Preserving IP addresses during DC migration with LISP and ASR 1000

White Paper
# Contents

Executive Summary ........................................................................................................... 4
Cisco Services ..................................................................................................................... 4
Introduction ........................................................................................................................ 5
Needs and benefits of keeping the server IP address during DC migrations ..................... 6
Existing Challenges .......................................................................................................... 7
Benefits of LISP for DC migrations .................................................................................. 8
Positioning of Layer 3-based Data Centers migration ..................................................... 9
LISP and OTV co-existence ............................................................................................... 9
Scope ................................................................................................................................ 9
terminology ....................................................................................................................... 10
Solution Overview ............................................................................................................. 11
Solution Considerations ................................................................................................. 11
Seamless Integration into existing production network ................................................ 12
Map Server/Map Resolver placement ............................................................................. 12
Transport network ............................................................................................................ 12
Routing considerations .................................................................................................... 12
LISP Stretched Subnets Routing ..................................................................................... 13
No Changes to Virtual or Physical Servers ...................................................................... 13
Traffic Symmetry - Firewall and Load Balancer Considerations .................................... 13
Selecting the ASR 1000 option ....................................................................................... 13
Scalability and Latency .................................................................................................... 14
Using non-LISP device as default gateway in Greenfield DC ......................................... 14
Deploying LISP on Cisco ASR 1000 for Data Center Migration .................................... 14
Implementation Details on the Source Data Center ....................................................... 15
Detection of Servers (EIDs) in the Source DC with EEM-script ..................................... 16
Implementation Details on the Greenfield Data Center .................................................. 16
Connectivity between the ASR1000 LISP Routers ....................................................... 17
Discovery of Servers and Registration with the Map-Servers ........................................ 17
Traffic flows ..................................................................................................................... 19
Configuring the Source Site Cisco ASR 1000 Series Router as a LISP PxTR .................. 23
Configuring the Destination Site Cisco ASR 1000 Series Router as a LISP xTR, Map-Server and Map-Resolver ................................................................. 26
Multicast Configuration for LISP Map-Notify Messages in a Multi-homed Environment .... 29
Overview of Steps to Troubleshoot LISP Mobility .......................................................... 75
Step 1: Verify Underlay Routing .................................................................................. 75
Step 2: Verify LISP Control-Plane ........................................................................... 75
Step 3: Verify LISP Data-Plane ................................................................................ 76
Conclusion .................................................................................................................. 76
Appendix ..................................................................................................................... 76
Overview of LISP ........................................................................................................ 76
Cisco LISP Contact Information and Authors .............................................................. 79
Executive Summary

Data Center migration projects usually are complex and involve careful planning and coordination between multiple teams, including Application, Server, Network, Storage and Facilities teams.

It’s common to hear that a Data Center migration project is taking longer than expected, and that coordination between Network and Application/Server teams was one of the reasons for the delay.

The traditional ways of performing Data Center migrations have limitations that often lead to delays and high costs, some of the traditional methods and their limitations are:

- Application migration with IP address change – Expensive and difficult to perform due to the requirement for full documentation of existing application interactions and the associated complexity of migration caused by IP address change. Many applications, particularly legacy applications, still have IP addresses hard coded into the application, so a change of their IP requires a rewrite of the application which is often expensive to do and has a high risk.
- Physically migrate Server network by re-patching or re-build of the source (legacy) network as an extension to target (new) DC – Complex due to the requirement for large volume of data gathering before the project start, as well as in some cases conflicting VLAN numbers between source and target network add to the complexity. Usually this approach involves moving existing servers which does not allow initiatives like server virtualization to happen together with DC migration project, requiring follow on projects.
- Whole Data Center ‘big bang’ migration – Usually not viable due to the requirement for a large volume of data gathering before the project start, high risk associated, as well as the scale of the change with a whole Data Center outage during the migration event. This approach often requires a large workforce.

A better solution for Data Center migrations is one that would allow customers to migrate servers with IP mobility and also remove affinity group constraints of traditional approaches. That is, move a server (physical or virtual) and keep the IP address, subnet mask, default gateway and hostname. Such solution also allows decoupling the server migration process and schedule from network constraints.

On this paper a new solution for Data Center migration is described. It makes use of Locator/ID Separation Protocol (LISP, RFC 6830) running on Cisco’s ASR 1000 routers and simplifies and accelerates Data Center migration. The benefits delivered by this solution include:

- Ability to de-couple the server migration activities (planning, affinity group migration, schedules, cut-overs etc.) from network constraints.
- IP address mobility: IP address, subnet mask, default gateway and hostname of migrated servers do not need to change.
- Small migration waves, that is enables even single server migration (if required), or the migration of a group of servers.
- Lower hardware cost than alternative solution, just four devices required.

Customers who have adopted this solution were able to execute a DC migration with a much lower risk and much faster. In fact some of them expect to reduce the migration window by up to 95%.

Cisco Services

Cisco Services organization is available to assist with the planning, design, deployment, support and optimization of the solution described on this whitepaper.
Effective design is essential to reducing risk, delays, and the total cost of network deployments. Cisco services can deliver a high-level design and/or an implementation-ready detailed design for the solution described on this whitepaper.

Integrating devices and new capabilities without compromising network availability or performance is critical to success. Cisco Deployment services can help by providing expert assistance to develop implementation plans and to install, configure, and integrate the solution described on this paper in your production network. They offer project management, post-implementation support, and ongoing knowledge transfer. After deployment, Cisco services can assist ensuring that your deployment continues to run optimally via Cisco’s Optimization Services.

Cisco Services for the solution described on this whitepaper are available globally and can be purchased from Cisco and Cisco Certified Partners. Service delivery details might vary by region and depending on which service options you choose. For more information about Cisco Services, visit www.cisco.com/go/services.

Introduction

This whitepaper will explain a network solution based on Locator/ID Separation Protocol (LISP, RFC 6830) that helps accelerating Data Center migrations projects and make them run smoother.

The target of this solution is the scenario where a customer has a source environment, usually a data center, and a destination environment, usually a target data center and is trying to migrate servers from the source to the destination data center.

One common requirement on this scenario is the ability to migrate the servers without making any changes to their IP configuration. In particular, server administrators would like to avoid changing the server IP address, subnet mask, and default gateway settings.

Figure 1: Non-Intrusive Insertion of LISP DC Migration Routers

You can use LISP to address this requirement. Figure X represents a functional view of what LISP enables; server 10.1.1.7 is moved to destination data center while other servers in the same subnet remain active on the source data center. No changes required on server 10.1.1.7 IP setting.

LISP separates location and identity, thus allowing the migration or creation of new servers on the target data center with the same IP address (identity of server), subnet mask, and default gateway configurations as the server used on the source data center. The details on how the solution works
will be covered on other sections of the paper, but in short LISP routers update on their database the endpoint ID-to-router locator (EID-to-RLOC) mapping of the server when a server is moved to reflect the new location that, in this example, is the target data center. No changes are required to the end systems, users, or servers, because LISP handles the mapping between identity (server IP address) and location (source or target data center), transparently to the users trying to reach the server.

LISP operates as an overlay, encapsulating the original packet to/from the server into a User Datagram Protocol (UDP) packet along with an additional outer IPv4 or IPv6 header, which holds the source and destination RLOCs. This encapsulation allows the server administrators to have the server in the target DC using the same IP address that existed in the source DC, removing the constraint of having a subnet only present on a single location. The LISP encapsulated packets can cross multiple layer 3 boundaries/hops.

Another important property of LISP that is relevant to enable a safer, lower risk data center migration, is that it enables IP portability by routing (Layer 3) to the right location where the server is, providing total isolation of broadcast (Layer 2) domains between the source and destination data centers.

Non-LISP-enabled sites communicate to the servers moved to the target data center through the source data center, where LISP is deployed. The solution documented on this paper does not require LISP to be enabled globally, but instead its deployed by enabling LISP on just the source and destination data center, with minimal impact on the operations of both sites.

The optional deployment of LISP at remote sites (branch offices) provides data-path optimization, because the LISP-encapsulated traffic is routed directly to the data center where the target server is located.

On the solution documented on this paper, IP mobility service (enabled by LISP) is provided in the network by a Cisco ASR 1000 and supports all kinds of servers - physical or virtual and if virtual running on any hypervisor.

The LISP-enabled ASR 1000 deployed within the source data center does not need to be the default gateway for the local servers (physical and virtual machines) therefore this solution can be introduced non-disruptively into an existing production environment.

In summary, the goal of the solution explained on this paper is to allow a customer to move the servers (physical or virtual) between DCs while keeping their IP address, subnet mask, default gateway and without requiring changes on firewall rules and other access-lists.

The next sections on this paper will cover the needs and benefits provided by LISP for data center migration, then will position LISP as the technology to enable IP mobility in relation to extending layer 2 between data centers. A solution overview, steps for deploying this solution, failure scenarios and convergence time are also analysed on this paper.

Needs and benefits of keeping the server IP address during DC migrations

As mentioned before it’s common to find that server and applications teams would prefer to keep the server IP address during DC migrations, this section of the paper will analyse this requirement.
**Existing Challenges**

Without a solution that provides IP mobility, moving a server/application to new DC requires change of IP address, default gateway and hostname.

*Figure 2: Challenges with Server Migrations*

In this case it takes longer to start moving servers due to data gathering / documentation of application interfaces, interactions and traffic flows. There is also the complexity of ensuring interfaces and flows are maintained, and the effects on even non-moved / non-migrated systems. Figure X1 above illustrate that change in the address affects several communication flows. DNS updates may not always help with legacy applications where the IP address is hard coded. Applications local and remote may need to be amended, as well as firewall rules. The risk associated with such change can be significant.

Another consideration when migrating servers is that some servers have multiple interfaces, for example a server may have an interface for production traffic, another for management, and another for backup and restore, as illustrated on Figure 3. Without IP Mobility, if one does not want to change the IP address of the servers it requires to move all server of a subnet together, however as illustrated below the end result is that a large number of servers need to be moved together, making this approach a “big bang” approach.

*Figure 3: All servers of subnet A, B and C would need to be migrated together.*
Benefits of LISP for DC migrations

The benefits of using the solution proposed on this paper to keep the server IP address during DC migrations can be summarized as:

- You can perform the server migrations in much smaller waves which lowers the risk of the project. It means that even just a single server can be migrated without affecting any other server on any subnet that server is connected to.
- Server Migrations can begin much faster, as soon as the data for that server is available on target data center.
- The amount of data to be kept in synch is minimized, reducing risk and WAN requirements.
- Path optimization from the user to the application is possible, eliminating latency concerns and reducing WAN bandwidth requirements. This requires adoption of LISP on remote sites.
- Removes affinity group constraints. Each server can be migrated independently.

The following table demonstrates the impact of LISP for DC migration by comparing existing approach that provides no IP mobility and LISP where a server keeps its IP address during DC migrations.

<table>
<thead>
<tr>
<th>Migration Wave (numbers of servers to be migrated at once)</th>
<th>Today’s approach (Without IP mobility)</th>
<th>With LISP (With IP Mobility)</th>
<th>Impact of LISP on Data Center Migration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smallest “chunk” that can be migrated is all the servers in the same subnet; usually large number of servers.</td>
<td>Smallest “chunk” that can be migrated is a single server.</td>
<td>Lower risk; Servers can be migrated faster with less dependency.</td>
<td></td>
</tr>
<tr>
<td>When can we start activating the servers on target DC.</td>
<td>Only after all the data for all the servers in the same subnet is migrated to target DC.</td>
<td>As soon as the data for a single server is available, that server can be moved.</td>
<td>Servers can be activated on target DC much sooner than before; Reduces the amount of time large data sets have to be kept in synch.</td>
</tr>
</tbody>
</table>
Positioning of Layer 3-based Data Centers migration

Layer 2 (VLAN) extension can also be used to provide IP mobility during data center migrations, however the requirement for a Layer 3-based (routed based) solution that provides IP mobility is growing because customers prefer not to extend the broadcast (Layer 2) domain between their environments.

The main difference between Layer 2-based technologies, like Cisco Overlay Transport Virtualization (OTV), VPLS, and LISP that provides a Layer 3-based solution is the fact that with LISP the broadcast / Layer 2 failure domain is not extended between sites. Broadcast is not propagated by LISP, with Layer 2-based solutions broadcast packets are flooded.

Another consideration is that a pair of OTV-enabled devices would usually connect to a single pair of aggregation switches given it’s connected at Layer 2, however with LISP a single pair of LISP-enabled routers can connect to multiple aggregation blocks on the source and destination data centers given that they are connected at Layer 3 and therefore does not represent the risk of bridging between aggregation blocks.

It’s important to note that Layer 2-based solutions support stretching cluster members that require Layer 2 connectivity between data centers, LISP cannot support that given it does not flood layer 2 broadcast or link local multicast packets.

Live migration (e.g. VMware vMotion) is another application that requires layer 2 connectivity between hosts, and therefore can only be supported by layer 2-based solution. The LISP-based solution presented on this paper supports “cold” migration between data centers.

LISP and OTV co-existence

LISP supports a deployment mode called Extended Subnet mode where LISP is combined for the same VLAN/subnet together with a LAN Extension solution (for example OTV or VPLS), in this case LISP provides path optimization and the LAN Extension solution provides IP mobility. The solution presented on this whitepaper is not LISP Extended Subnet mode, however as documented on the section “Coexistence with OTV” it’s important to note that it’s also possible to combine OTV and LISP on the same ASR 1000 where OTV is used for some VLANs and LISP is used for others, for example OTV is used to extended VLAN 10, which has subnet 10.10.10.0/24 configured on it, while LISP is used to provide IP mobility for subnet 10.20.20.0/24, VLAN 20. Note that LISP does not extend VLANs therefore the VLAN ID is irrelevant for LISP-based forwarding.

Some customers are taking the approach “Route when you can, bridge when you must” and therefore a Layer 3-based data center migration as covered on this whitepaper is required.

Scope
This paper documents a solution that allows servers to be migrated while keeping their IP address, subnet mask and default gateway. The solution is based on LISP running on the Cisco ASR 1000 deployed on the source and destination data center.

This solution requires the ASR 1000 running Cisco IOS® XE Software Release 3.10 or later with the Advanced IP Services or Advanced Enterprise Services feature set.

Although not described directly on this paper, a Cisco CSR 1000V running IOS® XE Software Release 3.11 or later with the Premium or AX license package can be used with same results.

LISP is supported on several other Cisco platforms, the use of other routers or switches that support LISP to provide the solution described on this paper is outside the scope of this document as their implementation of LISP could vary from the implementation on IOS® XE Software used by ASR 1000 and CSR 1000V.

**Terminology**

**Note:** More detailed terminology is discusses later in the document.

**CSR 1000V:** Cisco’s virtual router offering that you can deploy in private, public, or hybrid cloud environments.

**Locator/ID Separation Protocol (LISP):** A tunnel protocol that uses a central database in which endpoint location is registered. LISP enables an IP host-based mobility of endpoints.

**LISP-enabled virtualized router:** A virtual machine or appliance that supports routing and LISP functions, including host mobility.

**Endpoint ID (EID):** IPv4 or IPv6 identifier of the devices connected at the edge of the network. Used in the first (most inner) LISP header of a packet.

**Routing locator (RLOC):** IPv4 or IPv6 addresses used to encapsulate and transport the flow between LISP nodes.

**Ingress tunnel router (ITR):** A router that has two functions: it resolves the location of an EID by querying the database, and then it performs the encapsulation toward the remote RLOC.

**Egress tunnel router (ETR):** A router that has two functions: it registers the endpoint or location associated with the database, and then it decapsulates the LISP packet and forwards it to the right endpoint.

**xTR:** A generic appellation for a device performing both ITR and ERT functions.

**Proxy-ITR (PITR):** Acts like an ITR but does so on behalf of non-LISP sites that send packets to destinations at LISP sites.

**Proxy-ETR (PETR):** Acts like an ETR but does so on behalf of LISP sites that send packets to destinations at non-LISP sites.

**PxTR:** A generic appellation for a device that performs both PITR and PERT functions.
Solution Overview

Data-Center Migration requires the mobility of any workload with IP address retention, in a plug and play solution, agnostic to server type and hypervisor independent. It must allow partial migration, means keeping a full IP subnet active on both Brownfield and Greenfield DC at the same time. But, in addition, this IP mobility must be performed in total safe connection without extending the fault domain from a site to the other. In the proposed solution, LISP is offering a routed IP mobility, aka a stretched subnet connection via Layer 3 mobility. LISP is a host-based routing technology using a central database and local caching to enable IP intercommunication. For further details on LISP, please see the LISP introduction section in the appendix of this document.

Figure 4: Reference Topology

Solution Considerations

Migration is performed from a legacy brownfield Data-Center toward a Greenfield DC. No constraint is imposed to any of these Data-Centers. Most often the legacy DC is built upon the Aggregation/Access standard architecture, while the new DC is either in the same topology, or even in the Fabric approach with Spine/Leaf concept. But in reality the solution exposed in this document just requires access to the VLANs of the Data-Center without constraint on the internal design.
Seamless Integration into existing production network

To interconnect the DC, the Data-Center Interconnect option is making usage of two pairs of LISP nodes deployed on a stick in each DC, with an IP connection in between that could be the IP infrastructure of the enterprise, or even a direct connection LISP node to LISP node when the migration occurs on short distance. The concept of “on the stick deployment” relies on devices that are not inserted in the common data-path, and so are not used by the main application sessions. The LISP connection will be used only for the workload under migration. The devices are just connected with two links, one toward the core just allowing IP to run, on which the LISP encapsulated packet will fly, then another link in VLAN trunk mode which has to be connected to the distribution layer or to a leaf in order to get access to the subnets in migration.

There are several LISP functions that are used in this design, but they all reside in only two pairs of physical devices. There is no need for any other LISP deployment anywhere else.

In the brownfield DC ASR1K (or CSR1Kv) pair:
- Proxy-ARP: the LISP node will respond to ARP directed to any migrated workload, this attracts traffic to LISP.
- PITR: Get the flow from any source to be transported by LISP
- PETR: Attract traffic that return from the new DC to ensure symmetrical path, if needed

In the Greenfield DC ASR1K (or CSR1Kv) pair:
- Default-Gateway: During the migration the ASR1K is the gateway for the subnet under migration
- ETR: to transmit traffic coming from LISP to DC
- ITR: to transmit traffic coming from the DC to LISP
- Use-PETR option to force all traffic returning back to original DC

Map Server/Map Resolver placement

In addition, the LISP database, composed of the Map-server (MS) and the map-resolver (MR) has to be hosted on one pair of the devices. This could be anywhere, for this paper, it has been decided to host it on the Greenfield side.

Transport network

For the solution described on this whitepaper, the only requirement from the transport network is that it provides IP connectivity between the LISP-enabled routers located in the source and destination data centers. We refer to this network as the transport network.

The transport network can be IP based or MPLS-based, as long as there is IP connectivity between the LISP-enabled routers the solution works. The IP connectivity can be provided by dedicated links interconnecting the sites as per Figure 5: Reference Topology or the LISP flows can go over the WAN.

Routing considerations

As stated, the LISP nodes just require being reachable between each other thru an IP network. If this IP connection is the Enterprise network, two considerations have to be taken in account. One is the MTU size. LISP encapsulates packets under UDP and extends their size. LISP adds 36 bytes for IPv4 and 56 bytes for IPv6 encapsulation. LISP tunnel does support dynamic MTU adaptation through PMTUD, and LISP nodes do support packet fragmentation, but the easiest way would be to have the IP network supporting the large MTU. The other consideration to take in account is the fast convergence. LISP is converging upon node failure at the speed of the advertisement by the IGP of
the failure of the Route-Locator, which is the tunnel tail-end address. So, if the IGP is slow convergence, so is LISP. Optionally LISP offers the enabling of regular probing, but with a minimum of 60s for detection. In very rare case, usage of SLA probes would give back fast convergence to LISP even if the infrastructure is slow. In the special, but common case, where the LISP nodes are directly connected DC to DC, the IP network is just this connection. Here, the LISP IP network is independent from the Enterprise Core and WAN, it just has to be considered as an isolated IP network, with its own local IGP, tuned to fast convergence.

**LISP Stretched Subnets Routing**
The pair of LISP PXTR in the Brownfield DC is interacting with the local DC only via Proxy-ARP. When one server is moved to the new DC it will be detected and registered into the LISP Database, and from now the local pair of PXTR will reply with their own MAC to any ARP toward the remote server. Reachability throughout the stretched subnet is then established.

**No Changes to Virtual or Physical Servers**
As the subnet is extended smoothly, and there is a default-gateway on each DC with the same Virtual-IP address, there is absolutely no change to be performed on the migrated server. In addition, as the IP address and reachability of the moved workload has absolutely not changed, neither the Firewall rules nor the Load-Balancer definition have to be updated. During the migration, the service nodes are still running on the old Data-Center, and will be moved at the end of migration.

**Traffic Symmetry - Firewall and Load Balancer Considerations**
Most of the time, due to the presence of a Firewall or/and a Load-balancer, the traffic coming back from the moved workload has to be pushed back toward the Brownfield DC. For this, during the migration, the ASR1K pair on the Greenfield DC is maintained as the Default-Gateway for the moved servers, and is forcing traffic to be back to the primary DC using LISP tunneling toward the PETR. From there, the traffic is delivered either natively to the L3 network going through the site Firewall, or through the L2 LAN itself via Policy-Based Routing (PBR) in case the Firewall or the Load-Balancer are the local default-gateway.

**Selecting the ASR 1000 option**
All ASR 1000 routers are capable of supporting the solution described on this whitepaper. There are no hardware dependencies. The only difference between the ASR 1000 routers is their performance, number of interfaces and redundancy model (Software or Hardware).


The same solution, with exactly the same configuration, can be used for scenarios requiring lower throughput, for example by using an ASR 1001-X, or in scenarios where 100 Gbps+ throughput is required an ASR 1006 or ASR 1013 can be utilized.

For more information about the Cisco ASR 1000 Series, visit http://www.cisco.com/go/asr1000 or contact your local Cisco account representative. For information about the Cisco ASR 1000 Series ordering and bundles, please refer to the Cisco ASR 1000 Ordering Guide.
Scalability and Latency

The migration nodes, one pair per site, could be any device supporting LISP mobility, what has been validated up to today is either the ASR1000 or the virtual router CSR1000v. Any combination of these devices is supported. Please refer to the ASR1000 part above for detail on the node choice depending on the needed throughput.

Regarding scalability, the solution described on this paper has been validated to support up to 5000 (five thousand) dynamic EIDs when deployed in an ASR 1000.

In terms of latency, each ASR 1000 LISP node adds 30 microseconds, which is negligible. The latency on the link connecting the sites needs to be considered.

Using non-LISP device as default gateway in Greenfield DC

The solution in this white-paper relies on the default-gateway of the greenfield site to be on the LISP XTR for the workload under migration. Only at the end of migration it can be moved toward the aggregation layer. This is the recommended and tested design. Now, it could happen that the requirement be different and that on the new DC the default-gateway has to be put on another device.

First and easy case is when the brownfield DC does not have any Firewall. In this case no symmetry of traffic is required, the traffic on the greenfield side can exit naturally through routing, there is no need for LISP encapsulation on the return traffic, and the default-gateway can be anywhere.

If the old DC is having a Firewall that requires symmetry of traffic, this means that the LISP XTR on the new DC must capture the return traffic. This means that the default-gateway has to force traffic across the LISP node by any way, could be a default-route, or could be a PBR based on source subnet under migration.

Deploying LISP on Cisco ASR 1000 for Data Center Migration

The reference topology shows two data centers. The source data center is the legacy data center where the servers are currently located. The destination data center is the new data center where the servers will be migrated to. This example shows two server subnets 10.1.1.0/24 and 10.1.2.0/24 which are in VLANs 200 and 201 respectively in the source data center. LISP mobility will be enabled on the ASR1000 routers for these two subnets, to allow servers to be migrated from the source to destination data center. In the destination data center there will be a new VLAN allocation scheme, so the subnets 10.1.1.0/24 and 10.1.2.0/24 will be in VLANs 4000 and 4001 respectively.

Note that there are no stateful devices such as loadbalancers or Firewalls in this initial example. The inclusion of firewalls or loadbalancers in the topology will be discussed in the section ‘Support for Stateful Devices’ later in the document.
Implementation Details on the Source Data Center

The source data center consists of a traditional 3-tier topology with servers connected to the access layer. The default gateway for the servers is the aggregation switches. If supported, the aggregation switches could use VSS, or run in standalone mode and use HSRP for first hop redundancy for the servers. The aggregation switches will advertise the server subnets into a dynamic routing protocol and have routed layer-3 interfaces facing the core devices. The core devices will in turn advertise the server subnets to the WAN to attract traffic from the remote sites to the source data center.

The ASR1000 routers in the source data center will be configured as LISP PxTRs. The aggregation switches will use Dot1Q trunks to connect to the PxTRs and trunk the server VLANs. The PxTRs will use routed Dot1Q sub-interfaces on these trunks for each server subnet that needs to be migrated.

The PxTRs will run HSRP for each server subnet to determine the active PxTR for egress traffic for each server subnet. This will be a separate HSRP group to the HSRP group used on the aggregation switches, and the servers will not use the PxTRs as their default gateway. In this example PxTR-01 will be HSRP active for both server subnets.

LISP mobility will be enabled for the server subnets on the PxTRs, hence these subnets will be dynamic-EID subnets. A lower RLOC priority will be given to PxTR-01 for both dynamic-EID subnets. PxTR-02 will be assigned a higher RLOC priority for both dynamic-EID subnets. Lower priority is preferred, hence inbound LISP encapsulated traffic will go via PxTR-01 during normal circumstances.
The destination data center ASR1000 routers will use source data center ASR1000 routers as Proxy Egress Tunnel Routers (PeTR). This will allow servers that have been migrated to send traffic destined to non-LISP subnets or remote sites via the source data center. This will enable traffic to flow symmetrically for servers that have migrated through any stateful devices in the source data center such as load-balancers or firewalls. A separate Dot1Q sub-interface on both PxTRs without LISP mobility enabled will be used for default gateway routing. A /29 subnet will be used for this VLAN. A static default-route will be used on the PxTRs with the next hop as the aggregation switches’ HSRP VIP or SVI for the VLAN if using VSS. This sub-interface will be used only for outbound traffic towards non-LISP subnets and remote sites. Since these sub-interfaces will only be used for outbound traffic from the PxTRs, HSRP is not required on the PxTRs for this subnet.

Detection of Servers (EIDs) in the Source DC with EEM-script

LISP mobility depends on the xTR receiving traffic from servers to determine their location. On the source data center the PxTRs are not the default gateways for the servers. Hence they depend on receiving broadcast traffic such as ARPs from the servers to detect them. In most cases this is not an issue since servers will regularly send broadcast ARPs either to resolve the MAC address for other servers on the subnet or to resolve the MAC address of the default gateway. However this may be a problem if a server has already resolved the MAC address of the default gateway before the PxTR routers are added to the network. Subsequent ARP requests from the server for the default gateway may be sent unicast to refresh its ARP cache.

Since the PxTR routers will not be the default gateways in the source data center they may never learn about servers that are not sending broadcasts. To solve this problem an EEM script can be used on the primaryPxTR to ping every IP address in the LISP mobility enabled subnets. Before pinging each IP address the PxTR needs to send an ARP request for the address of the server. Each server that responds with an ARP reply will be added to the PxTR’s local LISP database as a dynamic-EID. This solution works even if the server has a software firewall which blocks pings, since the PxTR can build its local LISP database based on the ARP replies even without getting an ICMP reply.

Examples of these EEM scripts will be shown later in the configuration section of this document.

Implementation Details on the Greenfield Data Center

The destination data center is based on a modern spine-leaf architecture. The ASR1000 routers in the destination data center will be LISP xTRs and LISP mapping-server/map-resolvers (MS/MR). The spine switches will use Dot1Q trunks to connect to the xTR-MS/MRs and trunk the server VLANs. The xTR-MS/MRs will use routed Dot1Q sub-interfaces on these trunks for each server subnet that needs to be migrated.

The xTR-MS/MRs will run HSRP for each server subnet to determine the active iTR for egress traffic for each server subnet. This will be the same HSRP group as the HSRP group used on the aggregation switches in the source data center, and the migrated servers will use the xTR-MS/MRs as their default gateway for the duration of the migration. This will allow the migrated servers to use the same IP address and MAC address for their default gateway after they have been migrated. In this example xTR-MSMR-01 will be HSRP active for both server subnets.
LISP mobility will be enabled for the server subnets on the xTR-MS/MRs, hence these subnets will be dynamic-EID subnets. A lower RLOC priority will be given to xTR-MSMR-01 for both dynamic-EID subnets. xTR-MSMR-02 will be assigned a higher RLOC priority for both dynamic-EID subnets. Lower priority is preferred, hence inbound LISP encapsulated traffic will go via xTR-MS/MR-01 during normal circumstances.

**Connectivity between the ASR1000 LISP Routers**

Each LISP router just needs layer-3 IP reachability to the RLOC addresses of the other LISP routers. So the solution is layer-1 and Layer-2 agnostic. The connectivity between the ASR1000 LISP routers can be over any physical medium such as dark fibre, DWDM, SONET, SDH. The connectivity could be over Layer-2 metroEthernet, MPLS L3VPNs or the internet. It is even possible to use the data centers existing WAN links for IP connectivity between the LISP routers. Typically for a data center migration dedicated links would be used for the duration of the migration. Dark fibre between the data centers would be more common for distances less than 10km, whereas DWDM or metroEthernet might be more common for distances above 10km.

This example will assume there is dedicated layer-1 or layer-2 links between the ASR1000 routers for the migration, i.e. the interfaces between the ASRs are layer-2 adjacent and are on the same subnet. A loopback interface will be used on each of the LISP routers for the RLOC. OSPF will be used as the routing protocol between the LISP routers. BFD may be used to improve convergence if the connectivity between the ASRs is over a layer-2 network such as metroEthernet. OSPF should only be enabled on the point-to-point links between the ASRs and the LISP loopback interface. OSPF should not be enabled on the sub-interfaces connecting to the data center switches and the data center server subnets should not be announced into OSPF.

**Discovery of Servers and Registration with the Map-Servers**

The LISP PxTR routers can be connected into the existing environments in the source and destination data center non-intrusively. No routing changes are required on the source data center. Since routed sub-interfaces are used on the PxTR routers facing the aggregation switches, there is no spanning-tree. It is recommended to use ‘spanning-tree portfast trunk’ on the trunk ports on the aggregation switches facing the ASRs for faster convergence. LISP mobility will be enabled on each server facing sub-interface on the PxTRs.

The PxTR routers will not be the default gateway for the servers in the source data center. The HSRP active PxTR will update its local LISP database based on broadcast packets such as ARPs it receives from servers within the subnets that LISP mobility is enabled. Each server detected will appear as a dynamic-EID in the local LISP database. The HSRP active PxTR will send multicast LISP map-notify messages back out the interface the server was detected on. The HSRP standby PxTR will update its local LISP database based on the information in map-notify messages received from the active PxTR.

Both PxTRs will send a map-register to both map-servers which are the LISP xTR-MSMR routers in the destination data center. The map-servers will update the EID-to-RLOC mapping database base on the information in the map-register messages. This information includes the RLOCs, their priority and weight values for each EID. Initially when no servers have been migrated the RLOC addresses for all EIDs registers in the EID-to-RLOC mapping database will be the RLOC addresses of the two PxTRs.

*Figure 7: Discovery of Servers and Registration with Map-Servers*
Similar to the source data center, the destination data center xTR-MSMR routers will be connected to the spine switches over a Dot1Q trunk with routed sub-interfaces on the xTR-MSMRs. Hence there is no spanning-tree interaction. Similarly it is recommended to use ‘spanning-tree portfast trunk’ on the ports on the spine switches facing the ASRs for faster convergence. Each sub-interface on the xTR-MSMRs will be for the new server VLANs in the destination data center and will have LISP mobility enabled.

When a server is migrated to the new data center it will ARP for its default gateway. In the destination data center the default gateway for the servers will be the xTR-MSMR routers. The xTR-MSMSR routers will update their Local LISP database to include the server that has ARP’d. They will then update the map-server EID-to-RLOC mapping database which is stored locally since these routers are the map-servers. They will then send a map-notify message to the PxTR routers to indicate that the server is now located in the destination data center. The PxTRs will remove this server from their local LISP data base and send a GARP out the sub-interface for the VLAN that the server previously resided. Other devices within that VLAN should update their ARP cache to use the HSRP VIP MAC address of the PxTR for the migrated server’s IP address.

Figure 8: Migration of a Server to the Destination Data Center
Traffic flows

The LISP routers can be connected into the existing environments in the source and destination data center non-intrusively. No routing changes are required on the source data center. Traffic to and from the WAN and servers in the source data center will still route in and out of the source data center. The LISP routers will not be in the traffic path for any flows between servers in the source data center and the WAN.

Figure 9: Traffic between Server still in the Source Data Center and the WAN
The LISP routers also will not be in the traffic path for any flows between servers within the same data center, whether it is intra-vlan or inter-vlan traffic. All traffic between servers in the same data center is kept local to that data center.

Figure 10: Inter-VLAN routing is Local between servers in the Same Data Center
The LISP routers only take part in traffic forwarding for flows between the data centers. For example traffic between migrated servers and servers still in the source data center. When a server that has been migrated to the destination data center needs to send traffic to a server in the same subnet that is still in the source data center it will send an ARP. Since ARPs are broadcast packets the xTR-MSMR that is HSRP active will check its local LISP database to see if the server (EID) is on its local data center. If not it will proxy-ARP for the destination EID and check its LISP map-cache for a mapping for the destination EID. If there is no entry in the map-cache it will query the map-server EID-to-RLOC database and update the map-cache if an entry exists. The originating server will now have an ARP entry for the remote server with the MAC address of the HSRP VIP of the xTR-MSMRs and can now send packets to the remote server. Base on its map-cache entry for the destination EID the xTR-MSMR that is HSRP active will LISP encapsulate these packets with a destination RLOC of the PxTR in the source data center that has the lowest priority. Upon receiving the LISP encapsulated packet the PxTR will decapsulate it and forward the original packet to the server in the source data center. The same process

Figure 11: Intra-VLAN Traffic between Data Centers

The xTR-MSMRs will be the default gateway for servers migrated to the destination data center. So for inter-VLAN traffic between data centers, the server in the destination data center will forward the traffic to its default gateway which is the HSRP VIP of the xTR-MSMRs. The HSRP active xTR-MSMR is HSRP active will check its map-cache as in the previous example and LISP encapsulate the packet to the source data center PxTR. The PxTR will decapsulate the packet and forward it to the server.

In the source data center the PxTRs are not the default gateway for servers, so for return traffic the server in the source data center will send the traffic to the aggregation switches which are its default gateway. The Aggregation switches will ARP for the destination, and the active PxTR will proxy-ARP for the server if it doesn’t have an entry for it in its local LISP database. Hence the aggregation
switches will use the PxTR’s HSRP VIP MAC address when forwarding the frame to the destination server. Then the PxTR will LISP encapsulate the packet with a destination RLOC of the xTR-MSMR with the lowest priority according to its map-cache.

**Figure 12: Inter-VLAN Traffic between Data Centers**

Since the source data center LISP routers are Proxy Ingress and Egress Tunnel Routers (PxTR) traffic to and from the WAN to servers that have migrated will get LISP encapsulated between the two data centers.

Traffic from the WAN to a server that has migrated to the destination data center will follow the IP route advertised by the Core switches in the source data center. This traffic will be routed to the aggregation switches which will ARP for the destination. The PxTR that is HSRP active will proxy ARP for the server if is not in its local LISP database. Hence the traffic will be attracted to the PxTR which will LISP encapsulate it destination data center xTR-MSMR. Since the PiTR function is enabled on the PxTRs they will not check the source address of the packet to make sure the source is from a LISP enabled subnet before forwarding it. This check is only done by an iTR.

For the traffic from the destination data center server to the WAN, the server will sent the traffic to its default gateway which is the HSRP VIP of the xTR-MSMRs. The use-PeTR function is enabled on the xTR-MSMRs. That means that if the xTR-MSMR gets a negative map-reply for the destination address it will LISP encapsulate it to a pre-configured Proxy-Egress Tunnel Router, which in this case is the PxTRs. A negative map-reply means that the map-server does not have any EID-to-RLOC mapping for the destination which is expected for any destination that is on a non-LISP site. Hence in this case the xTR-MSMR will LISP encapsulate the packet to the PxTR with the lowest configured priority. The PxTR will decapsulate the packet and forward it the aggregation switches via the sub-
interface used for default routing. The Aggregation switches will then route the packet via the Core switches to the remote site.

Figure 13: Traffic between Migrated Server in the Destination Data Center and the WAN

Configuring the Source Site Cisco ASR 1000 Series Router as a LISP PxTR

Enter the commands shown here to enable and configure LISP PeTR and PeTR (PxTR) functions on a Cisco ASR 1000 Series Router.

Configuration Commands

1. `configuration terminal`

2. `router lisp`

3. `ipv4 proxy-etr`

4. `ipv4 proxy-itr <locator_ip>`

5. `ipv4 etr`

6. `ipv4 itr map-resolver <map-resolver-address>`

7. `ipv4 etr map-server <map-server-address> key <authentication-key>`

8. `locator-set <locator-set-name>`

9. `<locator_ip> priority <priority-value> weight <weight-value>`
10. `eid-table default instance-id 0`

11. `dynamic-eid <dynamic-eid-name>`

12. `database-mapping <dynamic-eid-prefix> locator-set <locator-set-name>`

13. `map-notify-group <map-notify-group-ip>`

14. `exit`

15. `interface <interface-name>`

16. `lisp mobility <dynamic-eid-map-name>`

17. `no lisp mobility liveness test`

18. `ip proxy-arp`

19. `exit`

<table>
<thead>
<tr>
<th>Steps</th>
<th>Cisco IOS XE Commands</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router lisp</code></td>
<td>Enables and enters into the router LISP configuration mode</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ipv4 proxy-etr</code></td>
<td>Enables LISP PeTR functions for the IPv4 address family</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ipv4 proxy-itr &lt;locator_ip&gt;</code></td>
<td>Enables LISP PiTR functions for the IPv4 address family</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>ipv4 etr &lt;locator_ip&gt;</code></td>
<td>Enables LISP eTR functions for the IPv4 address family</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>ipv4 itr map-resolver &lt;map-resolver-address&gt;</code></td>
<td>Configures the IP address of the LISP Map-Resolver to which this router, acting as an IPv4 LISP ITR, will send LISP Map-Requests for destination EIDs.</td>
</tr>
</tbody>
</table>
| Step 7 | `ipv4 etr map-server <map-server-address> key <authentication-key>` | Configures the IP address of the LISP Map-Server to which this router, acting as an IPv4 LISP ETR, will register  
*Note: The Map-Server must be configured to accept map-registers for the EID prefixes configured on this ETR and with a key matching the one configured on this ETR.* |
<p>| Step 8 | <code>locator-set &lt;locator-set-name&gt;</code> | Locator-sets can be used to create a list of locator_ip addresses for the local site and assign a priority and weight to each locator_ip. This can help reduce the configuration for a multi-homed LISP site. Rather than needing multiple database mapping statements for each EID, a single locator-set can be referenced in the database mapping. |
| Step 9 | <code>&lt;locator_ip&gt; priority &lt;priority-value&gt; weight &lt;weight-value&gt;</code> | Defines each of the locator_ip addresses (RLOC) and the weight and priority associated with them. For a multi-homed LISP site, repeat this command to define the locator_ip, priority and weight for each eTR. Lower priority is preferred for inbound traffic. If priority is the same, then inbound traffic will be load-balanced based on the weight values. |</p>
<table>
<thead>
<tr>
<th>Steps</th>
<th>Cisco IOS XE Commands</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 10</td>
<td><code>eid-table default instance-id 0</code></td>
<td>Enters the LISP configuration for the global routing table (default) which is mapped to the LISP instance-id 0. This configuration example is for a dedicated environment using the global routing table. For a multitenant environment each VRF needs to be mapped into a LISP instance-id. Multitenant example: <code>eid-table vrf &lt;vrf-name&gt; instance-id &lt;instance-id&gt;</code> This command would enter the LISP configuration for a particular VRF.</td>
</tr>
<tr>
<td>Step 11</td>
<td><code>dynamic-eid &lt;dynamic-eid-map-name&gt;</code></td>
<td>Enters the dynamic-EID map configuration mode</td>
</tr>
<tr>
<td>Step 12</td>
<td><code>database-mapping &lt;dynamic-eid-prefix&gt; locator-set &lt;locator-set-name&gt;</code></td>
<td>Configures a dynamic-EID range and the RLOC mapping relationship and associated traffic policy for all IPv4 dynamic-EID prefixes for this LISP site based on the locator-set previously defined. Since this command is configured in the dynamic-EID map configuration mode, the LISP ETR will register a /32 host prefix with the mapping system after a dynamic-EID is detected in the configured range.</td>
</tr>
<tr>
<td>Step 13</td>
<td><code>map-notify-group &lt;map-notify-group-ip&gt;</code></td>
<td>If the LISP dynamic-EID site is multihomed, sends a message noting dynamic-EID detection by one ETR to the second ETR in the same site, so the traffic can be handled or load-balanced by both xTRs In this case, enter the <code>map-notify-group</code> command for the dynamic-EID map with a multicast group IP address. This address is used to send a Map-Notify message from the ETR to all other ETRs belonging to the same LISP and data center sites after a dynamic EID is detected. This multicast group IP address can be whatever the user wants other than an address that is already in use in the network.</td>
</tr>
<tr>
<td>Step 14</td>
<td><code>exit</code></td>
<td>Exits the LISP configuration mode</td>
</tr>
<tr>
<td>Step 15</td>
<td><code>interface &lt;interface-name&gt;</code></td>
<td>Enters the interface configuration mode. This is the interface or sub-interface on which LISP mobility is to be enabled. This interface or sub-interface must be in the same VLAN as the servers to be migrated.</td>
</tr>
<tr>
<td>Step 16</td>
<td><code>lisp mobility &lt;dynamic-eid-map-name&gt;</code></td>
<td>Enables the interface for LISP mobility. Configures the interface to allow dynamic-EIDs to be detected within the prefix defined by the database-mapping for the dynamic-eid-map-name in the LISP configuration. The <code>dynamic-eid-map-name</code> entry is the dynamic EID map name configured in Step 11.</td>
</tr>
<tr>
<td>Step 17</td>
<td><code>no lisp mobility liveness test</code></td>
<td>Optional. Disables the LISP liveness test which is enabled by default when LISP mobility is enabled on an interface. The liveness test will send a ping every 60 seconds to every dynamic EID detected, to make sure it is still reachable. This is not required for the data center migration use-case.</td>
</tr>
<tr>
<td>Step 18</td>
<td><code>ip proxy-arp</code></td>
<td>Enables proxy-arp on the interface. Proxy-arp is enabled by default and is required for intra-vlan traffic to work.</td>
</tr>
</tbody>
</table>
### Configuring the Destination Site Cisco ASR 1000 Series Router as a LISP xTR, Map-Server and Map-Resolver

Enter the commands shown here to enable and configure LISP map-server, map-resolver, iTR and eTR (xTR) functions on a Cisco ASR 1000 Series Router.

**Configuration Commands**

1. `configuration terminal`
2. `router lisp`
3. `ipv4 map-server`
4. `ipv4 map-resolver`
5. `site <site-name>`
6. `authentication-key <authentication-key>`
7. `eid-prefix <eid-prefix> accept-more-specifics`
8. `exit`
9. `ipv4 itr`
10. `ipv4 etr`
11. `ipv4 use-petr <petr-locator-ip> priority <priority-value> weight <weight-value>`
12. `ipv4 itr map-resolver <map-resolver-address>`
13. `ipv4 etr map-server <map-server-address> key <authentication-key>`
14. `locator-set <locator-set-name>`
15. `<locator_ip> priority <priority-value> weight <weight-value>`
16. `eid-table default instance-id 0`
17. `dynamic-eid <dynamic-eid-name>`
18. `database-mapping <dynamic-eid-prefix> locator-set <locator-set-name>`
19. `map-notify-group <map-notify-group-ip>`
20. `exit`

### Cisco IOS XE Commands

<table>
<thead>
<tr>
<th>Steps</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>using LISP mobility between sites.</td>
<td></td>
</tr>
<tr>
<td>exits the interface configuration mode</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
</tbody>
</table>
21. `interface <interface-name>`

22. `lisp mobility <dynamic-eid-map-name>`

23. `no lisp mobility liveness test`

24. `ip proxy-arp`

25. `exit`

<table>
<thead>
<tr>
<th>Steps</th>
<th>Cisco IOS XE Commands</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router lisp</code></td>
<td>Enables and enters into the router LISP configuration mode</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ipv4 map-server</code></td>
<td>Enables LISP Map-Server functions for the IPv4 address family</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>ipv4 map-resolver</code></td>
<td>Enables LISP Map-Resolver functions for the IPv4 address family</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>site &lt;site-name&gt;</code></td>
<td>Creates the indicated LISP site and enters the LISP site configuration mode for the map-server</td>
</tr>
</tbody>
</table>
| Step 6 | `authentication-key <authentication-key>` | Enters the authentication key type and password for the LISP site being configured.  
**Note:** The password must match the one configured on the ETR for the ETR to register successfully. |
| Step 7 | `eid-prefix <eid-prefix> accept-more-specifics` | Enters the EID prefix for which the LISP site being configured is authoritative and configures the site to accept more specific prefixes in the event of dynamic-EID map configurations in the eTR  
**Note:** If the eTR is configured with a dynamic-EID map with a prefix to roam, that prefix should be configured in the Map-Server using this command.  
If the EID prefixes configured on the eTRs are contiguous then single larger prefix that covers all the smaller prefixes can be defined here to reduce the configuration.  
**Note:** This example only applies to the global routing table. When using LISP for multiple VRFs then the instance-id needs to be defined with the eid-prefix command. |
| Step 8 | `exit` | Exits the LISP site configuration mode |
| Step 9 | `ipv4 itr` | Enables LISP itr functions for the IPv4 address family |
| Step 10 | `ipv4 etr` | Enables LISP eTR functions for the IPv4 address family |
| Step 11 | `ipv4 use-petr <petr-locator-ip> priority <priority-value> weight <weight-value>` | Optional. If symmetric routing of traffic is required back to the source data center from servers that have migrated to remote non-LISP enabled sites, then the use-PeTR function can be used. When there is a negative map-reply for a destination IP, then traffic to that destination will get LISP encapsulated to the PeTR.  
If there are multiple PeTRs, then repeat this command to... |
<table>
<thead>
<tr>
<th>Steps</th>
<th>Cisco IOS XE Commands</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>define the locator-ip, priority and weight for each PeTR.</td>
</tr>
<tr>
<td>Step 12</td>
<td>ipv4 itr map-resolver &lt;map-resolver-address&gt;</td>
<td>Configures the IP address of the LISP Map-Resolver to which this router, acting as an IPv4 LISP ITR, will send LISP Map-Requests for destination EIDs.</td>
</tr>
</tbody>
</table>
| Step 13 | ipv4 etr map-server <map-server-address> key <authentication-key> | Configures the IP address of the LISP Map-Server to which this router, acting as an IPv4 LISP ETR, will register.  
**Note:** The Map-Server must be configured to accept map-registers for the EID prefixes configured on this ETR and with a key matching the one configured on this ETR. |
| Step 14 | locator-set <locator-set-name> | Locator-sets can be used to create a list of locator_ip addresses for the local site and assign a priority and weight to each locator_ip. This can help reduce the configuration for a multi-homed LISP site. Rather than needing multiple database mapping statements for each EID, a single locator-set can be referenced in the database mapping. |
| Step 15 | <locator_ip> priority <priority-value> weight <weight-value> | Defines each of the locator_ip addresses (RLOC) and the weight and priority associated with them. For a multi-homed LISP site, repeat this command to define the locator_ip, priority and weight for each eTR. Lower priority is preferred for inbound traffic. If priority is the same, then inbound traffic will be load-balanced based on the weight values. |
| Step 16 | eid-table default instance-id 0 | Enters the LISP configuration for the global routing table (default) which is mapped to the LISP instance-id 0. This configuration example is for a dedicated environment using the global routing table.  
For a multitenant environment each VRF needs to be mapped into a LISP instance-id.  
Multitenant example:  
eid-table vrf <vrf-name> instance-id <instance-id>  
This command would enter the LISP configuration for a particular VRF. |
| Step 17 | dynamic-eid <dynamic-eid-map-name> | Enters the dynamic-EID map configuration mode.  
**Note:** The dynamic-eid-map-name entry can be any user-defined name. |
| Step 18 | database-mapping <dynamic-eid-prefix> locator-set <locator-set-name> | Configures a dynamic-EID range and the RLOC mapping relationship and associated traffic policy for all IPv4 dynamic-EID prefixes for this LISP site based on the locator-set previously defined.  
Since this command is configured in the dynamic-EID map configuration mode, the LISP ETR will register a /32 host prefix with the mapping system after a dynamic-EID is detected in the configured range. |
| Step 19 | map-notify-group <map-notify-group-ip> | If the LISP dynamic-EID site is multihomed, sends a message noting dynamic-EID detection by one ETR to the second ETR in the same site, so the traffic can be handled or load-balanced by both xTRs.  
In this case, enter the map-notify-group command for the dynamic-EID map with a multicast group IP address. This address is used to send a Map-Notify message from the ETR to all other ETRs belonging to the same LISP. |
<table>
<thead>
<tr>
<th>Steps</th>
<th>Cisco IOS XE Commands</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>and data center sites after a dynamic EID is detected. This multicast group IP address can be whatever the user wants other than an address that is already in use in the network.</td>
</tr>
<tr>
<td>Step 20</td>
<td><code>exit</code></td>
<td>Exits the LISP configuration mode</td>
</tr>
<tr>
<td>Step 21</td>
<td><code>interface &lt;interface-name&gt;</code></td>
<td>Enters the interface configuration mode. This is the interface or sub-interface on which LISP mobility is to be enabled. This interface or sub-interface must be in the VLAN that the servers are being migrated to.</td>
</tr>
<tr>
<td>Step 22</td>
<td><code>lisp mobility &lt;dynamic-eid-map-name&gt;</code></td>
<td>Enables the interface for LISP mobility. Configures the interface to allow dynamic-EIDs to be detected within the prefix defined by the database-mapping for the dynamic-eid-map-name in the LISP configuration. The <code>dynamic-eid-map-name</code> entry is the dynamic EID map name configured in Step 17.</td>
</tr>
<tr>
<td>Step 23</td>
<td><code>no lisp mobility liveness test</code></td>
<td>Optional. Disables the LISP liveness test which is enabled by default when LISP mobility is enabled on an interface. The liveness test will send a ping every 60 seconds to every dynamic EID detected, to make sure it is still reachable. This is not required for the data center migration use-case.</td>
</tr>
<tr>
<td>Step 24</td>
<td><code>ip proxy-arp</code></td>
<td>Enables proxy-arp on the interface. Proxy-arp is enabled by default and is required for intra-vlan traffic to work using LISP mobility between sites.</td>
</tr>
<tr>
<td>Step 25</td>
<td><code>exit</code></td>
<td>Exits the interface configuration mode</td>
</tr>
</tbody>
</table>

**Multicast Configuration for LISP Map-Notify Messages in a Multi-homed Environment**

The ASR 1000 series routers do not support multicast host mode. Therefore multicast routing need to be enabled to allow the site-local multicast LISP map-notify message to be processed. This is only required for a multi-homed site to keep the LISP databases in sync between the two xTRs on the site. Enter the commands shown here to enable multi-homing a Cisco ASR 1000 Series Router.

**Configuration Commands**

1. `configuration terminal`
2. `ip multicast-routing`
3. `interface Loopback <number>`
4. `ip address <loopback-ip-address> <subnet-mask>`
5. `ip pim sparse-mode`
6. `ip pim rp-address <loopback-ip-address>`
7. `interface <interface-name>`
8. ip pim sparse-mode

9. exit

<table>
<thead>
<tr>
<th>Steps</th>
<th>Cisco IOS XE Commands</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enters the global configuration mode</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip multicast-routing</td>
<td>Enables multicast routing for the global routing table</td>
</tr>
<tr>
<td>Step 3</td>
<td>interface Loopback &lt;number&gt;</td>
<td>Create a new loopback interface to be used as the PIM RP</td>
</tr>
<tr>
<td>Step 4</td>
<td>ip address &lt;loopback-ip-address&gt; &lt;subnet-mask&gt;</td>
<td>Configure the loopback interface with an IP address not already in use</td>
</tr>
<tr>
<td>Step 5</td>
<td>ip pim sparse-mode</td>
<td>Enable PIM sparse-mode on the loopback interface</td>
</tr>
<tr>
<td>Step 6</td>
<td>ip pim rp-address &lt;loopback-ip-address&gt;</td>
<td>Synchronously configure the router to use its only loopback interface address defined in step 4 as its PIM RP</td>
</tr>
<tr>
<td>Step 7</td>
<td>interface &lt;interface-name&gt;</td>
<td>Enter the interface configuration for the interfaces or sub-interfaces that have been configured for LISP mobility. These are the internal interfaces on the server VLANs</td>
</tr>
<tr>
<td>Step 8</td>
<td>ip pim sparse-mode</td>
<td>Enable PIM sparse-mode for the interfaces that have LISP mobility enabled</td>
</tr>
<tr>
<td>Step 9</td>
<td>exit</td>
<td>Exit interface configuration mode</td>
</tr>
</tbody>
</table>

**Configuration Examples**

The following configuration examples show the full configuration ASR 1000 series router configuration for the sample multi-homed data center migration topology. This example enables LISP mobility on two subnets 10.1.1.0/24 and 10.1.2.0/24 so servers within those subnets can be migrated from the source to the destination data center.

**Source Data Center ASR 1000 Routers**

<table>
<thead>
<tr>
<th>PxTR-01</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname PxTR-01 ! ip multicast-routing ! ip cef ! track timer interface msec 500 track timer ip route msec 500 ! track 1 interface TenGigabitEthernet0/0/0 line-protocol delay up 180 !</td>
<td>Multicast routing enabled for LISP site-local map-notify messages Tracking timers reduced for faster detection of failures Tracking object 1 tracks the line-protocol of the internal interface facing the aggregation switch</td>
</tr>
<tr>
<td><strong>PxTR-01</strong></td>
<td><strong>Comments</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>track 2 ip route 3.3.3.3 255.255.255.255 reachability delay up 180 !</td>
<td>Tracking object 2 and 3 track the route for the xTR-MSMR’s RLOC addresses</td>
</tr>
<tr>
<td>track 3 ip route 4.4.4.4 255.255.255.255 reachability delay up 180 !</td>
<td>Tracking object 4 is a Boolean OR of object 2 and 3. Therefore object 4 will only go down if both object 2 and object 3 are down, i.e. if PxTR-01 loses its route to both xTR-MSMRs.</td>
</tr>
<tr>
<td>track 4 list boolean or object 2 object 3 !</td>
<td>Loopback 0 is the RLOC</td>
</tr>
<tr>
<td>interface Loopback0 ip address 1.1.1.1 255.255.255.255 ip ospf 1 area 0 !</td>
<td>Loopback 1 is the PIM RP</td>
</tr>
<tr>
<td>interface Loopback1 ip address 11.11.11.11 255.255.255.255 ip pim sparse-mode !</td>
<td>Interface Ten0/0/0 connects to the aggregation switch in the source data center</td>
</tr>
<tr>
<td>interface LISPO !</td>
<td>Ten0/0/0.200 is the sub-interface for VLAN 200 server subnet 10.1.1.0/24. LISP Mobility is enabled for this subnet.</td>
</tr>
<tr>
<td>interface TenGigabitEthernet0/0/0 no ip address !</td>
<td>For all sub-interfaces with LISP Mobility enabled PxTR-01 is given a higher HSRP priority than PxTR-2. So PxTR-01 will be HSRP active during normal conditions.</td>
</tr>
<tr>
<td>interface TenGigabitEthernet0/0/0.200 encapsulation dot1Q 200 ip address 10.1.1.252 255.255.255.0 ip pim sparse-mode standby delay minimum 180 reload 300 standby 100 ip 10.1.1.254 standby 100 timers 1 3 standby 100 priority 105 standby 100 preempt standby 100 track 4 decrement 10 no lisp mobility liveness test lisp mobility LISP-SUBNET-A !</td>
<td>HSRP on all LISP enabled sub-interfaces on PxTR-01 tracks object 4. Therefore if PxTR-01 loses its routes to both xTR-MSMRs, then PxTR-01 will become HSRP active. And PxTR-02 will become HSRP active.</td>
</tr>
<tr>
<td>interface TenGigabitEthernet0/0/0.201 encapsulation dot1Q 201 ip address 10.1.2.252 255.255.255.0 ip pim sparse-mode standby delay minimum 180 reload 300 standby 100 ip 10.1.2.254 standby 100 timers 1 3 standby 100 priority 105 standby 100 preempt standby 100 track 4 decrement 10 no lisp mobility liveness test lisp mobility LISP-SUBNET-B !</td>
<td>Ten0/0/0.201 is the sub-interface for VLAN 201 server subnet 10.1.2.0/24. LISP Mobility is enabled for this subnet.</td>
</tr>
<tr>
<td>interface TenGigabitEthernet0/0/0.500 encapsulation dot1Q 500 ip address 172.16.1.4 255.255.255.248 !</td>
<td>Ten0/0/0.500 is the sub-interface for used for default-gateway routing to the aggregation layer switches in the source data center. LISP is not enabled on this sub-interface.</td>
</tr>
<tr>
<td>interface TenGigabitEthernet0/1/0 ip address 192.168.100.1 255.255.255.252 ip ospf network point-to-point ip ospf 1 area 0 bfd interval 500 min_rx 500 multiplier 4 !</td>
<td>Ten0/1/0 is the link to PxTR-02.</td>
</tr>
<tr>
<td>interface TenGigabitEthernet1/0/0 ip address 192.168.100.5 255.255.255.252 ip ospf network point-to-point ip ospf 1 area 0</td>
<td>OSPF and BFD are enabled on the links between the LISP routers.</td>
</tr>
</tbody>
</table>

Tracking object 2 and 3 track the route for the xTR-MSMR’s RLOC addresses.
In the LISP configuration a locator-set is used to specify the RLOCs for the source data center, i.e. the RLOCs of PxTR-01 and PxTR-02. A lower priority is used for PxTR-01 so incoming LISP traffic will be directed to PxTR-01 during normal circumstances.

LISP instance-id 0 is used since all LISP enabled subnets are in the global routing table.

The two server subnets for LISP mobility are defined and mapped to the locator-set defined above.

A unique multicast group is used for each LISP mobility subnet for the site-local LISP map-notify messages.

The PxTRs are enabled as Proxy Ingress and Egress Tunnel Routers.

The map-servers and map-resolvers are defined as the LISP routers in the destination data center xTR-MSMR-01 and xTR-MSMR-02.

OSPF is used to advertise the RLOC addresses (Loopback 0) to the other LISP routers.

Each LISP router is statically configured with itself (Loopback 1) as the PIM RP. This is required for the site-local LISP map-notify messages.

Static default route is defined with the aggregation switches in the source data center as the next hop out subinterface Ten0/0/0.500.

An EEM script is used to shut down the RLOC interface Loopback 0 on PxTR-01 if the interface Ten0/0/0 facing the aggregation switch goes down (Tracked object 1 defined above). This is required so that the xTR-MSMRs will see the RLOC of PxTR-01 go down and so they won’t forward LISP traffic to it during this failure scenario. This will force the incoming LISP traffic over to PxTR-02.

Another EEM script is used to bring the RLOC interface Loopback 0 on PxTR-01 back up after the interface.
Ten0/0/0 facing the aggregation switch comes back up

Multicast routing enabled for LISP site-local map-notify messages
Loopback 0 is the RLOC
Loopback 1 is the PIM RP
Interface Ten0/0/0 connects to the aggregation switch in the source data center
Ten0/0/0.200 is the sub-interface for VLAN 200 server subnet 10.1.1.0/24. LISP Mobility is enabled for this subnet.
For all sub-interfaces with LISP Mobility enabled PxTR-01 is given a higher HSRP priority than PxTR-2. So PxTR-01 will be HSRP active during normal conditions.
Ten0/0/0.201 is the sub-interface for VLAN 201 server subnet 10.1.2.0/24. LISP Mobility is enabled for this subnet.
Ten0/0/0.500 is the sub-interface for used for default-gateway routing to the aggregation layer switches in the source data center. LISP is not enabled on this sub-interface.
Ten0/1/0 is the link to PxTR-01.
OSPF and BFD are enabled on the links between the LISP routers.
Ten1/0/0 is the link to xTR-MSMR-
Detection of EIDs with EEM-script

Since the PxTR routers are not the default gateways in the source data center they depend on receiving broadcasts such as ARP requests from servers to detect them and add them to their local LISP database as dynamic-EIDs. To make sure the PxTRs learn about servers that may not be sending broadcast ARP requests within the LISP enabled subnets, the following EEM scripts can be used to generate a unicast ping to each IP address in the subnets. Before each ping is sent the PxTR will send an ARP request to resolve the MAC address that corresponds to the IP address. Once the server
replies to the ARP the PxTR will detect it an add it to its LISP database as a dynamic-EID. Since only the ARP reply is needed it does not matter if the server blocks the ICMP ping.

Note that these scripts are only required on the primary PxTR in the source data center. Once the primary PxTR learns about the dynamic-EIDs it will update the secondary PxTR using the LISP multicast map-notify message.

The following scripts can be run manually using the CLI:

<table>
<thead>
<tr>
<th>EEM Applet to Ping All IP Addresses in multiple /24 Subnets</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>event manager applet SUBNET -PING-SLASH24</td>
<td></td>
</tr>
<tr>
<td>event cli pattern sweep24 enter maxrun 3600 ratelimit 60</td>
<td></td>
</tr>
<tr>
<td>action 001 cli command &quot;enable&quot;</td>
<td></td>
</tr>
<tr>
<td>action 002 foreach _NETWORK &quot;10.1.1 10.1.2 10.1.3&quot;</td>
<td></td>
</tr>
<tr>
<td>action 003 set HOST 1</td>
<td></td>
</tr>
<tr>
<td>action 004 while $HOST lt 255</td>
<td></td>
</tr>
<tr>
<td>action 005 cli command &quot;ping $NETWORK.$HOST repeat 1 timeout 0&quot;</td>
<td></td>
</tr>
<tr>
<td>action 006 syslog priority debugging msg &quot;$_cli_result&quot;</td>
<td></td>
</tr>
<tr>
<td>action 007 increment HOST</td>
<td></td>
</tr>
<tr>
<td>action 008 end</td>
<td></td>
</tr>
<tr>
<td>action 009 end</td>
<td></td>
</tr>
<tr>
<td>action 010 syslog msg &quot;SUBNET PING COMPLETE&quot;</td>
<td></td>
</tr>
</tbody>
</table>

This EEM applet can be run by typing the command **sweep24** in exec mode. It will ping all IP addresses in three /24 subnets: 10.1.1.0/24, 10.1.2.0/24 and 10.1.3.0/24. If logging level is set to level 7 (debugging) then the results of each ping will be displayed.

<table>
<thead>
<tr>
<th>EEM Applet to Ping All IP Addresses in multiple /16 Subnets</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>event manager applet SUBNET -PING-SLASH16</td>
<td></td>
</tr>
<tr>
<td>event cli pattern sweep16 enter maxrun 172800 ratelimit 60</td>
<td></td>
</tr>
<tr>
<td>action 001 cli command &quot;enable&quot;</td>
<td></td>
</tr>
<tr>
<td>action 002 foreach _NETWORK &quot;10.2 172.16 192.168&quot;</td>
<td></td>
</tr>
<tr>
<td>action 003 set 3OCT 0</td>
<td></td>
</tr>
<tr>
<td>action 004 while $3OCT lt 255</td>
<td></td>
</tr>
<tr>
<td>action 005 set 4OCT 1</td>
<td></td>
</tr>
<tr>
<td>action 006 while $4OCT lt 255</td>
<td></td>
</tr>
<tr>
<td>action 007 cli command &quot;ping $_NETWORK.$3OCT.$4OCT repeat 1 timeout 0&quot;</td>
<td></td>
</tr>
<tr>
<td>action 008 syslog priority debugging msg &quot;$_cli_result&quot;</td>
<td></td>
</tr>
<tr>
<td>action 009 increment 4OCT</td>
<td></td>
</tr>
<tr>
<td>action 010 end</td>
<td></td>
</tr>
<tr>
<td>action 011 increment 3OCT</td>
<td></td>
</tr>
<tr>
<td>action 012 end</td>
<td></td>
</tr>
<tr>
<td>action 013 end</td>
<td></td>
</tr>
<tr>
<td>action 014 syslog msg &quot;SUBNET PING COMPLETE&quot;</td>
<td></td>
</tr>
</tbody>
</table>

This EEM applet can be run by typing the command **sweep16** in exec mode. It will ping all IP addresses in three /16 subnets: 10.2.0.0/16, 172.16.0.0/16 and 192.168.0.0/16. If logging level is set to level 7 (debugging) then the results of each ping will be displayed.

It is also possible to automatically run the EEM scripts whenever the physical interface on the PxTR facing the data center aggregation switches comes up. An automatic script is useful in a single homed deployment where there is only a single xTR in the data center. With a single xTR using an automatic script to detect dynamic-EIDs can speed up convergence if the xTR is reloaded or if it looses its connection to the aggregation switches. Without an automatic script the xTR would have
to wait until it receives a packet from the servers before it can detect them and add them to its local LISP database as dynamic-EIDs.

For a multihomed environment with two xTRs in each datacenter if the either of the xTRs are reloaded or lose their connection to the aggregation switches, upon convergence they will learn about the dynamic-EIDs via the LISP multicast map-notify message from the other xTR. So a script to detect dynamic-EIDs in a multihomed environment is really only needed when the xTRs are initially added to the network.

Below is an example of an EEM script to detect dynamic-EIDs for three /24 subnets automatically when the interface facing the aggregation switches comes up:

<table>
<thead>
<tr>
<th>EEM Applet to Ping All IP Addresses in multiple /24 Subnets</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>track 1 interface TenGigabitEthernet0/0/0 line-protocol</td>
<td>This EEM applet will run automatically 60 seconds after interface Ten0/0/0 facing the aggregation switch comes up. It will ping all IP addresses in three /24 subnets: 10.1.1.0/24, 10.1.2.0/24 and 10.1.3.0/24. If logging level is set to level 7 (debugging) then the results of each ping will be displayed.</td>
</tr>
<tr>
<td>delay up 60</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>event manager applet AUTOMATIC-SUBNET -PING-SLASH24</td>
<td></td>
</tr>
<tr>
<td>event track 1 state up maxrun 3600</td>
<td></td>
</tr>
<tr>
<td>action 001 cli command &quot;enable&quot;</td>
<td></td>
</tr>
<tr>
<td>action 002 foreach _NETWORK &quot;10.1.1 10.1.2 10.1.3&quot;</td>
<td></td>
</tr>
<tr>
<td>action 003 set HOST 1</td>
<td></td>
</tr>
<tr>
<td>action 004 while $HOST lt 25</td>
<td></td>
</tr>
<tr>
<td>action 005 cli command &quot;ping $_NETWORK.$HOST repeat 1 timeout 0&quot;</td>
<td></td>
</tr>
<tr>
<td>action 006 syslog priority debugging msg &quot;$_cli_result&quot;</td>
<td></td>
</tr>
<tr>
<td>action 007 increment HOST</td>
<td></td>
</tr>
<tr>
<td>action 008 end</td>
<td></td>
</tr>
<tr>
<td>action 009 end</td>
<td></td>
</tr>
<tr>
<td>action 010 syslog msg &quot;SUBNET PING COMPLETE&quot;</td>
<td></td>
</tr>
</tbody>
</table>

**Destination Data Center ASR 1000 Routers**

<table>
<thead>
<tr>
<th>xTR-MSMR-01</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname xTR-MSMR-01</td>
<td>Multicast routing enabled for LISP site-local map-notify messages</td>
</tr>
<tr>
<td>!</td>
<td>Tracking timers reduced for faster detection of failures</td>
</tr>
<tr>
<td>ip multicast-routing</td>
<td>Tracking object 1 tracks the line-protocol of the internal interface facing the aggregation switch</td>
</tr>
<tr>
<td>!</td>
<td>Tracking object 2 and 3 track the route for the PxTR’s RLOC addresses</td>
</tr>
<tr>
<td>ip cef</td>
<td>Tracking object 4 is a Boolean OR of object 2 and 3. Therefore object 4 will only go down if both object 2 and object</td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>track timer interface msec 500</td>
<td></td>
</tr>
<tr>
<td>track timer ip route msec 500</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>track 1 interface TenGigabitEthernet0/0/0 line-protocol</td>
<td></td>
</tr>
<tr>
<td>delay up 180</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>track 2 ip route 1.1.1.1 255.255.255.255 reachability</td>
<td></td>
</tr>
<tr>
<td>delay up 180</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>track 3 ip route 2.2.2.2 255.255.255.255 reachability</td>
<td></td>
</tr>
<tr>
<td>delay up 180</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>xTR-MSMR-01</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| track 4 list boolean or object 2 object 3 ! interface Loopback0 ip address 3.3.3.3 255.255.255.255 ip ospf 1 area 0 ! interface Loopback1 ip address 33.33.33.33 255.255.255.255 ip pim sparse-mode ! interface LISP0 ! interface TenGigabitEthernet0/0/0 no ip address ! interface TenGigabitEthernet0/0/0.4000 encapsulation dot1Q 4000 ip ospf 1 area 0 ip pim sparse-mode standby delay minimum 180 reload 300 standby 1 ip 10.1.1.1 standby 1 timers 1 3 standby 1 priority 105 standby 1 preempt standby 1 track 4 decrement 10 no lisp mobility liveness test lisp mobility LISP-SUBNET-A ! interface TenGigabitEthernet0/0/0.4001 ip address 10.1.2.2 255.255.255.0 ip pim sparse-mode standby delay minimum 180 reload 300 standby 1 ip 10.1.2.1 standby 1 timers 1 3 standby 1 priority 105 standby 1 preempt standby 1 track 4 decrement 10 no lisp mobility liveness test lisp mobility LISP-SUBNET-B ! interface TenGigabitEthernet0/1/0 ip address 192.168.100.13 255.255.255.252 ip ospf network point-to-point ip ospf 1 area 0 bfd interval 500 min_rx 500 multiplier 4 ! interface TenGigabitEthernet1/0/0 ip address 192.168.100.6 255.255.255.252 ip ospf network point-to-point ip ospf 1 area 0 bfd interval 500 min_rx 500 multiplier 4 ! router lisp locator-set DC2 3.3.3.3 priority 1 weight 100 4.4.4.4 priority 2 weight 100 exit ! eid-table default instance-id 0 dynamic-eid LISP-SUBNET-A | 3 are down, i.e. if xTR-MSMR-01 looses its routes to both PxTRs. Loopback 0 is the RLOC Loopback 1 is the PIM RP Interface Ten0/0/0/0 connects to the spine switch in the destination data center Ten0/0/0.4000 is the sub-interface for VLAN 4000 server subnet 10.1.1.0/24. LISP Mobility is enabled for this subnet. For all sub-interfaces with LISP Mobility enabled xTR-MSMR-01 is given a higher HSRP priority than xTR-MSMR-02. So xTR-MSMR-01 will be HSRP active during normal conditions. HSRP on all LISP enabled sub-interfaces on xTR-MSMR-01 tracks object 4. Therefore if xTR-MSMR-01 loses its routes to both PxTRs, then xTR-MSMR-01 will become HSRP standby. And xTR-MSMR-02 will become HSRP active. Ten0/0/0.4001 is the sub-interface for VLAN 4001 server subnet 10.1.2.0/24. LISP Mobility is enabled for this subnet. Ten0/1/0 is the link to xTR-MSMR-02. OSPF and BFD are enabled on the links between the LISP routers. Ten1/0/0 is the link to PxTR-01. In the LISP configuration a locator-set is used to specify the RLOCs for the destination data center, i.e. the RLOCs of xTR-MSMR-01 and xTR-MSMR-02. A lower priority is used for xTR-MSMR-01 so incoming LISP traffic will be directed to xTR-MSMR-1 during normal circumstances. LISP instance-id 0 is used since all LISP enabled subnets are in the global routing table. The two server subnets for LISP mobility are defined and mapped to the...
<table>
<thead>
<tr>
<th><strong>xTR-MSMR-01</strong></th>
<th><strong>Comments</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>database-mapping 10.1.1.0/24 locator-set DC2</code></td>
<td>locator-set defined above.</td>
</tr>
<tr>
<td><code>map-notify-group 239.0.0.1</code></td>
<td>A unique multicast group is used for each LISP mobility subnet for the site-local LISP map-notify messages.</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>The LISP site configuration defines the authentication-key and the prefixes that the map-server will accept map-registers for.</td>
</tr>
<tr>
<td><code>!</code></td>
<td>Both xTR-MSMRs are configured as map-servers and map-resolvers and to use themselves as the map-server and map-resolvers</td>
</tr>
<tr>
<td><code>dynamic-eid LISP-SUBNET-B</code></td>
<td>OSPF is used to advertise the RLOC addresses (Loopback 0) to the other LISP routers.</td>
</tr>
<tr>
<td><code>database-mapping 10.1.2.0/24 locator-set DC1</code></td>
<td>Each LISP router is statically configured with itself (Loopback 1) as the PIM RP. This is required for the site-local LISP map-notify messages</td>
</tr>
<tr>
<td><code>map-notify-group 239.0.0.2</code></td>
<td>An EEM script is used to shut down the RLOC interface Loopback 0 on xTR-MSMR-01 if the interface Ten0/0/0 facing the spine switch goes down (Tracked object 1 defined above). This is required so that the PxTRs will see the RLOC of xTR-MSMR-01 go down and so they won't forward LISP traffic to it during this failure scenario. This will force the incoming LISP traffic over to xTR-MSMR-02</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Another EEM script is used to bring the RLOC interface Loopback 0 on xTR-MSMR-01 back up after the interface Ten0/0/0 facing the spine switch comes back up</td>
</tr>
<tr>
<td><code>!</code></td>
<td>!</td>
</tr>
<tr>
<td><code>site DC-MIGRATION</code></td>
<td>!</td>
</tr>
<tr>
<td><code>authentication-key CISCO123</code></td>
<td>!</td>
</tr>
<tr>
<td><code>eid-prefix 10.1.0.0/16 accept-more-specifics</code></td>
<td>!</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 locator reachability exclude-default</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 map-server</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 map-resolver</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 use-petr 1.1.1.1 priority 1 weight 100</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 use-petr 2.2.2.2 priority 2 weight 100</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 map-cache-limit 5000</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 itr map-resolver 3.3.3.3</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 itr map-resolver 4.4.4.4</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 itr</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 etr map-server 3.3.3.3 key CISCO123</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 etr map-server 4.4.4.4 key CISCO123</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ipv4 etr</code></td>
<td>!</td>
</tr>
<tr>
<td><code>exit</code></td>
<td>!</td>
</tr>
<tr>
<td><code>router ospf 1</code></td>
<td>!</td>
</tr>
<tr>
<td><code>router-id 3.3.3.3</code></td>
<td>!</td>
</tr>
<tr>
<td><code>auto-cost reference-bandwidth 100000</code></td>
<td>!</td>
</tr>
<tr>
<td><code>timers throttle spf 10 100 5000</code></td>
<td>!</td>
</tr>
<tr>
<td><code>timers throttle lsa 10 100 5000</code></td>
<td>!</td>
</tr>
<tr>
<td><code>timers lsa arrival 90</code></td>
<td>!</td>
</tr>
<tr>
<td><code>bfd all-interfaces</code></td>
<td>!</td>
</tr>
<tr>
<td><code>ip pim rp-address 33.33.33.33</code></td>
<td>!</td>
</tr>
<tr>
<td><code>!</code></td>
<td>!</td>
</tr>
<tr>
<td><code>event manager applet INTERNAL-INTERFACE-IS-DOWN</code></td>
<td>!</td>
</tr>
<tr>
<td><code>event track 1 state down</code></td>
<td>!</td>
</tr>
<tr>
<td><code>action 1.0 cli command &quot;enable&quot;</code></td>
<td>!</td>
</tr>
<tr>
<td><code>action 1.1 cli command &quot;conf t&quot;</code></td>
<td>!</td>
</tr>
<tr>
<td><code>action 2.0 cli command &quot;interface loop0&quot;</code></td>
<td>!</td>
</tr>
<tr>
<td><code>action 3.0 cli command &quot;shut&quot;</code></td>
<td>!</td>
</tr>
<tr>
<td><code>action 9.0 syslog msg &quot;INTERNAL INTERFACE DOWN, RLOC 3.3.3.3 HAS BEEN SHUTDOWN&quot;</code></td>
<td>!</td>
</tr>
<tr>
<td><code>event manager applet INTERNAL-INTERFACE-IS-UP</code></td>
<td>!</td>
</tr>
<tr>
<td><code>event track 1 state up</code></td>
<td>!</td>
</tr>
<tr>
<td><code>action 1.0 cli command &quot;enable&quot;</code></td>
<td>!</td>
</tr>
<tr>
<td><code>action 1.1 cli command &quot;conf t&quot;</code></td>
<td>!</td>
</tr>
<tr>
<td><code>action 2.0 cli command &quot;interface loop0&quot;</code></td>
<td>!</td>
</tr>
<tr>
<td><code>action 3.0 cli command &quot;no shut&quot;</code></td>
<td>!</td>
</tr>
<tr>
<td><code>action 9.0 syslog msg &quot;INTERNAL INTERFACE UP, RLOC 3.3.3.3 HAS BEEN RESTORED&quot;</code></td>
<td>!</td>
</tr>
<tr>
<td><code>end</code></td>
<td>!</td>
</tr>
<tr>
<td>xTR-MSMR-02</td>
<td>Comments</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>
| hostname xTR-MSMR-02  
  !  
  ip multicast-routing  
  !  
  ip cef  
  !  
  interface Loopback0  
  ip address 4.4.4.4 255.255.255.255  
  ip ospf 1 area 0  
  !  
  interface Loopback1  
  ip address 44.44.44.4 255.255.255.255  
  ip pim sparse-mode  
  !  
  interface LISP0  
  !  
  interface TenGigabitEthernet0/0/0  
  no ip address  
  !  
  interface TenGigabitEthernet0/0/0.4000  
  encapsulation dot1Q 4000  
  ip address 10.1.1.1 255.255.255.0  
  ip pim sparse-mode  
  standby 1 ip 10.1.1.1  
  standby 1 timers 1 3  
  standby 1 preempt  
  no lisp mobility liveness test  
  lisp mobility LISP-SUBNET-A  
  !  
  interface TenGigabitEthernet0/0/0.4001  
  encapsulation dot1Q 4001  
  ip address 10.1.2.1 255.255.255.0  
  ip pim sparse-mode  
  standby 1 ip 10.1.2.1  
  standby 1 timers 1 3  
  standby 1 preempt  
  no lisp mobility liveness test  
  lisp mobility LISP-SUBNET-B  
  !  
  interface TenGigabitEthernet0/1/0  
  ip address 192.168.100.4 255.255.255.252  
  ip ospf network point-to-point  
  ip ospf 1 area 0  
  bfd interval 500 min_rx 500 multiplier 4  
  !  
  interface TenGigabitEthernet1/0/0  
  ip address 192.168.100.10 255.255.255.252  
  ip ospf network point-to-point  
  ip ospf 1 area 0  
  bfd interval 500 min_rx 500 multiplier 4  
  !  
  router lisp  
  locator-set DC2  
  3.3.3.3 priority 1 weight 100  
  4.4.4.4 priority 2 weight 100  
  exit  
  !  
  eid-table default instance-id 0  
  dynamic-eid LISP-SUBNET-A  
  database-mapping 10.1.1.0/24 locator-set DC2  
  map-notify-group 239.0.0.1  
  exit  
  !  | Multicast routing enabled for LISP site-local map-notify messages  
  Loopback 0 is the RLOC  
  Loopback 1 is the PIM RP  
  Interface Ten0/0/0 connects to the spine switch in the destination data center  
  Ten0/0/0.4000 is the sub-interface for VLAN 4000 server subnet 10.1.1.0/24. LISP Mobility is enabled for this subnet.  
  For all sub-interfaces with LISP Mobility enabled xTR-MSMR-01 is given a higher HSRP priority than xTR-MSMR-02. So xTR-MSMR-01 will be HSRP active during normal conditions.  
  Ten0/0/0.4001 is the sub-interface for VLAN 4001 server subnet 10.1.2.0/24. LISP Mobility is enabled for this subnet.  
  Ten0/1/0 is the link to xTR-MSMR-01.  
  OSPF and BFD are enabled on the links between the LISP routers.  
  Ten1/0/0 is the link to PxTR-02.  
  In the LISP configuration a locator-set is used to specify the RLOCs for the destination data center, i.e. the RLOCs of xTR-MSMR-01 and xTR-MSMR-02. A lower priority is used for xTR-MSMR-01 so incoming LISP traffic will be directed to xTR-MSMR-1 during normal circumstances.  
  LISP instance-id 0 is used since all LISP enabled subnets are in the global routing table.  
  The two server subnets for LISP mobility are defined and mapped to the locator-set defined above. |
### Verification and Traffic Flows for the Different Stages of the Migration

Using two servers from each of the subnets that have been enabled for LISP mobility, this section will outline the output from the verification commands and describe the traffic flows between the servers.

**Initial State – LISP Routers have been implemented but no servers have been migrated**

When the LISP routers are initially connected to both the source and destination data center switches, the PxTRs in the source data center will update their LISP database when they detect packets from servers with source addresses within the LISP dynamic-EID subnets. Since the PxTRs are not the default gateway for the servers, they depend on receiving broadcast packets such as ARPs from the servers. The ping sweep EEM script can be used to make sure the PxTRs detect every server within the dynamic-EID subnets. Each dynamic-EID that the PxTRs detect will be registered with the map-servers in the destination data center.

---

**Figure 14: Start-of-Migration – All Servers Still in Source Data Center**
To verify the PxTRs have detected the dynamic EIDs (servers still in source data center):

**On PxTR-01:**

```
PxTR-01#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify

Dyn-EID Name | Dynamic-EID     | Interface | Uptime  | Last    | Pending  | Packet | Ping Count
--------------|-----------------|-----------|---------|---------|----------|--------|-------------
LISP-SUBNET-A | 10.1.1.5        | Te0/0/0.200 | 00:00:10| 00:00:10| 0        |
LISP-SUBNET-A | 10.1.1.6        | Te0/0/0.200 | 00:01:23| 00:01:23| 0        |
LISP-SUBNET-B | 10.1.2.5        | Te0/0/0.201 | 00:00:04| 00:00:04| 0        |
LISP-SUBNET-B | 10.1.2.6        | Te0/0/0.201 | 00:02:11| 00:02:11| 0        |
```

```
PxTR-01#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x3, 4 entries

10.1.1.5/32, dynamic-eid LISP-SUBNET-A, locator-set DC1
Locator Priority Source State
1.1.1.1 1/100 cfg-addr site-self, reachable
2.2.2.2 2/100 cfg-addr site-other, report-reachable

10.1.1.6/32, dynamic-eid LISP-SUBNET-A, locator-set DC1
Locator Priority Source State
1.1.1.1 1/100 cfg-addr site-self, reachable
2.2.2.2 2/100 cfg-addr site-other, report-reachable
```

10.1.2.5/32, dynamic-eid LISP-SUBNET-B, locator-set DC1
Locator Priority Source State
1.1.1.1 1/100 cfg-addr site-self, reachable
2.2.2.2 2/100 cfg-addr site-other, report-reachable

10.1.2.6/32, dynamic-eid LISP-SUBNET-B, locator-set DC1
Locator Priority Source State
1.1.1.1 1/100 cfg-addr site-self, reachable
2.2.2.2 2/100 cfg-addr site-other, report-reachable

10.1.2.7/32, dynamic-eid LISP-SUBNET-B, locator-set DC1
Locator Priority Source State
1.1.1.1 1/100 cfg-addr site-self, reachable
2.2.2.2 2/100 cfg-addr site-other, report-reachable
Locator  Pri/Wgt  Source     State
1.1.1.1   1/100  cfg-addr   site-self, reachable
2.2.2.2   2/100  cfg-addr   site-other, report-reachable
10.1.2.6/32, dynamic-eid LISP-SUBNET-B, locator-set DC1

On PxTR-02:

Note that the asterix beside the Dynamic-EID entries indicated that it has been learned via the site-local multicast map-notify message from PxTR-01.

On xTR-MSMR-01:

xTR-MSMR-02#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify

Dyn-EID Name   Dynamic-EID      Interface  Uptime    Last Pending Packet Ping Count
LISP-SUBNET-A *10.1.1.5   Te0/0/0.200  00:08:59  00:00:36  0
LISP-SUBNET-A *10.1.1.6   Te0/0/0.200  00:11:15  00:00:36  0
LISP-SUBNET-B *10.1.2.5   Te0/0/0.201  00:08:53  00:08:53  0
LISP-SUBNET-B *10.1.2.6   Te0/0/0.201  00:11:00  00:11:00  0

The output below from the xTR-MSMR routers show that no servers have been detected on the Destination Data Center yet.
On xTR-MSMR-02:

xTR-MSMR-02#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify

<table>
<thead>
<tr>
<th>Dyn-EID Name</th>
<th>Dynamic-EID</th>
<th>Interface</th>
<th>Uptime</th>
<th>Last Pending</th>
<th>Packet</th>
<th>Ping Count</th>
</tr>
</thead>
</table>

To verify the Dynamic-EIDs Detected in the Source Data Center have been Registered with the Map-Servers:

Note the output from the commands below should be similar on both Map-Servers xTR-MSMR-01 and xTR-MSMR-02

On xTR-MSMR-01:

xTR-MSMR-01#show lisp site
LISP Site Registration Information

<table>
<thead>
<tr>
<th>Site Name</th>
<th>Last Register</th>
<th>Up</th>
<th>Who Last Registered</th>
<th>Inst ID</th>
<th>EID Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC-MIGRATION</td>
<td>never</td>
<td>no</td>
<td>--</td>
<td></td>
<td>10.1.0.0/16</td>
</tr>
<tr>
<td></td>
<td>00:00:50</td>
<td>yes</td>
<td>192.168.100.5</td>
<td>10.1.1.5/32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00:00:38</td>
<td>yes</td>
<td>192.168.100.5</td>
<td>10.1.1.6/32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00:00:50</td>
<td>yes</td>
<td>192.168.100.5</td>
<td>10.1.2.5/32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00:00:50</td>
<td>yes</td>
<td>192.168.100.5</td>
<td>10.1.2.6/32</td>
<td></td>
</tr>
</tbody>
</table>

To look more in more detail at the map-registration information for a specific EID, specify the EID IP address/prefix after the show lisp site command. The command below gives the information on the EID-to-RLOC mapping for the EID 10.1.1.6 as well as the priority and weight for each RLOC. Note that the RLOC addresses are the RLOC addresses of PxTR-01 and PxTR-02, indicating the server is still in the source data center.

xTR-MSMR-01#sh lisp site 10.1.1.5/32
LISP Site Registration Information

Site name: DC-MIGRATION
Allowed configured locators: any
Requested EID-prefix:
EID-prefix: 10.1.1.5/32
First registered: 00:43:13
Routing table tag: 0
Origin: Dynamic, more specific of 10.1.0.0/16
Merge active: No
Proxy reply: No
TTL: 1d00h
State: complete
Registration errors:
Authentication failures: 0
Allowed locators mismatch: 0
ETR 192.168.100.9, last registered 00:00:40, no proxy-reply, map-notify
TTL 1d00h, no merge, hash-function sha1, nonce 0x1B67E72C-0x26F64FF3
state complete, no security-capability
Mid-Migration state – Some Servers have been migrated to the Destination Data Center

Figure 15: Mid-Migration – Some Servers have been migrated to Destination Data Center

To verify the xTR-MSMRs have detected the dynamic EIDs (Servers that have migrated):

On xTR-MSMR-01:

\[xTR-MSMR-01#\] sh ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x3, 2 entries

10.1.1.6/32, dynamic-eid LISP-SUBNET-A, locator-set DC2
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
4.4.4.4 2/100 cfg-addr site-other, report-reachable

10.1.2.6/32, dynamic-eid LISP-SUBNET-B, locator-set DC2
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
4.4.4.4 2/100 cfg-addr site-other, report-reachable

xTR-MSMR-01#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify

<table>
<thead>
<tr>
<th>Dyn-EID Name</th>
<th>Dynamic-EID</th>
<th>Interface</th>
<th>Uptime</th>
<th>Last Pending</th>
<th>Packet</th>
<th>Ping Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISP-SUBNET-A</td>
<td>10.1.1.6</td>
<td>Te0/0/0.4000</td>
<td>00:00:24</td>
<td>00:00:24</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LISP-SUBNET-B</td>
<td>10.1.2.6</td>
<td>Te0/0/0.4001</td>
<td>00:00:24</td>
<td>00:00:24</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

On xTR-MSMR-02:

xTR-MSMR-02#sh ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x3, 2 entries

10.1.1/32, dynamic-eid LISP-SUBNET-A, locator-set DC2
   Locator Pri/Wgt Source State
   3.3.3.3   1/100 cfg-addr site-other, report-reachable
   4.4.4.4   2/100 cfg-addr site-self, reachable
10.1.2/32, dynamic-eid LISP-SUBNET-B, locator-set DC2
   Locator Pri/Wgt Source State
   3.3.3.3   1/100 cfg-addr site-other, report-reachable
   4.4.4.4   2/100 cfg-addr site-self, reachable

xTR-MSMR-02#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify

<table>
<thead>
<tr>
<th>Dyn-EID Name</th>
<th>Dynamic-EID</th>
<th>Interface</th>
<th>Uptime</th>
<th>Last Pending</th>
<th>Packet</th>
<th>Ping Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISP-SUBNET-A *10.1.1.6</td>
<td>Te0/0/0.4000</td>
<td>00:01:34</td>
<td>00:00:35</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LISP-SUBNET-B *10.1.2.6</td>
<td>Te0/0/0.4001</td>
<td>00:01:34</td>
<td>00:01:34</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The output below shows that the migrated servers are no longer in the local LISP database on the PxTR routers in the source data center.

On PxTR-01:

PxTR-01#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify

<table>
<thead>
<tr>
<th>Dyn-EID Name</th>
<th>Dynamic-EID</th>
<th>Interface</th>
<th>Uptime</th>
<th>Last Pending</th>
<th>Packet</th>
<th>Ping Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISP-SUBNET-A</td>
<td>10.1.1.5</td>
<td>Te0/0/0.200</td>
<td>00:51:12</td>
<td>00:51:12</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>LISP-SUBNET-B</td>
<td>10.1.2.5</td>
<td>Te0/0/0.201</td>
<td>00:43:17</td>
<td>00:31:21</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

On PxTR-02:

PxTR-02#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify

<table>
<thead>
<tr>
<th>Dyn-EID Name</th>
<th>Dynamic-EID</th>
<th>Interface</th>
<th>Uptime</th>
<th>Last</th>
<th>Pending</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISP-SUBNET-A</td>
<td>10.1.1.5</td>
<td>Te0/0/0.200</td>
<td>00:51:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LISP-SUBNET-B</td>
<td>10.1.2.5</td>
<td>Te0/0/0.201</td>
<td>00:43:17</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To verify the Dynamic-EIDs EID-To-RLOC Mapping Database has been updated on the Map-Servers for the Servers that have migrated:

**On xTR-MSMR-01:**

```
xTR-MSMR-01#show lisp site
LISP Site Registration Information

<table>
<thead>
<tr>
<th>Site Name</th>
<th>Last Register</th>
<th>Up</th>
<th>Who Last Registered</th>
<th>Inst</th>
<th>EID Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC-MIGRATION</td>
<td>never</td>
<td>no</td>
<td>--</td>
<td></td>
<td>10.1.0.0/16</td>
</tr>
<tr>
<td></td>
<td>00:00:45</td>
<td>yes</td>
<td>192.168.100.9</td>
<td>10.1.1.32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00:00:02</td>
<td>yes</td>
<td>3.3.3.3</td>
<td>10.1.1.32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00:00:45</td>
<td>yes</td>
<td>192.168.100.9</td>
<td>10.1.2.32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>00:00:02</td>
<td>yes</td>
<td>3.3.3.3</td>
<td>10.1.2.32</td>
<td></td>
</tr>
</tbody>
</table>
```

To look more in more detail at the map-registration information for a specific EID, specify the EID IP address/prefix after the show lisp site command. The command below gives the information on the EID-to-RLOC mapping for the EID 10.1.1.6 as well as the priority and weight for each RLOC. Note that the RLOC addresses are now the RLOC addresses of xTR-MSMR-01 and xTR-MSMR-02, indicating the server is now in the destination data center.

```
xTR-MSMR-01#sh lisp site 10.1.1.6/32
LISP Site Registration Information

Site name: DC-MIGRATION
Allowed configured locators: any
Requested EID-prefix:
  EID-prefix: 10.1.1.6/32
  First registered: 01:08:23
  Routing table tag: 0
  Origin: Dynamic, more specific of 10.1.0.0/16
  Merge active: No
  Proxy reply: No
  TTL: 1d00h
  State: complete
  Registration errors:
    Authentication failures: 0
    Allowed locators mismatch: 0
  ETR 3.3.3.3, last registered 00:00:42, no proxy-reply, map-notify
    TTL 1d00h, no merge, hash-function sha1, nonce 0x5830FE1F-0x760E5E1F
    state complete, no security-capability
    xTR-ID 0xBA4E54B1-0x3EA73127-0x3CAF2136-0xA3DB905F
    site-ID unspecified
  Locator  Local  State      Pri/Wgt
  3.3.3.3  yes    up           1/100
  4.4.4.4  no     up           2/100
ETR 192.168.100.14, last registered 00:00:44, no proxy-reply, map-notify
  TTL 1d00h, no merge, hash-function sha1, nonce 0xE36F0D17-0x5FEA1373
  state complete, no security-capability
  xTR-ID 0x5FCE9CA4-0x6F33E30D-0x32BB88B7-0x6C969C4BB
  site-ID unspecified
  Locator  Local  State      Pri/Wgt
```

xTR-MSMR-01
Generate Traffic between a Migrated Server and a server still in the Source Data Center

When traffic is generated to an EID that is not in the local data center the iTR will send a map-request to the map-server to determine what destination RLOC address to use in the outer header of LISP encapsulated packets to that remote EID. The map-server will forward the map-reply to the eTR that registered the EID. The eTR will send a map-reply to the iTR indicating what RLOCs to use to reach the EID as well as the priority and weight values for the RLOCs. The eTR will then store this EID-to-RLOC mapping in its map-cache. By default the entries in the map-cache will be timed out if there is no traffic destined to the remote EID for a period of 24 hours.

In the example below, traffic is generated between the server 10.1.1.5 in the source data center and 10.1.1.6 which is now in the destination data center.

Before Traffic is generated between the Servers 10.1.1.5 and 10.1.1.6:

```
PxTR-01#sh ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 2 entries
10.1.1.0/24, uptime: 01:28:08, expires: never, via dynamic-EID, send-map-request
   Negative cache entry, action: send-map-request
10.1.2.0/24, uptime: 01:28:08, expires: never, via dynamic-EID, send-map-request
   Negative cache entry, action: send-map-request
```

```
xTR-MSMR-01#sh ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 3 entries
0.0.0.0/0, uptime: 01:27:09, expires: never, via static send map-request
   Negative cache entry, action: send-map-request
10.1.1.0/24, uptime: 01:27:09, expires: never, via dynamic-EID, send-map-request
   Negative cache entry, action: send-map-request
10.1.2.0/24, uptime: 01:27:09, expires: never, via dynamic-EID, send-map-request
   Negative cache entry, action: send-map-request
```

After Traffic is generated between the Server 10.1.1.5 and 10.1.1.6:

```
PxTR-01#sh ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 3 entries
10.1.1.0/24, uptime: 01:34:39, expires: never, via dynamic-EID, send-map-request
   Negative cache entry, action: send-map-request
10.1.1.6/32, uptime: 00:00:03, expires: 23:59:56, via map-reply, complete
   Locator Uptime State Pri/Wgt
   3.3.3.3 00:00:03 up   1/100
   4.4.4.4 00:00:03 up   2/100
10.1.2.0/24, uptime: 01:34:39, expires: never, via dynamic-EID, send-map-request
   Negative cache entry, action: send-map-request
```

```
xTR-MSMR-01#sh ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 4 entries
0.0.0.0/0, uptime: 01:35:00, expires: never, via static send map-request
```
Negative cache entry, action: send-map-request
10.1.1.0/24, uptime: 01:35:00, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request
10.1.1.5/32, uptime: 00:00:27, expires: 23:59:32, via map-reply, complete
Locator Uptime State Pri/Wgt
1.1.1.1 00:00:27 up 1/100
2.2.2.2 00:00:27 up 2/100
10.1.2.0/24, uptime: 01:35:00, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request

The commands below show how to check the data plane and verify the router is LISP encapsulating packets to the remote EID.

On PxTR-01:

PxTR-01#sh ip cef 10.1.1.5
10.1.1.5/32
nexthop 10.1.1.5 TenGigabitEthernet0/0/0.200

PxTR-01#sh ip cef 10.1.1.6
10.1.1.6/32
nexthop 3.3.3.3 LISP0

PxTR-01#sh ip lisp forwarding eid remote
Prefix Fwd action Locator status bits
10.1.1.0/24 signal 0x00000000 packets/bytes 2/186
10.1.1.6/32 encap 0x00000003 packets/bytes 43569/4356900
t 10.1.2.0/24 signal 0x00000000 packets/bytes 3/272

PxTR-01#sh ip lisp forwarding eid remote 10.1.1.6
Prefix Fwd action Locator status bits
10.1.1.6/32 encap 0x00000003 packets/bytes 44902/4490200
path list 0486C48C, flags 0x49, 4 locks, per-destination
ifnums:
LISP0(12): 3.3.3.3
1 path
path 0258FC68, path list 0486C48C, share 100/100, type attached nexthop, for IPv4
nexthop 3.3.3.3 LISP0, adjacency IP midchain out of LISP0, addr 3.3.3.3 0258ECA0
1 output chain
chain[0]: IP midchain out of LISP0, addr 3.3.3.3 0258ECA0 IP adj out of TenGigabitEthernet1/0/0,
addr 192.168.100.6 027497A0

On xTR-MSMR-01:

xTR-MSMR-01#sh ip cef 10.1.1.5
10.1.1.5/32
nexthop 1.1.1.1 LISP0
The xTR-MSMRs will use the PxTRs as their Proxy Egress Tunnel Router (PeTR). This enables symmetrical routing through stateful devices such as Firewalls or Loadbalancers in the source datacenter. However, if there are no stateful devices in the source datacenter then another design option would be to route the traffic directly to the WAN from the destination datacenter.

With the use-PeTR function configured on the xTR-MSMRs when traffic is received from a migrated server to an address not in the map-server EID-to-RLOC database then the traffic will still get LISP encapsulated to the PxTRs. The xTR-MSMR will create a summary entry in its map-cache for the destination address which will not overlap with any of the other entries in the map-cache.

In the example below traffic is generated from the migrated server 10.1.1.6 to the server 10.50.50.50 on remote non-LISP site reachable via the WAN. The entry 10.32.0.0/11 is created in map-cache on xTR-MSMR-01. Traffic destined to addresses within this dynamically created summary prefix will be encapsulated to the Proxy ETR.
Below shows how to verify that the data-plane is LISP encapsulating the packets to the PxTRs for traffic to the non-LISP server.

```
xTR-MSMR-01#show ip lisp forwarding eid remote
Prefix Fwd action Locator status bits
0.0.0.0/0 signal 0x00000000
packets/bytes 1/100
10.1.1.0/24 signal 0x00000000
packets/bytes 1/100
10.1.1.5/32 encap 0x00000003
packets/bytes 1418211/141821100
10.1.2.0/24 signal 0x00000000
packets/bytes 0/0
10.32.0.0/11 fwd native 0x00000000
packets/bytes 1415332/141533200
```

```
xTR-MSMR-01#show ip lisp forwarding eid remote 10.32.0.0
Prefix Fwd action Locator status bits
10.32.0.0/11 fwd native 0x00000000
packets/bytes 1418552/141855200
path list 050B0654, flags 0x49, 5 locks, per-destination
ifnums:
  LISP0(12): 1.1.1.1
  1 path
  path 01008148, path list 050B0654, share 100/100, type attached nexthop, for IPv4
  nexthop 1.1.1.1 LISP0, adjacency IP midchain out of LISP0, addr 1.1.1.1 010090F0
  1 output chain
  chain[0]: IP midchain out of LISP0, addr 1.1.1.1 010090F0 IP adj out of TenGigabitEthernet1/0/0,
  addr 192.168.100.5 010095B0
```

**End-of-Migration State – All Servers have been migrated to the Destination Data Center**

*Figure 16: End-of-Migration – All Servers have been migrated to Destination Data Center*
To verify the xTR-MSMRs have detected the dynamic EIDs (Servers that have migrated):

**On xTR-MSMR-01:**

xTR-MSMR-01#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify

<table>
<thead>
<tr>
<th>Dyn-EID Name</th>
<th>Dynamic-EID</th>
<th>Interface</th>
<th>Uptime</th>
<th>Last</th>
<th>Pending</th>
<th>Packet</th>
<th>Ping Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>LISP-SUBNET-A 10.1.1.5</td>
<td>Te0/0/0.4000</td>
<td>00:01:27</td>
<td>00:01:27</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LISP-SUBNET-A 10.1.1.6</td>
<td>Te0/0/0.4000</td>
<td>00:03:37</td>
<td>00:03:37</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LISP-SUBNET-B 10.1.2.5</td>
<td>Te0/0/0.4001</td>
<td>00:01:17</td>
<td>00:01:17</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LISP-SUBNET-B 10.1.2.6</td>
<td>Te0/0/0.4001</td>
<td>00:03:37</td>
<td>00:03:37</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

xTR-MSMR-01#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x3, 4 entries

10.1.1.5/32, dynamic-eid LISP-SUBNET-A, locator-set DC2
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
4.4.4.4 2/100 cfg-addr site-other, report-reachable

10.1.1.6/32, dynamic-eid LISP-SUBNET-A, locator-set DC2
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
4.4.4.4 2/100 cfg-addr site-other, report-reachable

10.1.2.5/32, dynamic-eid LISP-SUBNET-B, locator-set DC2
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
4.4.4.4 2/100 cfg-addr site-other, report-reachable
10.1.2/32, dynamic-eid LISP-SUBNET-B, locator-set DC2
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-self, reachable
4.4.4.4 2/100 cfg-addr site-other, report-reachable

On xTR-MSMR-02:

xTR-MSMR-02#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify
Dyn-EID Name Dynamic-EID Interface Uptime Last Pending
Packet Ping Count
LISP-SUBNET-A *10.1.1.5 Te0/0/0.4000 00:01:07 00:01:07 0
LISP-SUBNET-A *10.1.1.6 Te0/0/0.4000 00:02:32 00:02:32 0
LISP-SUBNET-B * 10.1.2.5 Te0/0/0.4001 00:00:56 00:00:56 0
LISP-SUBNET-B *10.1.2.6 Te0/0/0.4001 00:02:13 00:02:13 0

xTR-MSMR-02#show ip lisp database
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBS: 0x3, 4 entries

10.1.1.5/32, dynamic-eid LISP-SUBNET-A, locator-set DC2
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-other, report-reachable
4.4.4.4 2/100 cfg-addr site-self, reachable
10.1.1.6/32, dynamic-eid LISP-SUBNET-A, locator-set DC2
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-other, report-reachable
4.4.4.4 2/100 cfg-addr site-self, reachable
10.1.2.5/32, dynamic-eid LISP-SUBNET-B, locator-set DC2
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-other, report-reachable
4.4.4.4 2/100 cfg-addr site-self, reachable
10.1.2.6/32, dynamic-eid LISP-SUBNET-B, locator-set DC2
Locator Pri/Wgt Source State
3.3.3.3 1/100 cfg-addr site-other, report-reachable
4.4.4.4 2/100 cfg-addr site-self, reachable

Verify that EIDs are no longer in the PxTR’s local LISP database.

On PxTR-01:

PxTR-02#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify
Dyn-EID Name Dynamic-EID Interface Uptime Last Pending
Packet Ping Count

On PxTR-02

PxTR-02#show lisp dynamic-eid summary
LISP Dynamic EID Summary for VRF "default"

* = Dyn-EID learned by site-based Map-Notify
To verify the Dynamic-EIDs EID-To-RLOC Mapping Database has been updated on the Map-Servers for the Servers that have migrated:

The EID-to-RLOC mapping database on the map-servers no show all EIDs registered by the xTR-MSMRs in the destination data center.

On xTR-MSMR-01:

```
xTR-MSMR-01#show lisp site
LISP Site Registration Information

<table>
<thead>
<tr>
<th>Site Name</th>
<th>Last Register</th>
<th>Up</th>
<th>Who Last Registered</th>
<th>Inst</th>
<th>EID Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC-MIGRATION</td>
<td>never</td>
<td>no</td>
<td>--</td>
<td></td>
<td>10.1.0.0/16</td>
</tr>
<tr>
<td>00:00:45</td>
<td>yes</td>
<td>3.3.3.3</td>
<td>01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:00:02</td>
<td>yes</td>
<td>3.3.3.3</td>
<td>01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:00:45</td>
<td>yes</td>
<td>3.3.3.3</td>
<td>01</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:00:02</td>
<td>yes</td>
<td>3.3.3.3</td>
<td>01</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

End of Migration Steps to Decommission LISP Routers

This section provides the steps required to be performed to conclude the migration of a subnet from the legacy DC to the New DC. The goal of this procedure is to enable the removal of the ASRs and LISP from the network after a subnet has been completed migrated to the new DC. Following this procedure for all subnets will allow the complete removal of the ASRs and LISP from the network.

In this example, Subnet 10.1.1.0/24 which is VLAN 4000 on the New DC and VLAN 200 on the Legacy DC is decommissioned on the ASR1k after all servers have been migrated to the new DC.

**Step 1: Moving the default gateway for Servers onto the New DC Switches**

**Step 1.1** - Add VLAN 4000 interfaces on the aggregation switch in the New DC. Use the same HSRP group as corresponding sub-interface (in this case Ten0/0/0.4000) on the ASR1k’s in the New DC.

The HSRP Virtual IP will be the same as the HSRP virtual IP on the ASR, i.e. the IP address that migrated hosts on that subnet are using as their default gateway. The “physical IP” addresses on the VLAN interfaces can be any addresses not already in use on the destination DC. It is possible to use the same IP addresses that are currently used on the source DC ASRs. Before enabling the vlan interfaces make sure to give them a lower HSRP priority than the sub-interfaces on the xTR-MSMRs.

In this case 30 and 20 were used as the HSRP priorities on the destination DC switches. Enable the vlan interfaces (no shut) and make sure they go into the HSRP listen state.

**Destination DC Spine Switch-1**

```
interface vlan 4000
ip address 10.1.1.252 255.255.255.0   << Can use the same physical IP as PxTR-01 in the source DC
standby 1 ip 10.1.1.1   <<< This is the same HSRP Virtual IP as the xTR-MSMRs in the Destination DC
standby 1 timers 1 3    <<< HSRP group number & timers should also match the xTR-MSMRs
standby 1 preempt       <<< Pre-emption should be enabled
standby 1 priority 30   <<< priority set lower than the xTR-MSMRs
no shut
```
Destination DC Spine Switch-2
interface vlan 4000
ip address 10.1.1.253 255.255.255.0  
standby 1 ip 10.1.1.1  
standby 1 timers 1 3  
standby 1 preempt  
no shut

<< Can use the same physical IP as PxTR-02 in the source DC
<< This is the same HSRP Virtual IP as the xTR-MSMRs in the Destination DC
<< HSRP group number & timers should also match the xTR-MSMRs
<< Pre-emption should be enabled
<< priority set lower than the xTR-MSMRs

Can use the same physical IP as PxTR-02 in the source DC
This is the same HSRP Virtual IP as the xTR-MSMRs in the Destination DC
HSRP group number & timers should also match the xTR-MSMRs
Pre-emption should be enabled
priority set lower than the xTR-MSMRs

Verify the destination DC Spine Switches become part of the same HSRP group as the new DC ASRs.
And that the switches go into the HSRP listen state using the commands:
#show standby
#show standby brief
#show standby vlan [vlan-id]

---

**Step 1.2** – Note that before starting step 1.2, be aware that step 1.2 and step 1.3 need to be done in quick succession. After verifying that the destination DC switches are in the listen state for the same HSRP group as the xTR-MSMRs, increase the HSRP priority of the switches so that they pre-empt the xTR-MSMRs and become HSRP active and standby.

Destination DC Spine Switch-1
interface vlan 4000
standby 1 priority 170
!

Destination DC Spine Switch-2
interface vlan 4000
standby 1 priority 165

---

**Step 1.3** - Remove HSRP configuration on the xTR-MSMRs for VLAN 4000:

xTR-MSMR-01
inter Te0/0/0.4000
no standby 1

xTR-MSMR-02
inter Te0/0/0.4000
no standby 1

As stated above steps 1.2 and 1.3 should be done in quick succession. This is to avoid traffic black holing from hosts on other LISP mobility subnets in the new DC to the subnet being migrated (HSRP Active/standby) on the destination DC spine switches. This is because once the xTR-MSMRs go into the HSRP listen state they will not ARP for hosts on that subnet. By removing HSRP on the sub-interface before ARP times out will avoid this traffic from being dropped. Ideally step 1.1 and step 1.2 should be done within 30 seconds of each other. If step 1.2 and step 1.3 are done in quick succession (before ARP times out on the ASRs) then there should be no service disruption.
Step 2: Advertise the Route for the migrated subnet from the Destination DC

Note that before starting Part 2, be aware that step 2.1, step 2.2 and step 2.3 need to be done simultaneously or in very quick succession. It is recommended to use a script so these two changes so they can be done within 1-2 seconds of each other to reduce any traffic disruption.

This section will depend on the routing protocol that is being used to advertise the server subnets to the WAN. The convergence times will also depend on the routing protocol used as well as the timers and size of the WAN network.

Step 2.1 - Advertise the subnet to the WAN from the Destination DC

Advertise the subnet 10.1.1.0/24 into whatever routing protocol is being used on the WAN from the destination DC. For example add the network statement for 10.1.1.0/24 under the routing protocol configuration.

Step 2.2 – Shut down the subnet’s VLAN Interface on the Aggregation Switches in the Source DC

shut down the related SVI (VLAN 200) on The Source DC Aggregation Switch-1

    interface vlan 200
    shutdown

shut down the related SVI (VLAN 200) on the source DC Aggregation Switch-2:

    interface vlan 200
    shutdown

Step 2.3 – Stop advertising the subnet to the WAN from the Source DC

Stop advertising the subnet 10.1.1.0/24 from the switches in the source DC towards the WAN. For example remove the network statement for 10.1.1.0/24 under the routing protocol configuration on the source DC switches that are originating the route.

Warning:

DO NOT shut down any of the sub-interfaces on the ASRs. All sub-interfaces need to remain up until every subnet has had their default gateway addresses migrated to the destination DC switches and the routing for every subnet is being announced from the destination DC. Only after the end of migration steps outlined above have been completed for all subnets should the interfaces on the ASRs be shut down and the ASRs removed from the network.

Failure and Recovery Analysis

The following sections will describe some of the possible failure scenarios that could happen and the mechanisms that are used to prevent traffic loss and speed up convergence.
Route-Watch to Track the Reachability of the remote eTRs

Locator route-watch is enabled by default. With route-watch each iTR will track the routes to the eTR RLOC addresses for the EID-RLOC mappings in its map-cache. If route to remote eTR RLOC goes down then the iTR will update its map-cache so the remote RLOC is not used. This provides fast convergence but requires a /32 route to each RLOC. In the configuration example in this paper OSPF is used to advertise a /32 route for the RLOC interface Loopback 0 for each ASR 1000. BFD is also used on the links between the LISP routers for faster convergence if the ASR 1000 routers are connected via a layer-2 network.

The example below will look at how route-watch is used to failover traffic. An intra-VLAN flow between a server in the source data center 10.1.1.5 and a server in the destination data center 10.1.1.6 is used for this example.

Figure 17: Intra-VLAN Flow during normal conditions

During normal conditions PxTR-01 will LISP encapsulate traffic destined for the EID 10.1.1.5 with a destination RLOC of 3.3.3.3 which is the RLOC of xTR-MSMR-01.

```
PxTR-01#show ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 3 entries
10.1.1.0/24, uptime: 00:02:25, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request
10.1.1.6/32, uptime: 00:02:23, expires: 23:59:41, via map-reply, complete
Locator  Uptime  State  Pri/Wgt
3.3.3.3  00:02:23  up    1/100
4.4.4.4  00:02:23  up    2/100
```
10.1.2.0/24, uptime: 00:02:25, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request

PxTR-01#show ip lisp forwarding eid remote 10.1.1.6
Prefix Fwd action Locator status bits
10.1.1.6/32 encap 0x00000003
packets/bytes 47026/4702600
path list 0274AB04, flags 0x49, 4 locks, per-destination
ifnums:
LISP0(12): 3.3.3.3
1 path
path 027497B8, path list 0274AB04, share 100/100, type attached nexthop, for IPv4
nexthop 3.3.3.3 LISP0, adjacency IP midchain out of LISP0, addr 3.3.3.3 03D31888
1 output chain
chain[0]: IP midchain out of LISP0, addr 3.3.3.3 03D31888 IP adj out of TenGigabitEthernet1/0/0,
addr 192.168.100.6 03D319B8

After Failure of xTR-MSMR-01:

PxTR-01#sh ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 3 entries

10.1.1.0/24, uptime: 00:02:58, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request
10.1.1.6/32, uptime: 00:02:56, expires: 23:57:03, via map-reply, complete
Locator Uptime State Pri/Wgt
3.3.3.3 00:02:56 no-route 1/100
4.4.4.4 00:02:56 up 2/100
10.1.2.0/24, uptime: 00:02:58, expires: never, via dynamic-EID, send-map-request
Negative cache entry, action: send-map-request

PxTR-01#show ip lisp forwarding eid remote 10.1.1.6
Prefix Fwd action Locator status bits
10.1.1.6/32 encap 0x00000002
packets/bytes 1616/161600
path list 0274AC44, flags 0x49, 4 locks, per-destination
ifnums:
LISP0(12): 4.4.4.4
1 path
path 0274997B8, path list 0274AC44, share 100/100, type attached nexthop, for IPv4
nexthop 4.4.4.4 LISP0, adjacency IP midchain out of LISP0, addr 4.4.4.4 03D314F8
1 output chain
chain[0]: IP midchain out of LISP0, addr 4.4.4.4 03D314F8 IP adj out of TenGigabitEthernet0/1/0,
addr 192.168.100.2 029054E0

Figure 18: Intra-VLAN Flow during failure of xTR-MSMR-01
In this scenario when xTR-MSMR-01 goes down completely. xTR-MSMR-02 will become HSRP active and will LISP encapsulate the traffic back to the server 10.1.1.5 with a destination RLOC of 1.1.1.1 which is the RLOC of PxTR-01 since it has a lower priority than PxTR-02.

In certain topologies using locator route-watch may not be possible, for example if the ASR 1000 routers are connected to each other over the internet since service-providers will accept /32 routes to be announced on the internet. For that case RLOC probing can be used instead of route-watch. RLOC probing is not enabled by default. It allows an iTR to periodically probe remote eTRs to determine if they are reachable. RLOC probing will have slower convergence than route-watch and is not scalable in larger deployments.

**HSRP Tracking to Force Failover when iTR loses both routes to remote eTRs**

In the scenario where the primary iTR for the data center loses connectivity to both eTRs in the remote data center HSRP needs to failover to the backup iTR. Otherwise from servers will still be sent to the primary iTR and it will not know how to forward it to the remote data center. On the primary iTR in the data center object tracking is used to track the /32 routes of the remote data center eTRs.

For the reference topology this HSRP tracking is required on PxTR-01 and xTR-MSMR-01. Below is an example of the partial configuration on PxTR-01. All sub-interfaces with LISP mobility configured will track object 4. Only one sub-interface is shown below for brevity.
### Route Tracking Partial Configuration from PxTR-01

| Comments |
|------------------|--------------------------------------------------|
| Object 2 tracks the route to the RLOC address of xTR-MSMR-01 |
| Object 3 tracks the route to the RLOC address of xTR-MSMR-02 |
| Object 4 is a Boolean OR of object 2 and 3. Therefore object 4 will only go down if both object 2 and 3 are down |
| On the LISP enabled sub-interface for the server subnet HSRP tracks object 4 and will decrement the HSRP priority if object 4 goes down. Hence making PxTR-02 become HSRP active |

| route 2 ip route 3.3.3.3 255.255.255.255 reachability delay up 180 |
| route 3 ip route 4.4.4.4 255.255.255.255 reachability delay up 180 |
| track 4 list boolean or object 2 object 3 |
| interface TenGigabitEthernet0/0/0.200 |
| encapsulation dot1Q 200 |
| ip address 10.1.1.252 255.255.255.0 |
| ip pim sparse-mode |
| standby delay minimum 180 reload 300 |
| standby 100 ip 10.1.1.254 |
| standby 100 timers 1 3 |
| standby 100 priority 105 |
| standby 100 preempt |
| standby 100 track 4 decrement 10 |
| no lisp mobility liveness test |
| lisp mobility LISP-SUBNET-A |

This failure scenario is illustrated below, where PxTR-01 loses connectivity to the other LISP routers. For example if the links go down or there is a circuit failure on the service provider network.

*Figure 19: PxTR-01 Loses connectivity to the other LISP Routers*
Before Failure:

PxTR-01#show track brief
<table>
<thead>
<tr>
<th>Track</th>
<th>Object</th>
<th>Parameter</th>
<th>Value</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ip route</td>
<td>3.3.3.3/32</td>
<td>reachability</td>
<td>Up</td>
</tr>
<tr>
<td>3</td>
<td>ip route</td>
<td>4.4.4.4/32</td>
<td>reachability</td>
<td>Up</td>
</tr>
<tr>
<td>4</td>
<td>list</td>
<td>boolean</td>
<td>Down</td>
<td>00:00:09</td>
</tr>
</tbody>
</table>

PxTR-01#show standby brief

P indicates configured to preempt.

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp</th>
<th>Pri</th>
<th>P</th>
<th>State</th>
<th>Active</th>
<th>Standby</th>
<th>Virtual IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te0/0.200</td>
<td>100</td>
<td>105</td>
<td>P</td>
<td>Active</td>
<td>local</td>
<td>10.1.1.253</td>
<td>10.1.1.254</td>
</tr>
<tr>
<td>Te0/0.201</td>
<td>100</td>
<td>105</td>
<td>P</td>
<td>Active</td>
<td>local</td>
<td>10.1.2.253</td>
<td>10.1.2.254</td>
</tr>
</tbody>
</table>

After Failure:

PxTR-01#show track brief

<table>
<thead>
<tr>
<th>Track</th>
<th>Object</th>
<th>Parameter</th>
<th>Value</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>ip route</td>
<td>3.3.3.3/32</td>
<td>reachability</td>
<td>Down</td>
</tr>
<tr>
<td>3</td>
<td>ip route</td>
<td>4.4.4.4/32</td>
<td>reachability</td>
<td>Down</td>
</tr>
<tr>
<td>4</td>
<td>list</td>
<td>boolean</td>
<td>Down</td>
<td>00:00:09</td>
</tr>
</tbody>
</table>

PxTR-01#show standby brief

P indicates configured to preempt.
EEM Scripts to force failover of incoming LISP traffic when The Internal interface on Primary eTR goes down

When the internal interface facing the aggregation or spine switch on the primary eTR for the data center goes down HSRP will failover to the backup eTR. However the iTRs at the remote site have no way of knowing that the primary eTR is no longer able to reach the servers in its local site. For this scenario object tracking and EEM scripts are used to shut down the RLOC interface on the primary eTR when its internal interface facing the data center switches goes down. Then route-watch on the remote data center iTRs will update their map-caches and send the LISP traffic to the backup eTR. This object tracking and EEM scripts are required on both PxTR-01 and xTR-MSMR-01. Below shows a partial configuration from PxTR-01 showing the object tracking and EEM scripts:

<table>
<thead>
<tr>
<th>Interface Tracking and EEM Scripts from PxTR-01</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>track 1 interface TenGigabitEthernet0/0/0 line-protocol delay up 180</td>
<td>Tracked object 1 tracks the internal interface facing the aggregation switches</td>
</tr>
<tr>
<td>event manager applet INTERNAL-INTERFACE-IS-DOWN event track 1 state down action 1.0 cli command &quot;enable&quot; action 1.1 cli command &quot;conf t&quot; action 2.0 cli command &quot;interface loop0&quot; action 3.0 cli command &quot;shut&quot; action 9.0 syslog msg &quot;INTERNAL INTERFACE DOWN, RLOC 1.1.1.1 HAS BEEN SHUTDOWN&quot;!</td>
<td>An EEM script is used to shut down the RLOC interface Loopback 0 on PxTR-01 if the interface Ten0/0/0 facing the aggregation switch goes down (Tracked object 1). This is required so that the xTR-MSMRs will see the RLOC of PxTR-01 go down and so they won’t forward LISP traffic to it during this failure scenario. This will force the incoming LISP traffic over to PxTR-02</td>
</tr>
<tr>
<td>event manager applet INTERNAL-INTERFACE-IS-UP event track 1 state up</td>
<td>Another EEM script is used to bring the...</td>
</tr>
</tbody>
</table>
Interface Tracking and EEM Scripts from PxTR-01

<table>
<thead>
<tr>
<th>Action</th>
<th>CLI Command</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>config t</td>
<td></td>
</tr>
<tr>
<td>2.0</td>
<td>interface loop0</td>
<td></td>
</tr>
<tr>
<td>3.0</td>
<td>no shut</td>
<td></td>
</tr>
<tr>
<td>9.0</td>
<td>syslog msg</td>
<td>RLOC interface Loopback 0 on PxTR-01 back up after the interface Ten0/0/0 facing the aggregation switch comes back up</td>
</tr>
</tbody>
</table>

The Diagram below illustrates this failure scenario. No that in this case there would be OSPF equal-cost path between PxTR-02 and xTR-MSMR-01 so traffic would be load-balanced across the two paths. The diagram below just shows one path for simplicity.

Figure 20: Failure of Internal Interface on PxTR-01

Failover of Traffic between a Server in the Destination Data Center and a non-LISP enabled WAN Site

Both xTR-MSMR routers use the PxTR routers as their Proxy Egress Tunnel routers with the use-PeTR function. Beginning in IOS XE version 3.11 LISP locator route-watch can be used to automatically track the reachability of Proxy Egress Tunnel Routers. Therefore if PxTR-01 becomes unreachable the xTR-MSMR routers will update their map-cache to send traffic destined for the WAN to PxTR-02.

Figure 21: Failover of WAN traffic when primary PeTR goes down
Note that prior to IOS XE version 3.11 route-watch was not available for the use-PeTR function. For versions prior to IOS XE 3.11 an EEM script could be used to reconfigure the use-PeTR priorities in the event the iTR loses its route to the primary PeTR.

**Before Failure of PxTR-01:**

```
xTR-MSMR-01#show ip lisp forwarding eid remote
Prefix       Fwd action Locator status bits
0.0.0.0/0    signal  0x00000000
packets/bytes  1/100
10.1.1.0/24  signal  0x00000000
packets/bytes  2/200
10.1.1.5/32  encap  0x000000003
packets/bytes  750114/75011400
10.1.2.0/24  signal  0x00000000
packets/bytes  0/0
10.32.0.0/11  fwd native  0x00000000
packets/bytes  59450/5945000
```

```
xTR-MSMR-01#show ip lisp forwarding eid remote 10.32.0.0
Prefix       Fwd action Locator status bits
10.32.0.0/11  fwd native  0x00000000
packets/bytes  66045/6604500
path list 051773F4, flags 0x49, 5 locks, per-destination ifnums:
  LISP0(12): 1.1.1.1
  1 path
```
After Failure of PxTR-01:

```
xTR-MSMR-01#show ip lisp forwarding eid remote 10.32.0.0
Prefix     Fwd action Locator status bits
10.32.0.0/11  fwd native 0x00000000
packets/bytes 168796/16879600
path list 051776C4, flags 0x49, 5 locks, per-destination
ifnums:
  LISP0(12): 2.2.2.2
1 path
  path 04633650, path list 051776C4, share 100/100, type attached nexthop, for IPv4
  nexthop 2.2.2.2 LISP0, adjacency IP midchain out of LISP0, addr 2.2.2.2
1 output chain
chain[0]: IP midchain out of LISP0, addr 2.2.2.2 050F6AC0 IP adj out of TenGigabitEthernet0/1, addr 192.168.100.14 050F7310
```

Optional Deployment Variations

This section covers some deployment options that are variations from the reference topology described previously. Specifically it’s explained how to configure LISP in a multi-VRF environment to support overlapping IP addresses between multiple tenants. Co-existence with OTV is explained, and considerations if one chooses to deploy this solution without redundancy are also covered. A topology where a non-LISP device is used as the default gateway in the Greenfield DC is presented, and finally it’s covered how to configure LISP for interfaces that have secondary IP addresses on them.

Support for multi-VRF environments

LISP natively provides support for multi-tenancy. On the LISP packet header the field Instance ID is used to provide a means of maintaining unique address spaces (or “address space segmentation”) in the control and data plane. Instance IDs are numerical tags.

Virtualization at the device level use virtual routing and forwarding (VRF) to create multiple instances of Layer 3 routing tables, LISP binds VRFs to instance IDs (IIDs), and then these IIDs are included in the LISP header to provide data plane (traffic flow) and control plane separation for single or multihop needs, in other words LISP binds VRFs to instance IDs to extend the device virtualization to become a network wide virtualization.

Recalling that LISP implements Locator ID separation and, in so doing, creates two namespaces (EIDs and RLOCs), it is easy to see that LISP virtualization can consider both EID and RLOC namespaces for virtualization. That is, either or both can be virtualized.

- EID virtualization—Enabled by binding a LISP instance ID to an EID VRF.
• RLOC virtualization—Tying locator addresses and associated mapping services to the specific VRF within which they are reachable enables RLOC virtualization.

Because LISP considers virtualization of both EID and RLOC namespaces, two models of operation are defined: shared model and parallel model. When using the solution described on this paper it’s possible to use LISP virtualization in shared model or parallel model, however the remaining on this section will focus on a shared model implementation where VRFs are used to segment the EID space and they use a RLOC space configured in the global table.

Figure 22. LISP shared model virtualization resolves EIDs within VRFs tied to Instance IDs. RLOC addresses are resolved in a common (shared) address space. The default (global) routing table is shown as the shared space.

Figure 22: LISP Shared Virtualization Model

Below you can find a configuration example for VRF named BIO. In particular it covers the main differences from what has been previously described on the whitepaper that makes the solution presented support multi-VRF environments. Please note that the RD, interface, IP address and .1q numbers used are examples only.

On the xTR configuration below VRF BIO is mapped to LISP instance-id 102. In this example LISP mobility is enabled for the subnet 172.16.133.0/24 which is within the BIO VRF. For a multi-homed environment with two xTRs in the data center multicast routing and pim need to be enabled on the xTRs for the VRF. This is required for correct processing of the LISP multicast map-notify message.

```
vrf definition BIO
rd 119:1

ip multicast-routing vrf BIO distributed

interface Loopback1
vrf forwarding BIO
ip address 111.1.1.1 255.255.255.255
ip pim sparse-mode

interface TenGigabitEthernet0/0/0.849
description EID-BIO
encapsulation dot1Q 849
```
vrf forwarding BIO
ip address 172.16.133.252 255.255.255.0
ip pim sparse-mode
standby delay minimum 180 reload 300
standby 89 ip 172.16.133.254
standby 89 priority 105
standby 89 preempt
standby 89 track 1 decrement 10
no lisp mobility liveness test
lisp mobility LISP-BIO-1

router lisp
locator-set EXAMPLE
  11.11.11.11 priority 1 weight 100
  22.22.22.22 priority 2 weight 100
exit

eid-table vrf BIO instance-id 102 << mapping from VRF to instance-id
dynamic-eid LISP-BIO-1
database-mapping 172.16.133.0/24 locator-set EXAMPLE
  map-notify-group 239.0.0.3
exit

ip pim vrf BIO rp-address 111.1.1.1

LISP control-plane messages include the instance-id so that EIDs can be registered and resolved for their corresponding instance-id. Hence the map-servers must also be instance-id aware. The mapping database stores the instance-id with the EID-to-RLOC mappings. The sample partial map-server configuration below will accept more-specific map-registers for EIDs within the 172.16.0.0/16 network that have an instance-id of 102 and the correct authentication key.

router lisp
site DC-MIGRATION
  authentication-key CISCO123
  eid-prefix instance-id 102 172.16.0.0/16 accept-more-specifics
exit

**Coexistence with OTV**

LISP supports a deployment mode called Extended Subnet mode where LISP is combined for the same VLAN/subnet together with a LAN Extension solution (for example OTV or VPLS), in this case LISP provides path optimization and the LAN Extension solution provides IP mobility.

The solution presented on this whitepaper is **not** LISP Extended Subnet mode, therefore LISP is used exclusively for providing IP mobility (without OTV or any other Layer 2 extension technology), however it’s important to note that it’s possible to combine OTV and LISP on the same ASR 1000 where OTV is used for certain VLANs and LISP is used for others, for example OTV is used to extended VLAN 10, which has subnet 10.10.10.0/24 configured on it, while LISP is used to provide IP mobility for subnet 10.20.20.0/24, VLAN 20. Note that LISP does not extend VLANs therefore the VLAN ID is irrelevant for LISP-based forwarding.
This capability that the ASR 1000 offers where OTV is used for some VLANs and LISP is used for others is useful when deploying the solution presented on this paper and you find during the deployment that a certain application has a mandatory requirement to preserve layer 2 adjacency between hosts in the original (brownfield) data center and hosts migrated to the new data center; for example members of a cluster that communicate at layer 2 via link local multicast traffic. This requirement for layer 2 adjacency between hosts is becoming less and less relevant given that most if not all hosts communicate at layer 3, however if needed OTV can be used to meet this requirement for that specific VLAN while LISP is used for all other subnets.

Another scenario where the use of OTV for a particular VLAN/subnet is useful is for the case where there are no IP addresses available on the subnet where mobility is desired. As detailed on the section “Deploying LISP on Cisco ASR 1000 for Data Center Migration” on the Brownfield (original) data center when the ASRs are connected to the subnet where mobility is required, three IP addresses from that subnet are required for the implementation of the solution, one for each ASR and one used as the Virtual IP (HSRP IP) shared between the routers. It could be the case that there are no IP addresses available on the subnet where mobility is required, in this case LISP can’t be implemented and therefore the use of OTV is an attractive alternative.

Following is an example of a configuration where on the same internal interface, i.e. interface from ASR connected to subnet/VLAN where mobility is required, OTV is used to extend VLAN 621 and LISP is used for subnet 11.10.1.0/24 associated with VLAN 501.

**OTV basic config, VLAN 620 used as OTV site VLAN and VLAN 621 extended by OTV to remote site.**

```
ottv site bridge-domain 620
ottv isis hello-interval 3
!
ottv fragmentation join-interface TenGigabitEthernet0/2/0
ottv site-identifier ACDC.ACDC.0001
ottv isis Overlay1
log-adjacency-changes all

bridge-domain 621

interface Overlay1
no ip address
ottv join-interface TenGigabitEthernet0/2/0
no otv filter-fhrp
ottv use-adjacency-server A.B.C.D A.B.C.E unicast-only
ottv isis hello-interval 3
service instance 621 ethernet
encapsulation dot1q 621
bridge-domain 621
```

Interface config where VLAN 621 is extended to remote site via OTV and LISP is used for IP mobility for subnet 11.10.1.0/24 associated with VLAN 501. VLAN 620 is OTV site VLAN.

```
interface GigabitEthernet0/0/1
description INTERNAL INTERFACE TO DC
```
no ip address
service instance 620 ethernet
encapsulation dot1q 620
bridge-domain 620
!
service instance 621 ethernet
encapsulation dot1q 621
bridge-domain 621

interface GigabitEthernet0/0/1.2000
encapsulation dot1q 500
ip address AA.BB.CC.DD 255.255.255.0
ip pim sparse-mode
standby 20 ip AA.BB.CC.DE
standby 20 timers 1 3
standby 20 preempt
no lisp mobility liveness test
lisp mobility LISP2060

Non-redundant deployment considerations

On the previous reference diagrams and detailed deployment sections it’s described and recommended that a pair of ASR 1000 is deployed on each data center, therefore providing redundancy. It’s possible to deploy the solution described on this paper with a single ASR 1000 per data center, without redundancy. In addition to the obvious risks of not having redundancy one must also consider what happens on the event of a reboot or failure and then recover of the ASR 1000 connected to the brownfield (original) data center.

As previously explained, in the brownfield data center the ASR 1000 is not the default gateway and therefore as covered under section “Implementation Details on the Brownfield Data Center” after implementation the detection of EIDs is performed by using an EEM-script. On non-redundant deployments, after the ASR in the brownfield reloads it will come up with an empty EID table and as such the same EEM script used during initial deployment must be executed. Until the EEM script is finished it’s likely that there will be packet loss and intermittent communication in the network because for example traffic from a host in the green field data center to a host in the brownfield that has not yet been detected would be dropped as there won’t be an entry on the map-server.

In summary, although technically possible to deploy this solution without redundancy, Cisco’s recommendation is that it’s always deployed with redundant nodes unless the situation described above is understood and acceptable.

Support for Secondary IP addressing

Occasionally in data centers if a server subnet runs out of IP addresses and secondary subnets need to be used for the same server VLAN. LISP Mobility supports multiple dynamic-EID prefixes configured on the same sub-interface. The sub-interface that the LISP dynamic-EID prefixes are configured on is local to the LISP router. This means that on one site multiple subnets can belong to one VLAN whereas on another site these subnets can be assigned to individual VLANs. Hence LISP
mobility for data center migrations enables the network admin to plan a new and improved VLAN numbering scheme for the new data center.

If there are multiple subnets sharing the same VLAN in the source data center and secondary addresses are used on the VLAN interfaces on aggregation switches, then multiple LISP dynamic EIDs can be used on respective sub-interfaces on the ASR 1000 series routers. In the destination data center the subnets can be presented on a single VLAN or split into individual VLANs. The example below shows the configuration required for LISP mobility to be enabled for two subnets in the same VLAN 200 in the source data center 10.1.1.0/24 and 10.1.3.0/24. In the destination data center these subnets have been split into VLAN 4000 and VLAN4003 respectively. Note that for LISP mobility the xTR does not need to have an IP address on the sub-interface in the same subnet as the dynamic-EIDs. For Brevity the HSRP configuration has been omitted. Only a single HSRP group is required is using multiple dynamic-EID prefixes on the same sub-interface.

<table>
<thead>
<tr>
<th>Partial Config from PxTR-01 with Two Subnets on single VLAN</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>router lisp</td>
<td>Two LISP dynamic-EID prefixes are defined for the two subnets 10.1.1.0/24 and 10.1.3.0/24</td>
</tr>
<tr>
<td>locator-set DC1</td>
<td>Two LISP dynamic-EID prefixes</td>
</tr>
<tr>
<td>1.1.1.1 priority 1 weight 100</td>
<td></td>
</tr>
<tr>
<td>2.2.2.2 priority 2 weight 100</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Both LISP dynamic-EIDs are assigned to interface Ten0/0/0.200</td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>eid-table default instance-id 0</td>
<td></td>
</tr>
<tr>
<td>dynamic-eid LISP-SUBNET-A</td>
<td></td>
</tr>
<tr>
<td>database-mapping 10.1.1.0/24 locator-set DC1</td>
<td></td>
</tr>
<tr>
<td>map-notify-group 239.0.0.1</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>dynamic-eid LISP-SUBNET-C</td>
<td></td>
</tr>
<tr>
<td>database-mapping 10.1.3.0/24 locator-set DC1</td>
<td></td>
</tr>
<tr>
<td>map-notify-group 239.0.0.3</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>interface TenGigabitEthernet0/0/0.200</td>
<td></td>
</tr>
<tr>
<td>encapsulation dot1Q 200</td>
<td></td>
</tr>
<tr>
<td>ip address 10.1.1.252 255.256.255.0</td>
<td></td>
</tr>
<tr>
<td>no lisp mobility liveness test</td>
<td></td>
</tr>
<tr>
<td>lisp mobility LISP-SUBNET-A</td>
<td></td>
</tr>
<tr>
<td>lisp mobility LISP-SUBNET-C</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Partial Config from xTR-MSMR-01 with Single Subnet on each VLAN</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>router lisp</td>
<td>Two LISP dynamic-EID prefixes</td>
</tr>
<tr>
<td>locator-set DC2</td>
<td></td>
</tr>
<tr>
<td>3.3.3.3 priority 1 weight 100</td>
<td></td>
</tr>
<tr>
<td>4.4.4.4 priority 2 weight 100</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>!</td>
<td></td>
</tr>
<tr>
<td>eid-table default instance-id 0</td>
<td></td>
</tr>
<tr>
<td>dynamic-eid LISP-SUBNET-A</td>
<td></td>
</tr>
<tr>
<td>database-mapping 10.1.1.0/24 locator-set DC2</td>
<td></td>
</tr>
</tbody>
</table>
Support for Stateful Devices

Most data centers will have some form of stateful devices such as firewalls or loadbalancers. It is important that traffic traverses these stateful devices symmetrically to maintain state. Therefore any data center migration solution needs to take this into account. This section will look at the different design options based on the placement of the stateful devices in the source datacenter.

Figure 23: Reference Topology With Firewalls in Source and Destination Data Centers
Firewall Placement between Aggregation and Core Layer

This is the most common deployment of firewalls within traditional 3-tier data centers. In this design, the server’s default gateway will be the aggregation switches. The Firewall inside interface will logically connect at layer 3 to the aggregation switches and the Firewall outside interfaces will logically connect at layer-3 to the core switches. There is no special configuration required for the LISP data center migration solution to work with this type of firewall placement. Traffic to and from servers that have migrated to the destination data center will route symmetrically through the firewalls. The diagram below will shows a logical layer-3 routing representation of this design as well as the traffic flow to and from the WAN and a server that has been migrated to the destination data center.

Figure 24: Firewall Logical Layer-3 Placement between Aggregation and Core Layer in Source Data Center
As the diagram shows traffic is symmetric through the firewall between the WAN and a server that has been migrated to the destination data center. The PxTR routers use the aggregation switches as their default gateway over the VLAN 500 subnet.

Firewall Placement between Servers and Aggregation Layer

In some data centers for certain subnets the firewalls may be logically placed between the servers and the aggregation layer, i.e. the servers use the firewall inside interface as their default gateway. Since the PxTR routers use a single subnet for default routing towards the aggregation switches the firewall will be bypassed for return traffic from servers that have migrated to the destination data center towards the WAN. This will prevent the firewall from maintaining state on the traffic flows and may also block the flows inbound from the WAN since the firewall has no way of determining the flows originated from the inside network. The diagram below illustrates this problem when the firewall is logically placed between the servers and the aggregation layer.

Figure 25: Firewall logical Layer-3 placement between Servers and Aggregation Layer in source Data Center
To overcome this issue the PxTRs must send traffic destined to the WAN to the inside interface of the firewall for subnets with this topology rather than using the default route to the aggregation switches. This can be achieved using policy-based routing on the LISP0 interface of the PxTRs. The policy simply matches on the source address of the packets. If the source address is from a subnet that has the firewall between the servers and the aggregation switches then the policy sets the next hop to be the inside interface of the firewall.

Figure 26: Policy-Based Routing on PxTRs for Firewall Logical Layer-3 placement between Servers and Aggregation Layer in Source Data Center
The table below shows a configuration example for policy-based routing to maintain symmetrical traffic through a firewall when it is the default gateway for servers on the subnet 10.1.1.0/24.

<table>
<thead>
<tr>
<th>Policy-Based Routing on the PxTR Routers for Subnets with Firewall between Servers and Aggregation Layer</th>
<th>Comments</th>
</tr>
</thead>
</table>
| interface LISP0  
  ip policy route-map PBR-LISP  
  !  
  access-list 101 permit ip 10.1.1.0 0.0.0.255 any  
  !  
  route-map PBR-LISP permit 10  
  match ip address 101  
  set ip next-hop recursive 10.1.1.1  
  ! | This policy will set the next hop to be 10.1.1.1 for any traffic that the PxTR receives from the destination data center that needs to be routed. Note that the recursive option is needed with the `set ip next-hop` command. This is because the PxTR will have a /32 route in its routing table for the firewall address 10.1.1.1 learned from LISP. |
Policy-Based Routing on the PxTR Routers for Subnets with Firewall between Servers and Aggregation Layer

<table>
<thead>
<tr>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>The recursive option is needed for any routes that are not connected routes in the routing table.</td>
</tr>
</tbody>
</table>

Overview of Steps to Troubleshoot LISP Mobility

Troubleshooting LISP can be broken down into the following main steps:

Step1: Verify Underlay Routing  
Step2: Verify LISP Control-Plane  
Step3: Verify LISP Data-Plane

Step 1: Verify Underlay Routing
The underlay routing is the IP routing for the RLOC address space. LISP xTRs within the same RLOC routing domain must have IP reachability to each other’s RLOC address. Problem with the underlay routing will most likely affect multiple if not all EID prefixes.

Step 2: Verify LISP Control-Plane
Before an xTR can begin to LISP encapsulate data-packets to an EID located at another LISP site it must have a map-cache entry to the destination EID. The map-cache entries are data driven based on packets received by an iTR destined for remote EIDs. If the iTR does not create a map-cache entry to a destination EID upon receiving packets for that EID, then begin to troubleshoot the LISP control-plane. It is recommended to start with the eTR and work back to the iTR when troubleshooting the LISP control-plane. This approach needs to taken in both directions i.e. a LISP xTR will be an iTR in one traffic direction and an eTR in the other traffic direction.

2.1 Make sure dynamic EIDs have been detected by eTR
   - The Following commands can be used to determine this on the eTR:
     
     ```
     show lisp dynamic-eid summary
     show ip lisp database [EID-prefix]
     ```
   - If local dynamic EIDs are not detected by eTR, then check layer-2 connectivity, LISP dynamic-EID config, multicast and HSRP

2.2 Check that eTR has registered the EIDs with the map-server
   - The Following command can be used to determine this on the Map-Server:
     
     ```
     show lisp site [detail ]
     ```

2.3 Check iTR adds entry in its map-cache when traffic is sent to destination EID
   - The Following command can be used to determine this on the iTR:
     
     ```
     show ip lisp map-cache [ destination-EID | detail ]
     ```
Step 3: Verify LISP Data-Plane

When the LISP iTRs have map-cache entries for the remote EIDs then packets received by the iTR destined for the remote EID should get LISP encapsulated. Provided those packets reach the remote site eTR then they should get decapsulated and forwarded to the EID.

3.1 Check hardware forwarding table (CEF table)

```show ip cef [prefix | {detail| internal}]```

3.2 Check iTR is LISP encapsulating data packets

```show ip lisp forwarding eid remote [destination-EID | detail ]```

3.3 Make sure eTR is receiving the LISP encapsulated data packets
- Netflow ingress on eTR or Wireshark could be used to verify this
- If not then check if LISP data-plane packets (UDP destination port 4341) are being blocked on the transport network.

Conclusion

This whitepaper provided deployment guidance for a solution that enables IP addresses preservation during DC migration with LISP and ASR 1000. Customers who have adopted this solution were able to execute a DC migration with a much lower risk and much faster. In fact some of them expect to reduce the migration window by up to 95%.

The solution explained makes use of Locator/ID Separation Protocol (LISP, RFC 6830) running on Cisco’s ASR 1000 routers. The benefits delivered by the solution covered on this whitepaper include:
- Ability to de-couple the server migration activities (planning, affinity group migration, schedules, cut-overs etc.) from network constraints.
- IP address mobility: IP address, subnet mask, default gateway and hostname of migrated servers do not need to change.
- Small migration waves, that is enables even single server migration (if required), or the migration of a group of servers.

Cisco Services organization is available to assist with the planning, design, deployment, support and optimization of the solution described on this whitepaper.

Appendix

Locator/ID Separation Protocol (LISP, RFC 6830) is a key enabler for the solution described on this paper. On this appendix a brief overview of LISP is provided.

Overview of LISP

Locator/Identifier Separation Protocol

With the emergence of the cloud architecture, innovation is required in networking to allow IP to gain two mandatory missing features: IP mobility and VPNs.

The Locator Identity Separation Protocol (LISP) is a routing architecture that creates a new paradigm by splitting the device identity, known as an endpoint identifier (EID), and its location, known as its
routing locator (RLOC), into two different numbering spaces. This capability brings renewed scale and flexibility to the network in a single protocol, enabling mobility, scalability, and security.

LISP is an overlay routing protocol in the sense that it allows decoupling of the core transport, which can be any IP transport method, from the edge, which can be any IP application site. LISP is intended for the cloud because it allows dynamic resource provisioning independently from the network infrastructure. In short, any IP address can be positioned anywhere it is needed.

LISP is a routing architecture, not a feature; it gives IP a full set of capabilities that it does not natively have. LISP enables IP address portability, which can be seen in two ways. First, it allows the mobility of a host anywhere without changing the host IP address. Second, it allows defining an edge host IP address independently from the site IP structure it will reside on. The decoupling of the application definition from the network is critical for cloud flexibility.

LISP enables network VPN, allowing interconnecting Virtual Route Forwarding (VRF) instances over any IP network, giving to IP a similar capability as MPLS, but not limited to the core of the network, because virtualization is extended to any edge.

Cloud clearly requires huge scalability, and LISP also differentiates itself in this domain. LISP is based on a “pull” model. Similar to Domain Name System (DNS), LISP has one central mapping system where any node registers. When somewhere else in an organization an association between an edge identity versus routing location is required, then it is pulled from this mapping database. This feature differentiates LISP from OSPF or Border Gateway Protocol (BGP), which are “push” models where the full routing information is stored in the forwarding plane of every node. Like DNS, LISP is massively scalable.

The overlay aspect of LISP should also be emphasized. LISP is an over-the-top technology, tunneling over the IP core and all the IP edge flows. This tunneling allows LISP to use any type of transport, meaning the Internet, a multi-Autonomous System (multi-AS) network, a private infrastructure, IPv4 or IPv6, as well as IP VPN services provided through MPLS. LISP can be encrypted natively in point-to-point or multipoint IPsec. This isolation of the edge world that becomes agnostic from the transport is critical for the cloud architecture.

Finally, LISP is an open standard service with no intellectual property rights; LISP is also very active at the IETF (lisp@ietf.org) and the object of several multivendor implementations.

**LISP Basic Concepts**

To understand LISP, it is important to understand the concept of “Location to Identity Separation” (Figure 27).

*Figure 27: Location to Identity Separation*
In traditional IP, the IP edge routing subnets are advertised all over the network using either an Interior Gateway Protocol (IGP) or an Exterior Gateway Protocol (EGP); it is very rare to advertise any host address (subnet mask /32). Most of the time, subnets larger or equal to /24 are used. In IP because all routes are advertised everywhere and installed in the forwarding plane, it is important to limit the amount of entries. To do so, IP subnets are strictly limited to a geographical area, and a subnet is managed by only one pair of routers - the default gateway, implying that if a node moves location, then its IP address must be updated accordingly to the local default gateway and subnet. This constraint is very cumbersome; in order to escape from it, we see more and more across-site VLAN extensions with all the drawbacks this approach can raise.

With LISP, such constraints disappear; LISP splits the host ID (EID) from the RLOC, allowing any host to move from location to location while keeping its unique identity. LISP architecture is composed of several elements, including the following:

1. ETR: Egress tunnel router
   ● It registers the EID address space it is authorized for
   ● It is identified by one (or more) RLOCs
   ● It receives and decapsulates the LISP frames

2. Map server:
   ● This server is the database where all EID and RLOC associations are stored
   ● It can be deployed simply on a pair of devices
   ● Or it can be a hierarchy of devices, organized like a DNS system for massive scale implementation (LISP–DDT)

3. ITR: Ingress tunnel router
   ● Sends requests toward the map resolver
   ● Populates its local map cache with the learned association
   ● Responsible to perform the LISP encapsulation

4. Map resolver:
   ● Receives the request and selects the appropriate map server

5. Proxy xTR:
   ● The point of interconnection between an IP network and a LISP network, playing the role of ITR and ETR at this peering point

An ETR is authoritative for a subnet, and registers it using a “map-register” message to the map server.

When triggered on the data plane by a packet destined to a remote EID, the ITR performs a “map request” toward the map resolver, which forwards it to the right map server, which then forwards it to the authoritative ETR. This ETR replies to the requesting ITR using a “map-reply” message that
contains the list of the RLOCs that can reach the requested EID, with their characteristics in terms of priority of usage and weighted load repartition.

**Cisco LISP Contact Information and Authors**
If you have questions, comments, suggestions, or issues, please contact the Cisco LISP team by sending an email to: lisp-support@cisco.com

The Cisco LISP Team is proud to provide direct access and support to customers and partners. We will do our best to answer all emails in a prompt and accurate manner.

This whitepaper has been authored by:
- Santiago Freitas, Cisco Customer Solutions Architect, CCIE#18776
- Patrice Bellagamba, Cisco Distinguished Systems Engineer
- Niall Masterson, Cisco Network Consulting Engineer, Advanced Services, CCIE #44398