LISP Control-Plane in Campus Fabric

A Practical Guide to Understand the Operation of Campus Fabric

Toni Pasanen, CCIE 28158

Table of Contents

Chapter 3: LISP Control-Plane: EID-to-RLOC Registration

The LISP Control-Plane operation can be split into two-part. First, registering EID-to-RLOC information to the Map-Server by Ingress Tunnel Routers (ITR). Second, finding the location of an endpoint by requesting EID-to-RLOC information from the Map-Server by Ingress Tunnel Router (ETR).

Registration Phase 1: TCP Probe

In figure 3-1, Host-A joins the network. It generates a Gratuitous-ARP message to verify that its IP address is unique and also to inform the first-hop-router Edge-1 that it has joined the network. When Edge-1 receives the GARP-messages, it starts the EID-to-RLOC registration process. Before sending a Map-Register message, the ETR Edge-1 verifies the IP connectivity to Map-Server by sending a TCP-message with an SYN-bit and destination port 4342. As a response to the TCP SYN message, Map-Server replies with TCP-message where both ACK and RST bits are set. The RST-bit set because Edge-1 uses TCP SYN message as a probe, not as a TCP-connection opening request, and there is no need to establish a TCP connection at this phase.

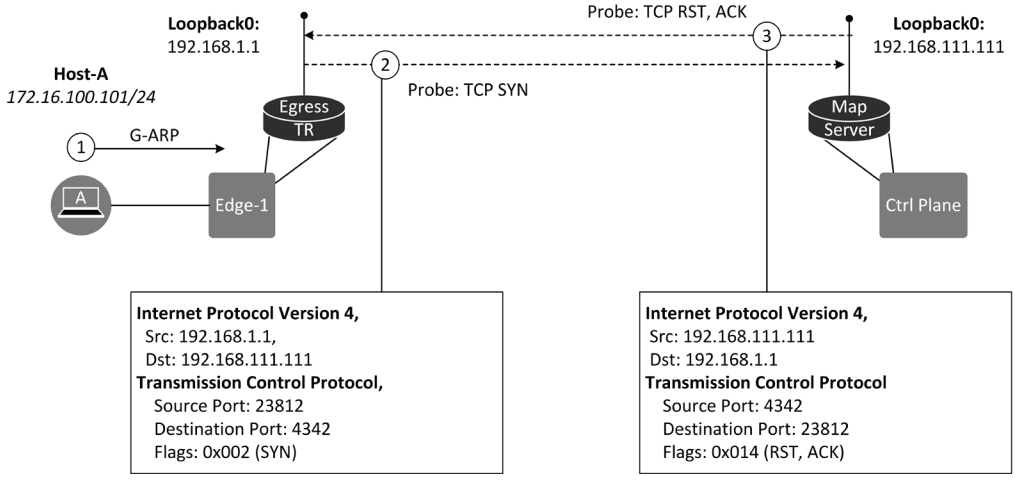


Figure 3-1: *EID-to-RLOC Registration - TCP Probe.*

Registration Phase 2: UDP based Map-Register from ETR to MS

After verifying the IP connectivity to Map-Server, ETR Edge-1 sends a *Map-Register* message to Map-Server. Figure 3-2 illustrates the partial packet captured from the core link of Edge-1, the complete capture is shown in Capture 3-1. The message is sent to Map-Server over unreliable UDP connection (dst. port 4342) by using Edge-1 ETR RLOC IP address as a source address. The type-field value 3 defines that this is a Map-Register message.

The *P-bit (Proxy-Map-reply):* When set states that a Map-Server can respond on behalf of Edge-1 to Map-Request concerning requested EID 172.16.100.101/32.

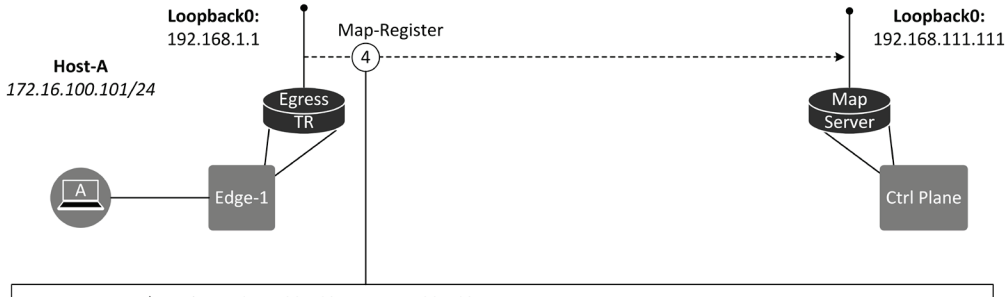
The *I-Bit (xTR-ID Present):* When set, it means that this message carries a randomly generated 128-bits XTR-ID identifier of Edge-1 and 64-bit site id (not defined).

The *M-bit (Want-Map-Notify):* When set, tells to receiving Map-Server that it should acknowledge the received Map-register message by replying with a *Map-Notify* message.

The eight octets "*Nonce"* filed is used for protecting against *Map-Register reply attacks.* When ERT Edge-1 receives the *Map-Notify* message used as an acknowledgment to Map-Register message, Edge-1 verifies that the "nonce" value matches to "nonce" value in the original Map-Register message. In addition, ETR Edge-1 keeps track of the "nonce" value that it has used and every time it sends a new Map-Register message, it increments the value. The Map-Server stores the "nonce" value received via the ETR Edge-1 Map-Register message into the EID-to-RLOC database along with XTR-ID. When the ETR component of Edge-1, identified with XTR-ID sends the next Map-Register message (or any other LISP message), the "nonce" value should be bigger than the last received and stored "nonce" value. If this is not true, the Map-Server concerns the message as a *"reply-attacks"* and drops the Map-Register message.

The Map-Register message describes the EID record and RLOC record. *The EID-record* describes the Instance-Id where the EID 172.16.100.101/32 belongs to and it is used as a VPN identifier. Note that we are not using a VRF aware Map-Server. Time-to-Live value describes how long this EID mapping information is valid. The default value is 1440 seconds (24 hours). An *Authoritative-bit,* when set, defines that sending ETR is the actual last-hop-router for this EID. The *Locator-record* describes the RLOC specific information. It describes RLOC IP address

mapped to EID, priority value used for setting the primary RLOC in a case where there is more than one ETR, RLOC weight used for load-balancing if multiple RLOC has the same priority value. In addition, the RLOC record carries information about xTR-Id and Site-Id.




```
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.111.111
User Datagram Protocol, Src Port: 4342, Dst Port: 4342
Locator/ID Separation Protocol
   Type: Map-Register (3)
   P  bit (Proxy-Map-Reply): Set
   I  bit (xTR-ID present): Set
   M bit (Want-Map-Notify): Set
   Nonce: 0xfd609a481fd1cdc6
   Mapping Record 1, EID Prefix: [100] 172.16.100.101/32, TTL: 1440, Action: No-Action, Authoritative
   Authoritative bit: Set
   EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
      EID Prefix: [100] 172.16.100.101
         LCAF: Instance ID: 100,
         Address: 172.16.100.101
      Locator Record 1, Local RLOC: 192.168.1.1, Reachable, Priority/Weight: 1/1, Multicast Priority/Weight: 1/1
      xTR-ID: df0cd73789859700c71c7927a9e2910c
      Site-ID: 0000000000000000
```

Figure 3-2: *Map-Register message from ETR Edge-1.*

Capture 3-1 shows the complete packet capture.

```
Ethernet II, Src: 50:00:00:01:00:02, Dst: 50:00:00:04:00:00
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.111.111
User Datagram Protocol, Src Port: 4342, Dst Port: 4342
Locator/ID Separation Protocol
    0011 .... .... .... .... .... = Type: Map-Register (3)
    .... 1... .... .... .... .... = P bit (Proxy-Map-Reply): Set
    .... .0.. .... .... .... .... = S bit (LISP-SEC capable): Not set
    .... ..1. .... .... .... .... = I bit (xTR-ID present): Set
    .... ...0 .... .... .... .... = R bit (Built for an RTR): Not set
    .... .... 0000 0000 0000 000. = Reserved bits: 0x0000
    .... .... .... .... .... ...1 = M bit (Want-Map-Notify): Set
    Record Count: 1
```

```
    Nonce: 0xfd609a481fd1cdc6
    Key ID: 0x0001
    Authentication Data Length: 20
    Authentication Data: 22c8e27db54073234d0685fe328f0ca865444daa
    Mapping Record 1, EID Prefix: [100] 172.16.100.101/32, TTL: 1440, Action:
No-Action, Authoritative
        Record TTL: 1440
        Locator Count: 1
        EID Mask Length: 32
        000. .... .... .... = Action: No-Action (0)
        ...1 .... .... .... = Authoritative bit: Set
        .... .000 0000 0000 = Reserved: 0x000
        0000 .... .... .... = Reserved: 0x0
        .... 0000 0000 0000 = Mapping Version: 0
        EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
        EID Prefix: [100] 172.16.100.101
            LCAF: Instance ID: 100, Address: 172.16.100.101
                LCAF Header: 00000220000a
                    Reserved bits: 0x00
                    Flags: 0x00
                    Type: Instance ID (2)
                    Reserved bits: 0x20
                    Length: 10
                Instance ID: 100
                Address AFI: IPv4 (1)
                Address: 172.16.100.101
        Locator Record 1, Local RLOC: 192.168.1.1, Reachable, Priority/Weight:
1/1, Multicast Priority/Weight: 1/1
            Priority: 1
            Weight: 1
            Multicast Priority: 1
            Multicast Weight: 1
            Flags: 0x0005
                0000 0000 0000 0... = Reserved: 0x0000
                .... .... .... .1.. = Local: Set
                .... .... .... ..0. = Probe: Not set
                .... .... .... ...1 = Reachable: Set
            AFI: IPv4 (1)
            Locator: 192.168.1.1
    xTR-ID: df0cd73789859700c71c7927a9e2910c
    Site-ID: 0000000000000000
```

Capture 3-1: *Map-Register message from ETR Edge-1.*

Debug 3-1 shows the partial the Map-Register message process taken from the ETR Edge-1 when it received the GARP message from Host-A. Note that the debug is taken from a different time than the previous file capture 3-1. That is why the nonce values are different in capture 3-1 and debug 3-1.

The LISP process starts when Edge-1 receives the GARP message from Host-A. Because the ingress interface is participating in dynamic-EID table 172_16_100_0_100-White that includes EID-prefix 172.16.100.0/24, Edge-1 verifies

if the source IP address of the received packet matches the list. Because the check is hit, Edge-1 adds the IP address 172.16.100.101/32 into the dynamic EID table of Insurance-100 (L2 VRF 100_White). Next, Edge-1 generates the nonce value, which is used as a message integrity check by receiving Map-Server and later by itself. Before sending an update to Map-Server, Edge-1 verifies the reachability of the EID.

```
LISP: Processing dyn-EID detection for BDI100 EID prefix 172.16.100.101/32

LISP-0: Local dynEID 172_16_100_0-100_White IID 100 prefix 172.16.100.101/32
RLOC 192.168.1.1 pri/wei=1/1, Created (IPv4 intf RLOC Loopback0) (state:
active, rl.

LISP: RIBtable [IPv4:100_White:172.16.100.101/32] created.

LISP: RIBtable [IPv4:100_White:172.16.100.101/32] add source dyn-EIDi.

LISP-0: DynEID IID 100 172.16.100.101 [172_16_100_0-100_White:BDI100] Created.

LISP-0: IPv4 Map Server IID 100 192.168.111.111, reg_group_ctx src=0.0.0.0
dst=0.0.0.0 nonce=0xB6001A19-0x690B1D93, reg_group No RLOCs no merge, Starting
period.

LISP-0: Local dynEID 172_16_100_0-100_White IID 100 prefix 172.16.100.101/32,
found RIB route 172.16.100.101/32 to EID prefix (state: active, rlocs: 1/1,
source.

LISP: RIB Watch Group 100_White 172.16.100.0/24 (no-default), scheduling RIB
update.

LISP: RIB Watch Group 100_White 172.16.100.101/32 (no-default), scheduling RIB
update.

LISP: RIB Watch Group 100_White 172.16.100.0/24 (no-default), installing in
RIB.

LISP: RIB Next-hop 100_White BDI100 172.16.100.0 lcl 172.16.100.1, deleting.

LISP: RIB Watch Group 100_White 172.16.100.101/32 (no-default), installing in
RIB.

LISP-0: IID 100 Update registration group links for 1 prefixes.

LISP: RIB Next-hop 100_White BDI100 172.16.100.101 lcl 172.16.100.1, notified.

LISP-0: Local dynEID 172_16_100_0-100_White IID 100 prefix 172.16.100.101/32,
found RIB route 172.16.100.101/32 to EID prefix (state: active, rlocs: 1/1,
source.

LISP-0: Ping [dynamic-eid] 0x7FC23A6675B0 liveliness 100_White IPv4 UNSPEC ->
172.16.100.101 Notify client 255% -> 100%.

LISP-0: IPv4 Map Server IID 100 192.168.111.111, Sending map-register (src_rloc
192.168.1.1) nonce 0xB6001A19-0x690B1D93.
```

Debug 3-1: *Edge-1 generates the UDP based Map-Register message to Map-Server.*

Registration Phase 3: UDP based Map-Notify from MS to ETR

When a Map-Server receives a Map-Register message from the ETR Edge-1, it verifies that the EID-prefix and the Instance-Id match to its configuration. This means that there has to be an EID-prefix 172.16.100.0/24 in Instance -100 under the site Network-Times. In addition, the "nonce" value has to be bigger than what is received with the previous Map-Register message from this the same ETR. When the verification process is passed successfully, the Map-Server copies the original "nonce" value, the EID-record and the RLOC-record information to the Map-Notify message which it sends to the ETR Edge-1.

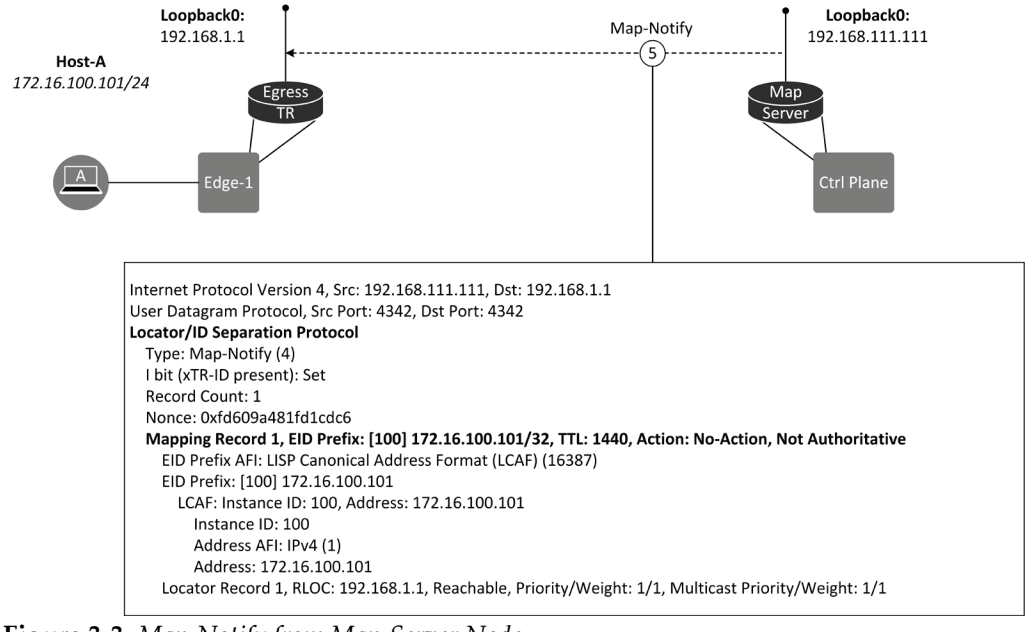


Figure 3-3: *Map-Notify from Map-Server Node.*

Capture 3-2 shows the complete packet capture.

```
Internet Protocol Version 4, Src: 192.168.111.111, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 4342, Dst Port: 4342
Locator/ID Separation Protocol
    0100 .... .... .... .... .... = Type: Map-Notify (4)
    .... 1... .... .... .... .... = I bit (xTR-ID present): Set
    .... .0.. .... .... .... .... = R bit (Built for an RTR): Not set
    .... ..00 0000 0000 0000 0000 = Reserved bits: 0x00000
    Record Count: 1
    Nonce: 0xfd609a481fd1cdc6
    Key ID: 0x0001
    Authentication Data Length: 20
    Authentication Data: c3ab7a993de62c5cb53ca97267817847733d9bac
```

```
    Mapping Record 1, EID Prefix: [100] 172.16.100.101/32, TTL: 1440, Action:
No-Action, Not Authoritative
        Record TTL: 1440
        Locator Count: 1
        EID Mask Length: 32
        000. .... .... .... = Action: No-Action (0)
        ...0 .... .... .... = Authoritative bit: Not set
        .... .000 0000 0000 = Reserved: 0x000
        0000 .... .... .... = Reserved: 0x0
        .... 0000 0000 0000 = Mapping Version: 0
        EID Prefix AFI: LISP Canonical Address Format (LCAF) (16387)
        EID Prefix: [100] 172.16.100.101
            LCAF: Instance ID: 100, Address: 172.16.100.101
                LCAF Header: 00000220000a
                Instance ID: 100
                Address AFI: IPv4 (1)
                Address: 172.16.100.101
        Locator Record 1, RLOC: 192.168.1.1, Reachable, Priority/Weight: 1/1,
Multicast Priority/Weight: 1/1
            Priority: 1
            Weight: 1
            Multicast Priority: 1
            Multicast Weight: 1
            Flags: 0x0001
                0000 0000 0000 0... = Reserved: 0x0000
                .... .... .... .0.. = Local: Not set
                .... .... .... ..0. = Probe: Not set
                .... .... .... ...1 = Reachable: Set
            AFI: IPv4 (1)
            Locator: 192.168.1.1
    xTR-ID: df0cd73789859700c71c7927a9e2910c
    Site-ID: 0000000000000000
```

Capture 3-2: *Map-Notify from Map-Server Node.*

Debug 3-2 illustrates the LISP process of Map-Server when it receives a UDP based unreliable Map-Register message from the ETR Edge-1. It creates a mapping record into the EID-to-RLOC mapping database. The EID-to-RLOC mapping entry is shown in figure 3-11. The entry is attached to the site Network-Times with an IID 100 and the TTL 24 hours (1440sec.) and with the RLOC 192.168.1.1 (which reachability is verified from RIB), and the registration is marked as Authorative (received from EID first-hop-router - RLOC). After creating an EID-to-RLOC database entry, Map-Server sends a Map-Notify message to the ETR Edge-1. From the notify message, we can see the XTR Edge-1 Identifier and the nonce value used with this particular update.

```
LISP: Processing received Map-Register(3) message on GigabitEthernet1 from
192.168.1.1:4342 to 192.168.111.111:4342

LISP: Processing Map-Register mapping record for IID 100 172.16.100.101/32 LCAF
2, ttl 1440, action none, authoritative, 1 locator 192.168.1.1 pri/wei=1/1 LpR

LISP-0: IID 100 Parsing SVC_IP_IAF_IPv4 registration for prefix
172.16.100.101/32.

LISP: Processing IP Map-Register mapping record for IID 100 172.16.100.101/32
LCAF 2, ttl 1440, action none, authoritative, 1 locator 192.168.1.1 pri/wei=1/1
LpR

LISP-0: IID 100 Processing SVC_IP_IAF_IPv4 registration for prefix
172.16.100.101/32.

LISP-0: MS EID IID 100 prefix 172.16.100.101/32 SVC_IP_IAF_IPv4 site *,
Created.

LISP-0: MS Site EID IID 100 prefix 172.16.100.101/32 SVC_IP_IAF_IPv4 site
Network-Times, Created dynamic site EID prefix entry.

LISP-0: MS registration IID 100 prefix 172.16.100.101/32 192.168.1.1
SVC_IP_IAF_IPv4 site Network-Times, Created new registration.

LISP-0: MS registration IID 100 prefix 172.16.100.101/32 192.168.1.1
SVC_IP_IAF_IPv4 site Network-Times, Adding locator 192.168.1.1.

LISP: RIB Watch Group default 192.168.1.1/32 , created.

LISP: RIB Watch Group default 192.168.1.1/32 , scheduling RIB update.

LISP-0: MS inst member IID 100 192.168.1.1 Became valid.

LISP: Session VRF default, Local UNSPEC, Peer 192.168.1.1, Role: Passive,
State: Unknown, Created (RX 0, TX 0).

LISP-0: MS EID IID 100 prefix 172.16.100.101/32 SVC_IP_IAF_IPv4 site Network-
Times, Scheduling map notifications for prefix 172.16.100.101/32.

LISP-0: MS EID IID 100 prefix 172.16.100.101/32 SVC_IP_IAF_IPv4 site Network-
Times, Scheduling unreliable map notification for prefix 172.16.100.101/32 to
ETR 192.168.1.1.

LISP: RIB Watch Group default 192.168.1.1/32 , installing in RIB.

LISP-0: MS EID IID 100 prefix 172.16.100.101/32 SVC_IP_IAF_IPv4 site Network-
Times, ALT route update/create.

LISP-0: ALTroute IID 100 prefix 172.16.100.101/32 <-> created.
```

```
LISP-0: ALTroute IID 100 prefix 172.16.100.101/32 <-> add source MS-EID.

LISP: Session VRF default, Local UNSPEC, Peer 192.168.1.1, Role: Passive,
State: Unknown, Destroyed with OS adaptor (RX 0, TX 0).

LISP-0: Map-Notify 192.168.111.111:4342->192.168.1.1:4342 xTR-ID 0xB11A62C9-
0x8683B62B-0x78A9C166-0xA4EBE930, sending with 1 prefix, nonce 0xB6001A19-
0x690B1D93
```

Debug 3-2: *Map-Server processing UDP based Map-Register message from ETR Edge-1*

Debug 3-3 shows how the ETR Edge-1 receives the Map-Notify message from Map-Server.

```
LISP: Processing received Map-Notify(4) message on GigabitEthernet1 from
192.168.111.111:4342 to 192.168.1.1:4342

LISP: Processing Map-Notify ID-included, no MS-RTR auth, no EID-notify, 1
record, nonce 0xB6001A19-0x690B1D93, key-id 1, auth-data-len 20, hash-function
sha1, xd

LISP: Processing Map-Notify mapping record for IID 100 172.16.100.101/32 LCAF
2, ttl 1440, action none, not authoritative, 1 locator 192.168.1.1 pri/wei=1/1
lpR

LISP-0: Local dynEID 172_16_100_0-100_White IID 100 prefix 172.16.100.101/32,
Received map notify (state: active, rlocs: 1/1, sources: dynamic).
```

Debug 3-3: *The ETR Edge-1 receives the Map-Notify from Map-Server.*

Registration Phase 4: TCP based Map-Refresh from MS to ETR

The first part of the Map-Register process is done using unreliable UDP for message exchange. Using UDP for sending Map-Registration message though has some drawbacks. ETR sends these messages to Map-Server (MS) every minute. This means that ETR has to construct the message and then send it to MS. MS, in turn, has to process received Map-Register messages and then acknowledge them by sending Map-Notify messages. As said, this is a reoccurring process that happens every minute. When there are more EIDs than can be packed inside one Map-Register message, the information is split into multiple Map-Register messages. This, in turn, increases the load on both ETR and MS. Note that from the MS point of view, there might be tens or even hundreds of ETRs sending Map-Request on a one-minute interval.

IOS-XE supports the Reliable Registration process using TCP. After receiving an acknowledgment from the Map-Server (UDP), Edge-1 starts a three-way TCP handshake process to establish a reliable TCP-connection with Map-Server. This session is used as a reliable transport channel when exchanging Map-Register messages. The status of TCP-connection is monitored by using a TCP ACK message (dst. port 4342). Figure 3-4 illustrates this process. The Map-Register message is now sent only once instead of a one-minute interval.

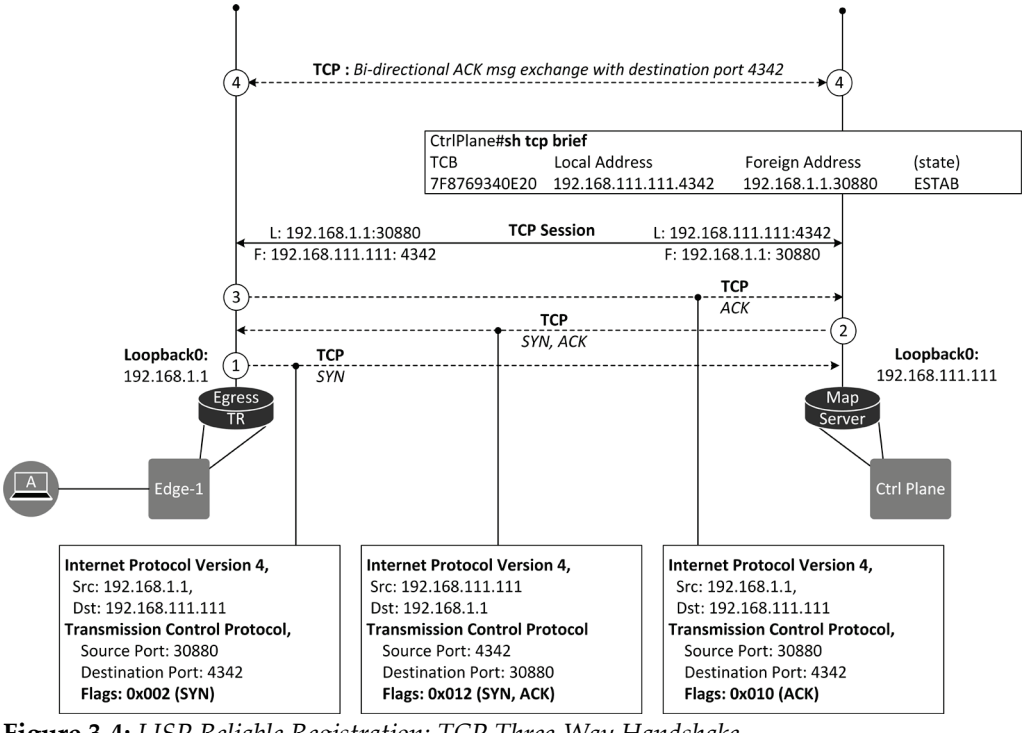


Figure 3-4: *LISP Reliable Registration: TCP Three-Way Handshake.*

After establishing the TCP session, the Map-Server sends a Registration-Refresh message where it asks ETR Edge-1 to send all EIDs that it has. Note that the end marker is always 0x9FACADE9.

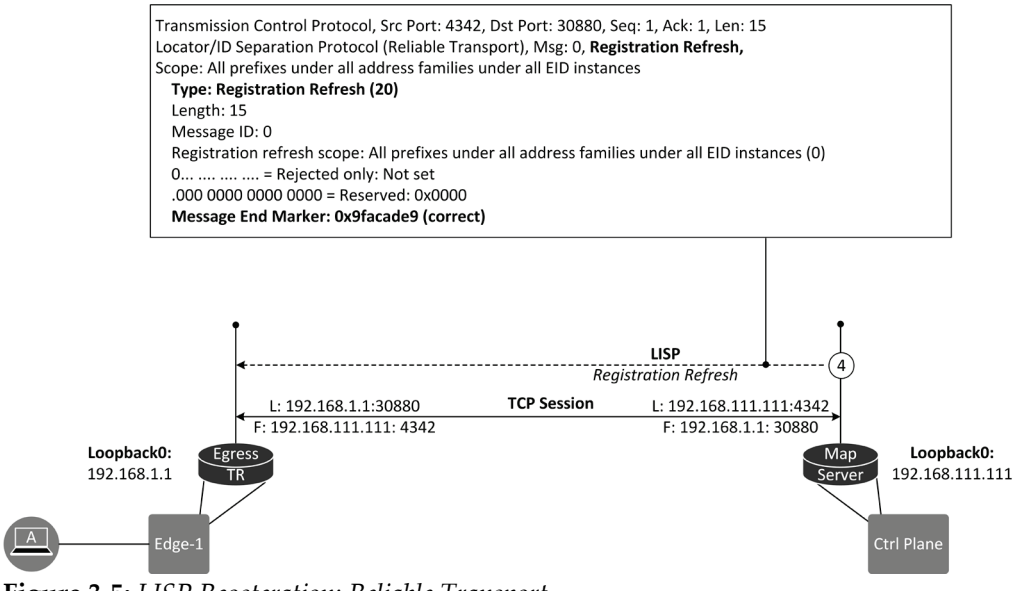


Figure 3-5: *LISP Regsteration: Reliable Transport.*

```
Internet Protocol Version 4, Src: 192.168.111.111, Dst: 192.168.1.1
Transmission Control Protocol, Src Port: 4342, Dst Port: 39626, Seq: 1, Ack: 1,
Len: 15
Locator/ID Separation Protocol (Reliable Transport), Msg: 0, Registration
Refresh, Scope: All prefixes under all address families under all EID instances
    Type: Registration Refresh (20)
    Length: 15
    Message ID: 0
    Registration refresh scope: All prefixes under all address families under
all EID instances (0)
    0... .... .... .... = Rejected only: Not set
    .000 0000 0000 0000 = Reserved: 0x0000
    Message End Marker: 0x9facade9 (correct)
```

Capture 3-3: *LISP Reliable Regsteration: Map-Refresh from Map-Server ControlPlane node.*

Example 3-1 shows that there is a TCP connection between the CtrlPlane node and ETR Edge-1.

```
CtrlPlane#sh tcp brief
TCB       Local Address               Foreign Address             (state)
7F8769340E20  192.168.111.111.4342       192.168.1.1.31299           ESTAB
7F87690709C0  192.168.111.111.4342       192.168.2.2.47876           ESTAB
```

Example 3-1: *TCP connection between ETR Edge-1 an Map-Server.*