draft-sajassi-bess-evpn-first-hop-security-00

A. Sajassi (Cisco), L. Krattiger (Cisco), K. Ananthamurthy (Cisco), S. Thoria(Cisco)

IETF 116, March 2023

Yokohama

Background

- DHCP Snoop Database
  - Stores valid IPv4/IPv6 MAC bindings by snooping DHCP messages
- First Hop Security (FHS)
  - ARP Inspection, ND Inspection and IPv4/IPv6 Source Guard make use of DHCP bindings
- FHS is widely deployed on access switches without standard based multihoming and host mobility

Problem Statement

- Extend application of FHS on EVPN PEs supporting Network Virtualization Overlay (NVO) and running multi-homing (All-Active or Single-Active) with host mobility
  - BGP extensions and new procedures for EVPN to support FHS in presence of EVPN multi-homing and host mobility by distributing DHCP Snoop bindings among EVPN PEs participating in that EVPN instance (EVI) are to be defined
- This drafts defines new EVPN route type to synchronize DHCP Snoop Database

Requirements

- Extend application of FHS
  - EVPN PEs supporting multihoming (All-Active or Single-Active)
  - Host mobility between the PEs participating in same EVPN instance
  - Support Bridge and IRB service

Primer: DHCP Snoop

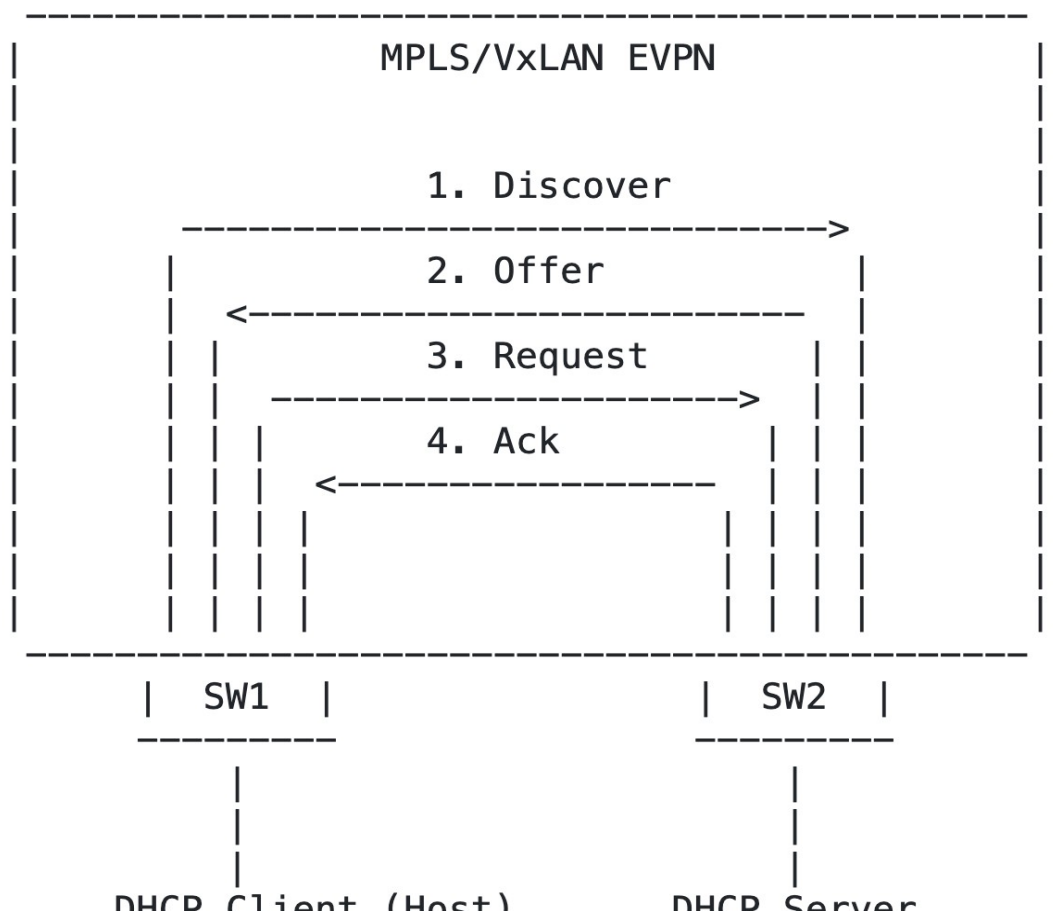
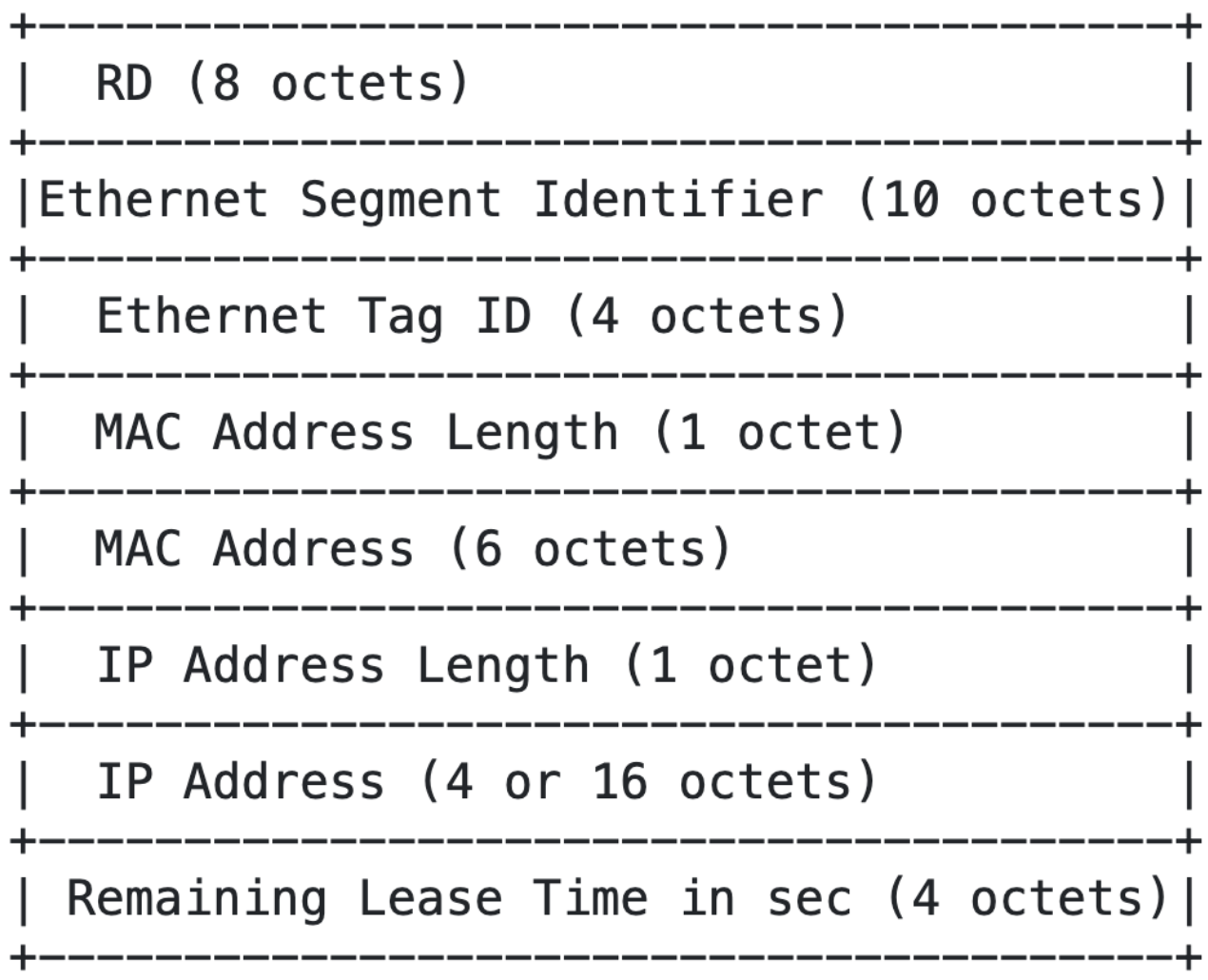


Figure 1: DHCP DORA Exchange over EVPN Fabric

DHCP Snoop Route format

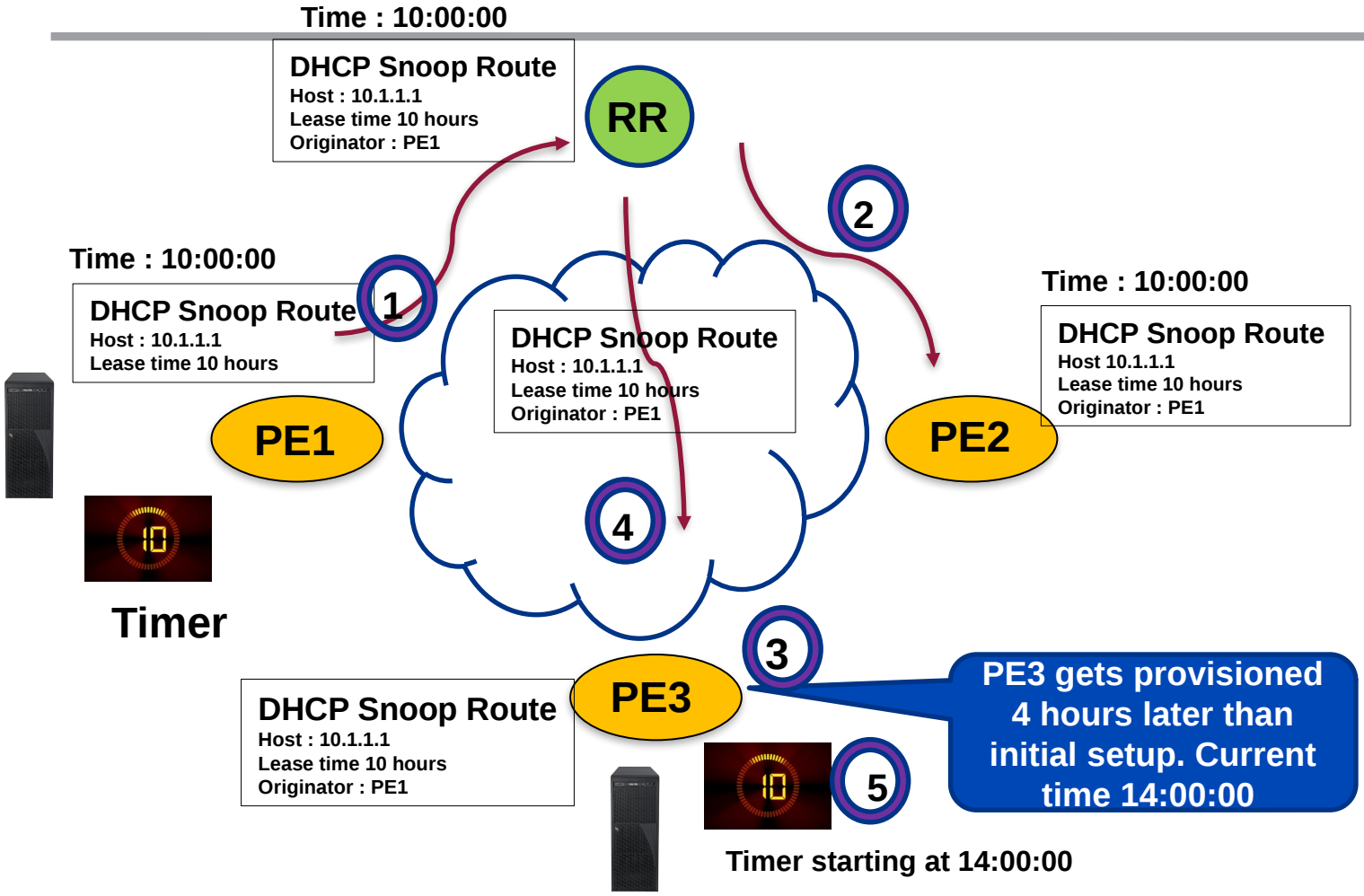


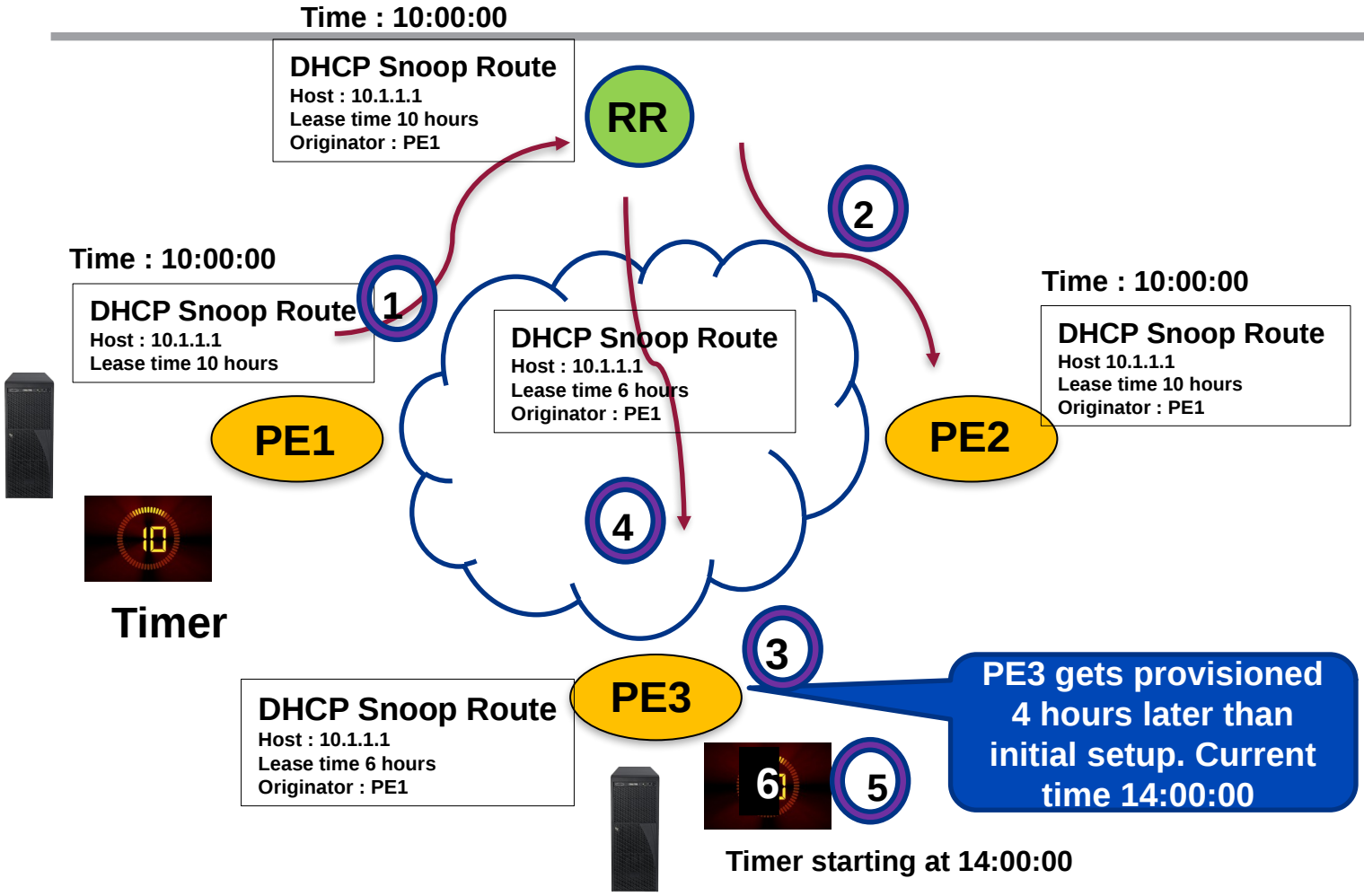
DHCP Snoop Route

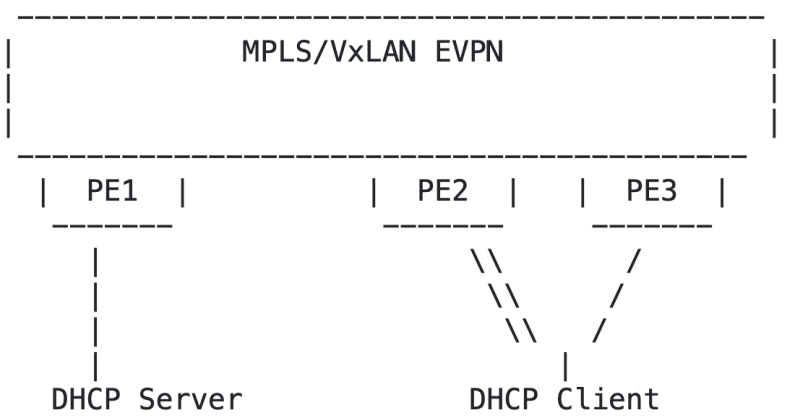
- PE where host is attached sends DHCP snoop route after completion of DORA exchange. This PE will be referred as **DHCP Snoop Anchor PE**
- Remote PE updates the DHCP Snoop Database after receiving DHCP snoop route
- When the host moves to new PE, it successfully validates the host
- Lease timer expiry will trigger withdraw
- DHCP lease renew will trigger DHCP snoop route update with remaining lease time

Remaining Lease Time

- DHCP renew lease time.
- Anchor PE sets the initial lease time received from the DHCP server
- BGP speakers maintain create/update timestamp of DHCP snoop route.
- Remaining lease time calculated as follows while advertising it to the BGP peers
  - Current timestamp: **`current_timestamp`**
  - Create/update timestamp**: `create_update_timestamp`**
  - Received remaining lease time: **`rcvd_rem_lease_time`**
  - Remaining lease time = **`rcvd_rem_lease_time - (current_timestamp - create_update_timestamp)`**
    - If value is negative then send ZERO

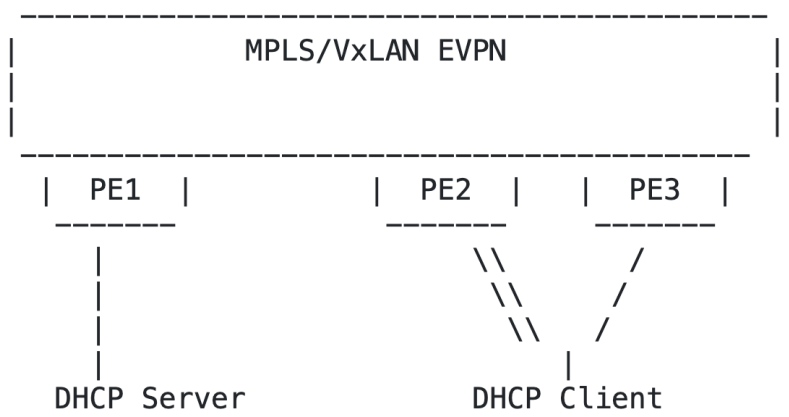

Time : 10:00:00
DHCP Snoop Route
Host : 10.1.1.1
Lease time 10 hours
Originator : PE1
RR
1
2
Time : 10:00:00
DHCP Snoop Route
Host : 10.1.1.1
Lease time 10 hours
DHCP Snoop Route
Host : 10.1.1.1
Lease time 10 hours
Originator : PE1
Time : 10:00:00
DHCP Snoop Route
Host 10.1.1.1
Lease time 10 hours
Originator : PE1
PE1
PE2
4
Timer
3
PE3
PE3 gets provisioned 4 hours later than initial setup. Current time 14:00:00
DHCP Snoop Route
Host : 10.1.1.1
Lease time 10 hours
Originator : PE1
5
Timer starting at 14:00:00


Time : 10:00:00
DHCP Snoop Route
Host : 10.1.1.1
Lease time 10 hours
Originator : PE1
RR
2
Time : 10:00:00
DHCP Snoop Route
Host : 10.1.1.1
Lease time 10 hours
1
Time : 10:00:00
DHCP Snoop Route
Host 10.1.1.1
Lease time 10 hours
Originator : PE1
DHCP Snoop Route
Host : 10.1.1.1
Lease time 6 hours
Originator : PE1
PE1
PE2
4
Timer
3
PE3
PE3 gets provisioned 4 hours later than initial setup. Current time 14:00:00
DHCP Snoop Route
Host : 10.1.1.1
Lease time 6 hours
Originator : PE1
5
Timer starting at 14:00:00



Bridge Service

- Single Active multihoming
  - DORA messages will arrive on single PE
  - Active PE will be the Anchor PE and originates DHCP snoop route
- All Active multihoming
  - No individual DORA message synchronization
  - Make use of Anchor PE DHCP snoop route
- Remote PEs in the same EVI
  - Updates the DHCP snoop database.
  - This DHCP state will be used when the host moves from its existing ESI to a new ESI.



IRB Service

- DORA messages are unicasted to DHCP server via DHCP Relay(s)
  - Source IP address in relay is unique to the PE, such thar server messages lands on the PE which initiated the relay message
- Single Active/All Active multihoming
  - DORA messages will arrive on single PE
  - Make use of Anchor PE DHCP snoop route
- Remote PEs in the same EVI
  - Updates the DHCP snoop database.
  - This DHCP state will be used when the host moves from its existing ESI to a new ESI.

DHCP Snoop Anchor Mobility (1)

- Host moves are determined via GARP/RARP
  - DHCP Snoop Entry is already synced in the fabric
  - Initiates rfc7432 mobility procedures and after completion DHCP Snoop Anchor will be moved
- Duplicate Case
  - Duplicate-wait-timer with default value of 30 sec
  - After the expiry of duplicate-wait-timer, anchor will be moved if MAC/IP in the DHCP snoop route is pointing local. If not then Anchor will not be moved. Subsequent Host mobility will again start the duplicate-wait-timer

DHCP Snoop Anchor Mobility (2)

- MAC Mobility extended community attribute defined rfc7432 will be used for DHCP snoop route
  - Sequence number is handling is similar to Mac mobility procedures defined in rfc7432

Next Step

- Work in progress to handle more scenarios.
- Solicit more input from WG

THANK YOU!