

# draft-sajassi-bess-evpn-first-hop-security-01

<https://datatracker.ietf.org/doc/html/draft-sajassi-bess-evpn-first-hop-security-01>

Ali Sajassi (Cisco),  
Lukas Krattiger (Cisco),  
Krishna Ananthamurthy (Cisco),  
Ssmir. Thoria(Cisco)

IETF 117, July 2023  
San Francisco

# Recap

- Presented in IETF-116
- Addressed comments related to NLRI modifications at transit router like Route Reflectors
- 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

# Changes in latest version

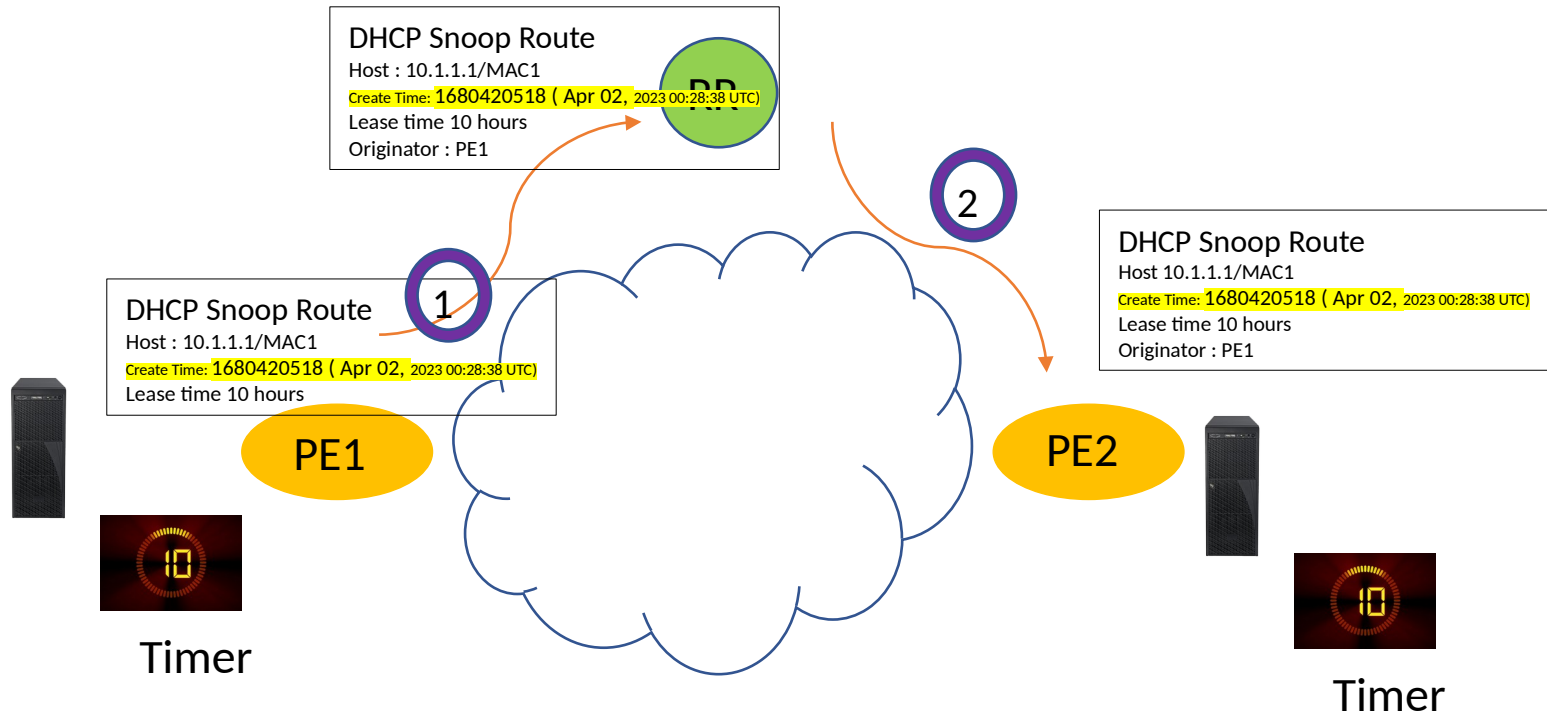
0 <sup>th</sup> version	1 <sup>st</sup> version
Remaining Lease Time	Lease Time
-	Create Time in seconds (EPOCH - 1 <sup>st</sup> January 1970)
Modification of NLRI on transit BGP speakers (Route Reflectors)	No modifications needed on transit BGP speakers
No requirement of network timestamp	Network timestamp is needed (devices are always timestamp synced in the network)
Lease time calculation uses local create time and remaining lease time	Lease time calculation on remote PE uses received create time from anchor PE, local time and lease time

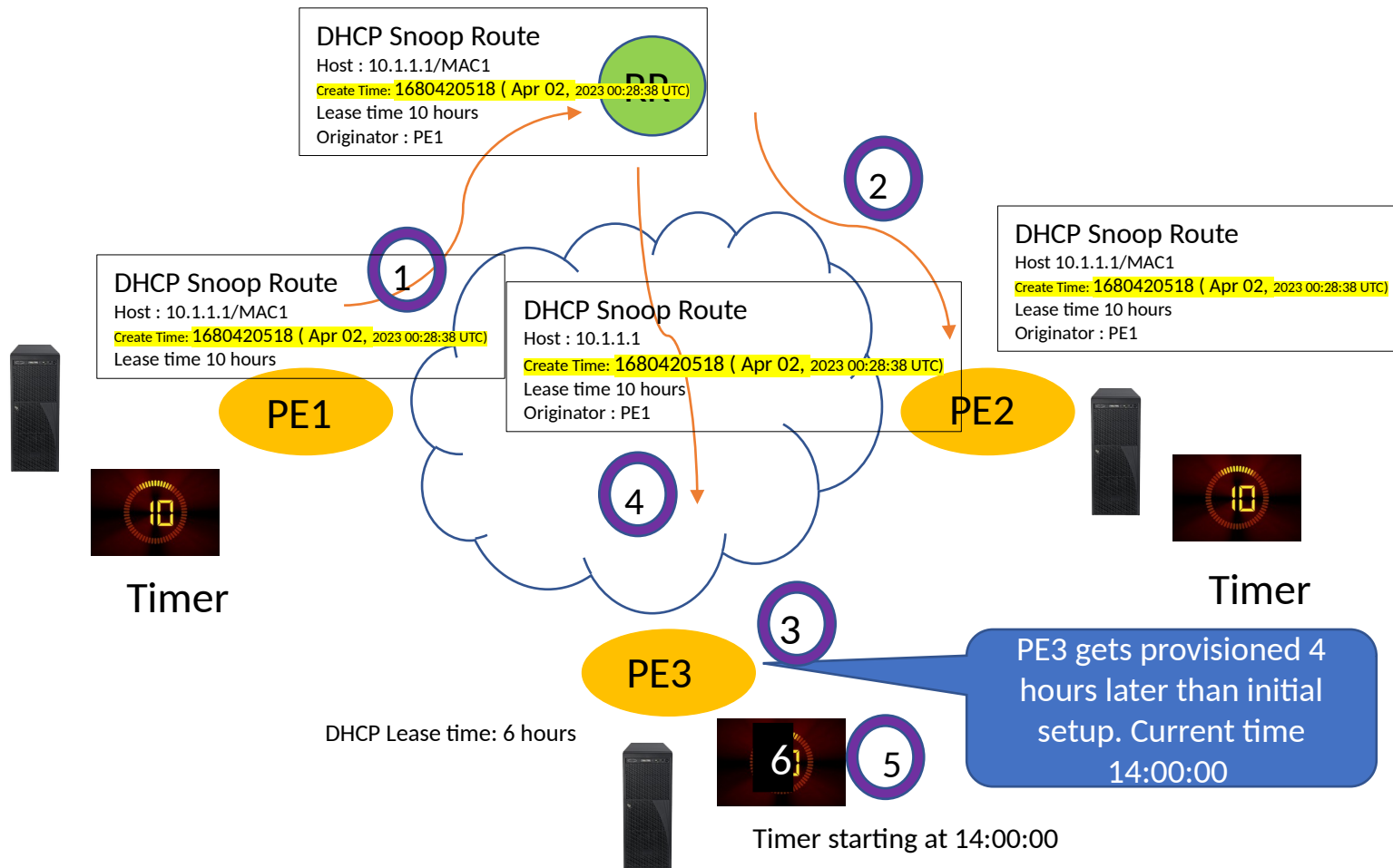
# DHCP Snoop Route format

```
+-----+
|  RD (8 octets)  |
+-----+
|Ethernet Segment Identifier (10 octets)|
+-----+
|  Ethernet Tag ID (4 octets)  |
+-----+
|  MAC Address Length (1 octet) |
+-----+
|  MAC Address (6 octets)      |
+-----+
|  IP Address Length (1 octet) |
+-----+
|  IP Address (4 or 16 octets) |
+-----+
| Create Time in sec (8 octets) |
+-----+
|  Lease Time in sec (4 octets) |
+-----+
```

# Remote PE: Lease Time Calculation

- Anchor PE propagates Create/Update lease time when DHCP snoop entry gets created together with lease time received from the DHCP server
- Transit BGP speakers transparently propagates NLRI without any modifications
- Time stamps should be synced via NTP (as an example)
- Lease time calculated as follows on remote PEs
  - Create timestamp received in NLRI: **create\_timestamp**
  - Local timestamp when DHCP snoop Route is received: **local\_timestamp**
  - Received lease time: **rcvd\_lease\_time**
  - Lease time to be used on remote PE =  $\text{rcvd\_lease\_time} - (\text{local\_timestamp} - \text{create\_timestamp})$





# Next Step

- Solicit more input from WG

Thank You!