-authentication using the cached information available on Switch3, which was stored using consistent hashing.



Note: In the diagram, Client connects to Switch1. Authentication Cache would be populated by Switch1. Authentication Cache is stored on Switch3 based on Hashing Algorithm. Client re-connect to Switch2. Switch2 runs the same Hash Algorithm to know the right Switch. Here it is Switch3. Switch2 retrieves Cache from Switch3. Switch2 re-authenticate the Client.

Figure-1

Figure-2 describe the above method with the help of flow diagram for Wireless Deployments. Here, mobile (wireless client) associated with AP1/WLC1 initially. Authentication Cache is populated on WLC1 and stored in WLC3 based on consistent hashing. Later when client re-joined to AP2/WLC2. WLC2 runs the same consistent hashing to find the right WLC (WLC3) where Cache is available. WLC2 retrieve the Cache and authenticates that client.

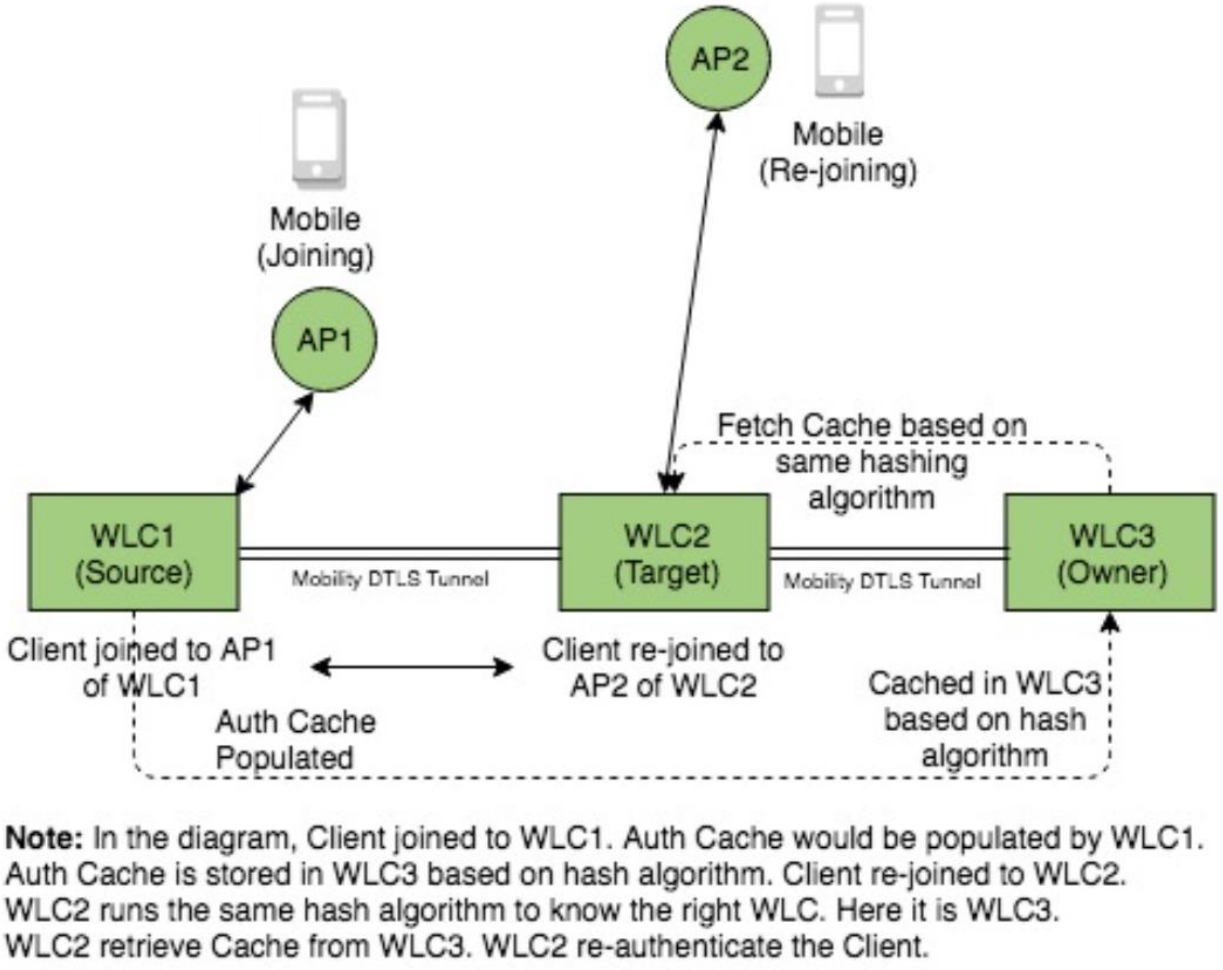


Figure-2

Figure-3 explain the step-by-step method using sequence diagram which shows the Authentication flow, Distributing Authentication Information based on consistent hashing, Retrieving Authentication Information using the same consistent hashing for Wired Deployments.

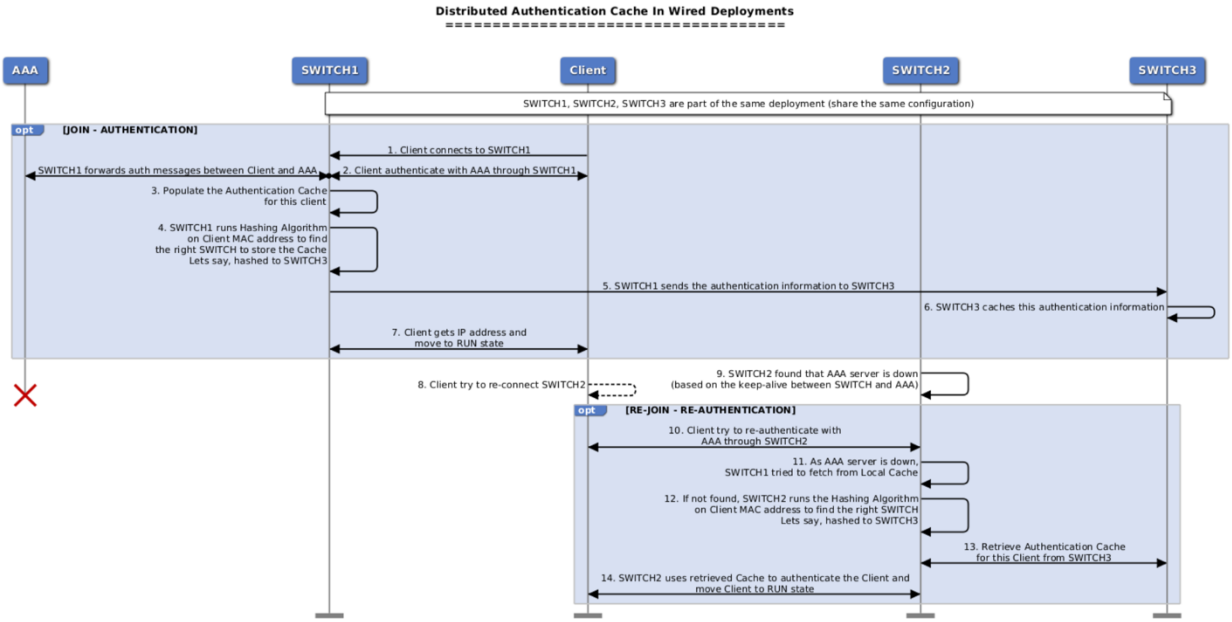


Figure-3

Figure-4 explain the step-by-step method using sequence diagram which shows the Authentication flow, Distributing Authentication Information based on consistent hashing, Retrieving Authentication Information using the same consistent hashing for Wireless Deployments.

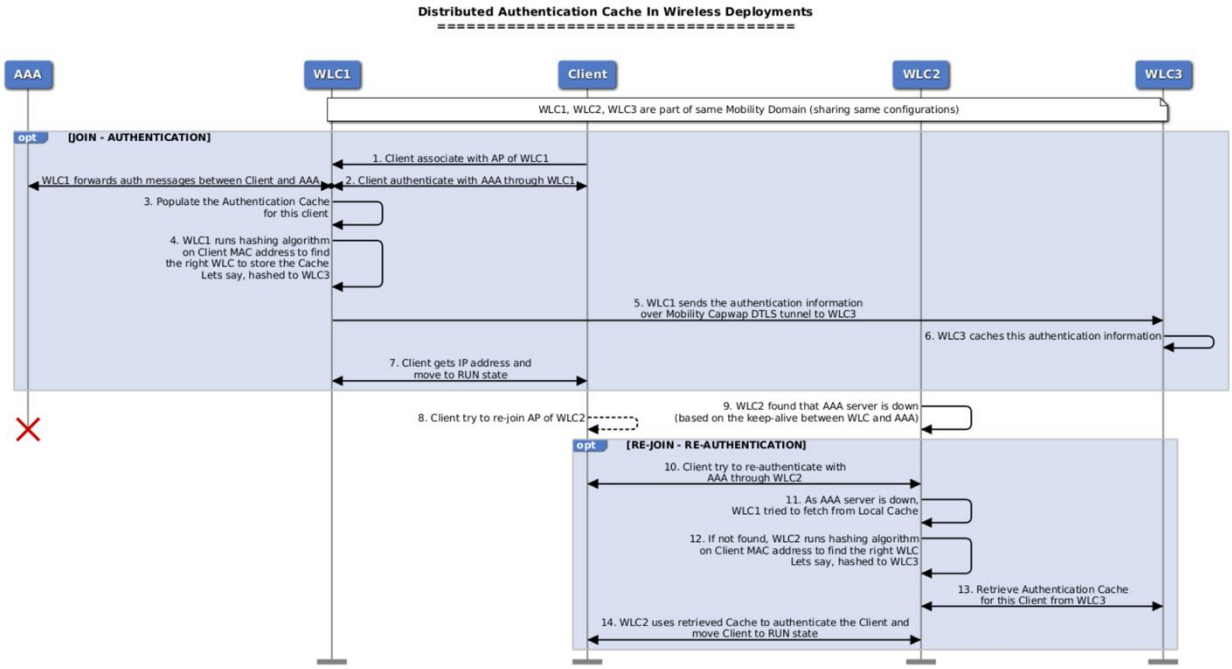


Figure-4

Notes:

- In Wireless Authentication can be at either at the WLC or at the AP. For simplicity, Central Authentication at WLC is considered, same is applicable for Local Authentication at AP.
- Here, method uses caching the NTHashed password exchanged between client and AAA server, same is used to authenticate during client re-connect.
- Even though transfer happens over the LAN, data is sensitive by nature and hence it is sent over existing encrypted tunnel.
- WLCs are manually added to the Mobility Domain and hence trust is established. Similarly, Switches are grouped manually to participate in a Consistent Hashing which in-turn provides trust.

In summary, the techniques presented herein describe method wherein client authentication during re-connect to different Switch/WLC would be successful even if AAA server(s) is/are still down OR not reachable. Here, client connect time would be improved by authenticating at Switch/WLC, using Cache as primary method instead of contacting AAA servers even if they are UP. Moreover, not replicating the authentication cache information on all the Switches/WLCs in the deployment, optimizes the memory requirements and there no multicast messaging to fetch the authentication cache information. Additionally, this method is scalable as number of clients supports in the deployment does not increase the memory requirement.