March 2023

PREDICTIVE AND ADAPTIVE MAC LEARNING AS A SERVICE FOR CLOUD AND WIRELESS ENVIRONMENTS

Madhan Sankaranarayanan

Jaganbabu Rajamanickam

Alejandro Eguiarte

Akram Sheriff

Nagendra Kumar Nainar

PREDICTIVE AND ADAPTIVE MAC LEARNING AS A SERVICE FOR CLOUD AND WIRELESS ENVIRONMENTS

AUTHORS:
Madhan Sankaranarayanan
Jaganbabu Rajamanickam
Alejandro Eguiarte
Akram Sheriff
Nagendra Kumar Nainar

ABSTRACT

The protocols typically used by overlay technologies, such as Ethernet Virtual Private Network (EVPN), Virtual Extensible Local Area Network (VxLAN), Network Virtualization Overlays (NVO3), etc. are not designed to perform Media Access Control (MAC) learning validation. Thus, overlay environments may be subject to Denial-of-Service (DOS attacks), MAC spoofing, and other potential attacks/issues. Presented herein are techniques to facilitate a centralized service that performs MAC learning, referred to herein as "MAC Learning-as-a-Service" (MLaaS), such that MAC addresses, Internet Protocol (IP) addresses, and network virtualization edge (NVE) devices can be learned for an overlay environment. Such techniques as presented herein can provide for increasing the MAC scale when compared to network devices, can facilitate providing MAC/AP address priorities in Ternary Content-Addressable Memory (TCAM) of NVE devices based on certain device groups, can facilitate efficient MAC/IP address validation via machine learning and simulated direct probing, and can prevent traffic loss during MAC movement, which can be predicted through machine learning.

DETAILED DESCRIPTION

Data center environments are commonly implemented as a combination of virtual private cloud solutions, hybrid cloud, and public cloud solutions in which it is common to see different Layer 2 (L2) sites interconnected using various overlay technologies (e.g., EVPN, VxLAN, NVO3, etc.). In these scenarios, the overlay edge nodes, such as network virtualization edge (NVE) devices, provider edge (PE) devices, etc. utilize a data plane-based MAC learning process that involves exchanging MAC reachability information via

Border Gateway Protocol (BGP) communications. An example overlay environment diagram is shown below in Figure 1.

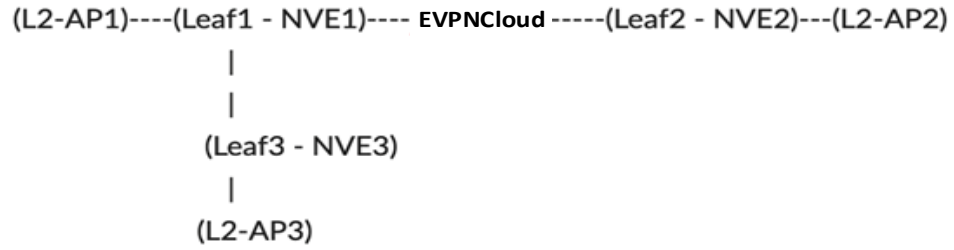

Figure 1: Example Overlay Environment

The protocols used by overlay technologies at NVE devices are not designed to perform MAC learning validation; therefore, such an environment could be subject to network attacks such as DOS attacks, MAC spoofing, or the like. For example, a DOS attack could cause an NVE device's MAC table to fill quickly with the MAC address of non-existent hosts, thereby causing the system to stop MAC learning temporarily, which could affect user traffic or stop traffic forwarding altogether.

In addition, another problem to which overlay transport networks are exposed is the high mobility of devices using the infrastructure. Current overlay protocols, such as EVPN, are able to allow MAC mobility via flooding and MAC advertising/learning mechanisms, however, there are no provisions to validate whether MAC movement events are legitimate and that they can be installed in target NVE devices in a timely manner. When mobile devices (e.g., user equipment, robots, automobiles, etc.) move from one access point (AP) to another, then updates for the MAC move state machine on the NVE devices could trigger a momentary packet loss at the devices.

For example in the diagram shown in Figure 1, above, if a mobile device moves from an AP connected to "L2-AP1" to "L2-AP3", then the traffic flowing from "L2-AP2" to "L2-AP1" will still continue flowing, however, until the mobile device MAC is learned on NVE3 and the MAC move state machine is stabilized on NVE3, traffic will not be received by the mobile device from the network.

Further, the NVE device's TCAM might not have enough space to store all the MAC addresses that the device has learned. Additionally, NVE devices typically do not include logic needed to validate MAC learning and could be susceptible to possible DOS

attacks. Currently in NVE devices, priority is not given to MAC addresses based on their grouping. Additionally, current overlay environments typically take a long time to detect, advertise, and learn the new location of a MAC address that moves across NVE devices in an overlay. Thus, until MAC mobility has reconverged for an overlay, traffic will not be forwarded for to a mobile device's new destination NVE, which can cause traffic loss for the device.

In order to address such issues, techniques of this proposal may facilitate a centralized service that performs MAC learning, referred to herein as "MAC Learning-as-a-Service" (MLaaS), such that MAC addresses, Internet Protocol (IP) addresses, and network virtualization edge (NVE) devices can be learned for an overlay environment.

The MLaaS service can be hosted anywhere in the transport network as a virtual machine (VM) or as a containerized application. The MLaaS service can include two components that can facilitate the MAC learning features of this proposal, a MAC Learning Module (MLM) and a MAC Query Module (MQM).

The MLM may perform various functions, such as learning MAC addresses and the NVE association of the learned MAC address through BGP or other similar protocol and storing newly learned MAC-to-NVE (M2N) mappings in a M2N inventory database (M2NDB) along with MAC metadata information that may include a MAC mapping lifespan (e.g., calculated via timestamps for the time at which MAC addresses are learned by different NVE), a group identifier (ID), and a preference level. The group ID and the preference level can be used for implementing advanced features, such as Quality of Service (QoS) features and/or MAC prediction features. The M2NDB can leverage any database redundancy and replication mechanisms currently known in the art. As every entry in the M2NDB will have a timestamp associated with NVE devices using the MLaaS service, preemptive MAC movement prediction and seamless MAC mobility can be facilitated in accordance with techniques of this proposal.

The MQM may also perform various functions, such that when an NVE EVPN VxLAN tunnel endpoint (VTEP) receives a packet in one of its interfaces, the NVE EVPN VTEP will send a query to the MQM component of the MLaaS that includes a MAC address and MAC metadata. If present in the M2NDB, the MQM will validate and then retrieve a corresponding MAC-to-NVE mapping for the queried MAC address, along with

the lifespan for the given MAC address. In case of a miss, the information will be transferred to the MLM for further MAC validation. Figure 2, below, illustrates an example details for a process flow that may be utilized to facilitate validating MAC entries for the MLaaS.

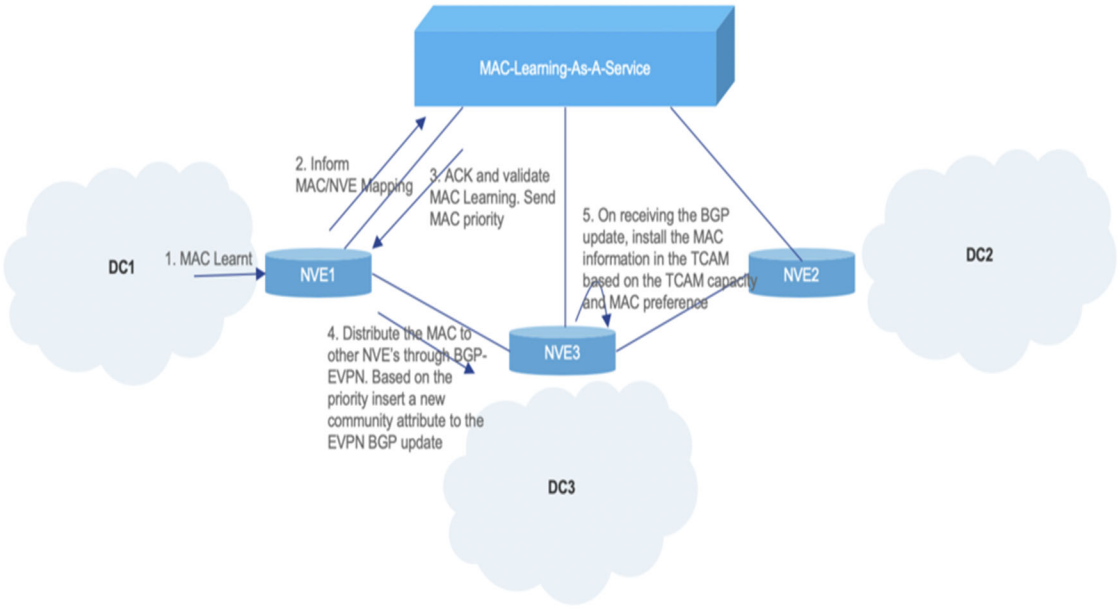

Figure 2: Example MAC Validation Process Flow

When an NVE device learns a MAC address on any of its interfaces, the device can send a query to the MQM to perform MAC validation on the address since the service stores the inventory and tracks MAC inventory. In case the MQM determines there has been a MAC validation failure due to a discrepancy in MAC locations or MAC alive time range, then the NVE device can request the MLM module to install a new MAC-to-NVE mapping. Optionally, MQM could inform the NVE device to block those MAC entries.

In some scenarios, when MAC addresses are learned, the MAC addresses could be grouped into a specific category based on the VLAN or a static pre-configuration that can be programmed via an association policy.

In still some scenarios, when a container or specific MAC move occurs from one NVE device to another NVE device, then information regarding the move could be passed to the MLaaS, which could trigger the MLaaS to install an egress replication for that MAC to its local port as well as the new NVE device involved in the MAC move. Figure 3,

below, illustrates example details for an example process flow that can be utilized to facilitate seamless mobility using the MLaaS as proposed herein.

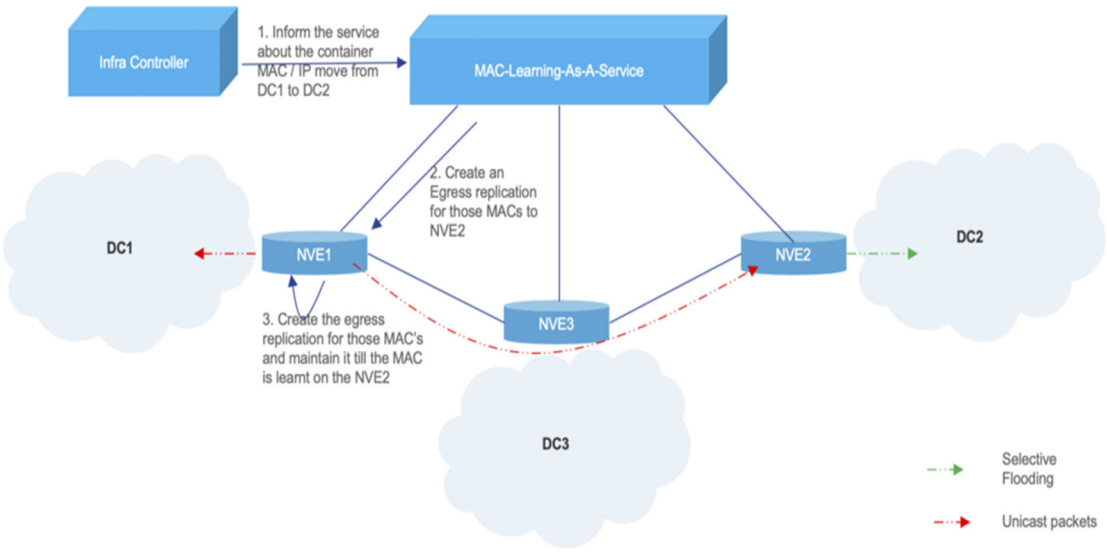

Figure 3: Facilitating Seamless Mobility Using the MLaaS

The MQM can also communicate with the egress NVE device so that the device installs a tentative MAC entry reachable via one of its interfaces at a specific time with a target MAC alive time range. The effect of such operations will be that packets for a given flow will be duplicated for a short period of time, one to the old destination NVE device and another to the new destination NVE device. The virtual network identifier (VNI) used to replicate the data traffic to the new NVE should be provided in such a way that it should flood the packets to all the VLAN ports on the new egress NVE device until the device learns the MAC address from their port.

Consider, for example, a scenario involving an example environment as shown below in Figure 4, in which a mobile device moves from an AP connected to "L2-AP1" to "L2-AP3."

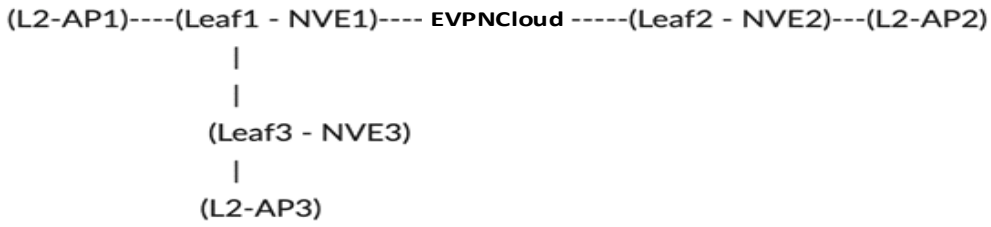

Figure 4: Example Environment

For the scenario involving Figure 4, the traffic flowing from "L2-AP2" to "L2-AP1" will still continue flowing and the packets should be replicated from Leaf1 to Leaf3 via an egress replication application. As the packets are replicated in Leaf3-NV3, there will be no packet drops when the device is moved from L2-AP1 to L2-AP3.

Accordingly, the techniques presented herein may solve MAC address learning problems that may arise in data center network environments via a MLaaS. The techniques proposed herein can provide various benefits for cloud environments involving L2 sites interconnected with different overlay technologies (e.g., Layer 3 (L3) Virtual Routing and Forwarding (VRF) environments in which each VRF has its own forwarding table and routing process (RIP, EIGRP, OSPF, BGP, etc.) and interconnect options (802.1q, GRE, sub-interfaces, physical cables, signaling, etc.) and a device may associate to one or more L3 interfaces on a router/switch) that may experience scalability challenges with compute devices becoming active for a brief period of time in different parts of the infrastructure.

Further, the MLaaS could provide various features, such as facilitating new host provider identity captures (involving dynamic host configuration protocol (DHCP) packets), storing MAC address and VLAN mappings, sending MAC event information, caching time-to-live (TTL) information, supporting or enabling GET/REMOVE application programming interfaces (APIs), supporting cluster modes, providing MAC filtering, preventing MAC spoofing, and/or facilitating prioritization of MAC addresses based newly proposed attributes, such as a group ID (e.g., virtual private cloud (VPC) ID) and a preference level. In some instances, the MLaaS can limit the overwriting of a MAC address entry of a high-priority Ethernet service instance only when the MAC address is learned on another high-priority Ethernet service instance and can be configured to include or otherwise be associated with an overlay edge node's MAC address, such as an NVE or PE address.