June 2023

HOST MOBILITY MECHANISM FOR AN IP NETWORK

Patrice Brissette

Andy Karch

Jiri Chaloupka

Mike RE Mallin

HOST MOBILITY MECHANISM FOR AN IP NETWORK

AUTHORS:
Patrice Brissette
Andy Karch
Jiri Chaloupka
Mike RE Mallin

ABSTRACT

Ethernet Virtual Private Network (EVPN) mechanisms are designed using bridge domains and integrated routing and bridging (IRB) capabilities that rely on data plane Media Access Control (MAC) learning to associate hosts to corresponding interfaces on provider edge (PE) routers. However, there are no existing mechanisms that allow for the ability to trigger seamless host mobility in the control plane when a Layer 3 (L3)/ Internet Protocol (IP) forwarding paradigm is used for a network environment. In order to address such issues, techniques are presented herein that provide for the ability to learn seamless host motion based only on an IP capability that leverages existing data plane constructs to trigger mobility such that a data plane redesign is not required. Through techniques presented herein, the IP security check punt path can be relied upon to learn host connectivity to a specific interface.

DETAILED DESCRIPTION

There is currently no data plane learning mechanism to trigger mobility between PE routers or even between different interfaces on the same PE router for L3/IP forwarding implementations. Rather, L3 relies on the control plane to provide forwarding information and mobility can be achieved by having a host or consumer edge (CE) device send protocol messages (e.g., Gratuitous Address Resolution Protocol (GARP) messages, etc.) to a PE.

However, seamless motion for a moving host/CE cannot be supported using such techniques when the host/CE simply keeps sending traffic towards a newly connected PE without announcing itself. Thus, no existing mechanisms allow for the ability to trigger seamless host mobility in the control plane when only a L3/IP forwarding paradigm is employed for a network environment.

In order to address such issues, techniques are presented herein that provide for the ability to learn seamless host motion based only on an IP capability that leverages existing data plane constructs to trigger mobility such that a data plane redesign is not required. Through techniques presented herein, the IP security check punt path can be relied upon to learn host connectivity to a specific interface.

During operation, IP security checks (such as unicast reverse-path-forwarding (uRPF) or the like) can be leveraged via data plane L3 capabilities provided by a network processing unit (NPU). Utilizing security check features (e.g., strict-uRPF features), the same functionality (including punt path) can be extended to support host mobility learning.

Mobility machinery typically relies on 2 factors:

- ARP/Neighbor Discovery (ND) based learning that can be used, for example, when a host announces itself on motion (e.g., GARP); and
- Security check-based learning that conceptually operates the same way as strict-uRPF without pruning such that a source IP security violation message can trigger IP Mobility.

ARP/ND-based learning mechanisms already exist in EVPN today. Techniques of this proposal do not require modification of such existing approaches. Rather, novelty for the techniques of this proposal involve the usage of security check functionality to punt the proper messages (per host motion) to the control plane. For example, a security check mechanism can be utilized to punt any incoming IP packet to software when the localization of the source IP address changes.

In the case of a host motion, the source IP that is sent from a remote PE becomes locally learned. The same concept can also be utilized for cases in which motion occurs between local interfaces since the localization changes too. However, it is important that an implementation ensure dropping repeated packets such that only a single notification is provided to CPU. The notification may be sent directly to an ARP/ND module at which the adjacency of the moved host is learned directly.

In some instances, a security policy may be applied prior to learning. In still some instances, an ARP/ND module may decide to probe for newly learned host. Motion notifications sent to other PE routes can be provided in a similar manner as current EVPN

mechanisms as provided by Internet Engineering Task Force (IETF) Request For Comments (RFC) 7432.

In some instances, techniques of this proposal can also be extended to provide a solution for speculative host motion such that on a first motion detection, all hosts under a specific MAC may be marked as moved. Probing may be used to validate these motions.

Since the IP security check learning capability is based on well-known hardware capability (e.g., strict-URPF feature), proper special handling can be utilized to avoid clashes with motion detection. Table 1, below, illustrates various example details regarding IP security check learning features that may be realized in accordance with the techniques presented herein.

TABLE 1

Mobility IP Security	OFF	ARP/ND based learning
OFF	Forward packet	Forward packet ARP resolution (Wait for ARP to move on new AC)
Loose	Punt and drop	Punt and forward (Wait for ARP to move on new AC)
Strict	Punt and drop	Punt and drop (Wait for ARP to move on new AC)

Different types of motion may be supported using the techniques of this proposal, such as, for example:

1) MACx-IPx to MACx-IPx - Detection can be provided via security checks by seeing a new localization of the IP address.
2) MACx-IPx to MACx-IPy – Analogous to learning a brand-new host, EVPN machinery handles the motion as per standards-based mechanisms.
3) MACx-IPx to MACy-IPx – Similar scenario (1) from the learning point of view, MAC motion can be handled with current EVPN machinery.

4) MACx-IPx to MACy-IPy – Similar to scenario (2), EVPN machinery can handle the motion as per standards-based mechanisms.

Accordingly, techniques herein provide for the ability to learn seamless host motion based only on an IP capability that leverages existing data plane constructs to trigger mobility such that a data plane redesign is not required. The IP security check punt path can be relied upon to learn host connectivity to a specific interface. Various advantages may be realized through use of such techniques, such is limiting the mixing of Layer 2 (L2) and L3 constructs in order to support seamless host motion including bridge domains and MAC learning functionality. Further, the techniques can be implemented for both pure L3 solutions and for L3 forwarding chains and can reuse existing NPU/hardware capabilities. A similar punt rate as MAC learning can also be achieved through the techniques of this proposal and security policies can be easily applied directly in ARP/ND protocols. Further, probing to approve motion is purely optional. Thus, techniques of this proposal can be viewed as completely RFC and standard compliant and can be utilized to enhance service overlay solution platforms using purely IP capabilities for any combination of operational, provisioning, debugging, service assurance, and/or telemetry aspects of such platforms.