# Locator-ID Separation Protocol in Traditional & SDN Networks

Ragavi Swarnalatha Raman, Srikanth Gopalakrishnan, Aparajita Bagchi

*Software Defined Networking, North Carolina State University*

## 1. Purpose

The purpose of the project is to demonstrate the LISP (Locator/ID separation protocol) in traditional and SDN networks. The idea behind the development of LISP is as follows: The Internet routing and addressing architecture uses a single namespace, the IP address, to simultaneously express two functions about a device: its identity, and its location within the network. One very visible and detrimental result of this single namespace has been manifested in the rapid growth of the Internet's DFZ (default-free zone) i.e. the group of Autonomous Systems(AS) that form the core network. Also, the increase in the routing table entries of routers in the core network is a concern to the entire internet. This happens as a consequence of multihoming, traffic engineering, non aggregatable address allocations, and business events such as mergers and acquisitions. Further, as devices such as laptops or smartphones move around, they connect to the nearest available network, and this causes TCP connection losses among those devices. We need a way for a Clients should be able to move around different network domains while still being able to receive traffic that originated before the client made a shift.

The aim of this project is to demonstrate how LISP overcomes this mobility issue by separating the single namespace i.e. IP addresses into addresses that are routable (RLOCs) and addresses that are private(EIDs). This project implements the LISP principles in a Traditional Network conforming to the RFCs 6830 and 6833. And in an SDN network using an SDN controller and OpenvSwitch.

Terms Used:

- **LISP :** Locator/ID Separation Protocol

- **EID:** Endpoint Identifier
- **RLOC:** Routing Locators
- **ITR:** Ingress Tunnel Router - Router present at incoming point that receives packets from source end systems, encapsulates them in LISP header, and sends them to RLOCs connected to destination end hosts.
- **ETR:** Egress Tunnel Router- Router present at outgoing point that receives the LISP encapsulated packets from ITRs, decapsulates them and sends them to the destination end points.
- **xTR:** ITR/ETR
- **Map Request:** Request message sent from ITR to Map Resolver for EID to RLOC mapping
- **Map Reply:** Response message sent by Map-Server/Map-Resolver or ETR to ITR providing EID to RLOC mapping.
- **Map Register:** Message sent by ETR to Map-Server specifying its EID-prefix to RLOC associations.
- **MS: Map Server** - Distributed database that maintains EID prefix to RLOC mapping.
- **MR: Map Resolver** - Resolves EID to RLOC map request of ITR.
- **OVS:** OpenvSwitch
- **OOR:** Open Overlay Router

### *1.1. Locator ID Separation protocol*

LISP is based on the concept of dynamic encapsulation and decapsulation of a packet header. It is a network layer protocol that enables separation of IP addresses into two new numbering spaces:

1. Endpoint Identifiers (EIDs) and
2. Routing Locators (RLOCs).

The EIDs and RLOCs are in practice the same as IPv4 or IPv6 addresses. This enables backward compatibility with existing internet infrastructure. It is only their semantics that differs. RLOCs can be thought of as the IP address space present only in the Core network side, while EIDs are a unique IP address on the sub-network which may have different prefix matching.New LISP capable routers will have to be deployed, in addition to a MAP resolver for this approach, but the core network can remain the same.

#### *1.1.1. LISP site devices:*

**ITR :** An ingress tunnel router that receives packets from the client (source EID) in its LISP site , encapsulates the packets and sends them to a remote LISP site where the destination EID is attached to via the underlying core network. The ITR also sends Map Requests to the Map Server / Map Resolver querying for EID-RLOC mappings and processes the Map Reply messages.

**ETR :** An Egress tunnel router that receives packets from the core network ,decapsulates them and sends it to the destination EID (client) at it LISP site. The ETR also registers with the Map Server to inform its EID-to-RLOC mappings and responds to Map Request messages from the Map Server.

#### *1.1.2. LISP Infrastructure devices:*

**Map Server :** The Mapping System or Map Server (MS), is a distributed database that maintains the association between EIDs and respective RLOCs. The MS also receives Map Requests from the ITRs and forwards it to the registered ETRs that is authoritative for the EID prefix being queried.

**Map Resolver :** The Map Resolver receives Map Requests from ITRs and resolves it to the corresponding RLOC address sending the resolved address back to the ITR. The Map Resolver also sends negative map replies to ITRs that query for EIDs prefixes that are not present in registered LISP sites handled by the Map Server.

## 2. COMPONENTS OF THE PROJECT

#### *2.0.1. Platform:*

**Platform :** ExoGENI is used to create the network topology. Each node is a Ubuntu 16.04 LTS Linux Box with the appropriate tools installed. The tools installed on each box have been mentioned in the next section

**Components :** All nodes are Linux boxes with Ubuntu 16.04 LTS installed on them. Additional tools / applications such as BIRD and OOR are compiled from source and run on these boxes to give their respective functionality. These are mentioned below.

**1.Traditional Approach :** The traditional network has the following nodes:

- Tunnel Routers: ITRs and ETRs. These are directly connected to the end hosts or clients on one side and the core network on the other. The OOR (an open source implementation to deploy overlay networks) is installed and configured on these routers.

- Core Routers: These routers form the network core. Bird routing daemon is installed on these routers to enable routing between them using OSPF that we had to manually configure. They are identified as RLOCs as per the LISP terminology.

- Clients: These are the endpoints of the network identified by EIDs.

- Map Server/Resolver: Maintains the mapping between EIDs and RLOCs, interacts with the ITRs to receive Map requests and to resolve the EID-RLOC mappings and with the ETRs to register the EID-RLOC mapping. The OOR (Open Overlay Router) has a Map Resolver/Server module that is used to set up the Map Server/Resolver. This MS/MR should be able to receive Map request/resolve messages from xTR's

**2.SDN Approach :** The core routers and clients remain as is, according to the traditional network topology. The additional components in the SDN topology are:

- SDN Controller (Ryu) and Map Server/Resolver : Ryu Controller , an open source, component based controller is used to manage the OVS switches. The Map Server/Resolver that takes care of resolving the EID-RLOC mapping and manages the mapping database is implemented as an application and is interfaced with the SDN controller. Ryu uses southbound APIs to interact/manage the switches and uses northbound APIs to interact with the controller applications.

- OpenvSwitch : The tunnel routers are replaced by OVS switches working in L3 mode. These OVS switches are connected to the EIDs , the core network and the SDN controller. The SDN controller manages the flow table entries of these switches. The OVS will take the place of traditional ETRs and ITRs.

## 3. Design and Develepment Plan

### *3.1. HIGH LEVEL DESIGN*

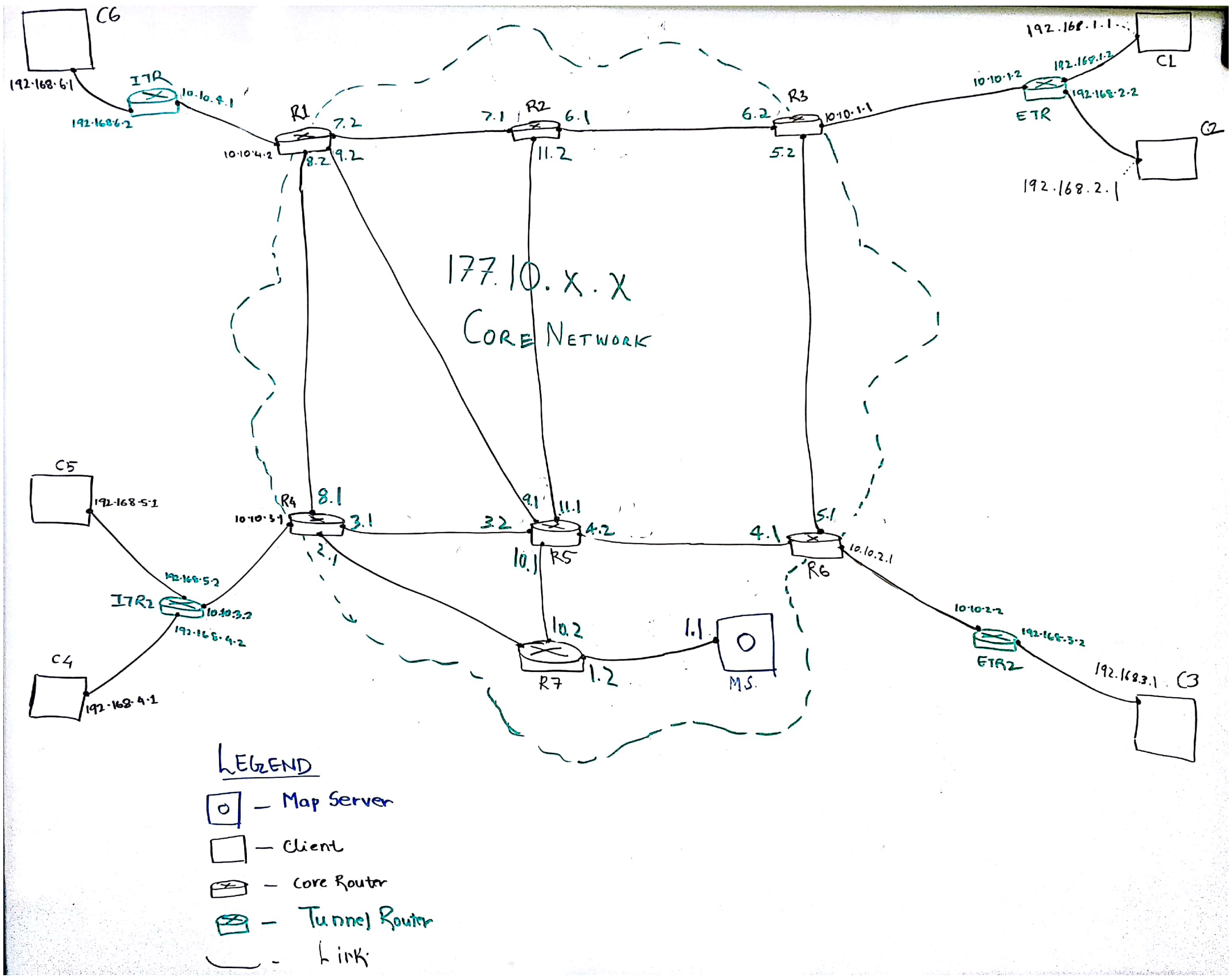


Figure 1: 192.168.x.x/16 are private. 10.10.x.x/16 are xTR to Core interface networks. 177.10.x.x/16 is the Core Network.

The above topology / design is setup for both the traditional and SDN approaches except in the SDN approach the tunnel routers (ITRs and ETRs) are replaced with OVS switches and the Map Server/Resolver replaced with a SDN controller and the function of the Map Server/Resolver written as a controller application.

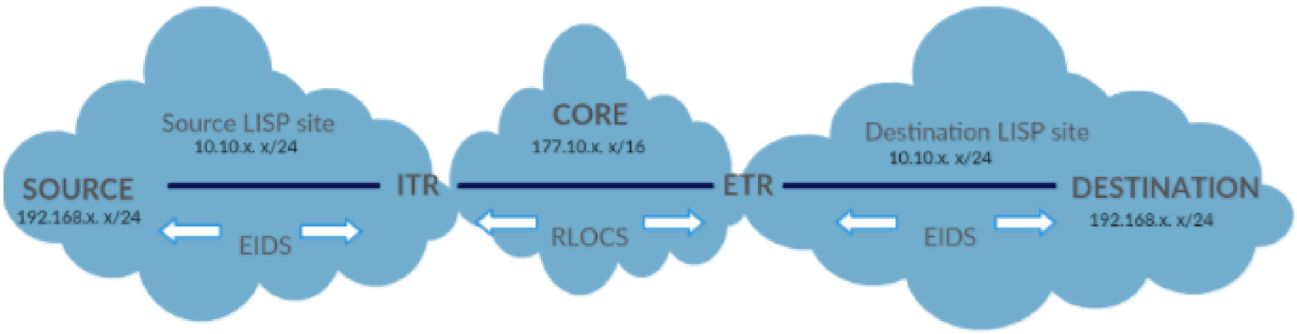


Figure 2: Subnet plan for Client to Client communication

The clients / EIDs have private IP addresses and no information about the core network and the interfaces facing the core network on the xTRs. Communication between the EIDs in different LISP sites happens with the help of LISP Tunneling where an additional RLOC header is added on top of the header containing EIDs with the help of a Map Server / Resolver. This Map Server/Resolver maps the EID-RLOC pairs. The movement of one EID to a different RLOC gets updated in the Map Server and thereby gets updated in the respective ITRs when these ITRs needs to reach the relocated EID.

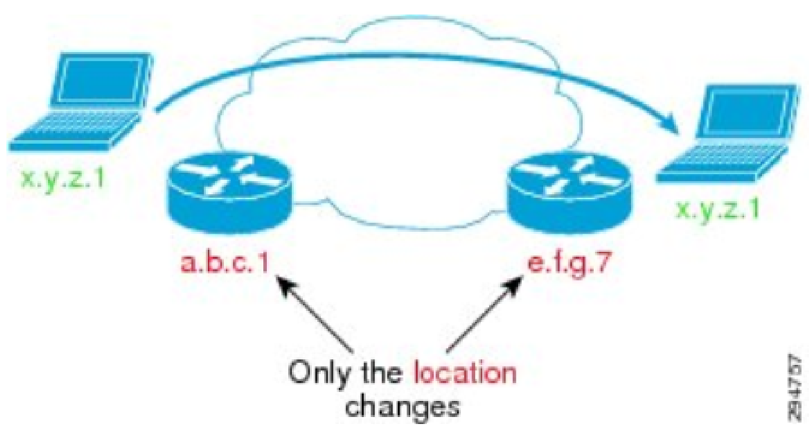


Figure 3: How EID mobility works, **source:** www.cisco.com

*3.2. Low Level Design*

*3.2.1. Traditional Network*

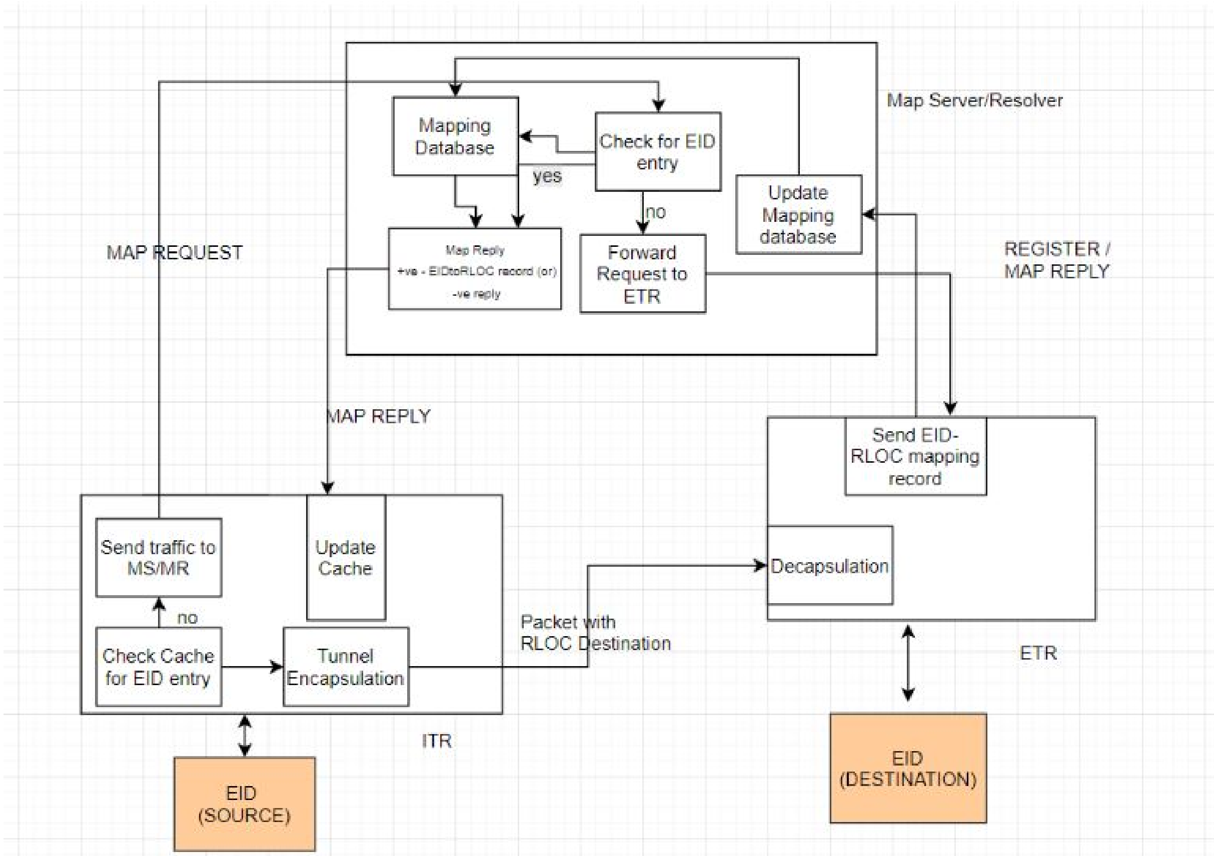


Figure 4: Traditional

**Stage 1 - Map Server Registration and Learning :**

On boot up, the Map Servers database is empty and listens for Registrations from ETRs. ETRs register with the Map Server and send their Map Records containing EID-RLOC mapping ie) the list of clients in the ETRs own LISP site. The Map Server adds these entries to its database and the ETR receives a successful registration message. An error in registering would be informed to the ETR via appropriate error messages. The ETRs re-register their Mapping records to the Map Server every 60 seconds throughout the time period when LISP is enabled.

**Stage 2 - ITR sends Map Requests to Map Resolver:**

When a source EID attached to an ITR in a LISP site pings an EID present in another LISP site, the ICMP request packets created at the source EID reaches the ITR. The ITR realizes that it is a private address and checks its cache for EID-RLOC mapping record that helps the packet to reach the destination EID via a tunnel interface. If no cache entry for the destination EID prefix exists, the ITR sends a mapping request to the Map Resolver asking for the EID-RLOC mapping.

**Stage 3 - Map Replies by Map Resolver / ETR :**

When a Map Resolver/Server receives the Map Request, it checks its Mapping database to find the appropriate EID-RLOC mapping record. If no records are found, the Map Resolver forwards the request to its registered ETRs to check if they have an EID-RLOC mapping for the requested destination EID prefix. The ETR replies with its EID-RLOC mapping which in turn is sent to the ITR as a Map Reply. If the Map Resolver finds no matching EID-RLOC mapping record, it responds with a negative Map Reply.

**Stage 4 - Packet Encapsulation and Tunneling :**

On learning the RLOC address of the destination EID, the ITR adds the entry to its cache,does encapsulation of the original packet, adds a LISP header , and a tunnel header with the outer destination address as the RLOC address. The encapsulated packet is now sent to the ETR via a tunnel established between tunnel interfaces at the ITR and ETR.

**Stage 5 - Packet Decapsulation and forward to destination EID:**

The encapsulated packet on reaching the ETR is decapsulated , the outer header and the LISP headers are removed, the ETR now processes the inner header of the packet. The inner header of the packets destination address is the EID that is present in the LISP site of the ETR and the ETR has routing entries to reach it. The packet is now forwarded to the appropriate destination EID.

**Mobility:**

When an EID moves from one LISP site to another LISP site, the ETR of the new LISP site to which the EID has relocated updates the Map Server with the new EID-RLOC mapping. The ITR keeps sending its traffic to the EID to the old RLOC address until its cache gets cleared. A subsequent new Map Request updates the ITR with the new EID-RLOC mapping and the ITR now forwards the packet to the new ETR to whose LISP site the EID has relocated to.

*3.2.2. SDN Network*

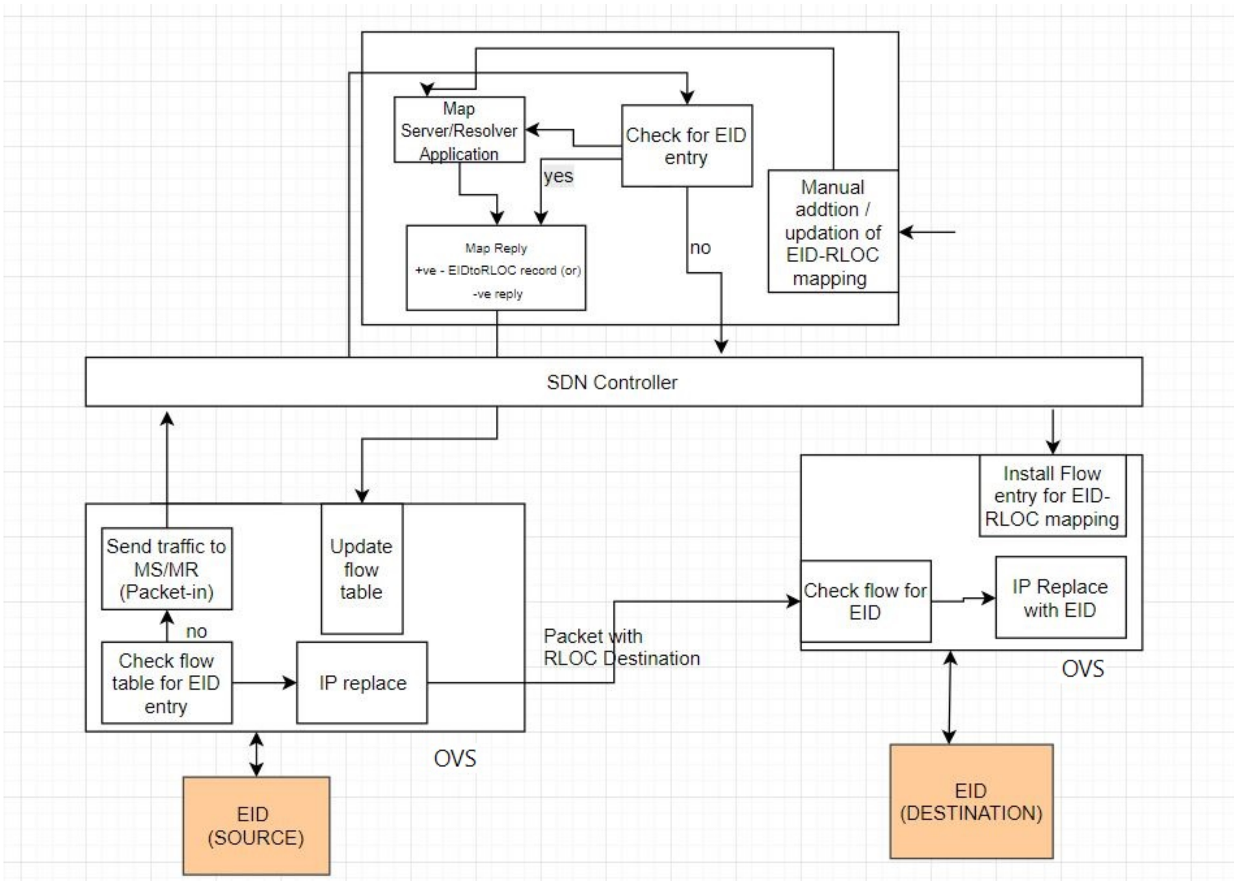


Figure 5: Traditional

**Stage 1 - Map Server Learning and Destination OVS Flow table installation:**

On boot up, the Map Server applications database is empty and Map Records containing EID-RLOC mapping ie) the list of clients connected to the destination OVS switch LISP site are updated manually. The entries do not change until the records are re-updated.The EID-RLOC mappings are installed as flow table updates in the corresponding OVS switches functioning as ETRs.

**Stage 2 - Source OVS sends Packet-In to SDN Controller:**

When a source EID attached to a source OVS switch in a LISP site pings an EID present in another LISP site, the ICMP request packets created at the source EID reaches the OVS switch. The OVS realizes that it is a private address and checks its flow table for EID-RLOC mapping record that helps the packet to reach the destination EID. If no cache entry for the destination EID prefix exists, the OVS s sends a PAcket-In to the Controller which in turn interfaces with the Map Resolver application asking for the EID-RLOC mapping. If the mapping is present the Controller installs a flow table update in the OVS switch indicating what to do with the subsequent flows ie) change flow destination or drop.

**Stage 3 - Flow table Update and IP Re-write:**

The OVS switch on receiving the flow table update, updates its flow table entry and adds a match and action pair to it. The match and action are as follows: Match: The source and destination IP addresses of the flow are the EIDs. Action: Replace the source and destination EIDs with the RLOC (OVS switch) source and destination IP addresses. The traffic flows are now sent to the re-written RLOC addresses.

**Stage 4 - IP Rewrite at destination and forward to EID:**

The OVS switch at the destination receives the flow and finds a flow table entry that matches the source and destination RLOC addresses. The flow table entries are installed by the SDN controller at the destination OVS switches after startup. Action : The source and destination RLOC addresses are replaced with the source and destination EIDs from the flow table entries. The flow is now forwarded to the appropriate destination EID.If no flow table match is found, the traffic is dropped.

**Mobility:**

When a EID moves from one LISP site to another, the OVS switches do not self-realize the change that has happened. The updated EID-RLOC mapping needs to be added in the Map Resolver application and reinstalled in both the source and destination OVS switches as new flow table updates. The old table entries are removed after a certain timeout. Now when the source EID traffic tries to reach the relocated EID in a new LISP site, the updated flow table entry changes the flow destination address to the new LISP sites RLOC and sends the traffic.

# 4. Implementation

## *4.1. Traditional Network*

The following configuration was given and slightly modified for each core network router. This was done to implement OSPF routing using BIRD

```
protocol ospf v2 MyOSPF {
    tick 2;
    rfc1583compat yes;
    area 0.0.0.0 {
        stub no;
        networks {
            177.10.0.0/16;
        };
        interface "ens6" {
            hello 9;
            retransmit 6;
            cost 10;
            transmit delay 5;
            dead count 5;
            wait 50;
            type broadcast;
        };
        interface "ens7" {
            hello 9;
            retransmit 6;
            cost 10;
            transmit delay 5;
            dead count 5;
            wait 50;
            type broadcast;
        };
        interface "ens8" {
            hello 9;
            retransmit 6;
            cost 10;
            transmit delay 5;
            dead count 5;
            wait 50;
            type broadcast;
        };
        interface "ens9" {
            hello 9;
            retransmit 6;
            cost 10;
            transmit delay 5;
            dead count 5;
            wait 50;
            type broadcast;
        };
    };
```

xTR's and Clients were configured with manual routes to reach the core network. Client can only reach the xTR's. An example of an ITR routing table is given below.

```
[2018/4/14 4:43:33] DEBUG:
Starting xTR ...

[2018/4/14 4:43:33] WARNING: No Proxy-ETR defined. Packets to non-LISP destinations will be forwarded natively (no LISP encapsulation). This may prevent mobility in some scenarios.
[2018/4/14 4:43:35] DEBUG: ****** Summary of the xTR configuration ******
[2018/4/14 4:43:35] DEBUG: ***************** LISP Local Mappings ****************

[2018/4/14 4:43:35] DEBUG: EID: (IID 1/32, EID 192.168.6.0/24), ttl: 10, loc-count: 1, action: no-action, auth: 1
 RLOC: 10.10.4.1, Up, 2/10, 255/0

[2018/4/14 4:43:35] DEBUG: *******************************************************

[2018/4/14 4:43:35] DEBUG: **************** LISP Mapping Cache *****************

[2018/4/14 4:43:35] DEBUG: ENTRY UPTIME: 00:00:02, EXPIRES: 00:09:58, TYPE: Static, ACTIVE: Yes
EID: (IID 3/32, EID 192.168.1.0/24), ttl: 10, loc-count: 1, action: no-action, auth: 0
 RLOC: 10.10.1.2, Up, 2/10, 255/0


[2018/4/14 4:43:35] DEBUG: *******************************************************

[2018/4/14 4:43:35] DEBUG: ****************** Map-Servers list ******************************
[2018/4/14 4:43:35] DEBUG: |               Locator (RLOC)            |       Key Type          |
[2018/4/14 4:43:35] DEBUG: |                              177.10.1.1 |     HMAC-SHA-1-96       |
[2018/4/14 4:43:35] DEBUG: ************* Map Resolvers ***************
[2018/4/14 4:43:35] DEBUG: [1] =>  177.10.1.1
[2018/4/14 4:43:35] DEBUG: ***************** Proxy ETRs List for IPv4 EIDs **********************
[2018/4/14 4:43:35] DEBUG: |               Locator (RLOC)            | Status | Priority/Weight |
[2018/4/14 4:43:35] DEBUG: ***************** Proxy ETRs List for IPv6 EIDs **********************
[2018/4/14 4:43:35] DEBUG: |               Locator (RLOC)            | Status | Priority/Weight |
[2018/4/14 4:43:35] DEBUG: *************    Proxy-ITRs ***************
[2018/4/14 4:43:35] DEBUG: add_rule: Add rule -> Send packets with source address 192.168.6.0/24 and destination address _NULL_ to the table 100 with priority 100.
[2018/4/14 4:43:35] DEBUG: add_rule: Add rule -> Send packets with source address _NULL_ and destination address 192.168.6.0/24 to the table 254 with priority 99.
[2018/4/14 4:43:35] DEBUG: Balancing locator vector for (IID 1/32, EID 192.168.6.0/24):
[2018/4/14 4:43:35] DEBUG:   IPv4 locators vector (1 locators):   10.10.4.1
[2018/4/14 4:43:35] DEBUG:   IPv6 locators vector (0 locators):
[2018/4/14 4:43:35] DEBUG:   IPv4 & IPv6 locators vector (0 locators):
[2018/4/14 4:43:35] DEBUG: Map-Register -> flags:pirM record-count: 1 nonce a3f505157bd9f6f7, EID: (IID 1/32, EID 192.168.6.0/24), MS: 177.10.1.1
[2018/4/14 4:43:35] DEBUG: Sent control message IP: 10.10.4.1 -> 177.10.1.1 UDP: 4342 -> 4342
[2018/4/14 4:43:35] DEBUG: Sent Map-Register for mapping (IID 1/32, EID 192.168.6.0/24) to 177.10.1.1
[2018/4/14 4:43:35] DEBUG: Reprograming SMR in 1 seconds
[2018/4/14 4:43:35] INFO:

 Open Overlay Router (v1.2.0): started...


[2018/4/14 4:43:35] DEBUG:
**** Re-Register and send SMRs for mappings with updated RLOCs ****
[2018/4/14 4:43:35] DEBUG: Map-Register -> flags:pirM record-count: 1 nonce 4c133d157bf196ff, EID: (IID 1/32, EID 192.168.6.0/24), MS: 177.10.1.1
[2018/4/14 4:43:35] DEBUG: Sent control message IP: 10.10.4.1 -> 177.10.1.1 UDP: 4342 -> 4342
[2018/4/14 4:43:35] DEBUG: Sent Map-Register for mapping (IID 1/32, EID 192.168.6.0/24) to 177.10.1.1
[2018/4/14 4:43:35] DEBUG: Start SMR for local EID (IID 1/32, EID 192.168.6.0/24)
[2018/4/14 4:43:35] DEBUG: Sending SMRs to PITRs
[2018/4/14 4:43:35] DEBUG: Multicast packets not supported for now!
[2018/4/14 4:43:35] DEBUG: Multicast packets not supported for now!
[2018/4/14 4:43:35] DEBUG: Received Map-Notify-> flags:ir, record-count: 1, nonce A3F505157BD9F6F7, IP: 177.10.1.1 -> 10.10.4.1, UDP: 4342 -> 4342
[2018/4/14 4:43:35] DEBUG: No Map Register sent with nonce: a3f505157bd9f6f7 Discarding message!
[2018/4/14 4:43:35] DEBUG: xTR: Failed to process LISP control message
[2018/4/14 4:43:35] DEBUG: Received Map-Notify-> flags:ir, record-count: 1, nonce 4C133D157BF196FF, IP: 177.10.1.1 -> 10.10.4.1, UDP: 4342 -> 4342
[2018/4/14 4:43:35] DEBUG:   Mapping-record -> ttl: 10 loc-count: 1 action: no-action auth: 1 map-version: 0 eid: (IID 1/32, EID 192.168.6.0/24)
[2018/4/14 4:43:35] DEBUG:     Locator-record -> flags: L=1,p=0,R=1, p/w: 2/10 255/0, addr: 10.10.4.1
[2018/4/14 4:43:35] DEBUG: Map-Notify message confirms correct registration of (IID 1/32, EID 192.168.6.0/24).Programing next Map-Register in 60 seconds
```

Figure 7: an ITR config

### 4.2. SDN Network

The same Configuration of OSPF as the traditional network is used. The rest of the OVS switches and Controller are in progress of being implemented.

## 5. Test Plan

### *5.1. Test Application*

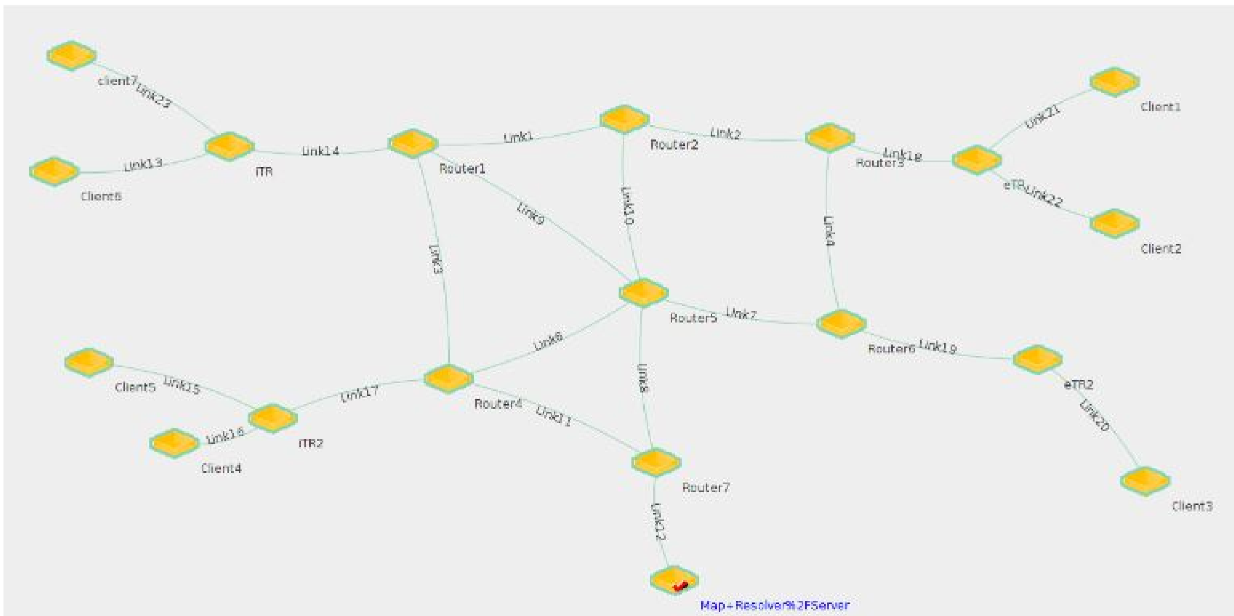


Figure 8: Traditional

Table 1: Test Plan

| Case | Setup | Action | Expected Observation | Recorded Observation |
|---|---|---|---|---|
| 1 | xTR's are running and MS/MR is running | Ping from source EID to destination EID | The ETR registers its EID-RLOC mapping to the Map Server. The ITR sends a map request to the Map Server asking for the destination EID-RLOC mapping. The Map server responds with this information through a map reply message. A LISP tunnel is established and now the source EID should be able to reach the destination EID. | Source EID is able to send ICMP packets to destination EID. On debugging, the messages from the ETR to the MS/MR, ITR's map request and MS map reply are visible in the respective xTR's terminal |
| 2 | MS/MR off at the beginning, xTR's are running | Ping from source EID to destination EID | The ETR is not able to register EID-RLOC mapping with the MS/MR. The ITR's map-request is not served and the LISP tunnel is not successfully established. Source EID should not be able to reach destination EID | ICMP packets do not reach the destination because the xTRs are not able to register the clients with the MS/MR. |

Table 2: Test Plan - Contd1

| Case | Setup | Action | Expected Observation | Recorded Observation |
|---|---|---|---|---|
| 3 | MS/MR turned off after ETR's registration, xTR's are running | Ping from source EID to destination EID | Mapping information messages were never sent by the MS/MR, hence without local cache ping would fail | ICMP packets do not reach the destination because mapping information has not been exchanged between ITR and MS/MR |
| 4 | MS/MR turned off after one EID pings at least one other EID connected to an ETR | Ping from source EID to destination EID | ETR registers the destination EID-RLOC mapping. ITR sends a map-request for destination EID-RLOC mapping. MS/MR responds with mapping information, which is stored in the ITR's cache. LISP tunnel is established and ping from source EID should reach destination EID regardless of MS/MR | After the MS/MR is turned off, ping still works to the original EID that was first pinged. different EIDs pings to the same RLOC is yet to be tested |
| 5 | MS/MR turned off after one EID pings all other EIDs connected to the ETRs | Ping from source EID to destination EID | Local cache obtained from MS/MR would still allow pings from the source EID to still work with all other EIDs till timeout | ICMP packets reach all EIDs as the ITR has stored all the EID prefix to RLOC mapping in its cache before the MS/MR was turned off. |

Table 3: Test Plan

| Case | Setup | Action | Expected Observation | Recorded Observation |
|---|---|---|---|---|
| 6 | xTRs turned off, but MS/MR is running | Ping from source EID to destination EID | No routing information is available from the private address space to the public address space, ping will fail. | ICMP packets do not reach destination because the tunnel routers that connect the clients in the private network to the public network are down. There is no mapping information associated with this ping. |
| 7 | Simulate Client Mobility by changing EID of destination while pinging. | Continuously Ping from source EID to destination EID. Ping should be close to the local mapping timeout | ICMP packets are received(after packet loss) at the xTR responsible for the moved destination EID. Indicating successful RLOC-EID re-mapping. A | To be done |

## 6. SDN Test Plan

### *6.1. Test Application*

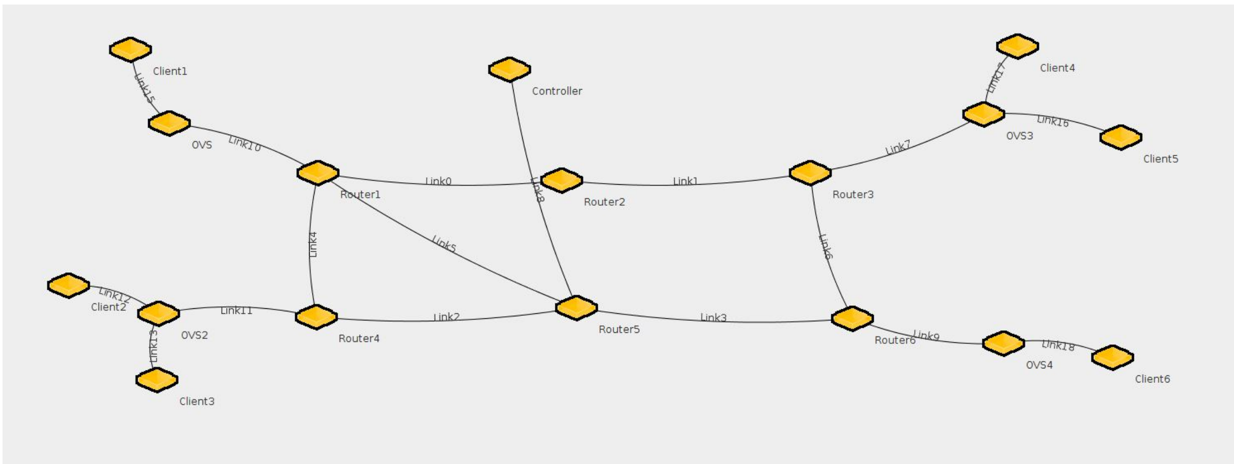


Figure 9: Traditional

Match: The source and destination IP addresses of the flow are the EIDs. Action: Replace the source and destination EIDs with the RLOC (OVS switch) source and destination IP addresses. The test plan below refers to the match and action defined above.

Table 4: SDN Test Plan

| Case | Setup | Action | Expected Observation | Recorded Observation |
|---|---|---|---|---|
| 1 | OVS switches are running, MS/MR application is running in the controller | Ping from source EID to destination EID | If SDN controller obtains mappings from MS/MR it will update the flows of the OVS | TBD |
| 2 | MS/MR application in the controller is not running at the beginning, source and destination OVS switches are running | Ping from source EID to destination EID | No flows are added into the Map server application. The source OVS switch's packet in message to the map server via the controller is not served and there is neither a match nor an action. Source EID should not be able to reach destination EID | TBD. |
| 3 | MS/MR turned off after one EID pings at least one other EID connected to an OVS switch | Ping from source EID to destination EID | Local cache obtained from MS/MR would still allow pings from the source EID to that particular EID, other pings would likely fail | TBD |
| 4 | MS/MR turned off after one EID pings all other EIDs connected to the ETRs | Ping from source EID to destination EID | Local cache obtained from MS/MR would still allow pings from the source EID to still work with all other EIDs till timeout | TBD |

Table 5: SDN Test Plan - Contd2

| Case | Setup | Action | Expected Observation | Recorded Observation |
|---|---|---|---|---|
| 5 | Source and destination OVS switches turned off, but MS/MR application is running in the controller | Ping from source EID to destination EID | flow table entries will not be manually loaded into the MS/MR application. If the source OVS switch is down, there will be no packet-in message to MS/MR via the controller for mapping information so there will be no entries in the source OVS switch's flow table. There will be no flow table match and hence no action will be performed | TBD |
| 6 | Simulate Client Mobility by changing EID of destination while pinging | Continuously Ping from source EID to destination EID | ICMP packets are received(after packet loss) at the OVS switch responsible for the moved destination EID. Indicating successful RLOC-EID re-mapping. | TBD |

## 7. Demo Plan

### *7.1. Demo Plan Topology*

The traditional topology consists of: 6 clients C1, C2, C3, C4, C5, C6, four tunnel routers ITR, ITR2, ETR, ETR2 , and a core network The SDN topology consists of: A controller with the Map Server/Resolver application, 6 clients C1, C2, C3, C4, C5, C6, four OVS switches OVS, OVS2, OVS3, OVS4 , and a core network

Table 6: Demo Plan: Traditional implementation

| Case | Scenario | Expected Observation | Conclusion |
|---|---|---|---|
| 1 | MS/MR and xTRs are in running state. ICMP packets are sent from source EID to destination EID | ETR should send registration messages to MS/MR. ITR should send map-request messages to MS/MR. MS/MR must respond to ITR with mapping information in the map-reply message. LISP tunneling is established. Debug messages can also be observed in the xTRs. Unencapsulated and LISP encapsulated messages can be observed on the xTR interfaces. The map-request and reply messages can be observed on ITR interface and the outgoing interface of MS/MR respectively. Tshark can be used to observe the captured packets. The ICMP packets should successfully reach from source EID to destination EID. | ITR updates its local cache with the mapping information received from MS/MR. ITR sends LISP encapsulated messages with the RLOCs in the header. Packet is decapsulated at ETR and forwarded to destination EID. |

Table 7: Demo Plan: traditional implementation

| Case | Scenario | Expected Observation | Conclusion |
|---|---|---|---|
| 2 | Client Mobility by changing EID | Client moves from old RLOC to new RLOC. New ETR registers updated EID-RLOC mapping with the MS/MR. ITR sends map-request to MS/MR after cache expiry. MS/MR responds to ITR with updated mapping information. Map-request/reply messages can be observed at ITR's and MS/MR's interface respectively. LISP tunnel is established. LISP encapsulated messages can be observed at the ITR's outgoing interface. | The LISP encapsulated messages consist of the new RLOC in the header. ETR decapsulates the LISP packets and forwards the unencapsulated packets to the destination EID. Ping is successful between the source EID and the moved client. |

Table 8: Demo Plan: SDN implementation

| Case | Scenario | Expected Observation | Conclusion |
|---|---|---|---|
| 1 | MS/MR application in the controller and OVS switches are in running state. Flow entries are added manually in the MS/MR application. ICMP packets are sent from source EID to destination EID | Source OVS switch sends packet-in messages to MS/MR application via the controller. MS/MR application checks for EID entry. SDN controller responds to OVS with updated flow table entry. OVS switch performs match and action. | IP rewrite of RLOC address takes place. Flow reaches destination OVS. IP rewrite to EID takes place. EID receives the packets.Ping is successful from source EID to destination EID. |
| 2 | Client Mobility by changing EID | Client moves from old RLOC to new RLOC. Manual updation of EID-RLOC mapping at the MS/MR application updated flow table entries installed at destination OVS switch. Packet-in message from source OVS to controller returns updated EID-RLOC mapping as new flow table entry. | IP rewrite of new RLOC address takes place. Flow reaches new destination OVS. IP rewrite to EID takes place. EID receives the packets.Ping is successful from source EID to destination EID. |

## 8. Self-Study

*8.1. Base Case:*

- Clients are connected to the xTR's, but LISP tunnel feature is turned off, i.e they act as regular routers.
- No Map resolver is present in the system.

*8.2. Characteristics to observe*

- Direct end-to-end client pings will be observed.
- Clients and Routers(xTR's with tunnel off) will require additional routing table entries for packets to travel end-to-end. Pinging end-to-end is observed for this scenario
- xTR's have their tunnel featured turned on. And the additional routing table entries are removed. Ping will observed for such a scenario. Be reminded that a route does not exist between the private address space of the clients to the public address space of the network.
- xTR's are activated in tunnel mode, map resolver is not active, and a ping is observed.
- MS/MR is activated along with xTR's being in LISP tunnel mode. Ping between clients is observed.
- Client with a an EID is moved across to an xTR with a different RLOC. A 10 minute wait is introduced to trigger xTR cache timeouts and a ping is observed from a source client to a client with a different RLOC.

*8.3. Range of scenarios to investigate*

- The separation of private and public address space, before and after LISP tunneling should be investigated.
- EID mobility, i.e. an EID associated with a certain RLOC detaches itself and moves to a different RLOC should be able to retain its connections after possible packet loss.

## 9. References


1. RFC 6830: The Locator/ID Separation Protocol (LISP)
2. Open Overlay Router : https://openoverlayrouter.org/
3. Bird Internet Routing Daemon : http://bird.network.cz/
4. LispMob: https://github.com/LISPmob/lispmob