May 14, 2018

DYNAMIC WIRELESS LOCAL AREA NETWORK ACCESS CONTROL LIST PROVISIONING

Chethan Channappa

Mahesh Satyanarayana

DYNAMIC WIRELESS LOCAL AREA NETWORK ACCESS CONTROL LIST PROVISIONING

AUTHORS:
Chethan Channappa
Mahesh Satyanarayana

ABSTRACT

Techniques are described herein for optimizing Ternary Content-Addressable Memory (TCAM) space through a digital network architecture controller by preventing Access Control List (ACL) rules from being downloaded to TCAM until a client is associated with that Service Set Identifier (SSID). The space on the TCAM is freed once the last client on that particular SSID has disassociated.

DETAILED DESCRIPTION

Ternary Content-Addressable Memory (TCAM) is commonly used for packet classifiers and to represent Access Control Lists (ACLs). TCAM is a fast class of memory for matching packet headers against a set of entries represented as tuples of *value* and *mask* words. *Mask* serves to mask-out don't-care bits. Unfortunately, TCAM memory has a limited size, is a power drain, and impacts performance. As such, there is much interest in using smaller capacity TCAM. Smaller TCAM means less power consumption, less physical space, less price and faster lookup.

In the wireless world, each Wireless Local Area Network (WLAN) Service Set Identifier (SSID) typically has a WLAN ACL. The WLAN ACL is downloaded when the WLAN SSID is configured with the ACL and when the SSID comes up. This consumes space in TCAM even when no clients are connected to the SSID.

An Access Point (AP) supports up to 16 SSIDs and WLAN Controllers (WLCs) support approximately 512 WLANs. If an average of five rules per WLAN ACL are configured, approximately 2,500 rules may be stored in the TCAM. This limits the number of ACL rules that can be supported, increases power consumption, and prevents some services since TCAM space is limited or unavailable.

Normally, there are multiple WLANs configured across WLCs. However, there may not be any clients connected to those WLANs. In one example, the client limit may be reached on the controller and no more clients can join other WLANs. In another example, the WLANs are configured to support roaming but there are no roams occurring at the moment.

In accordance with techniques described herein, configuring WLAN ACLs at individual WLCs is removed. Instead, WLAN ACLs are configured and cached in a digital network architecture controller. WLAN ACLs may be downloaded on demand when the first client joins the SSID on that controller.

An example method for ACL download during client/device association is provided as follows. First, a device associates with an AP using a standard 802.11 association request. Second, the AP forwards this association request to the access WLC. Third, the access WLC detects this is the first client joining on this WLAN. Fourth, the access WLC sends a “Get WLAN ACL” request to an analytics engine (e.g., digital network architecture controller or identity services engine). Fifth, if the ACL exists for that WLAN, the analytics engine downloads the ACL to the access WLC. Sixth, once ACL download to TCAM and client join are successful, all client traffic is subjected to the WLAN ACL that is applied.

Figure 1 below illustrates the sequence for a first client join.

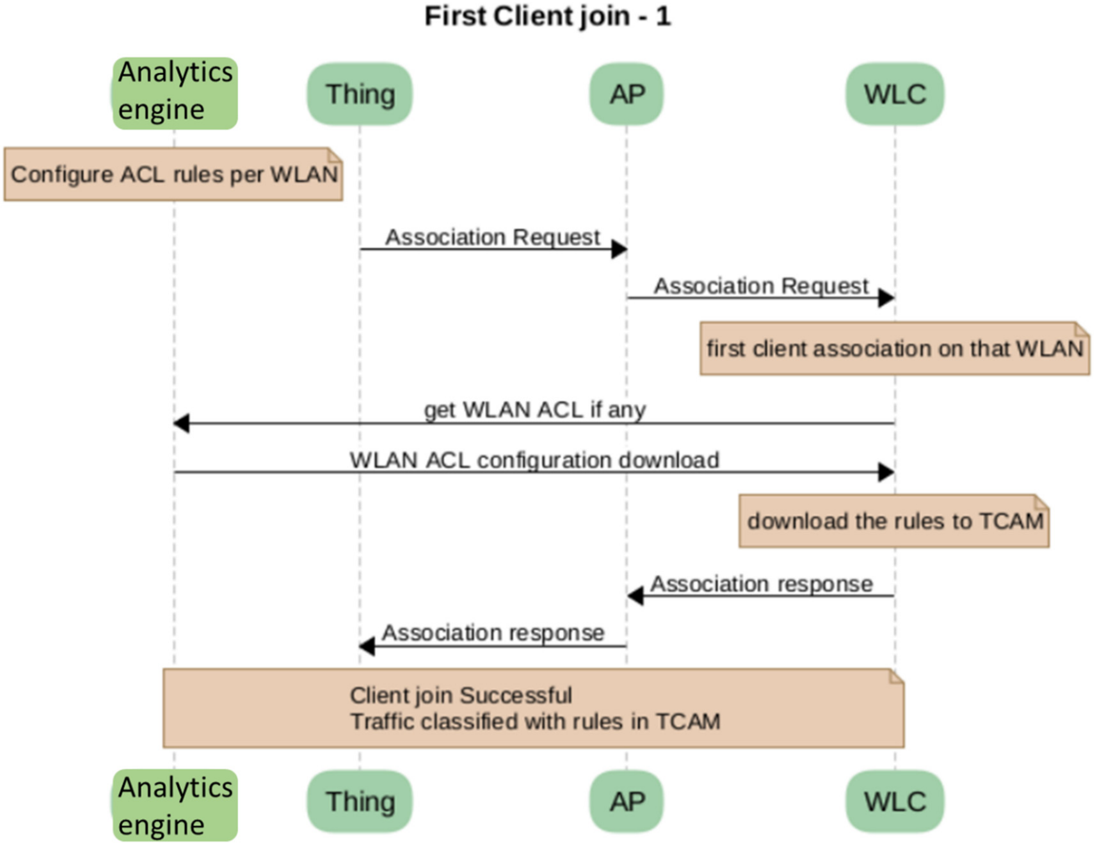

Figure 1

Subsequent client/device associations do not require obtaining the WLAN ACL since it is common for all clients under same WLAN. The sequence illustrated in Figure 1 above holds true even when the client roams to a different controller and is the first client associating with that controller.

When the last client/device disassociates/deauthenticates from the WLAN, the WLAN ACL is deleted from the TCAM and space is available to be used for other services.

Figure 2 below illustrates the sequence for a last client to deauthenticate.

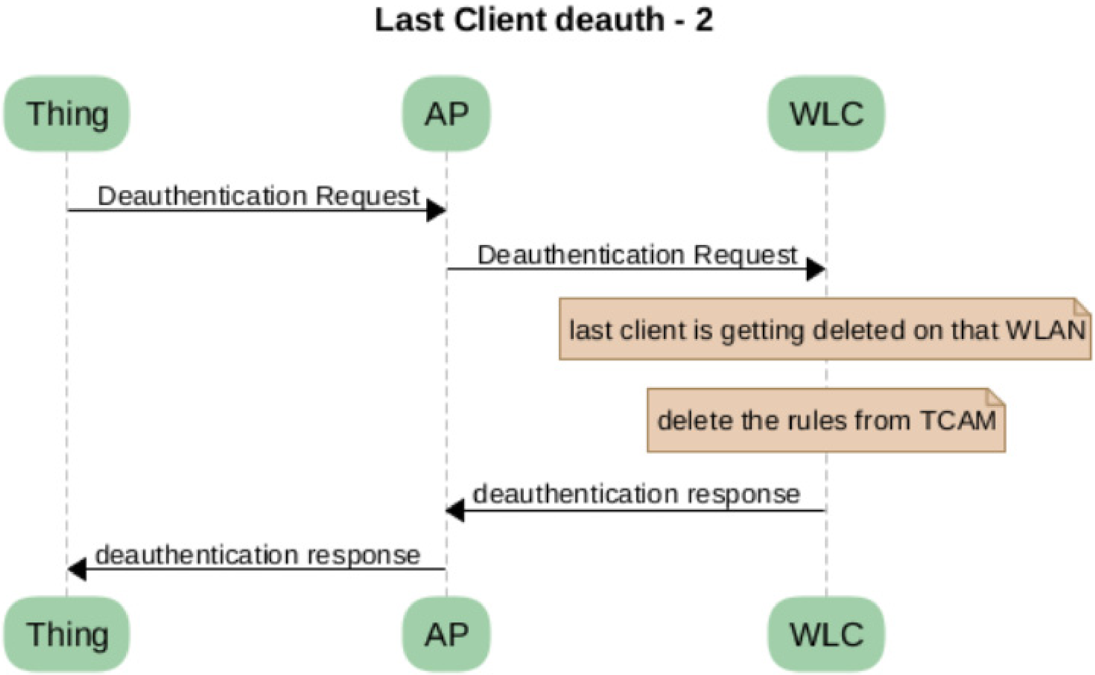
Last Client deauth - 2
Thing
AP
WLC
Deauthentication Request
Deauthentication Request
last client is getting deleted on that WLAN
delete the rules from TCAM
deauthentication response
deauthentication response
Thing
AP
WLC

Figure 2

In addition to saving TCAM space, another benefit to this approach is storing the WLAN ACL per SSID in a central location. This allows adding or updating ACL rules for a given SSID once and then propagating the change to all the devices instead of updating the ACL rules in every device.

In summary, techniques are described herein for optimizing TCAM space through a digital network architecture controller by preventing ACL rules from being downloaded to TCAM until a client is associated with that SSID. The space on the TCAM is freed once the last client on that particular SSID has disassociated.