Building scalable and secure multipoint L3-VPN: Mininet prototype

***Abstract*—In this short document we describe scalable and secure multipoint L3-VPN architecture. We implement the prototype in Mininet framework and evaluate end-to-end performance of the hosts which are part of the L3-VPN. We consider two setups: with hop-by-hop authentication and without. Furthermore, we consider that the authentication keys are distributed with Host Identity Protocol, and that the routers authenticate themselves using public keys. We conclude the paper with comparision of different approaches for building the VPLS networks.**

I. Introduction

Today many organizations are having multiple branch offices that are geographically separated. Connecting these offices with secure communication channels is a must. The number of offices can be a large number and, thus, scalability is another crucial requirement.

We consider a multipoint L3-VPN in this work. The routers which are part of this VPN are arranged in such a manner (hub-and-spoke arrangement) so that scalability requirement is fulfilled. To secure the network we use Host Identity Protocol [3]. We consider that routers perform so called base exchange to negotiate authentication key on hop-by-hop bases (a separate base exchange is performed between pairs of nodes). Although, encryption is prerogative of the customers, packet authentication is performed in a hop-by-hop manner by the routers on the path. To understand the performance of the proposed architecture we compare two setups: one with hop-by-hop packet authentication and the second without authentication header attached to the packets at every hop in L3-VPN network. Finally, we perform brief analysis of various approaches for building VPLS networks.

II. Architecture

The overall architecture which we have implemented in Mininet framework is shown in Figure 1. The architecture of the distributed L3-VPN network is of hub-and-spoke type. Hub nodes comprise the backbone of the network, whereas, multiple spoke PE elements are attached to the hubs. This allows to achieve scalability property. The security of the network is achieved by using Host Identity Protocol to negotiated the authentication keys, whereas, actual packet authentication is performed on hop-by-hop bases using HMAC-SHA256 algorithm [4].

The Mininet prototype is available online and can be found in GitHub [2].

III. Experimental evaluation

We compared performance of two different setups in Mininet framework. In Figure 2 we show the distribution of

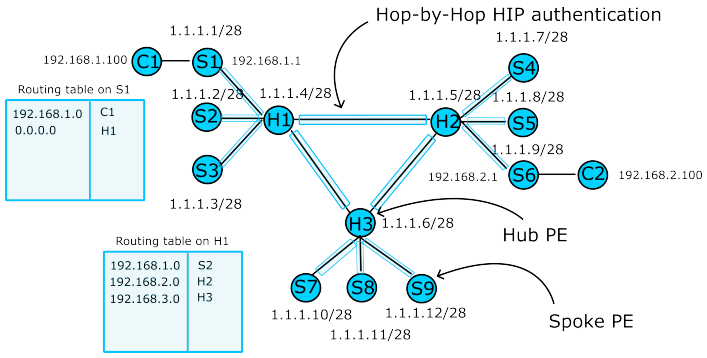

Fig. 1: High-level architecture of L3-VPN deployed in Mininet

throughput for setup with hop-by-hop authentication enabled and with authentication disabled. Clearly, performance consumes lots of resources. Better design can consider, using single key shared between all routers and employ authentication selectively in order to save computation power of the forwarding elements.

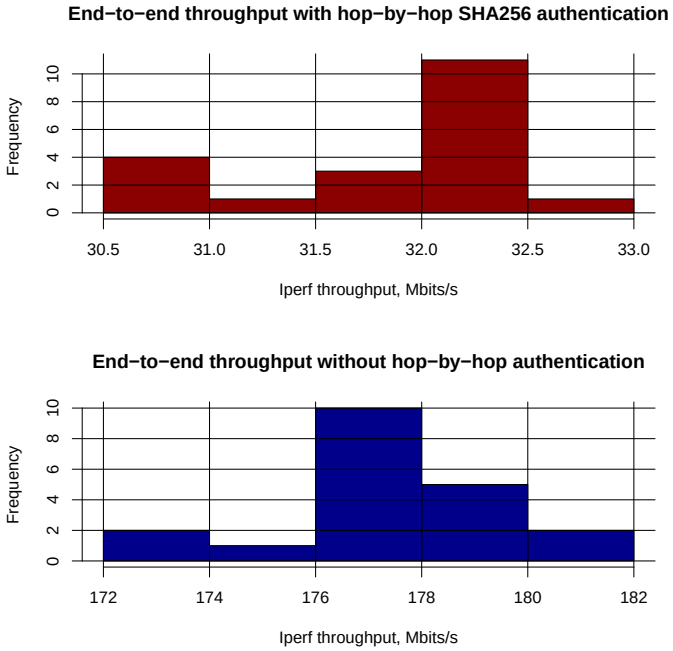

Fig. 2: Throughput comparison

Characteristic ↓ Overlay type →	L2-VPLS	L3-VPN	HIP-VPLS [1]
Size of forwarding/routing table	$O(n)$, n-number of hosts	$O(m)$, m - number of subnetworks	$O(n)$
Number of links in mesh	$O(k^2)$, k - number of Hub-PEs	$O(k^2)$	$O(l^2)$, l - number of PEs
Privacy	MACs are exposed to PEs	IPs are exposed to PEs	No exposure of MACs and IPs (PEs are part of customers infrastructure)
Encryption and authentication	Hop-by-hop	Hop-by-hop	End-to-end
Tunneling mode	Ethernet-in-IP	IP-in-IP	Ethernet-in-IP
Loop free-topology	802.1d protocol/central controller	Central controller	Not required

TABLE I: Comparison study of different multipoint VPLS/VPN designs

REFERENCES

[1] HIP-based Virtual Private LAN Service (HIPLS. https://datatracker.ietf.org/doc/draft-henderson-hip-vpls/.

[2] L3-VPN in Mininet. https://github.com/dmitriykuptsov/vpls-routing.

[3] A. Gurtov. *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*. Wiley Publishing, 2008.

[4] D. Stinson. *Cryptography: Theory and Practice, Second Edition*. CRC/C&H, 2nd edition, 2002.