

Locator/ID Separation Protocol (LISP) Virtual Machine Mobility Solution

White Paper



Notice: All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product and are incorporated herein by this reference. If you are unable to locate the software license or limited warranty, contact your Cisco representative for a copy.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided "as is" with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

Copyright © 2011 Cisco Systems, Inc. All rights reserved.

Contents

Introduction	5
IP Mobility Overview	5
IP Mobility Requirements	6
Existing IP Mobility Solutions	7
Document Use Prerequisites	8
LISP Name Spaces	8
LISP Site Devices	8
LISP Infrastructure Devices	9
LISP VM-Mobility	9
LISP VM-Mobility Use Cases	10
LISP VM-Mobility Prerequisites	12
LISP VM-Mobility Operation	12
Dynamic-EID Detection and Map Updates	14
Map-Server and Map-Resolver Considerations	15
Deploying LISP VM-Mobility in an Extended Subnet	17
LISP VM-Mobility in an Extended Subnet Prerequisites	18
Configuring a Cisco Nexus 7000 Series Switch as a LISP xTR	19
Configuration Commands	19
Configuring a Cisco Nexus 7000 Series Switch LISP xTR for Dynamic-EID Roaming	19
Configuration Commands	20
Configuring a Remote Site Cisco IOS Software Router as a LISP xTR	21
Configuration Commands	21
Configuring a LISP Map-Server and Map-Resolver on Cisco NX-OS	22
Configuration Commands	22
LISP VM-Mobility in an Extended Subnet: Configuration Example	23
Cisco Nexus 7000 Series N7K1A West Data Center xTR Configuration Example	24
Cisco Nexus 7000 Series N7K1B West Data Center xTR Configuration Example	24
Cisco Nexus 7000 Series N7K2A East Data Center xTR Configuration Example	25
Cisco Nexus 7000 Series N7K2B East Data Center xTR Configuration Example	27
Remote Site Cisco IOS Software xTR Configuration Example	27
Cisco NX-OS Map-Server and Map-Resolver Configuration Example	28
LISP VM-Mobility in an Extended Subnet Verification	28
Verifying a Cisco NX-OS Map-Server	29
Verifying Cisco Nexus 7000 Series Data Center xTRs	31
Verifying Cisco IOS Software Remote xTR	33
Verifying Dynamic-EID Detection, Mapping, and Map-Cache Updates	34
LISP VM-Mobility in an Extended Subnet Summary	38
Deploying LISP VM-Mobility Across Subnets	39
LISP VM-Mobility Across Subnets Prerequisites	40
Configuring a Cisco Nexus 7000 Series Switch as a LISP xTR	40
Configuration Commands	40
Configuring a Cisco Nexus 7000 Series Switch LISP xTR for Dynamic-EID Roaming	41
Configuration Commands	41
Configuring the Remote Site Cisco IOS Software Router as a LISP xTR	42
Configuration Commands	42
Configuring the LISP Map-Server and Resolver on Cisco NX-OS	43
Configuration Commands	43
LISP VM-Mobility Across Subnets: Configuration Example	44
Cisco Nexus 7000 Series N7K1A West Data Center xTR Configuration Example	45
Cisco Nexus 7000 Series N7K1B West Data Center xTR Configuration Example	46
Cisco Nexus 7000 Series N7K2A East Data Center xTR Configuration Example	46
Cisco Nexus 7000 Series N7K2B East Data Center xTR Configuration Example	47
Remote-Site Cisco IOS Software xTR Configuration Example	48

Cisco NX-OS Map-Server and Map-Resolver Configuration Example	48
LISP VM-Mobility Across-Subnet Verification	48
Verifying Cisco NX-OS Map-Server	49
Verifying Cisco Nexus 7000 Series Data Center xTRs	51
Verifying Cisco IOS Software Remote xTR	51
Verifying Dynamic-EID Detection, Mapping, and Map-Cache Updates	53
LISP VM-Mobility Across Subnets Summary	57

Introduction

Locator/Identity Separation Protocol (LISP) is a new routing architecture that creates a new model by splitting the device identity, known as the Endpoint Identifier (EID), and its location, known as the Route Locator (RLOC), into two different numbering spaces. This capability brings additional flexibility to the network in a single protocol, enabling mobility, scalability, and security.

For enterprises, LISP provides several main benefits, including simplified enterprise multihoming with ingress traffic engineering capabilities, multi-tenancy over the Internet, simplified IPv6 transition support, and IP mobility for geographically dispersed data centers and disaster recovery.

This document describes LISP use cases addressing today's enterprise data center challenges. Server virtualization and high availability across geographically dispersed data centers are common in data center deployments today. Workload virtualization requires location independence for server resources and the flexibility to move these server resources from one data center to another to meet increasing workloads and to support disaster recovery. This virtualization brings the challenge of route optimization when the virtual servers move to route traffic to its current location. It also brings the challenge of keeping the server's identity (IP address) the same across moves, so that clients can continue to send traffic regardless of the server's current location.

The LISP Virtual Machine Mobility (VM-Mobility) solution addresses these challenges transparently by enabling IP endpoints to change location while keeping their assigned IP addresses. The virtual servers may move between different subnets or across different locations of a subnet that has been extended with Cisco[®] Overlay Transport Virtualization (OTV) or another LAN extension mechanism. In either case, the LISP VM-Mobility solution helps ensure optimal routing between clients and the IP endpoint that moved, regardless of its location. In addition, LISP VM-Mobility does not require any change in the Domain Name System (DNS) infrastructure (since the mobile nodes preserve their original IP addresses), which overall reduces operating expenses for the data center administrator.

LISP VM-Mobility provides an automated solution to IP mobility with the following characteristics:

- Helps ensure optimal shortest-path routing to the moving endpoints
- Supports any combination of IPv4 or IPv6 locator or identity addressing
- Provides Internet-class scalability for global mobility
- Is IP-based for excellent transport independence
- Is transparent to the endpoints and to the IP core
- Provides an overlay solution that enables the extension of subnets across multiple autonomous systems

This document describes LISP VM-Mobility use cases for an enterprise data center deployment, detailing the operation of the LISP components and providing step-by-step configurations.

IP Mobility Overview

The increasing use of virtualization in the data center has enabled an unprecedented degree of flexibility in the management of servers and workloads. One important aspect of this newfound flexibility is mobility. As workloads are hosted on virtual servers, they are decoupled from the physical infrastructure and become mobile by definition.

As endpoints become detached from the physical infrastructure and are mobile, the routing infrastructure is challenged to evolve from a topology-centric addressing model to a more flexible architecture. This new architecture is capable of allowing IP addresses to move freely and efficiently across the infrastructure.

There are several ways of adding mobility to the IP infrastructure, and each of them addresses the problem with a different degree of effectiveness. LISP VM-Mobility is poised to provide a solution for virtual machine mobility with optimal effectiveness. This document describes the LISP VM-Mobility solution, contrasts it with other IP mobility options, and provides specific guidance for deploying and configuring the LISP VM-Mobility solution.

IP Mobility Requirements

The requirements for an IP mobility solution can be generalized to a few main points. To perform a fair comparison of existing solutions and clearly understand the additional benefits of the LISP VM-Mobility solution, this section briefly presents the requirements that must be addressed in an IP mobility solution.

- **Redirection:** The ultimate goal of IP mobility is to steer traffic to the valid location of the endpoint. This requirement is generally addressed by providing some sort of redirection mechanism to enhance the traffic steering already provided by basic routing. Redirection can be achieved by replacing the destination address with a surrogate address that is representative of the new location of the endpoint. Different techniques will allow the redirection of traffic either by replacing the destination's address altogether or by using a level of indirection in the addressing such as that achieved with tunnels and encapsulations. The different approaches affect applications to different degrees. The ultimate goal of IP mobility is to provide a solution that is totally transparent to the applications and allows the preservation of established sessions as endpoints move around the IP infrastructure.
- **Scalability:** Most techniques create a significant amount of detailed state information to redirect traffic effectively. The state information is necessary to correlate destination IP addresses with specific locations, either by means of mapping or translation. This additional state information must be handled in a very efficient manner to attain a solution that can support a deployable scale at a reasonable cost in terms of memory and processing.
- **Optimized routing:** As endpoints move around, traffic must be routed to these endpoints following the best possible path. Since mobility is based largely on redirection of traffic, the capability to provide an optimal path is largely a function of the location of the redirecting element. Depending on the architecture, the solution may generate suboptimal traffic patterns, often referred to as traffic triangulation, hairpinning, or tromboning in an attempt to describe the unnecessary detour that traffic needs to take when the destination is mobile. A good mobility solution can provide optimized paths regardless of the location of the endpoint.
- **Client independence:** The mobility solution must not depend on agents installed on the mobile endpoints or on the clients communicating with these endpoints. A network-based solution is highly desirable and is critical to the effective deployment of a mobility solution given a large installed base of endpoints that cannot be changed or managed at will to install client software.
- **Address-family agnostic:** The solution provided must work equally for IPv4 and IPv6 endpoints and networks. Since mobility relies on the manipulation of the mapping of identity to location, address families with longer addresses tend to provide alternatives not available with smaller address spaces. These address-dependent solutions have limited deployability because they usually call for an end-to-end deployment of IPv6. To cover the broad installed base of IPv4 networking resources and endpoints, the ideal solution should work for equally for IPv4 and IPv6 with no distinction between them.

Existing IP Mobility Solutions

Route Health Injection and Host Routing

One simple way to redirect traffic to a new location when a server (or group of servers) moves is to inject a more specific route to the moved endpoints into the routing protocol when the moves are detected. In the extreme case, this means injecting a host route from the landing location every time a host moves. Load balancers with the route health injection (RHI) function implemented on them can provide an automated mechanism for detecting server moves and inject the necessary host routes when the servers move.

This approach, although simple, pollutes the routing tables considerably and causes a large amount of churn in the routing protocol. Forcing churning of the routing protocol is a risky proposition as it can lead to instabilities and overall loss of connectivity, together with adding delays to roaming handoffs.

Mobile IPv4

Mobile IP is defined for IPv4 in IETF RFC 3344. Basically, mobile IPv4 provides a mechanism for redirecting traffic to a mobile node whenever this node moves from its home network to a foreign network. Every host has a home address within a home network that has a router front end that acts as a home agent and that advertises the home network to the routing protocol. Traffic destined for the home address will always be routed to the home agent. If the mobile node is in its home network, traffic will be forwarded directly to the host as in regular routing. If the host has moved to a foreign network, then traffic will be forwarded through IP tunneling by the home agent to an in-care-of address, which is the address of the gateway router for the foreign network.

With Mobile IPv4, a triangular traffic pattern always exists. Also, Mobile IPv4 does not offer a solution for multicast. Since the mobile node is usually sourcing traffic, if the foreign agent is not directly connected, host route injection is needed at the foreign site to get reverse-path forwarding (RPF) to work. In addition, multicast traffic from the mobile node always has to make a hairpin turn through the home agent since the distribution tree is built and rooted at the home agent.

Mobile IPv6

IETF RFC 3775 defines mobility support in IPv6. Mobile IPv6 goes beyond Mobile IPv4 by providing optimal data paths between the server and the client. The process in IPv6 is similar to that of IPv4 with a few additions.

Rather than having the home agent always redirect the traffic to the in-care-of address for the server that has moved, the home agent is taken out of the data path by distributing information about binding between the in-care-of address and the home address to the client itself. After the client has the in-care-of address information for a particular server, it can send traffic directly to the in-care-of address rather than triangulating it through the home address. This approach provides a direct path from the client to the server.

Although Mobile IPv6 provides direct path routing for mobile nodes, it is limited to IPv6-enabled endpoints, it requires that the entire data path be IPv6 enabled, and it requires that the endpoints have IPv6 mobility agents installed on them.

DNS-Based Redirection: Global Site Selector

You may be able to direct traffic to a moving server by updating the DNS entries for the moving server as the server moves locations. This scheme assumes that every time a server moves it is assigned a new IP address within the server's landing subnet. When the server moves, its DNS entry is updated to reflect the new IP address. Any new connections to the server will use the new IP address that is learned through DNS resolution. Thus, traffic is redirected by updating the mapping of the DNS name (identity) to the new IP address (location).

The new IP address assigned after the move may be assigned directly to the server, or it may be a new virtual IP address on a load balancer at the front end of the server at the new location. When you use load balancers on each location, the load balancers can be used to determine the location of a host by checking the servers' health with probes. When a change of location is detected, the integration of workflow in VMware vCenter updates the global site selector (GSS) of the new virtual IP address for the server, and the GSS in turn updates the DNS system with the new mapping of the virtual IP address to the server name. Established connections will continue to try to reach the original virtual IP address, so the load balancers must be able to redirect those connections to the new host location and create a hairpinned traffic pattern for the previously established connections. New connections will be directed to the new virtual IP address (assuming that the DNS cache has been updated on the client) and will follow a direct path to this new virtual IP address. Eventually, all old connections are completed, and there are no hair pinned flows.

The main limitations of this approach include the following:

- The refresh rate for the DNS cache may affect either the convergence time for the move or the scalability of the DNS system if the rate is too high.
- This approach works only for name-based connections, but many applications are moving to an IP-based connection model.
- Previously established connections are hairpinned, which implies that there is a period of time in which there are active connections to the old address and some new connections to the new address in the second data center. During this state the network administrator may not be able to ascertain that these two addresses are the same system (from the point of view of the application).

Document Use Prerequisites

This document assumes that the reader has prior knowledge of LISP and its network components. For detailed information about LISP components and their roles, operation, and configuration, refer to <http://www.cisco.com/go/lisp> and the [Cisco LISP Configuration Guide](#). To help the reader of this document, the basic fundamental LISP components are discussed here.

LISP uses a dynamic tunneling encapsulation approach rather than requiring preconfiguration of tunnel endpoints. It is designed to work in a multihoming environment and supports communications between LISP and non-LISP sites for interworking. A LISP-enabled network includes some or all of the components described here.

LISP Name Spaces

- **Endpoint Identifier (EID) addresses:** EID addresses consist of the IP addresses and prefixes identifying the endpoints. EID reachability across LISP sites is achieved by resolving EID-to-RLOC mappings.
- **Route Locator (RLOC) addresses:** RLOC addresses consist of the IP addresses and prefixes identifying the different routers in the IP network. Reachability within the RLOC space is achieved by traditional routing methods.

LISP Site Devices

- **Ingress Tunnel Router (ITR):** An ITR is a LISP site edge device that receives packets from site-facing interfaces (internal hosts) and encapsulates them to remote LISP sites or natively forwards them to non-LISP sites.
- **Egress Tunnel Router (ETR):** An ETR is a LISP site edge device that receives packets from core-facing interfaces (the Internet) and decapsulates LISP packets and delivers them to local EIDs at the site.

Note: Customer-edge devices typically implement ITR and ETR functions at the same time. When this is the case, the device is referred to as an xTR.

LISP Infrastructure Devices

- **Map-Server (MS):** A Map-Server is a LISP infrastructure device to which LISP site ETRs register with their EID prefixes. The Map-Server advertises aggregates for the registered EID prefixes to the LISP mapping system. All LISP sites use the LISP mapping system to resolve EID-to-RLOC mappings.
- **Map-Resolver (MR):** A Map-Resolver is a LISP infrastructure device to which LISP site ITRs send LISP Map-Request queries when resolving EID-to-RLOC mappings.
- **Proxy ITR (PITR):** A PITR is a LISP infrastructure device that provides connectivity between non-LISP sites and LISP sites by attracting non-LISP traffic destined for LISP sites and encapsulating this traffic for LISP sites. In the IPv6 transition case, the PITR can attract IPv6 non-LISP traffic and forward it to a LISP site using IPv4 as the transport.
- **Proxy ETR (PETR):** A PETR is a LISP Infrastructure device that allows IPv6 LISP sites that have only IPv4 RLOC connectivity to reach LISP and non-LISP sites that have only IPv6 RLOC connectivity.

EID namespace is used within the LISP sites for end-site addressing for hosts and routers. These EID addresses go in DNS records, just as they do today. Generally, EID namespace is not globally routed in the underlying Internet. RLOC namespace, however, is used in the (Internet) core. RLOCs are used as infrastructure addresses for LISP routers and core (service provider) routers and are globally routed in the underlying infrastructure, just as they are today. Hosts do not know about RLOCs, and RLOCs do not know about hosts.

The remainder of this document describes the LISP deployments that support common IP mobility use cases in the data center.

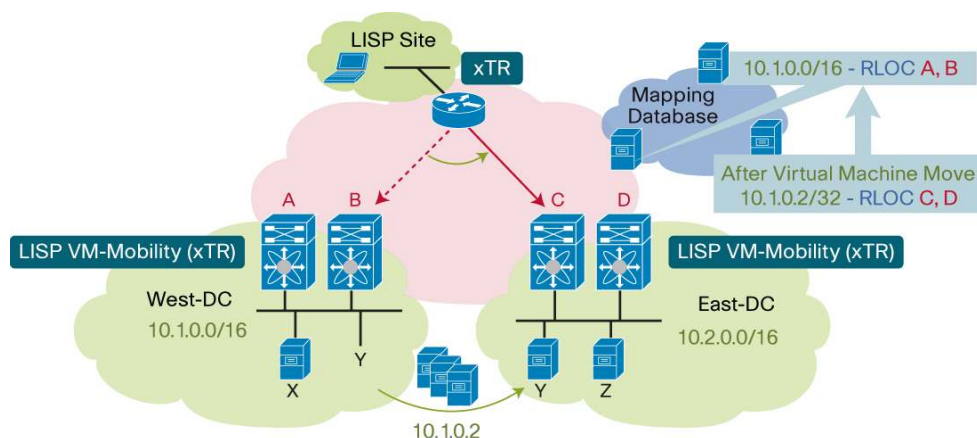
LISP VM-Mobility

The traditional IP addressing model associates both location and identity with a single IP address space, making mobility a very cumbersome process since identity and location are tightly bundled together. Because LISP creates two separate name spaces, that is, separates IP addresses into RLOCs and EIDs, and provides a dynamic mapping mechanism between these two address families, EIDs can be found at different RLOCs based on the EID-RLOC mappings. RLOCs remain associated with the topology and can be reached by traditional routing. However, EIDs can change locations dynamically and can be reached through different RLOCs, depending on where an EID attaches to the network. In a virtualized data center deployment, EIDs can be directly assigned to virtual machines, which are hence free to migrate between data center sites, preserving their IP addressing information.

The decoupling of identity from the topology is the core principle on which the LISP VM-Mobility solution is based. It allows the EID space to be mobile without affecting the routing that interconnects the RLOC IP space.

In the LISP VM-Mobility solution, virtual machine migration events are dynamically detected by the LISP xTR on the basis of data-plane events. When a move is detected, as illustrated in Figure 1, the mappings between EIDs and RLOCs are updated by the new xTR. By updating the RLOC-to-EID mappings, traffic is redirected to the new locations without causing any churn in the underlying routing.

Figure 1. A Virtual Machine Move Event Is Dynamically Detected by xTRs, and the New Location Is Updated in the LISP Mapping Database



LISP VM-Mobility detects moves by comparing the source in the IP header of traffic received from a host against a range of prefixes that are allowed to roam. These prefixes are defined as dynamic-EIDs in the LISP VM-Mobility solution.

When deployed at the first-hop router, LISP VM-Mobility provides adaptable and comprehensive first-hop router functions to service the IP gateway needs of the roaming devices that relocate.

LISP VM-Mobility Use Cases

LISP VM-Mobility is instrumental in providing location flexibility to IP endpoints within the data center network. By using LISP VM-Mobility, virtual machines and other endpoints can be deployed anywhere in the data center regardless of their IP addresses, and they can freely move across racks, rows, or even separate data center locations. This level of flexibility is critical in supporting the deployment scenarios and use cases listed in Table 1, in which IP endpoints must preserve their IP addresses to reduce startup time.

Table 1. Use Cases

Use Case	Requirements
Geoclusters	Optimized routing to IP subnets extended with Cisco OTV or Virtual Private LAN Service (VPLS)
Fast startup of disaster recovery facilities	Relocation of IP endpoints across different subnets
Cloud bursting	Relocation of IP endpoints across organizations

Figure 2 shows LISP VM-Mobility in an extended subnet between two enterprise-class data centers. The subnets and VLANs are extended from the West data center (West DC) to the East data center (East DC) using OTV or VPLS, or any other LAN extension technology. In traditional routing, this approach poses the challenge of ingress path optimization. LISP VM-Mobility provides transparent ingress path optimization by detecting the mobile EIDs (virtual servers) dynamically, and it updates the LISP mapping system with its current EID-RLOC mapping, which allows the virtual servers to be mobile between the data centers with ingress path optimization.

Figure 2. LISP VM-Mobility in an Extended Subnet Use Case

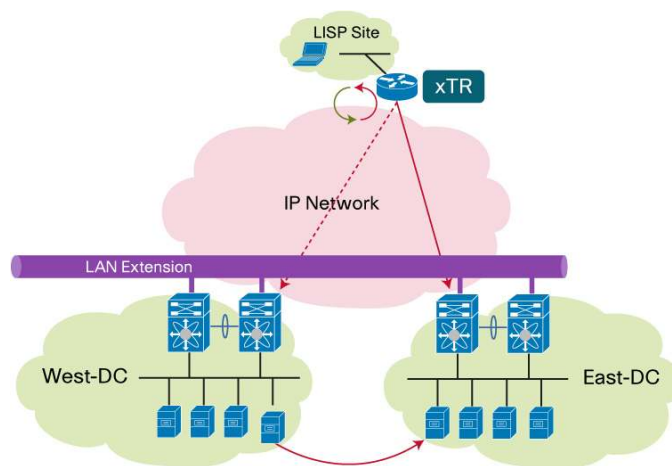
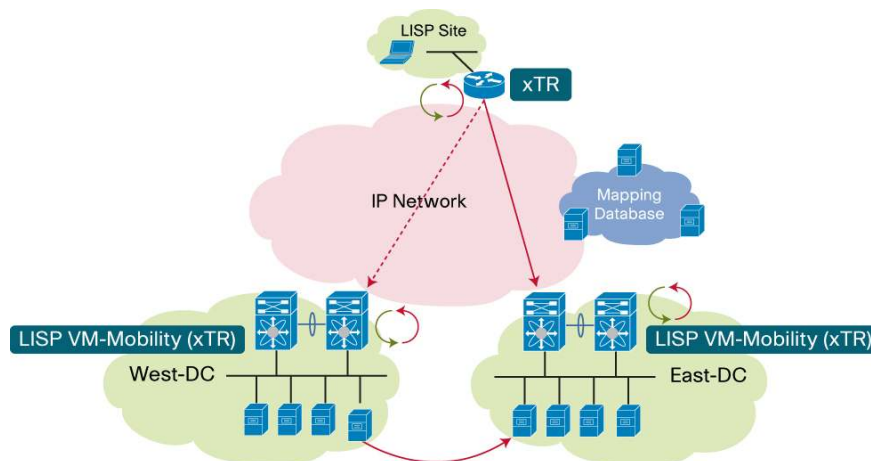


Figure 3 shows LISP VM-Mobility across subnets between two enterprise-class data centers. In this case, two different subnets exist, one in each data center, and subnet and VLAN extension techniques such as OTV and VPLS are not deployed. This mode can be used when an enterprise IT department needs to quickly start disaster recovery facilities when the network is not provisioned for virtual server subnets or, in case of cloud bursting, relocate EIDs across organization boundaries.

Figure 3. LISP VM-Mobility Across Subnets



These deployment scenarios address a variety of business needs, including:

- Improved application availability
- Streamlined disaster recovery procedures
- Flexible outsourcing options
- Increased resource utilization
- Flexible change management

This document discusses both of these modes in detail and provides configuration steps for each of the LISP network elements.

LISP VM-Mobility Prerequisites

- LISP VM-Mobility is supported in general Cisco NX-OS Software Release 5.2(1) or later. However, because of a problem that was discovered, you should deploy LISP VM-Mobility solutions using the upcoming Cisco NX-OS Release 5.2(3). An engineering build (Cisco NX-OS Release 5.2(1.lisp-r5-20)) containing the resolution for the problem can be downloaded from <http://lisp.cisco.com>. The configuration and show outputs contained in this document have been obtained using this specific Cisco NX-OS 5.2(1.lisp-r5-20) build.
- From a hardware perspective, LISP VM-Mobility is currently supported only in Cisco N7K-M132XP-12 and N7K-M132XP-12L line cards. The electrical programmable logical device (EPLD) upgrade to version 186.008 or later is required for these line cards.
- LISP VM-Mobility on the Cisco Nexus 7000 Series Switches can use Cisco F-Series modules for site-facing interfaces as long as one of the Cisco M-Series cards mentioned listed in the preceding paragraph is available. This requirement exists because only Cisco M1-32 line cards can perform LISP encapsulation and decapsulation in hardware, so Layer 2 traffic received on Cisco F1-Series interfaces must be internally sent to these Cisco M1-Series cards for that purpose. This function available on Cisco Nexus 7000 Series platforms is known as proxy mode.

Note: Only the Cisco F1-Series line cards support proxy mode at the time of writing of this document.

- Proxy mode is not supported between Cisco M-Series cards, so the site-facing interfaces can be only Cisco N7K-M132XP-12, N7K-M132XP-12L, or F-Series line cards.
- Traffic received on Cisco M-Series line cards other than the Cisco M132XP-12 cards will not be processed by LISP. Therefore, combining Cisco M132XP-12 cards with other Cisco M-Series cards in a LISP-enabled virtual device context (VDC) will result in two different types of traffic processing depending on which interface receives the traffic. In deployments in which other Cisco M-Series cards (N7K-M148GT-11, N7K-M148GT-11L, N7K-M148GS-11, N7K-M148GS-11L, or N7K-M108X2-12L) are part of the same VDC as the Cisco F1-Series and M1-32 cards, you must make sure that traffic received on any Cisco F1-Series interfaces is internally sent only to interfaces belonging to Cisco M1-32 cards. The **hardware proxy layer-3 forwarding use interface** command can be used to list only these specific interfaces to be used for proxy routing.

LISP VM-Mobility Operation

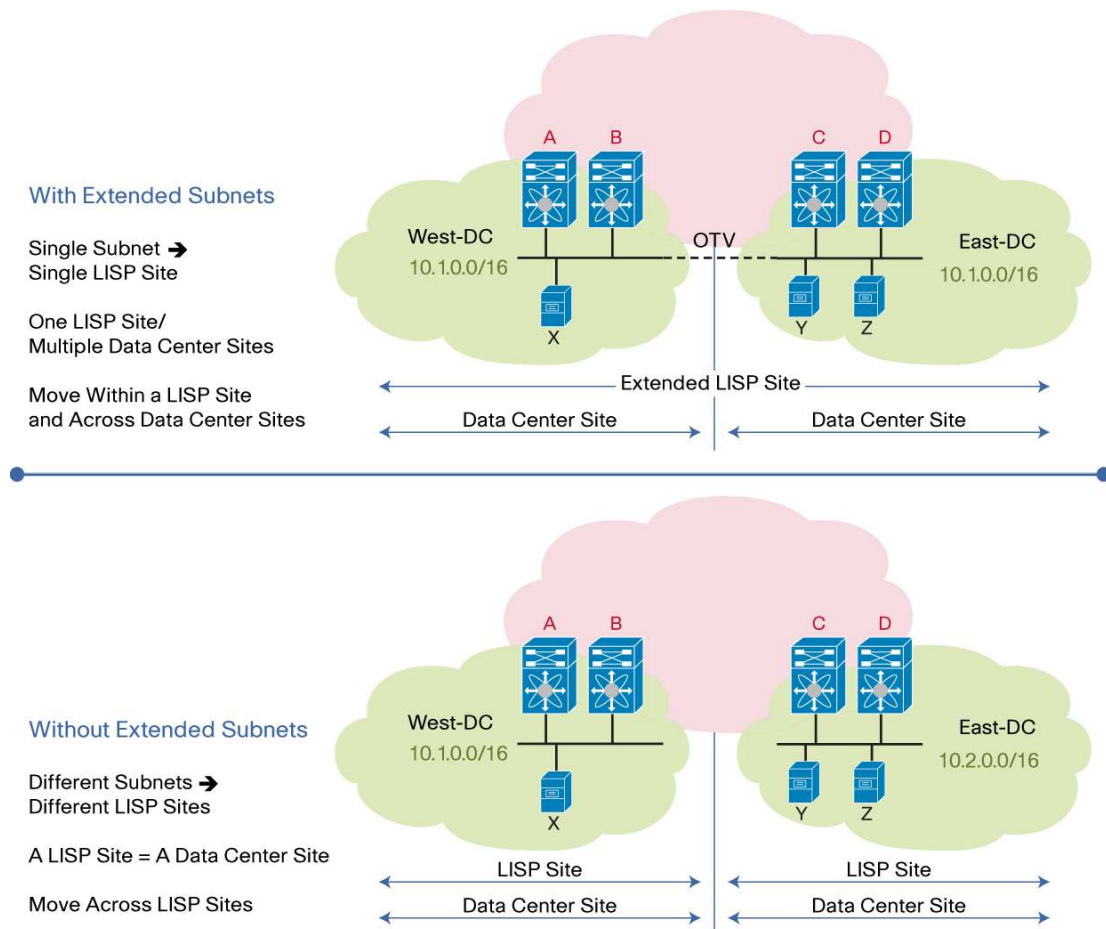
The LISP VM-Mobility function allows any IP addressable device (host) to move (or roam) from its subnet to a completely different subnet or to an extension of its subnet in a different location (for example, in a remote data center) while keeping its original IP address. In LISP terminology, a device that moves is called a roaming device, and its IP address is called its dynamic-EID. The LISP xTR configured with LISP VM-Mobility with a **dynamic-eid** clause is called a LISP-VM router. The **dynamic-eid** clause can represent one or more dynamic-EIDs. The LISP-VM router (xTR) devices dynamically determine when a dynamic-EID moves on or off one of its directly connected subnets. A LISP-VM router's IP addresses are the locators (RLOCs) used for encapsulation for traffic to and from the dynamic-EID.

Before exploring in more detail the mechanisms that allow a roaming device to move between physical locations, you should understand the concepts of LISP sites and data center sites and their relationship.

- LISP site: A logical construct composed of one or more EID prefixes that have a unique locator set
- Data center site: A physical construct composed of one or more xTRs participating in a LISP site
 - A LISP site is fully constituted by a single data center site when the EID prefixes and the unique locator set are wholly contained within that single data center site. In this case, a single data center site constitutes (and is equivalent to) an entire LISP site.
 - A LISP site is fully constituted by two or more data center sites when the EID prefixes and the unique locator set are contained among multiple data center sites. In this case, a single data center site constitutes a subset of the LISP site.
- Dynamic-EID: A host (physical or virtual machine) participating in LISP VM-Mobility that is capable of moving among multiple Layer 3 devices. When a dynamic-EID moves, the “moved-from” Layer 3 device and the “moved-to” Layer 3 device can have the exact same network prefix (and match that of the dynamic-EID), or the devices can have different network prefixes.
 - When the new (moved-to) Layer 3 device carries the same network prefix as that of the dynamic-EID, LISP VM-Mobility will be configured with **LISP_EXTENDED_SUBNET** commands and functions. When this is the case, a Layer 2 extension mechanism such as OTV must also be deployed.
 - When the new (moved-to) Layer 3 device carries a different network prefix from that of the dynamic-EID, LISP VM-Mobility will be configured with **LISP_ACROSS_SUBNET** commands and functions. When this is the case, a Layer 2 extension mechanism such as OTV is not required.

As shown in Figure 4, when OTV (or another LAN extension mechanism) is deployed to stretch a VLAN and IP subnet between separate physical locations, a single LISP site is defined as extending across two physical data center sites. However, if LISP is deployed without the support of a LAN extension function, you end up with separate LISP sites, each one mapped to a given physical data center site.

Figure 4. LISP Site and Data Center Site



The differences between these two deployments are described in detail in the following sections of this document, specifically when describing the configuration for each model.

Dynamic-EID Detection and Map Updates

This section describes the operation of the dynamic-EID detection mechanism and the update processes after a mobility event is detected. When a dynamic-EID roams, four types of updates need to take place as a result of the mobility event:

- The new LISP-VM router needs to detect the newly moved virtual machine. The new LISP-VM router refers to the xTR at which the dynamic-EID lands. It needs to register the /32 prefix for the dynamic-EID using its locators.
- The old LISP-VM router (xTR) that previously registered the EID needs to be notified of the move.
- The Map-Server needs to know the new locators for the EID.
- The remote ITRs and PITRs that have the dynamic-EID cached with old RLOC mapping need to be updated with the new mapping.

The LISP xTR configured as a LISP-VM router detects new dynamic-EID VM move events if:

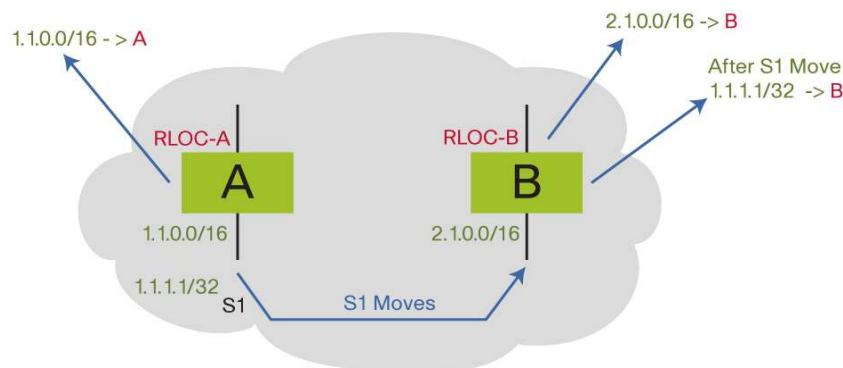
- It receives a data packet from a source (the newly arrived virtual machine) that is not on the configured subnets for that interface
- The source matches the dynamic-EID configuration applied to the interface

In the case of an extended subnet, the LISP-VM router interfaces are configured with the **lisp extended-subnet-mode** command. In this case, the LISP-VM router detects new virtual machine move events if it receives a data packet from a source that matches the dynamic-EID configured for that interface. This dynamic EID move detection by the LISP-VM router will trigger a Map-Register event to the Map-Server with the database mapping details from the dynamic-EID map configuration. Note that in the current implementation, an EID discovered in the extended subnet mode remains in the dynamic-EID table of the xTR device (LISP-VM router) until it moves to a separate data center site, independent of whether it may have gone silent or even become disconnected (in that case, the dynamic-EID table can be manually cleared).

In the across-subnet mode, the LISP-VM router continues to check for the existence of any previously discovered EID (a liveness check is performed by pinging the EID). An EID would hence be removed from the dynamic-EID table only if it becomes disconnected from the network (and not if it just stops sending traffic).

Consider Figure 5. If EID S1-1.1.1.1 roams to LISP-VM router B, router B will detect this move if it receives any data packet from subnet S1, because it is off-subnet traffic. Also, router B will register the EID prefix 1.1.1.1/32 with locator RLOC-B for the configured Map-Servers associated with the configured dynamic-EID. This registration is required so that packets can now be encapsulated to RLOC-B instead of RLOC-A for the host that has moved away.

Figure 5. Dynamic-EID Movement



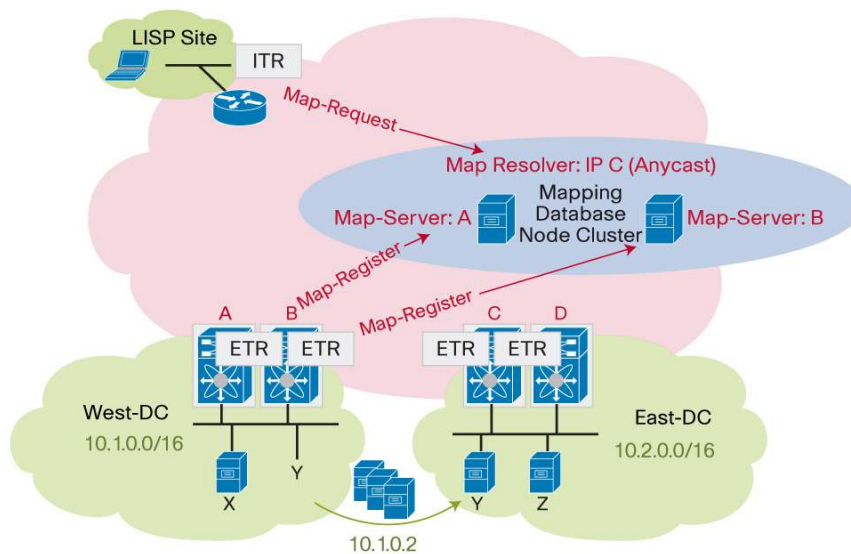
Map-Server and Map-Resolver Considerations

The Map-Server and Map-Resolver are critical components in a LISP deployment. They provide capabilities to store and resolve the EID-to-RLOC mapping information for the LISP routers to enable routing between LISP sites.

The Map-Server is a network infrastructure component that learns EID-to-RLOC mapping entries from ETRs, which are authoritative sources and which publish (register) their EID-to-RLOC mapping relationships with the Map-Server. A Map-Resolver is a network infrastructure component that accepts LISP-encapsulated Map-Requests, typically from an ITR, and finds the appropriate EID-to-RLOC mapping by checking with a co-located Map-Server (typically) or by consulting the distributed mapping system.

This section discusses Map-Server and Map-Resolver deployment considerations for an enterprise data center LISP deployment. Note that you should deploy redundant standalone coexistent Map-Servers and Map-Resolvers. When redundant standalone Map-Servers and Map-Resolvers are deployed, all xTRs must register with both Map-Servers so that each has a consistent view of the registered LISP EID namespace. For Map-Resolver functions, use of an anycast address is desirable, because it will improve mapping lookup performance by choosing the Map-Resolver that is topologically closest to the requesting ITR. The topology in Figure 6 shows this deployment model.

Figure 6. Redundant Standalone Map-Servers and Map-Resolvers



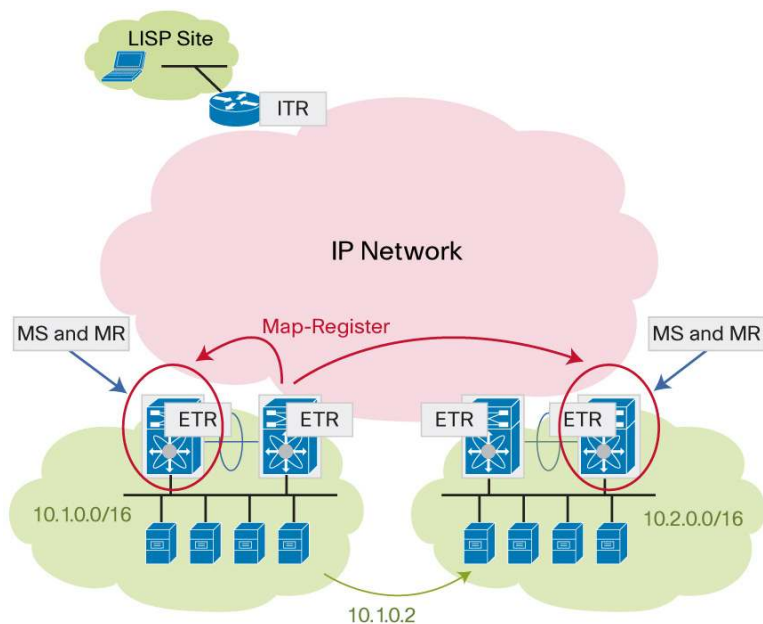
This document focuses only on a single standalone co-located Map-Server and Map-Resolver.

Note: The scenarios explored in this document focus on the case in which the Map-Server and Map-Resolver functions are located in the same network device. This document also focuses on a simple use case that does not require a distributed mapping database. Redundancy of the mapping database will be discussed but should not be confused with the distribution of the mapping database.

Note: For large-scale LISP deployments, the mapping database can be distributed and Map-Server and Map-Resolver functions dispersed onto different nodes. The distribution of the mapping database can be achieved in many ways; LISP-ALT is one example, but there are many approaches that can be used. Large-scale LISP deployments using distributed mapping databases are not discussed in this document.

Note that you could deploy a redundant standalone Map-Server and Map-Resolver model by using dedicated systems to perform the mapping functions (as shown in Figure 6) or by locating the Map-Server and Map-Resolver functions on the same network device already performing the xTR role (Figure 7).

Figure 7. Co-locating Map-Server and Map-Resolver and xTR Functions

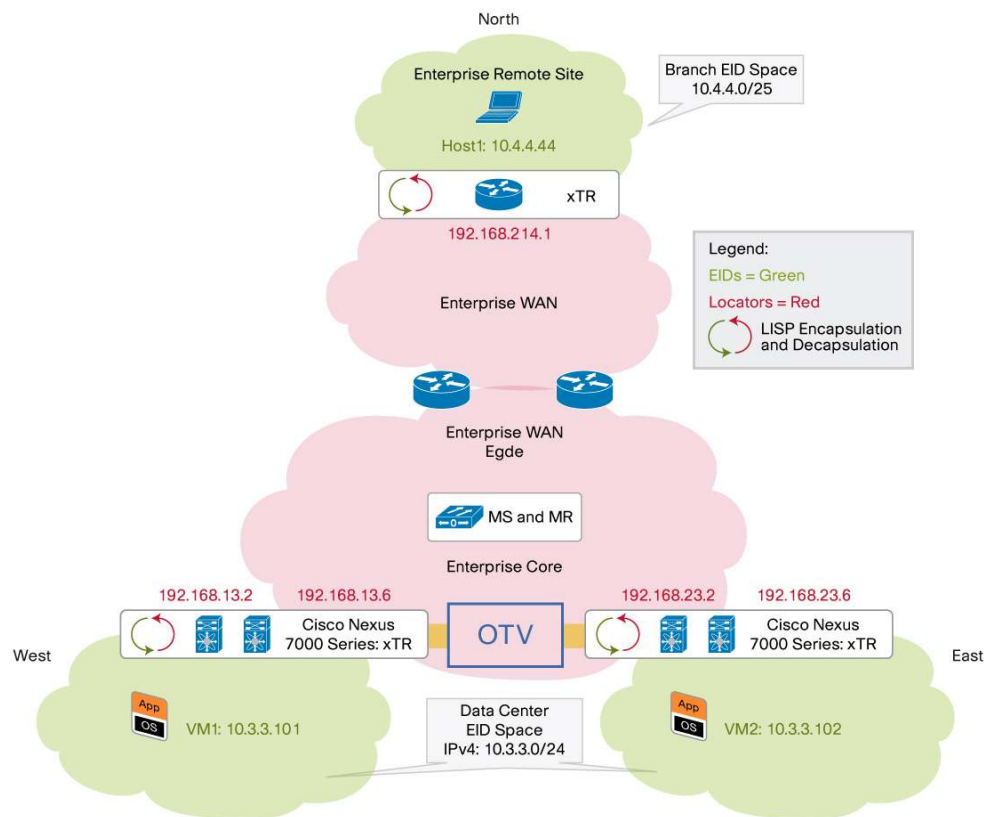


The co-located model shown in Figure 7 is particularly advantageous because it reduces the overall number of managed devices required to roll out a LISP VM-Mobility solution. Notice that the required configuration in both scenarios would remain identical, using unique IP addresses to identify the Map-Servers and an anycast IP address for the Map-Resolver.

Deploying LISP VM-Mobility in an Extended Subnet

Figure 8 shows an enterprise data center deployment topology in which the 10.3.3.0/24 subnet in VLAN 904 is extended between the West and East data centers using OTV and Cisco Nexus 7000 Series data center switches. The remote site is configured with a Cisco IOS® Software device hosting the 10.4.4.0/24 network. The Map-Server is deployed in the enterprise core. This section describes steps to configure these data center sites and remote Cisco IOS Software device sites as LISP sites with corresponding EID spaces. This section also describes the configuration required to enable configured prefix hosts to move between data centers.

Figure 8. Enterprise Data Center Extended Subnet Topology



LISP VM-Mobility in an Extended Subnet Prerequisites

- OTV or any other deployed LAN extension solution should filter the Hot Standby Router Protocol (HSRP) hello messages across the data centers, creating an active-active HSRP setup. This setup is mainly needed to provide an active default gateway in each physical data center location and to avoid asymmetric traffic handling when optimizing ingress traffic with LISP (HSRP localization handles only the egress flows). For more information about how to achieve HSRP localization when deploying OTV, please refer to http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns949/ns304/ns975/OTV_intro_wp.pdf.
- The default gateway virtual MAC and IP addresses in both data centers should remain consistent, because the mobile virtual machine will continue to send packets to the same gateway IP address. Virtual MAC address consistency is achieved by configuring the same HSRP group associated with the same subnet in separate data center sites.
- OTV or any other deployed LAN extension solution should have multicast support over the extended Layer 2 circuit for the proper operation of LISP VM-Mobility in the extended subnet mode.

Configuring a Cisco Nexus 7000 Series Switch as a LISP xTR

Enter the commands shown here to enable and configure LISP ITR and ETR (xTR) functions on a Cisco Nexus 7000 Series switch.

Configuration Commands

1. **configure terminal**
2. **feature lisp**
3. **ip lisp itr-etr**
4. **ip lisp database-map EID-prefix/prefix-length locator_ip priority priority weight weight**
5. **ip lisp etr map-server map-server-address key key-type authentication-key**
6. **ip lisp itr map-resolver <map-resolver-address>**
7. **exit**

Steps	Cisco NX-OS Commands	Purpose
Step 1	configure terminal	Enters global configuration mode
Step 2	feature lisp	Enables the LISP feature set (if it is not already configured) To obtain a grace period for lab experiments on LISP, use the license grace-period command. See the section Licensing Cisco NX-OS Software Features in the Cisco NX-OS Licensing Guide.
Step 3	ip lisp itr-etr	Enables LISP ITR and ETR functions for the IPv4 address family
Step 4	ip lisp database-mapping EID-prefix/prefix-length locator_ip priority priority weight weight	Configures an EID-to-RLOC mapping relationship and associated traffic policy for all IPv4 EID prefixes for this LISP site Note: If the site is assigned multiple EID prefix blocks, the ip lisp database-mapping command is configured for each EID prefix block assigned to the site and for each locator from which the EID prefix block can be reached. (Optional) Multihoming Considerations If the site has multiple locators associated with the same EID-prefix block, multiple ip lisp database-mapping commands are entered to configure all the locators for a given EID prefix block. In the extended subnet mode, all the xTRs belonging to the same LISP site (multiple separate data center sites) must be configured with consistent ip lisp database-mapping commands, listing the RLOCs of all the deployed xTRs that are part of the same LISP site.
Step 5	ip lisp etr map-server map-server-address key key-type authentication-key	Configures the IP address of the LISP Map-Server to which this router, acting as an IPv4 LISP ETR, will register When you are deploying a redundant pair of Map-Servers, one command per Map-Server is required.
Step 6	ip lisp itr map-resolver <map-resolver-address>	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 When you are deploying a redundant pair of Map-Resolvers, a single command is needed here, pointing to the anycast IP address that identifies both Map-Resolvers.
Step 7	exit	Exits the configuration mode

Configuring a Cisco Nexus 7000 Series Switch LISP xTR for Dynamic-EID Roaming

Enter the commands shown here to enable and configure dynamic-EID roaming functions for a given EID prefix on a Cisco Nexus 7000 Series Switch. By default, LISP assumes that the mobility event is across the subnet unless it is configured with the **lisp extended-subnet-mode** command.

Configuration Commands

1. **configure terminal**
2. **lisp dynamic-eid** <dynamic-eid-map-name>
3. **database-mapping** EID □ prefix/prefix □ length locator_ip **priority** priority **weight** weight
4. **map-notify-group** <multicast-group-ip>
5. **map-server** map □ server □ address **key** key □ type authentication □ key (This command is optional. It registers a dynamic-EID to a specific Map-Server other than the one configured in the global LISP configuration. If this command is not configured, LISP uses the Map-Server configured in the global configuration.)
6. **exit**
7. **interface** <interface-name>
8. **lisp mobility** <dynamic-eid-map-name>
9. **lisp extended-subnet-mode**
10. **exit**

Steps	Cisco NX-OS Commands	Purpose
Step 1	configure terminal	Enters the global configuration mode
Step 2	lisp 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 3	database-mapping EID □ prefix/prefix □ length locator_ip priority priority weight weight	Configures a dynamic-EID range, the RLOC mapping relationship, and the associated traffic policy for all IPv4 dynamic-EID prefixes for this LISP site 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. Note: If the site is assigned multiple dynamic-EID prefix blocks, the database mapping is configured for each dynamic-EID prefix block assigned to the site and for each locator from which the EID prefix block can be reached. Also, the subnet associated with the dynamic-EID prefixes must be more specific than the one used in the global database mapping configuration and the one used for the switch virtual interfaces (SVIs) on which the LISP map is applied. (Optional) Multihoming Considerations If the site has multiple locators associated with the same EID prefix block, multiple database mapping commands are entered to configure all the locators for a given EID prefix block. If a site is multihomed, all xTRs belonging to the same data center site must be configured with consistent database-mapping commands. In contrast to the ip lisp database-mapping command, only the RLOCs of the xTRs belonging to the same data center site should now be specified (and not the RLOCs for all the xTRs belonging to the same LISP site).
Step 4	map-notify-group <multicast-group-ip>	In the LISP extended subnet mode, sends a message noting dynamic-EID detection by one xTR to all the xTRs belonging to the same LISP site (that is, deployed across data center sites that are connected at Layer 2 through LAN extension technology) In such a case, configure the map-notify-group command in the dynamic-EID map with a multicast group IP. This address is used to send a Map-Notify message from the xTR to all other xTRs after a dynamic-EID is detected. The time-to-live (TTL) value for this notification message is set to 1. This multicast group IP address can be anything the user wants other than an address that is already in use in the user network. The multicast message is delivered using the LAN extension connection established between separate data center sites.

Steps	Cisco NX-OS Commands	Purpose
Step 5	map-server map□server□address key key□type authentication□key	(Optional) Configures the IP address of the LISP Map-Server to which this router will register dynamic-EID-to-RLOC mappings When you are deploying a redundant Map-Server pair, you can specify both IP addresses here. This configuration step is optional. You can use it to register dynamic-EID-to-RLOC mapping to a specific Map-Server other than the one configured in the global LISP configuration. If this command is not configured, LISP uses the Map-Server configured in the global configuration.
Step 6	exit	Exits the configuration mode
Step 7	interface <interface-name>	Enters the interface configuration mode The interface-name entry is the name of the interface to which or from which the dynamic-EIDs are expected to roam. SVIs are specifically used in this scenario.
Step 8	lisp mobility <dynamic-eid-map-name>	Configures the interface in Step 7 to allow a dynamic-EID to be detected when a roam event occurs The dynamic-eid-map-name entry is the dynamic-EID map name configured in Step 2.
Step 9	lisp extended-subnet-mode	Configures the interface in Step 7 to accept and detect dynamic-EID roaming on extended subnets
Step 10	exit	Exits the configuration mode.

Configuring a Remote Site Cisco IOS Software Router as a LISP xTR

Enter the commands shown here to enable and configure LISP ITR and ETR (xTR) functions on a Cisco IOS Software router.

Configuration Commands

1. **configuration terminal**
2. **router lisp**
3. **ipv4 itr**
4. **ipv4 etr**
5. **database□mapping** EID□prefix/prefix□length locator_ip **priority** priority **weight** weight
6. **ipv4 etr map□server** map□server□address **key** authentication-key
7. **ipv4 lisp itr map-resolver** <map-resolver-address>
8. **exit**

Steps	Cisco IOS Software Commands	Purpose
Step 1	configure terminal	Enters global configuration mode
Step 2	router lisp	Enables and enters the router LISP configuration mode
Step 3	ipv4 lisp itr	Enables LISP ITR functions for the IPv4 address family
Step 4	ipv4 lisp etr	Enables LISP ETR functions for the IPv4 address family
Step 5	database-mapping EID□prefix/prefix□length locator_ip priority priority weight weight	Configures an EID-to-RLOC mapping relationship and associated traffic policy for all IPv4 EID prefixes for this LISP site Note: If the site is assigned multiple EID prefix blocks, the IP LISP database mapping is configured for each EID prefix block assigned to the site and for each locator from which the EID prefix block can be reached. (Optional) Multihoming Considerations If the site has multiple locators associated with the same EID prefix block, multiple database-mapping commands are entered to configure all the locators for a given EID prefix block. If a site is multihomed, all ETRs must be configured with consistent database-mapping commands.

Steps	Cisco IOS Software Commands	Purpose
Step 6	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 As usual, two separate statements may be needed.
Step 7	ipv4 lisp itr map-resolver <map-resolver-address>	Configures the IP address of the LISP Map-Resolver to which this router, acting as an IPv4 LISP ITR, will send a LISP Map-Request for destination EIDs
Step 8	exit	Exits the configuration mode

Configuring a LISP Map-Server and Map-Resolver on Cisco NX-OS

This section describes an enterprise-class solution in which the Map-Server and Map-Resolver are located on the same network device. Enter the commands shown here to enable and configure LISP Map-Server and Map-Resolver functions for IPv4 address families on a Cisco Nexus 7000 Series switch running Cisco NX-OS. As mentioned in the “Map-Server and Map-Resolver Considerations” section, when deploying a redundant pair of Map-Server and Map-Resolver nodes, each Map-Server will be identified with its own IP address, whereas the two Map-Resolvers will use the same anycast IP address.

Configuration Commands

1. configure terminal
2. feature lisp
3. ip lisp map-server
4. ip lisp map-resolver
5. lisp site site-name
6. description
7. authentication-key key-type password
8. eid-prefix {EID-prefix } accept-more-specifics
9. exit

Steps	Cisco IOS Software Commands	Purpose
Step 1	configure terminal	Enters the global configuration mode
Step 2	feature lisp	Enables the LISP feature set (if it is not already configured) For Cisco NX-OS only, to obtain a grace period for lab experiments on LISP, enter license grace-period . See the section Licensing Cisco NX-OS Software Features in the Cisco NX-OS Licensing Guide.
Step 3	ip lisp map-server	Enables LISP Map-Server functions for the IPv4 address family
Step 4	ip lisp map-resolver	Enables LISP Map-Resolver functions for the IPv4 address family
Step 5	lisp site site-name	Creates the indicated LISP site and enters the LISP site configuration mode
Step 6	description description	Enters a description for the LISP site being configured
Step 7	authentication-key key-type password	Enters the authentication key type and password for the LISP site being configured Note: The password must match the one configured on the ETRs for the ETRs to register successfully.
Step 8	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 with this command.
Step 9	Exit	Exits the configuration mode

LISP VM-Mobility in an Extended Subnet: Configuration Example

Figure 9 shows a network setup with West and East data centers. The West data center hosts servers and services in the 10.3.0.0/16 network. VLAN 904, serving the 10.3.3.0/24 network, is extended between these two data centers using OTV or another LAN extension technology. This configuration makes the two data center sites a single LISP site.

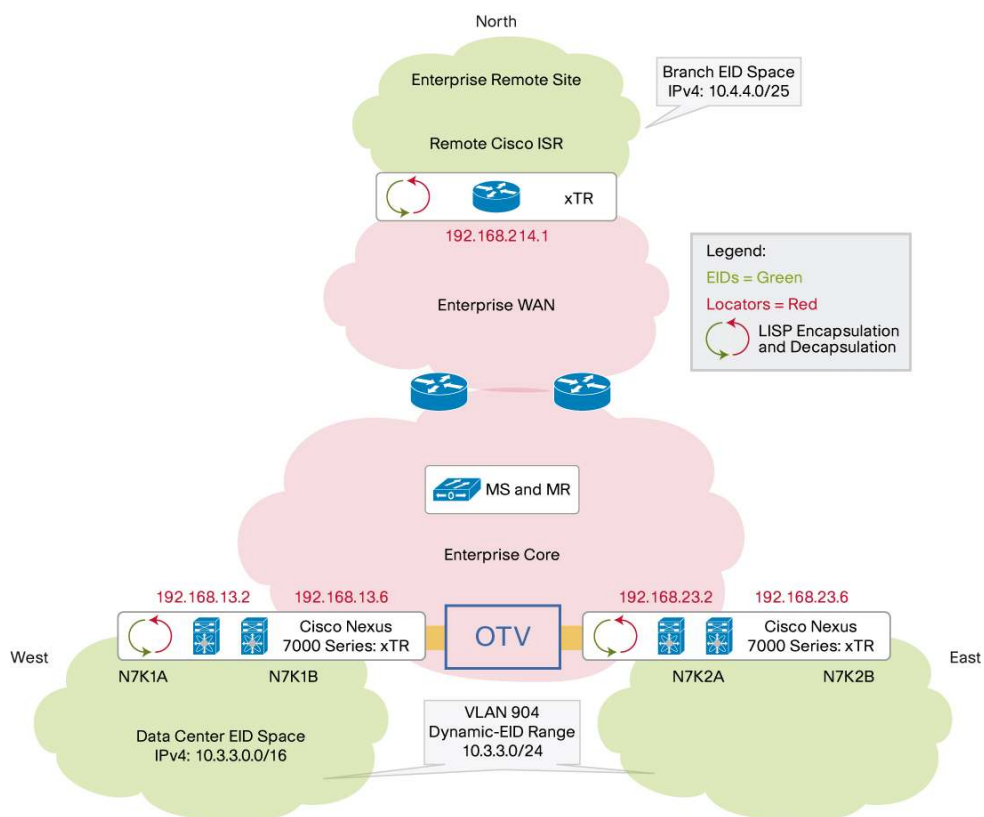
The workloads in VLAN 904 are moved between these two data centers, depending on the traffic patterns or business needs. The network 10.3.3.0/24 is configured as the dynamic-EID space in both data center xTRs, and the mobility events are dynamically detected and registered to the LISP mapping system by the data center LISP xTRs.

The 10.3.0.0/16 network is configured as the global LISP EID space on all the xTRs devices belonging to the same LISP site (that is, that are part of both the West and East data centers).

Both data centers are multihomed to the core, and HSRP is configured on VLAN 904 to serve the hosts. As a prerequisite for the LISP VM-Mobility solution, OTV is configured to filter HSRP hello messages over OTV between the data centers, creating an active-active HSRP domain. The same HSRP group is configured for the same subnet for the two data center sites to help automatically ensure availability of a consistent virtual MAC (vMAC) address for the default gateway.

The remote site is deployed with a Cisco Integrated Services Router (ISR) configured as a LISP ITR or ETR, and it hosts the 10.4.4.0/24 EID space. This section presents a configuration example for this setup for each component.

Figure 9. LISP VM-Mobility in an Extended Subnet: Configuration Example



Cisco Nexus 7000 Series N7K1A West Data Center xTR Configuration Example

```
feature lisp
ip lisp itr-etr
ip lisp database-mapping 10.3.0.0/16 192.168.13.2 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.13.6 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.23.2 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.23.6 priority 1 weight 25
ip lisp itr map-resolver 10.111.10.14
ip lisp etr map-server 10.111.10.14 key 0 cisco
!
lisp dynamic-eid LISP_EXTENDED_SUBNET
  database-mapping 10.3.3.0/25 192.168.13.2 priority 1 weight 50
  database-mapping 10.3.3.0/25 192.168.13.6 priority 1 weight 50
  map-notify-group 239.1.1.2
!
interface Vlan904
  ip address 10.3.3.2/24
  lisp mobility LISP_EXTENDED_SUBNET
  lisp extended-subnet-mode
  hsrp 100
    preempt delay minimum 300
    priority 200
  ip 10.3.3.1
```

Cisco Nexus 7000 Series N7K1B West Data Center xTR Configuration Example

```
feature lisp
ip lisp itr-etr
ip lisp database-mapping 10.3.0.0/16 192.168.13.2 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.13.6 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.23.2 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.23.6 priority 1 weight 25
ip lisp itr map-resolver 10.111.10.14
ip lisp etr map-server 10.111.10.14 key 0 cisco
!
lisp dynamic-eid LISP_EXTENDED_SUBNET
  database-mapping 10.3.3.0/25 192.168.13.2 priority 1 weight 50
  database-mapping 10.3.3.0/25 192.168.13.6 priority 1 weight 50
  map-notify-group 239.1.1.2
!
interface Vlan904
  ip address 10.3.3.3/24
  lisp mobility LISP_EXTENDED_SUBNET
  lisp extended-subnet-mode
  hsrp 100
    priority 190
```



```
ip 10.3.3.1
```

In the extended subnet mode a single LISP site spans separate data center locations, so each xTR device is configured identically for the global **ip lisp database-mapping** configuration, and the RLOCs for all the xTRs belonging to the same LISP site must be listed.

This requirement is not needed for the **dynamic-eid** portion of the configuration, in which only the RLOCs of the xTRs belonging to the same physical data center site must be listed. Notice also that in the preceding example, the same priority and weight were configured for each defined RLOC (default behavior). If you want, you can modify these parameters if the goal is not to load-balance incoming LISP traffic from other xTRs.

Important: You must make sure that the prefixes specified in the dynamic-EID portion of the configuration are more specific (from a subnet mask point of view) than the ones configured in the global **ip lisp database-mapping** section. Also, the dynamic-EID prefixes need to be more specific than the subnet mask configured on the Layer 3 interface on which the dynamic-EID map is applied (SVI 904 in the preceding example). In the example, /16 was the mask associated with the prefix in the global mapping, /24 was used as mask for the IP subnet associated with the SVI, and /25 was used in the dynamic-EID mapping.

Also, note that the map notification between multihomed xTRs is performed through multicast addressing. In the extended subnet mode, multicast support over the LAN extension (OTV or any other data center interconnect [DCI]) is required for proper operation. For this to be possible, you must use the same multicast address (for each defined dynamic-EID prefix) across all the xTR devices belonging to the same LISP site (239.1.1.2 in the preceding example hence is deployed on the xTRs belonging to data center sites 1 and 2).

Cisco Nexus 7000 Series N7K2A East Data Center xTR Configuration Example

The East data center xTRs are configured similarly as the West data center xTRs. Also notice the HSRP group and HSRP virtual IP configurations for the West and East data center xTRs. The configurations need to be identical in both data centers, so when the virtual machines move between these data centers, they continue to send traffic to the same gateway IP and MAC addresses, and the Address Resolution Protocol (ARP) does not need to be reapplied during mobility events. This configuration helps ensure live moves and keeps the traffic stream to and from the virtual machine intact and transparent to the underlying network.

Notice also that the Map-Notify group associated with the dynamic-EID range is the same on all the xTR devices belonging to West and East data center sites. As clarified later, this setup is required because these devices belong to the same LISP site, and they need to share information (by exchanging multicast messages) about where all the discovered dynamic-EIDs are physically located.

Note: The East and West LISP xTR configurations are almost identical. The only difference is the IP address of SVI 904.

```
feature lisp
ip lisp itr-etr
ip lisp database-mapping 10.3.0.0/16 192.168.13.2 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.13.6 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.23.2 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.23.6 priority 1 weight 25
ip lisp itr map-resolver 10.111.10.14
ip lisp etr map-server 10.111.10.14 key 0 cisco
!
lisp dynamic-eid LISP_EXTENDED_SUBNET
  database-mapping 10.3.3.0/25 192.168.23.2 priority 1 weight 50
  database-mapping 10.3.3.0/25 192.168.23.6 priority 1 weight 50
  map-notify-group 239.1.1.2
!
interface Vlan904
  ip address 10.3.3.4/24
  lisp mobility LISP_EXTENDED_SUBNET
  lisp extended-subnet-mode
  hsrp 100
    preempt delay minimum 300
    priority 180
  ip 10.3.3.1
```

Cisco Nexus 7000 Series N7K2B East Data Center xTR Configuration Example

```
feature lisp
ip lisp itr-etr
ip lisp database-mapping 10.3.0.0/16 192.168.13.2 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.13.6 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.23.2 priority 1 weight 25
ip lisp database-mapping 10.3.0.0/16 192.168.23.6 priority 1 weight 25
ip lisp itr map-resolver 10.111.10.14
ip lisp etr map-server 10.111.10.14 key 0 cisco
!
lisp dynamic-eid LISP_EXTENDED_SUBNET
  database-mapping 10.3.3.0/25 192.168.23.2 priority 1 weight 50
  database-mapping 10.3.3.0/25 192.168.23.6 priority 1 weight 50
  map-notify-group 239.1.1.2
interface Vlan904
  ip address 10.3.3.5/24
  lisp mobility LISP_EXTENDED_SUBNET
  lisp extended-subnet-mode
  hsrp 100
    priority 170
  ip 10.3.3.1
```

Remote Site Cisco IOS Software xTR Configuration Example

The following example shows the configuration for a LISP site using a Cisco IOS Software router such as a Cisco ISR.

```
router lisp
database-mapping 10.4.4.0/25 192.168.214.1 priority 1 weight 100
ipv4 itr map-resolver 10.111.10.14
ipv4 itr
ipv4 etr map-server 10.111.10.14 key cisco
ipv4 etr
```

Cisco NX-OS Map-Server and Map-Resolver Configuration Example

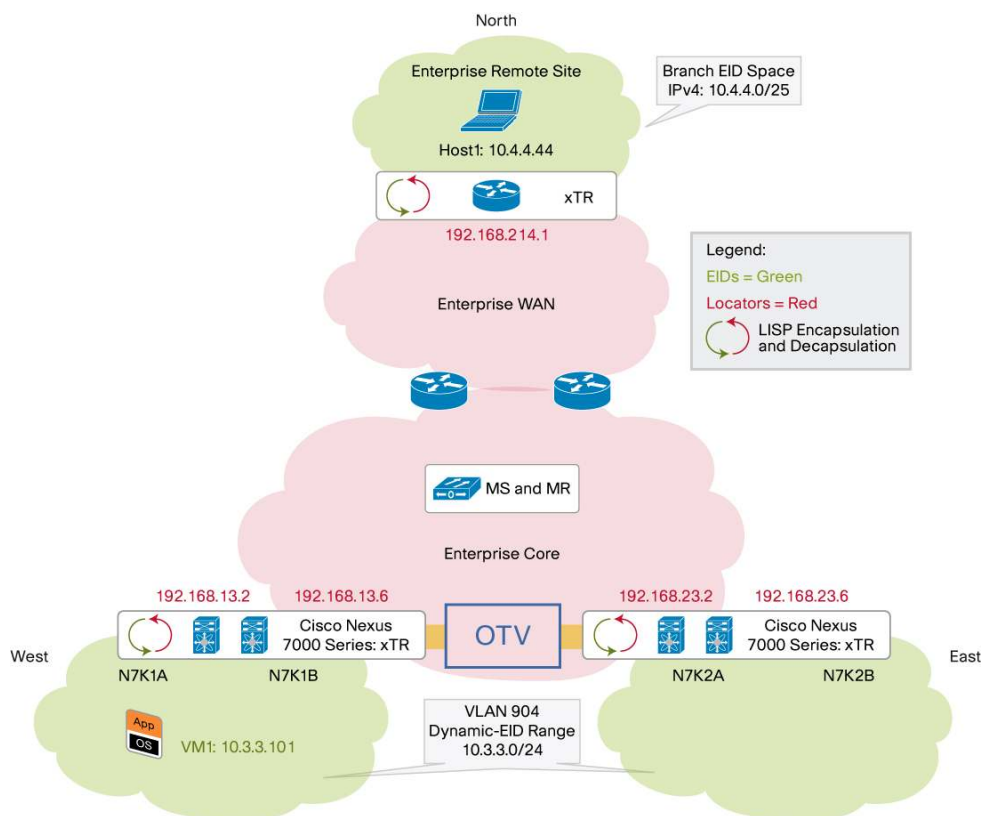
The following example shows the configuration for a LISP Map-Server and Map-Resolver on a Cisco NX-OS device.

```
feature lisp
!
ip lisp map-resolver
ip lisp map-server
!
lisp site BRANCH
  eid-prefix 10.4.4.0/25
  authentication-key 0 cisco
!
lisp site DATA_CENTER
  eid-prefix 10.3.0.0/16 accept-more-specifics
  authentication-key 0 cisco
```

LISP VM-Mobility in an Extended Subnet Verification

Figure 10 shows the same network setup used in the configuration examples, except a that a virtual machine in the West data center is talking to a host in the remote site. This section describes the verification steps for this scenario, including basic LISP operation, the dynamic-EID move and detection process, and path optimization by LISP.

Figure 10. Virtual Machine Talking to Remote Host



Verifying a Cisco NX-OS Map-Server

When the LISP components are configured according to the examples in the previous section, the Cisco Nexus 7000 Series multihomed data center xTRs and the Cisco IOS Software remote xTRs will register their configured EID spaces with the mapping system. Use the following steps to verify the xTRs' map registration for their respective EID spaces with their RLOC IP addresses.

Step 1. Enter **show lisp site** to display the LISP sites and their registration status.

```

MB1-CORE-LISP-MS1# show lisp site
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address, -x = more-specifics count

Site Name      Last      Actively   Who last    EID-prefix
                Registered Registered Registered
DATA_CENTER    00:00:20  yes       192.168.23.6  10.3.0.0/16-1
BRANCH         00:00:36  yes       192.168.214.1 10.4.4.0/25
MB1-CORE-LISP-MS1#
  
```

Note that the fourth field in the preceding output will change periodically depending on the periodic registrations from xTR devices belonging to the same LISP site. Also, the output for dynamic-EID prefix 10.3.0.0/16 highlights the existence of a more specific prefix (10.3.0.0/16-1) associated with an endpoint that has been dynamically discovered (specific information about this configuration is shown in Step 3).

Step 2. To view the site-specific EID registration status, enter **show lisp site <site-name>**.

```
MB1-CORE-LISP-MS1# show lisp site DATA_CENTER
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address, -x = more-specifics count

Site name:      "DATA_CENTER"
Description: none configured
Allowed configured locators: any
Configured EID-prefix: 10.3.0.0/16, instance-id: 0
  More-specifics registered: 1
  Currently registered:      yes
  First registered:          02:47:33
  Last registered:           00:00:03
  Who last registered:       192.168.23.6
  Routing table tag:         0x00000000
  Proxy Replying:           no
  Wants Map-Notifications:   yes
  Registering as a LISP-MN:   no
  Registered TTL:            1440 minutes
Registered locators:
  192.168.23.2, port: 47062 (up), priority: 1, weight: 25
  192.168.23.6, port: 47062 (up), priority: 1, weight: 25
  192.168.13.2, port: 47062 (up), priority: 1, weight: 25
  192.168.13.6, port: 47062 (up), priority: 1, weight: 25
Registration errors:
  Authentication failures: 0
  Allowed locators mismatch: 0
Registered locators:      none
Registration errors:
  Authentication failures: 0
  Allowed locators mismatch: 0
MB1-CORE-LISP-MS1#
```

In the preceding example, note that since data center xTRs in the West and East data centers are part of the same LISP site, they will register all RLOC IP addresses for their EID spaces.

Step 3. In LISP VM-Mobility, the dynamic-EID must be detected as part of a specific data center site, so the remote sites can send packets to the virtual machine's current location. Enter **show lisp site <dyn-eid-ip>** to verify that the data center xTR has registered the virtual machine's current locators.

```

MB1-CORE-LISP-MS1# show lisp site 10.3.3.101/32
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address, -x = more-specifics count

Site name:      "DATA_CENTER"
Description: none configured
Allowed configured locators: any
  Requested EID-prefix: 10.3.3.101/32, instance-id: 0
    Currently registered:      yes
    First registered:          00:20:19
    Last registered:           00:00:50
    Who last registered:       192.168.13.2
    Routing table tag:         0x00000000
    Proxy Replying:           no
    Wants Map-Notifications:   yes
    Registering as a LISP-MN:  no
    Registered TTL:            1440 minutes
  Registered locators:
    192.168.13.2, port: 47062 (up), priority: 1, weight: 50
    192.168.13.6, port: 47062 (up), priority: 1, weight: 50
  Registration errors:
    Authentication failures: 0
    Allowed locators mismatch: 0
MB1-CORE-LISP-MS1#

```

Verifying Cisco Nexus 7000 Series Data Center xTRs

If the end devices in the data center or at the remote site try to send traffic (for example, VM1 in the West data center and Host 1 in the North remote site), the xTRs will query the mapping system because they do not have native routes to the other sites. After the Map-Server receives the Map-Request from the xTR, it will forward the request to the last-registered RLOC (xTR). The ETR will reply to the Map-Request, and the ITRs that sent the Map-Request will populate their map cache tables. Subsequent packets between the sites are encapsulated and sent to RLOCs at the other sites. The receiving ITR will decapsulate the packet and deliver it to the destination.

Use the following steps to verify the information available on one of the Cisco Nexus 7000 Series data center xTRs:

Step 1. Enter **show ip route <remote-eid>** to verify that there is no native route present for the remote EID.

```

NX7K1A# show ip route 10.4.4.0/24 longer-prefixes
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
*** denotes best mcast next-hop
'[x/y]' denotes [preference/metric]

```

Step 2. Enter **show ip lisp map-cache** to verify that the remote-site EID prefix is cached with its corresponding RLOC IP address.

```

NX7K1A# show ip lisp map-cache

```

```
LISP IP Mapping Cache for VRF "default" (iid 0), 3 entries

10.4.4.0/25, uptime: 00:01:25, expires: 23:58:34, via map-reply, auth
Locator      Uptime      State      Priority/  Data      Control
              Weight      in/out    in/out
192.168.214.1 00:01:25   up         1/100     8/4*     2/1
```

Step 3. In LISP VM-Mobility in an extended subnet use case, a dynamic-EID is always detected by the xTRs available at the specific data center site to which the EID belongs (or to which it has migrated). This behavior occurs so the remote sites can send packets to the virtual machine's current location. Enter **show lisp dynamic-eid summary** to verify that the data center xTR has detected the virtual machine in its current location. VM1 is currently in the West data center xTR, so it is detected by one of the two West data center xTRs (the one that receives the first data-plane packet from the EID).

```
NX7K1A# 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_EXTENDED_ 10.3.3.101   Vlan904    00:56:36 00:02:55 0
```

Step 4. The Cisco Nexus 7000 Series data center xTR that detected the virtual machine will report the dynamic-EID to all the other data center xTRs belonging to the same LISP site through a Map-Notify message using the multicast group configured. Enter **show lisp dynamic-eid summary** on the second data center xTR located at the West data center site.

```
NX7K1B# 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_EXTENDED_*10.3.3.101   Vlan904    00:57:18 00:00:46 0
```

Note the asterisk (*) next to the dynamic-EID prefix, which indicates that this prefix was learned through the Map-Notify mechanism. Also note that only the peer xTR device belonging to the same West data center site will display the information shown here. The two xTRs belonging to the same LISP site but that are part of the East data center site will receive the EID discovery notification and internally record this information.

Important: In the extended subnet mode, the Map-Notify messages are exchanged by using the OTV logical connection between data center sites. This behavior eliminates the need for a multicast-enabled transport infrastructure between the different data center sites. For more information about how to configure an OTV data group to transport multicast traffic across OTV, refer to http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns949/ns304/ns975/OTV_intro_wp.pdf.

Verifying Cisco IOS Software Remote xTR

Use the following steps to verify the map cache population in the remote Cisco IOS Software xTR.

Step 1. Enter **show ip route <remote-eid>** to verify that there is no native route present for the remote EID.

```
BR-3825-E-R214#show ip route 10.3.3.0
% Subnet not in table
```



```
BR-3825-E-R214#show ip route 10.3.3.101
% Subnet not in table
BR-3825-E-R214#
```

Step 2. Enter **show ip lisp map-cache** to verify that the remote-site EID prefix is cached with its corresponding RLOC IP address.

```
BR-3825-E-R214#show ip lisp map-cache

10.3.0.0/16, uptime: 00:50:03, expires: 23:09:56, via map-reply, auth
  Locator    Uptime    State      Priority/  Data      Control
              Weight    in/out    in/out
192.168.23.2 00:50:03  up         1/10      -11902    0/0
192.168.23.6 00:50:03  up         1/10      12/0*     0/0
192.168.13.2 00:50:03  up         1/10      78/14*    0/0
192.168.13.6 00:50:03  up         1/10      0/1*      0/0

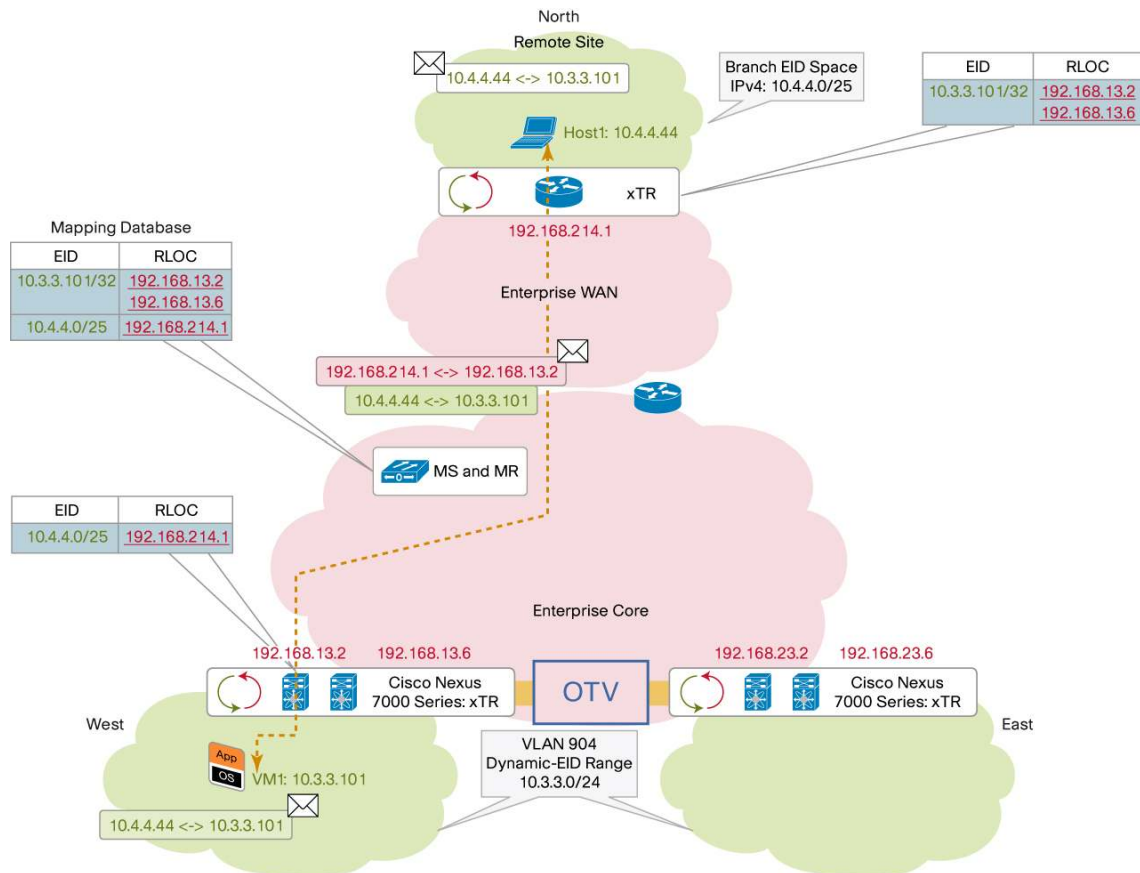
10.3.3.101/32, uptime: 00:44:52, expires: 23:15:50, via map-reply, auth
  Locator    Uptime    State      Priority/  Data      Control
              Weight    in/out    in/out
192.168.13.2 00:44:09  up         1/10      78/0*     0/0
192.168.13.6 00:44:09  up         1/10      0/1*      0/0

BR-3825-E-R214#
```

Note that the current location of dynamic-EID 10.3.3.101/32 is in the West data center. Refer to the IP address in Figure 10.

When the traffic flow uses LISP routing, the final traffic path, mapping database, and map caches in various xTRs look as shown in Figure 11.

Figure 11. Traffic Flow Using LISP Routing



Verifying Dynamic-EID Detection, Mapping, and Map-Cache Updates

While the traffic is routed with LISP between West data center VM1 and North remote-site Host 1, VM1 can be migrated by the system administrator using VMware vCenter (or another application) to the East data center. After the virtual machine has been moved, one of the xTRs in the East data center will detect the new VM1 and update the mapping system with its current locator IP address.

As shown in Figures 12, 13, and 14, VM1 is moved to the East data center using VMware vCenter.

Figure 12. LISP and VMware vCenter: VM1

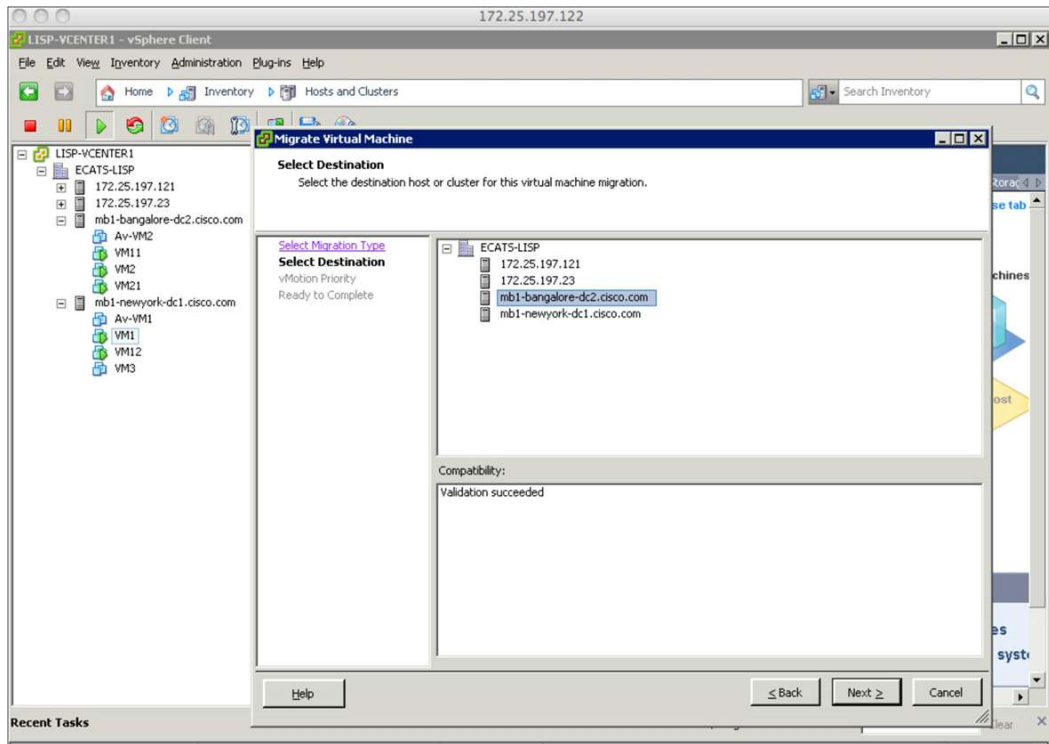


Figure 13. LISP and VMware vCenter: VM1 (Continued)

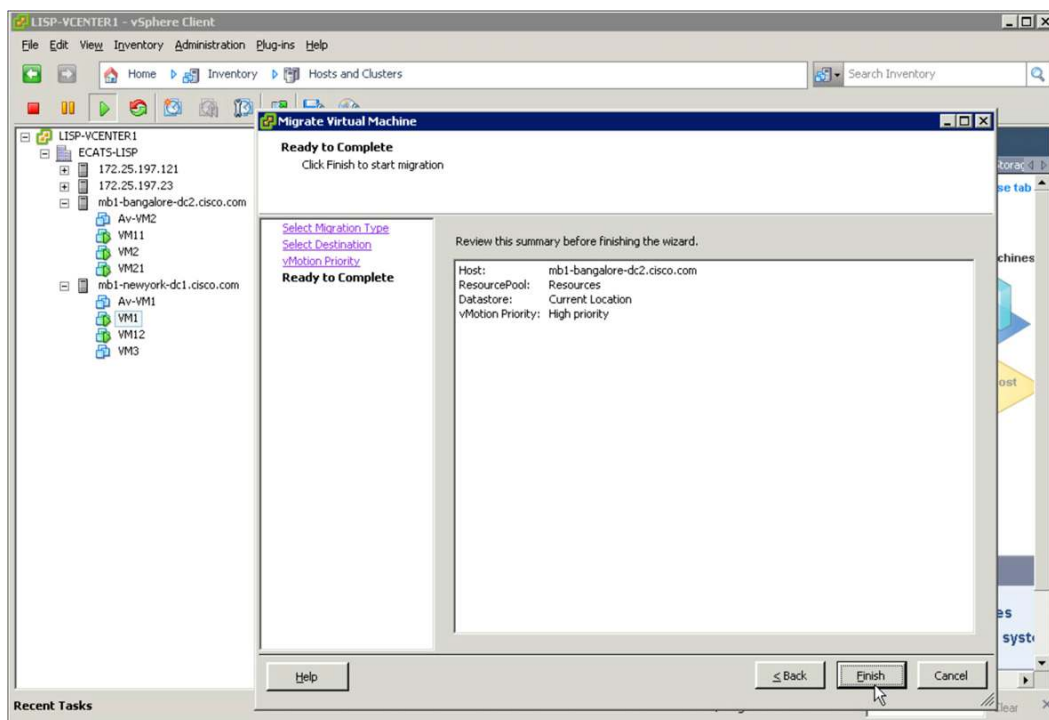
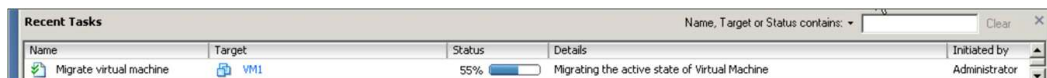


Figure 14. LISP and VMware vCenter: VM1 Move in Progress



After the move is completed, use the following steps to verify in the East data center xTR that VM1 is detected.

Step 1. Enter **show lisp dynamic-eid summary** to verify that VM1 has been detected in the East data center xTR.

```
NX7K2A# 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    Ping
                Packet    Count
LISP_EXTENDED_ 10.3.3.101    Vlan904     00:02:15  0.772286  0
```

Step 2. Since the East data center is multihomed, you can verify that the peer xTR learned the dynamic-EID through the Map-Notify message.

```
NX7K2B# 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    Ping
                Packet    Count
LISP_EXTENDED_*10.3.3.101    Vlan904     00:04:27  00:00:35  0
```

You can also verify that the xTRs in the West data center site removed the dynamic-EID entry as a result of the reception of the Map-Notify multicast message through OTV.

As shown here, dynamic-EID entries are removed in the West data center xTRs.

```
NX7K1A# 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

```

```
NX7K1B# 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

```

Step 3. Verify in the Map-Server that the VM1 dynamic-EID locators are updated by entering **show lisp site <dyn-eid-prefix>**.

```
MB1-CORE-LISP-MS1# show lisp site 10.3.3.101/32
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address, -x = more-specifics count

Site name:      "DATA_CENTER"
Description: none configured
Allowed configured locators: any
Requested EID-prefix: 10.3.3.101/32, instance-id: 0
  Currently registered:      yes
  First registered:          00:54:33
  Last registered:           00:00:13
  Who last registered:       192.168.23.2
  Routing table tag:         0x00000000
  Proxy Replying:           no
  Wants Map-Notifications:   yes
  Registering as a LISP-MN:  no
  Registered TTL:            1440 minutes
Registered locators:
  192.168.23.2, port: 47062 (up), priority: 1, weight: 50
  192.168.23.6, port: 47062 (up), priority: 1, weight: 50
Registration errors:
  Authentication failures: 0
  Allowed locators mismatch: 0
MB1-CORE-LISP-MS1#
```

Step 4. Since the traffic was originally flowing between a LISP xTR device at the remote site and the xTRs in the West data center, the cache information on the remote LISP device must be updated. This updating is performed as soon as the first packet is delivered to one of the West data center xTR devices; since they were previously notified that the specific EID is now located in the East data center, they should send a Solicit Map-Request (SMR) message to the remote xTR, which will force the remote xTR to request updated information from the Map-Server. Therefore, the traffic path is finally directed to the East data center. Enter **show ip lisp map-cache** in the remote xTR to verify the map cache update.

```
BR-3825-E-R214#show ip lisp map-cache
LISP IPv4 Mapping Cache, 2 entries

10.3.3.0/24, uptime: 00:19:13, expires: 23:40:46, via map-reply, auth
  Locator    Uptime    State    Priority/  Data      Control
            Uptime    State    Weight    in/out    in/out
192.168.23.2 00:19:13  up       1/10      362084    0/0
192.168.23.6 00:19:13  up       1/10      60/9*     0/0
192.168.13.2 00:19:13  up       1/10      4/0*      1/1
192.168.13.6 00:19:13  up       1/10      0/13*     0/0

10.3.3.101/32, uptime: 00:18:55, expires: 23:53:49, via map-reply, auth
```

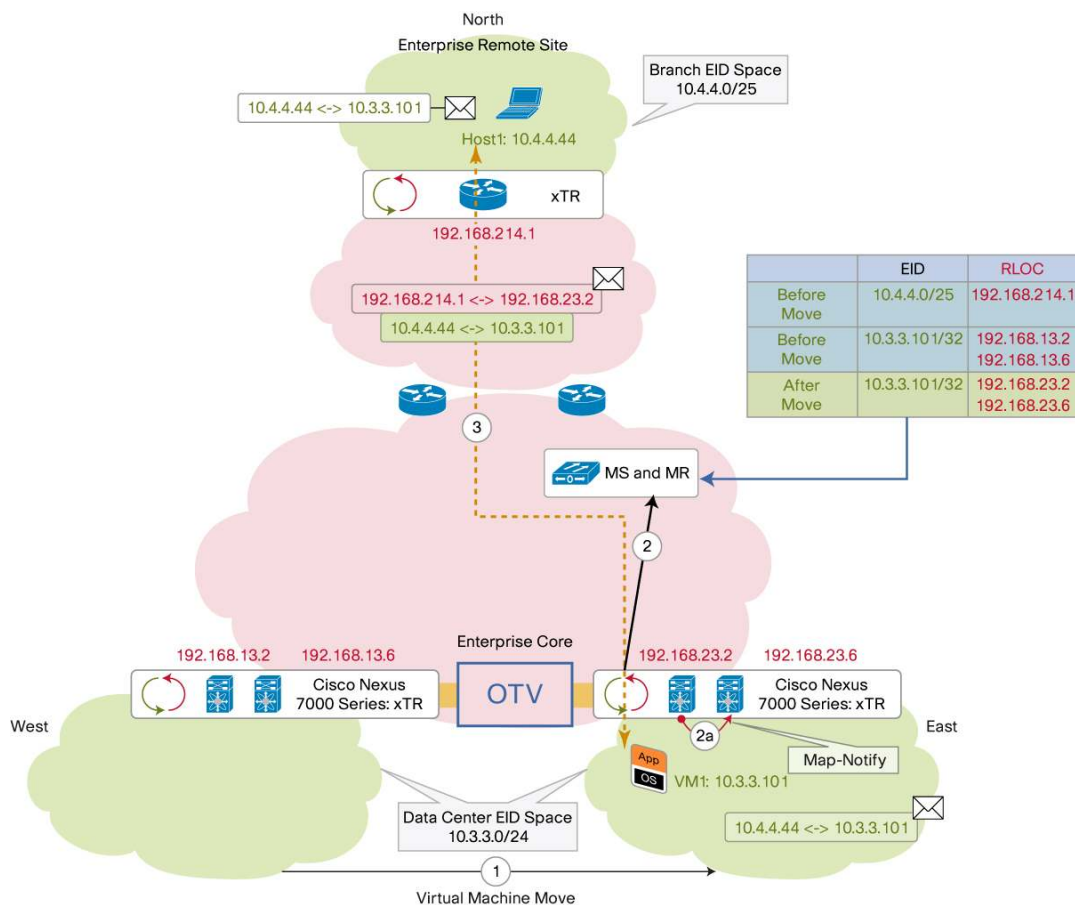
Locator	Uptime	State	Priority/ Weight	Data in/out	Control in/out
192.168.23.2	00:06:10	up	1/10	362084	0/0
192.168.23.6	00:06:10	up	1/10	60/9*	1/1

BR-3825-E-R214#

Use the preceding network diagram to confirm that the locators are updated to reflect the current virtual machine locations.

The final traffic path should look as shown in Figure 15.

Figure 15. Final Traffic Path



LISP VM-Mobility in an Extended Subnet Summary

In summary, the LISP VM-Mobility solution in an extended subnet provides the following main benefits:

- LISP co-existence with OTV
- Automated move detection
- Dynamic-EID discovery in a multihomed data center
- Direct path, which provides transparent ingress path optimization and avoids the traffic triangulation problem

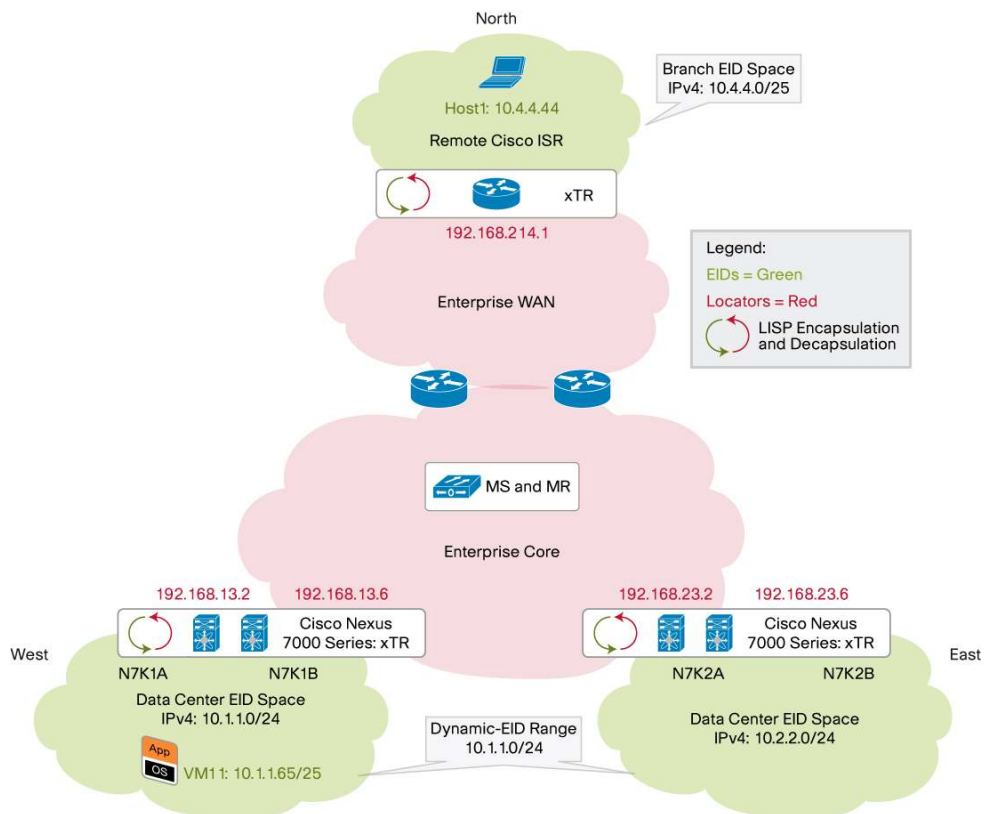
- Connections maintained across moves, making this deployment suitable for resolving hot migration use cases
- No routing reconvergence
- No DNS updates required
- Transparent to the hosts

Deploying LISP VM-Mobility Across Subnets

Figure 16 shows an enterprise data center deployment topology in which a 10.1.1.0/24 subnet is hosted in the East data center and a 10.2.2.0/24 subnet is hosted in the West data center using Cisco Nexus 7000 Series data center switches. The remote site deploys a Cisco IOS Software device that hosts the 10.4.4.0/24 network. The Map-Server is deployed in the enterprise core. This section presents the steps for configuring these data center sites and remote Cisco IOS Software device sites as LISP sites, with their corresponding EID spaces. This section also describes the configurations required for dynamic-EIDs to enable configured prefix hosts to move across subnets between data centers.

Note again that this deployment model does not require deployment of LAN extension technology between the separate data center sites. As a result, separate LISP sites exist, each coinciding with a different data center physical location.

Figure 16. LISP VM-Mobility Across Subnets



LISP VM-Mobility Across Subnets Prerequisites

- LISP VM-Mobility deployed across subnets requires the mobile virtual machines to have access to the same gateway IP address, even if they move across subnets.
- LISP VM-Mobility across subnets is currently mainly used to address cold migration scenarios, such as disaster recovery and workload mobility based on demand.

Configuring a Cisco Nexus 7000 Series Switch as a LISP xTR

Enter the commands shown here to enable and configure LISP ITR and ETR (xTR) functions on a Cisco Nexus 7000 Series Switch.

Configuration Commands

1. **configure terminal**
2. **feature lisp**
3. **ip lisp itr-etr**
4. **ip lisp database-mapping** EID□prefix/prefix□length locator_ip **priority** priority **weight** weight
5. **ip lisp etr map-server** map□server□address **key** key□type authentication□key
6. **ip lisp itr map-resolver** <map-resolver-address>
7. **exit**

Steps	Cisco NX-OS Commands	Purpose
Step 1	configure terminal	Enters the global configuration mode
Step 2	feature lisp	Enables the LISP feature set (if it is not already configured) For Cisco NX-OS only, to obtain a grace period for lab experiments on LISP, enter license grace-period . See the section Licensing Cisco NX-OS Software Features in the Cisco NX-OS Licensing Guide.
Step 3	ip lisp itr-etr	Enables LISP ITR and ETR functions for the IPv4 address family
Step 4	ip lisp database-mapping EID□prefix/prefix□length locator_ip priority priority weight weight	Configures an EID-to-RLOC mapping relationship and associated traffic policy for all IPv4 EID prefixes for this LISP site Note: If the site is assigned multiple EID prefix blocks, ip lisp database-mapping is configured for each EID prefix block assigned to the site and for each locator from which the EID prefix block can be reached. (Optional) Multihoming Considerations If the site has multiple locators associated with the same EID prefix block, multiple ip lisp database-mapping commands are entered to configure all the locators for a given EID prefix block. In a multihomed case, all ETRs belonging to the same LISP (and data center) site must be configured with consistent ip lisp database-mapping commands.
Step 5	ip lisp etr map-server map□server□address key key□type 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 with EID prefixes that match the EID prefixes configured on this ETR and with a key matching the one configured on this ETR.
Step 6	ip lisp itr map-resolver <map-resolver-address>	Configures the IP address of the LISP Map-Resolver to which this router, acting as an IPv4 LISP ITR, will send the LISP Map-Request for destination EIDs
Step 7	exit	Exits the configuration mode

Configuring a Cisco Nexus 7000 Series Switch LISP xTR for Dynamic-EID Roaming

Enter the commands shown here to enable and configure the dynamic-EID roaming functions for a given EID prefix on a Cisco Nexus 7000 Series Switch.

Configuration Commands

1. **configure terminal**
2. **lisp dynamic-eid** <dynamic-eid-map-name>
3. **database-mapping** EID□prefix/prefix□length locator_ip **priority** priority **weight** weight
4. **map-notify-group** <multicast-group-ip> (This command is required for multihoming; otherwise, it is optional.)
5. **map-server** map□server□address **key** key□type authentication□key (This command is optional. Use it to register a dynamic-EID to a specific Map-Server other than the one configured in the global LISP configuration. If this command is not configured, LISP uses the Map-Server configured in the global configuration.)
6. **exit**
7. **interface** <interface-name>
8. **lisp mobility** <dynamic-eid-map-name>
9. **ip proxy-arp**
10. **exit**

Steps	Cisco NX-OS Commands	Purpose
Step 1	configure terminal	Enters the global configuration mode
Step 2	lisp 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 3	database-mapping EID□prefix/prefix□length locator_ip priority priority weight weight	Configures a dynamic-EID range and the RLOC mapping relationship and associated traffic policy for all IPv4 dynamic-EID prefixes for this LISP site 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 Note: If the site is assigned multiple dynamic-EID prefix blocks, database-mapping is configured for each dynamic-EID prefix block and for each locator from which the EID prefix block can be reached. Multihoming Considerations If the site has multiple locators associated with the same EID prefix block, multiple database-mapping commands are entered to configure all the locators for a given EID prefix block. If a site is multihomed, all ETRs belonging to the same LISP and data center sites must be configured with consistent database-mapping commands.
Step 4	map-notify-group <multicast-group-ip> (Optional except for multihoming)	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 and data center sites after a dynamic EID is detected. The TTL for this notification message is set to 1. This multicast group IP address can be whatever the user wants other than an address that is already in use in the network.
Step 5	map-server map□server□address key key□type authentication□key	(Optional) Configures the IP address of the LISP Map-Server to which this router will register dynamic-EID-to-RLOC mappings Use this optional configuration step to register a dynamic-EID-to-RLOC mapping on a specific Map-Server other than the one configured in the global LISP configuration. If this command is not configured, LISP uses the Map-Server configured in the global configuration.
Step 6	exit	Exits the configuration mode

Steps	Cisco NX-OS Commands	Purpose
Step 7	interface <interface-name>	Enters the interface configuration mode The interface-name entry is the name of the interface to which or from which the dynamic EIDs are expected to roam.
Step 8	lisp mobility <dynamic-eid-map-name>	Configures the interface in Step 6 to allow a dynamic-EID to be detected when a roam event occurs The dynamic-eid-map-name entry is the dynamic EID map name configured in Step 2.
Step 9	ip proxy-arp	Configures the interface as proxy ARP
Step 10	exit	Exits the configuration mode

Configuring the Remote Site Cisco IOS Software Router as a LISP xTR

Enter the commands shown here to enable and configure LISP ITR and ETR (xTR) functions on a Cisco IOS Software router.

Configuration Commands

1. **configuration terminal**
2. **router lisp**
3. **ipv4 itr**
4. **ipv4 etr**
5. **database-mapping** EID□prefix/prefix□length locator_ip **priority** priority **weight** weight
6. **ipv4 etr map-server** map□server□address **key** authentication□key
7. **ipv4 lisp itr map-resolver** <map-resolver-address>
8. **exit**

Steps	Cisco IOS Software Commands	Purpose
Step 1	configure terminal	Enters the global configuration mode
Step 2	router lisp	Enables and enters into the router LISP configuration mode
Step 3	ipv4 lisp itr	Enables LISP ITR functions for the IPv4 address family
Step 3	ipv4 lisp etr	Enables LISP ETR functions for the IPv4 address family
Step 4	database-mapping EID□prefix/prefix□length locator_ip priority priority weight weight	Configures an EID-to-RLOC mapping relationship and associated traffic policy for all IPv4 EID prefixes for this LISP site Note: If the site is assigned multiple EID prefix blocks, the IP LISP database mapping is configured for each EID prefix block assigned and for each locator through which the EID-prefix block can be reached. (Optional) Multihoming Considerations If the site has multiple locators associated with the same EID prefix block, multiple database-mapping commands are entered to configure all the locators for a given EID prefix block. If a site is multihomed, all ETRs must be configured with consistent database-mapping commands.
Step 5	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 with EID prefixes that match the EID prefixes configured on this ETR and with a key matching the one configured on this ETR.
Step 6	ipv4 lisp itr map-resolver <map-resolver-address>	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.
Step 7	exit	Exits the configuration mode

Configuring the LISP Map-Server and Resolver on Cisco NX-OS

This section describes an enterprise-class solution in which the Map-Server and Map-Resolver are located on the same network device. Also, no redundancy is provided in the configuration samples shown here. For more information about this topic, please refer to the “Map-Server and Map-Resolver Considerations” section.

Enter the commands shown here to enable and configure LISP Map-Server and Map-Resolver functions for IPv4 address families on a Cisco Nexus 7000 Series Switch running Cisco NX-OS.

Configuration Commands

1. **configure terminal**
2. **feature lisp**
3. **ip lisp map-server**
4. **ip lisp map-resolver**
5. **lisp site site-name**
6. **description description**
7. **authentication-key key-type password**
8. **eid-prefix {EID-prefix } accept-more-specifics**
9. **exit**

Steps	Cisco NX-OS Commands	Purpose
Step 1	configure terminal	Enters global configuration mode
Step 2	feature lisp	Enables the LISP feature set To obtain a grace period for lab experiments on LISP, enter license grace-period . See the section Licensing Cisco NX-OS Software Features in the Cisco NX-OS Licensing Guide.
Step 3	ip lisp map-server	Enables LISP Map-Server functions for the IPv4 address family
Step 4	ip lisp map-resolver	Enables LISP Map-Resolver functions for the IPv4 address family
Step 5	lisp site site-name	Creates the indicated LISP site and enters the LISP site configuration mode
Step 6	description description	Enters a description for the LISP site being configured
Step 7	authentication-key key-type password	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 8	eid-prefix {EID-prefix } accept-more-specifics Optional; for the case of dynamic-EID configured on the ETR	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.
Step 9	exit	Exits the LISP site configuration mode

LISP VM-Mobility Across Subnets: Configuration Example

Figure 17 shows a network setup with West and East data centers. The West data center hosts servers and services in the 10.1.1.0/24 network in VLAN 907 and is configured as the LISP EID space in the West data center xTRs. The East data center hosts servers and services in the 10.2.2.0/24 network in VLAN 908 and is configured as the LISP EID space in the East data center xTRs. The workloads are moved between these two data centers, from VLAN 907 in the West data center (the home data center) to VLAN 908 in the East data center depending on the traffic patterns or business needs. The network 10.1.1.0/24 is configured as the dynamic-EID space in both data center xTRs.

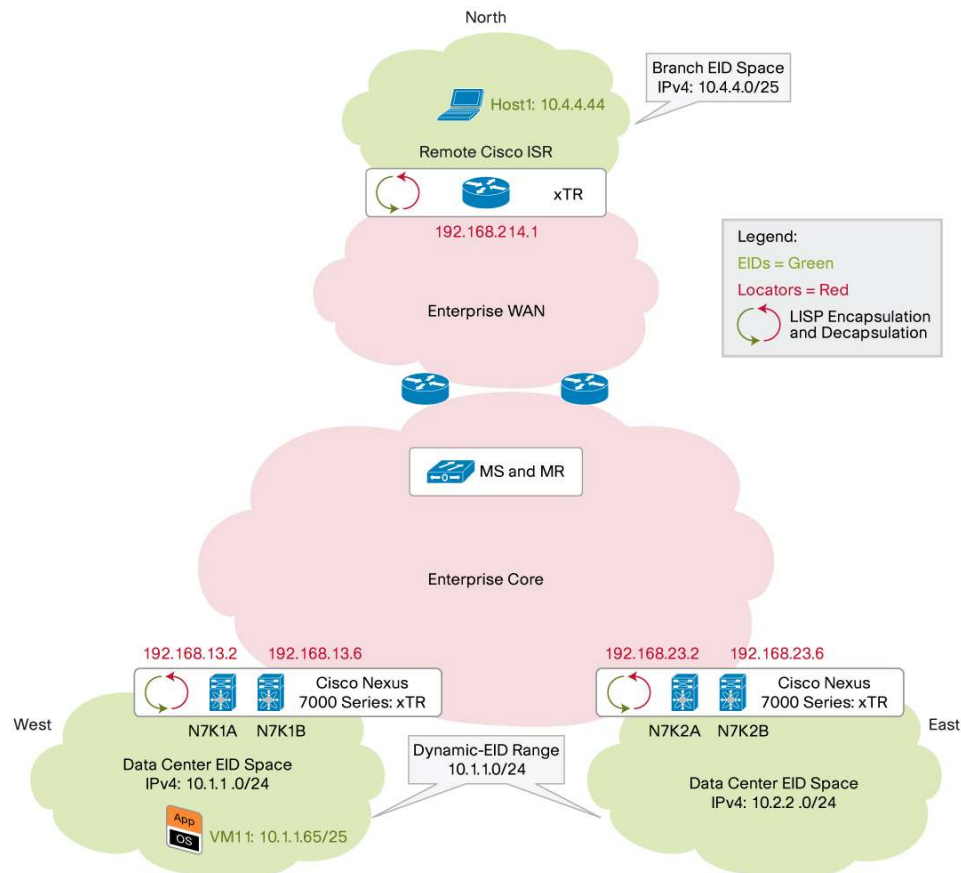
Important: If the traffic originated by the workload is IEEE 802.1q tagged (as is the case in example using the Cisco Nexus 1000V Series distributed virtual switch), you must make sure that the same VLAN is available in both LISP and data center sites, even if it can be associated with a separate IP subnet.

Both data centers are multihomed to the core, and HSRP is configured on VLAN 907 and VLAN 908 to serve the hosts in their respective data centers. As a prerequisite for LISP VM-Mobility in the across-subnet use case, a roaming workload needs to be able to continue sending traffic to the default gateway after migration is completed. This configuration can be achieved by manually setting the vMAC address associated with the HSRP group so that it is consistent across sites (or, alternatively, using the same HSRP group number, as previously discussed for the extended subnet mode). Also, proxy ARP configuration is required for both SVIs 907 and 908 to properly handle new ARP requests sent by the migrated workload.

The remote site is configured with a Cisco ISR configured as a LISP ITR and ETR and hosts the 10.4.4.0/24 EID space.

This section presents a configuration example for this setup for each component.

Figure 17. Example LISP VM-Mobility Across-Subnet Network Setup



Cisco Nexus 7000 Series N7K1A West Data Center xTR Configuration Example

```
feature lisp
ip lisp itr-etr
ip lisp database-mapping 10.1.1.0/24 192.168.13.2 priority 1 weight 50
ip lisp database-mapping 10.1.1.0/24 192.168.13.6 priority 1 weight 50
ip lisp itr map-resolver 10.111.10.14
ip lisp etr map-server 10.111.10.14 key 0 cisco
lisp dynamic-eid LISP_ACROSS_SUBNET
  database-mapping 10.1.1.0/24 192.168.13.2 priority 1 weight 50
  database-mapping 10.1.1.0/24 192.168.13.6 priority 1 weight 50
  map-notify-group 239.1.1.11
interface Vlan907
ip address 10.1.1.2/24
lisp mobility LISP_ACROSS_SUBNET
ip proxy-arp
hsrp 17
  mac-address 0000.0E1D.010C
  preempt delay minimum 300
```

```
priority 200
ip 10.1.1.1
```

Cisco Nexus 7000 Series N7K1B West Data Center xTR Configuration Example

```
feature lisp
ip lisp itr-etr
ip lisp database-mapping 10.1.1.0/24 192.168.13.2 priority 1 weight 50
ip lisp database-mapping 10.1.1.0/24 192.168.13.6 priority 2 weight 50
ip lisp itr map-resolver 10.111.10.14
ip lisp etr map-server 10.111.10.14 key 0 cisco
lisp dynamic-eid LISP_ACROSS_SUBNET
  database-mapping 10.1.1.0/24 192.168.13.2 priority 1 weight 50
  database-mapping 10.1.1.0/24 192.168.13.6 priority 1 weight 50
  map-notify-group 239.1.1.11
interface Vlan907
  ip address 10.1.1.3/24
  lisp mobility LISP_ACROSS_SUBNET
  ip proxy-arp
  hsrp 17
    mac-address 0000.0E1D.010C
    priority 190
    ip 10.1.1.1
```

Since in this setup the Cisco Nexus 7000 Series Switches are multihomed, both RLOC IP addresses must be configured identically in all the xTRs belonging to the same LISP and data center sites.

Notice also that in the preceding example, the same priority and weight were configured for each defined RLOC (default behavior). If you want, you can modify these parameters if the goal is not to load-balance incoming LISP traffic from other xTRs.

Note, however, that in across-subnet mode, you do not need more specific prefixes (from a subnet point of view) than the ones configured as part of the global IP LISP database mapping.

Cisco Nexus 7000 Series N7K2A East Data Center xTR Configuration Example

The East data center xTRs are configured the same way as the West data center xTRs but with their respective RLOC IP addresses as shown in the preceding topology. Also note that a static vMAC address is configured as part of the HSRP configuration, for consistency across data center locations. This configuration is required so that when the virtual machines move between these data centers, they continue to send traffic to the same gateway IP and MAC addresses, and ARP does not need to be reapplied during mobility events (using the same HSRP group number in West and East data center xTRs is an alternative way to achieve the same result). In addition, proxy ARP is enabled for the VLAN interfaces, to handle new ARP requests generated by the migrated workload.

Finally, in the across-subnet mode, you do not need to specify the same multicast group for use for Map-Notify messages between xTRs belonging to separate LISP and data center sites. This specification is not needed because these messages are now restricted to xTRs belonging to the same LISP and DC sites.

```

feature lisp
ip lisp itr-etr
ip lisp database-mapping 10.2.2.0/24 192.168.23.2 priority 1 weight 50
ip lisp database-mapping 10.2.2.0/24 192.168.23.6 priority 1 weight 50
ip lisp itr map-resolver 10.111.10.14
ip lisp etr map-server 10.111.10.14 key 0 cisco
!
lisp dynamic-eid LISP_ACROSS_SUBNET
  database-mapping 10.1.1.0/24 192.168.23.2 priority 1 weight 50
  database-mapping 10.1.1.0/24 192.168.23.6 priority 1 weight 50
  map-notify-group 239.1.1.12
!
interface Vlan908
  ip address 10.2.2.2/24
  lisp mobility LISP_ACROSS_SUBNET
  ip proxy-arp
  hsrp 17
    mac-address 0000.0E1D.010C
    priority 200
    preempt delay minimum 300
  ip 10.2.2.1

```

Cisco Nexus 7000 Series N7K2B East Data Center xTR Configuration Example

```

feature lisp
ip lisp itr-etr
ip lisp database-mapping 10.2.2.0/24 192.168.23.2 priority 1 weight 50
ip lisp database-mapping 10.2.2.0/24 192.168.23.6 priority 1 weight 50
ip lisp itr map-resolver 10.111.10.14
ip lisp etr map-server 10.111.10.14 key 0 cisco
!
lisp dynamic-eid LISP_ACROSS_SUBNET
  database-mapping 10.1.1.0/24 192.168.23.2 priority 1 weight 50
  database-mapping 10.1.1.0/24 192.168.23.6 priority 1 weight 50
  map-notify-group 239.1.1.12
!
interface Vlan908
  ip address 10.2.2.3/24
  lisp mobility LISP_ACROSS_SUBNET
  ip proxy-arp
  hsrp 17
    mac-address 0000.0E1D.010C
    priority 190
  ip 10.2.2.1

```

Remote-Site Cisco IOS Software xTR Configuration Example

Following is a configuration example for a LISP site using a Cisco IOS Software router such as a Cisco ISR.

```
router lisp
database-mapping 10.4.4.0/24 192.168.214.1 priority 1 weight 100
ipv4 itr map-resolver 10.111.10.14
ipv4 itr
ipv4 etr map-server 10.111.10.14 key cisco
ipv4 etr
```

Cisco NX-OS Map-Server and Map-Resolver Configuration Example

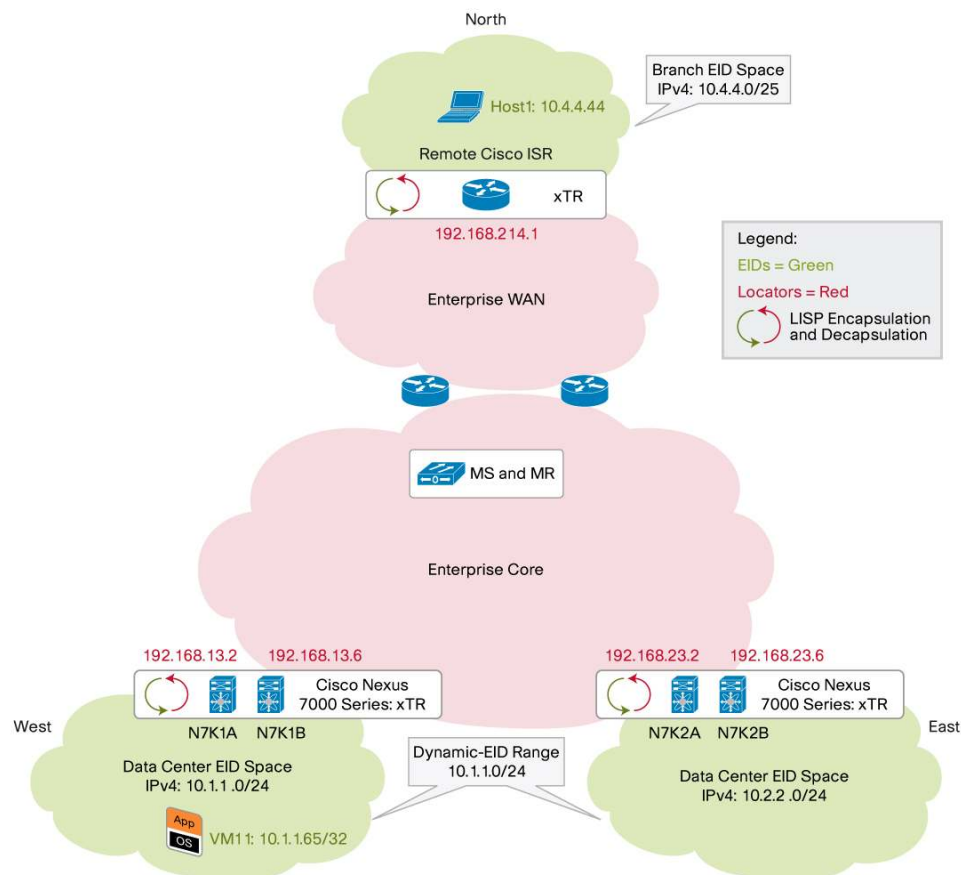
Following is a configuration example for a LISP Map-Server and Map-Resolver on a Cisco NX-OS device. Note that the 10.1.1.0/24 prefix is configured in the Map-Server to accept more specific prefixes, enabling the ETR to register a host-specific /32 prefix in case of a mobility event.

```
feature lisp
ip lisp map-resolver
ip lisp map-server
lisp site BRANCH
    eid-prefix 10.4.4.0/24
    authentication-key 0 cisco
lisp site DATA_CENTER
    eid-prefix 10.1.1.0/24 accept-more-specifics
    eid-prefix 10.2.2.0/24
    authentication-key 0 cisco
```

LISP VM-Mobility Across-Subnet Verification

Figure 18 shows the same network setup used in the configuration examples, with virtual machine VM11 in the West data center talking to a host at the remote site. This section describes the verification steps for basic LISP operation, the dynamic-EID move and detection process, and path optimization by LISP.

Figure 18. Example Network Setup



Verifying Cisco NX-OS Map-Server

When the LISP components are configured according to the examples in the previous section, the Cisco Nexus 7000 Series multihomed data center xTRs and the Cisco IOS Software remote xTR will register their configured EID spaces with the mapping system. Use the following steps to verify the xTRs' map registration for their respective EID spaces with their RLOC IP addresses.

Step 1. Enter **show lisp site** to display the LISP sites and their registration status.

```

MB1-CORE-LISP-MS1# show lisp site
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address, -x = more-specifics count

Site Name      Last          Actively      Who last      EID-prefix
Registered    Registered
DATA_CENTER    00:00:07     yes           192.168.13.6  10.1.1.0/24-0
               00:00:09     yes           192.168.23.6  10.2.2.0/24
BRANCH         00:00:01     yes           192.168.214.1 10.4.4.0/24

MB1-CORE-LISP-MS1#

```

Note that in the preceding example, since data center xTRs are multihomed, they will register both RLOC IP addresses for their EID spaces. Also note that dynamic-EID prefix 10.1.1.0/24 is registered by the West data center xTR (192.168.13.6), whereas 10.2.2.0/24 is registered by the East data center xTR (192.168.23.6). VM1 with IP address 10.1.1.65 is initially in the West data center, so there is no more specific EID mapping registered by the West data center xTR (hence, the -0 in the preceding output). This behavior differs from that in the extended subnet mode, in which a /32 EID prefix was always detected and registered independent of the specific data center location.

Step 2. To view the site-specific EID registration status, enter **show lisp site <site-name>**.

```
MB1-CORE-LISP-MS1# show lisp site DATA_CENTER
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address, -x = more-specifics count

Site name:      "DATA_CENTER"
Description: none configured
Allowed configured locators: any
  Configured EID-prefix: 10.1.1.0/24, instance-id: 0
    More-specifics registered: 0
    Currently registered:      yes
    First registered:          00:32:51
    Last registered:           00:00:03
    Who last registered:       192.168.13.2
    Routing table tag:         0x00000000
    Proxy Replying:           no
    Wants Map-Notifications:   yes
    Registering as a LISP-MN:  no
    Registered TTL:            1440 minutes
    Registered locators:
      192.168.13.2, port: 47083 (up), priority: 1, weight: 50
      192.168.13.6, port: 47083 (up), priority: 1, weight: 50
    Registration errors:
      Authentication failures: 0
      Allowed locators mismatch: 0
  Configured EID-prefix: 10.2.2.0/24, instance-id: 0
    Currently registered:      yes
    First registered:          00:28:43
    Last registered:           00:00:08
    Who last registered:       192.168.23.2
    Routing table tag:         0x00000000
    Proxy Replying:           no
    Wants Map-Notifications:   yes
    Registering as a LISP-MN:  no
    Registered TTL:            1440 minutes
    Registered locators:
      192.168.23.2, port: 47083 (up), priority: 1, weight: 50
```

```
192.168.23.6, port: 47083 (up), priority: 1, weight: 50
Registration errors:
  Authentication failures: 0
  Allowed locators mismatch: 0
MB1-CORE-LISP-MS1#
```

Verifying Cisco Nexus 7000 Series Data Center xTRs

If the end devices in the data center or in the remote site try to send traffic (for example, VM11 in the West data center and Host 1 in the North remote site), the xTRs will query the mapping system because they do not have native routes to the other site. After the Map-Server receives the Map-Request from the xTR, it will forward the request to the last-registered RLOC (xTR). The ETR will reply to the Map-Request, and the ITRs will populate their map cache tables. Subsequent packets between the sites are encapsulated and sent to the other site ETRs. The receiving-side ETR will decapsulate the packet and deliver it to the destination.

Use the following steps to verify the Cisco Nexus 7000 Series data center xTRs.

Step 1. Enter **show ip route <remote-eid>** to verify that there is no native route present for the remote EID.

```
NX7K1A# show ip route 10.4.4.0/24 longer-prefixes
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
```

Step 2. Enter **show ip lisp map-cache** to verify that the remote-site EID prefix is cached with its corresponding RLOC IP address.

```
NX7K1A# show ip lisp map-cache
LISP IP Mapping Cache for VRF "default" (iid 0), 3 entries

10.4.4.0/24, uptime: 00:02:26, expires: 23:57:33, via map-reply, auth
Locator      Uptime      State      Priority/  Data      Control
              Weight      in/out    in/out
192.168.214.1 00:02:26   up         1/100     12/138    1/0
```

Verifying Cisco IOS Software Remote xTR

Use the following steps to verify the map cache population in the remote Cisco IOS Software xTR.

Step 1. Enter **show ip route <remote-eid>** to verify that there is no native route present for the remote EID.

```
BR-3825-E-R214#show ip route 10.1.1.0
% Subnet not in table
BR-3825-E-R214#show ip route 10.1.1.65
% Subnet not in table
BR-3825-E-R214#
```

Step 2. Enter **show ip lisp map-cache** to verify that the remote-site EID prefix is cached with its corresponding RLOC IP address.

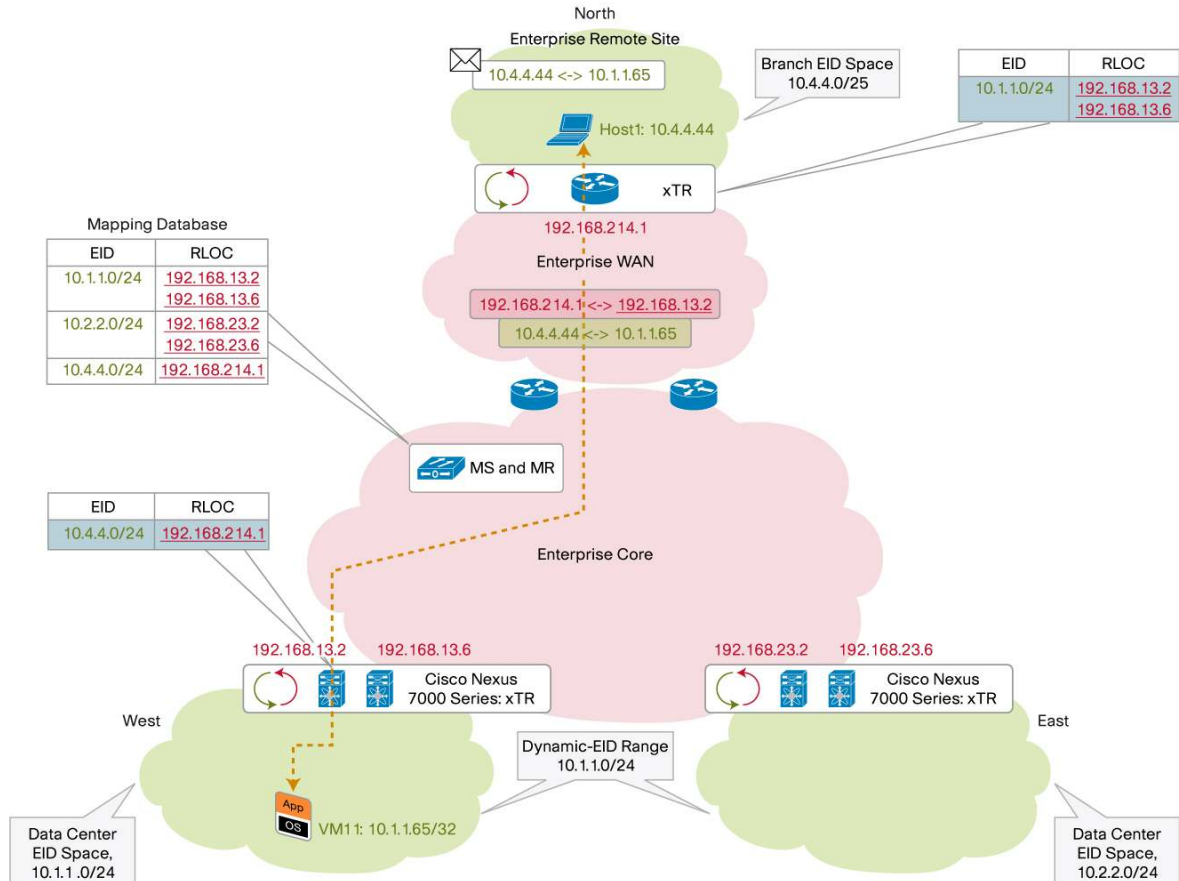
```
BR-3825-E-R214#show ip lisp map-cache
LISP IPv4 Mapping Cache, 3 entries

0.0.0.0/0, uptime: 01:28:38, expires: never, via static
Negative cache entry, action: send-map-request
10.1.1.0/24, uptime: 00:17:41, expires: 23:42:18, via map-reply, auth
Locator    Uptime    State      Priority/  Data      Control
           Weight    in/out    in/out
192.168.13.2 00:17:41 up         1/10      4/0*      1/1
192.168.13.6 00:17:41 up         1/10      0/17*     0/0
BR-3825-E-R214#
```

Note that the current location of dynamic-EID 10.1.1.0/24 is the West data center. Also, VM11 10.1.1.65 is currently in the original West site, so there is no more specific EID mapping registered by the West data center xTR. Hence, the remote xTR relies on the 10.1.1.0/24 prefix to reach VM1. Refer to the IP address in the previous network diagrams.

When traffic flows are established using LISP routing, the final traffic path, mapping database, and map caches in various xTRs look as shown in Figure 19.

Figure 19. Traffic Flow Using LISP Routing



Verifying Dynamic-EID Detection, Mapping, and Map-Cache Updates

While the traffic is routed with LISP between West data center VM11 and North remote-site Host 1, VM11 is moved by the system administrator using VMware vCenter (or another application) across the subnet to the 10.2.2.0/24 network in the East data center. After the virtual machine is moved to the East data center, the Cisco Nexus 7000 Series LISP xTR will detect the new VM1 and update the mapping system with its current locator IP addresses.

As shown in Figures 20, 21, and 22, VM11 is moved to the East data center using VMware vCenter.

Figure 20. VM1 Moving to East Data Center Using VMware vCenter

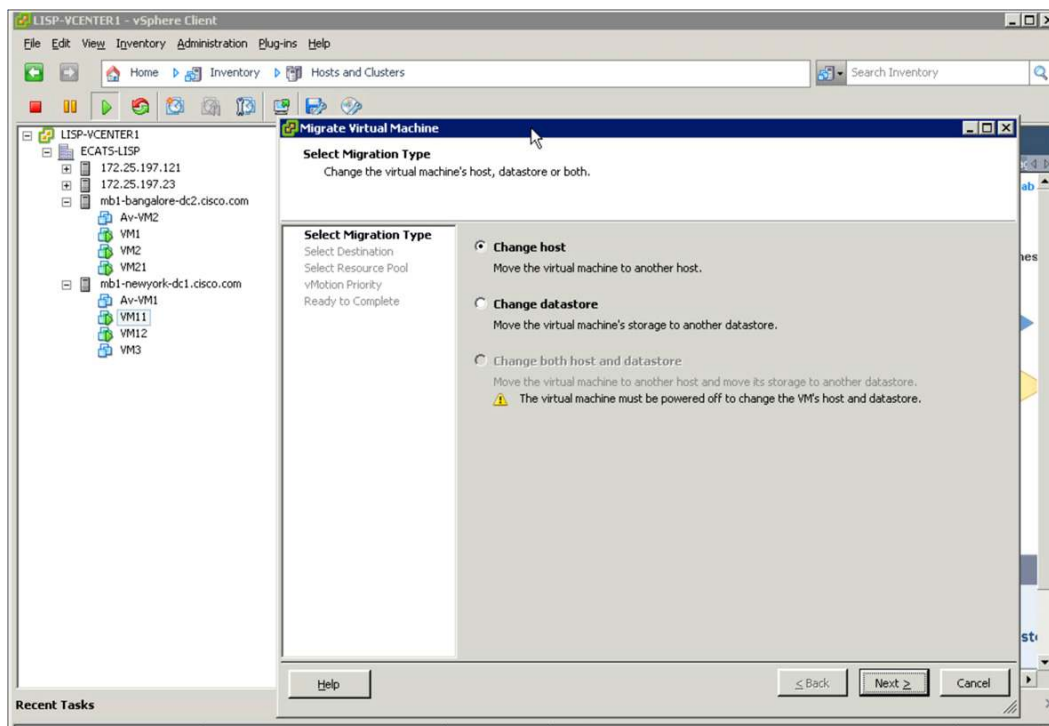


Figure 21. VM1 Moving to East Data Center Using VMware vCenter (Continued)

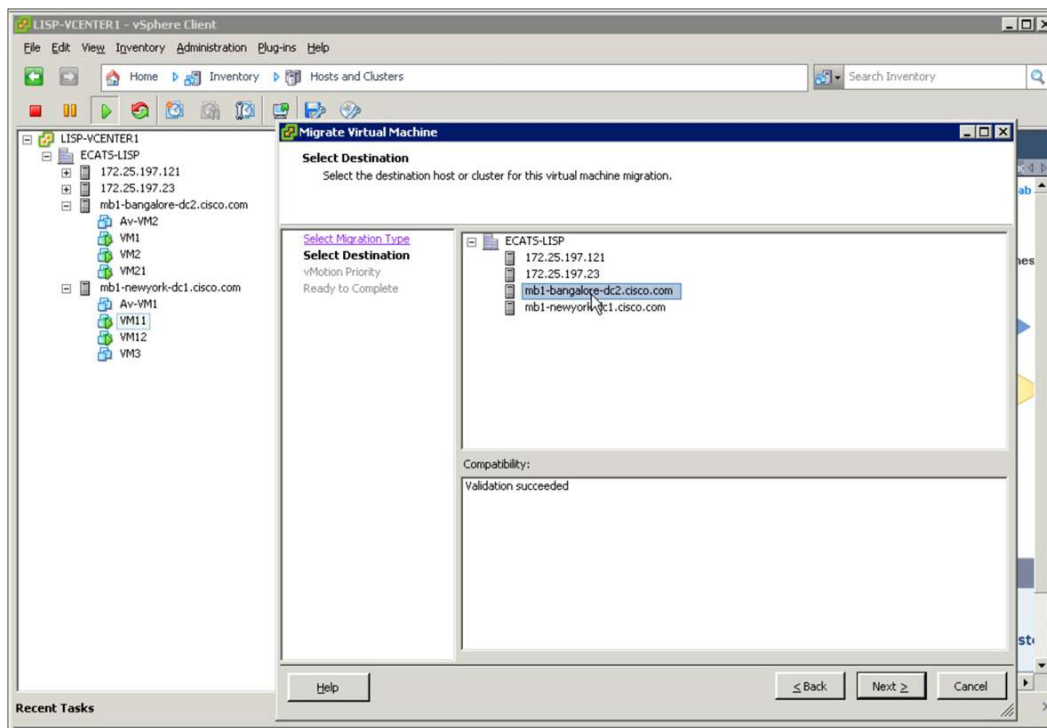
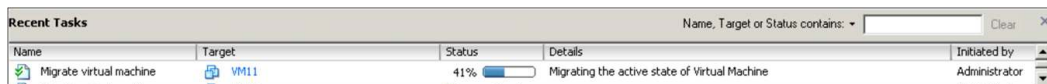


Figure 22. VM1 Move to East Data Center in Progress



After the move is completed, verify in the East data center xTR that the VM11 move is detected dynamically by using the following steps.

Step 1. Enter **show lisp dynamic-eid summary** to see if VM1 is detected in the East data center xTR.

```
NX7K2A# 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    Ping
                Dynamic-EID    Interface    Uptime    Packet  Count
LISP_ACROSS_SU  10.1.1.65        Vlan908      00:02:28  00:00:01  0
R23_NX7K2#
```

Step 2. Since the data center xTRs are multihomed, check the other data center xTR to confirm that the dynamic-EID is learned by using the Map-Notify message.

```
NX7K2B# 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      Ping
                  Dynamic-EID      Interface      Uptime      Packet    Count
LISP_ACROSS_SU*10.1.1.65      Vlan908      00:03:04      00:00:48      0
R23_NX7K2-2B#
```

The Map-Notify message is now exchanged only between the two xTR devices belonging to the same data center site.

Step 3. Verify in the Map-Server that the VM11 dynamic-EID locators are updated by entering **show lisp site <dyn-eid-prefix>**.

```
MB1-CORE-LISP-MS1# show lisp site 10.1.1.65/32
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address, -x = more-specifics count

Site name:      "DATA_CENTER"
Description: none configured
Allowed configured locators: any
Requested EID-prefix: 10.1.1.65/32, instance-id: 0
  Currently registered:      yes
  First registered:          00:08:54
  Last registered:           00:00:06
  Who last registered:       172.26.255.74
  Routing table tag:         0x00000000
  Proxy Replying:           no
  Wants Map-Notifications:   yes
  Registering as a LISP-MN:   no
  Registered TTL:            1440 minutes
Registered locators:
  192.168.23.2, port: 47083 (up), priority: 1, weight: 50
  192.168.23.6, port: 47083 (up), priority: 1, weight: 50
Registration errors:
  Authentication failures: 0
  Allowed locators mismatch: 0
MB1-CORE-LISP-MS1#
```

After the Map-Server receives the registration for the /32 EID prefix from the xTR device located in East data center, it communicates this information to the xTRs in the West data center that originally registered the /24 prefix. This step is critical to help ensure that both xTRs in West data center are aware that the specific /32 prefixed workload has been moved to the East data center side.

Step 4. Since traffic flowing between VM1 and remote-site Host 1 was originally exchanged between the remote LISP device and one of the West data center xTRs, the information in the map cache of the remote LISP

device must be refreshed. Similar to the process discussed for the extended subnet mode, this refresh is triggered by a Solicit Map-Request (SMR) message originated by the West data center xTR after it receives the first packet destined to the VM11 IP address. This process occurs because, as mentioned earlier, the West data center xTRs have been notified by the Map-Server that the workload has been discovered in the East data center site. Therefore, after the remote LISP device pulls updated information from the Map-Server, the traffic path is finally directed to the East data center. Enter **show ip lisp map-cache** in the remote xTR to verify the map cache update.

```
BR-3825-E-R214#show ip lisp map-cache
LISP IPv4 Mapping Cache, 4 entries

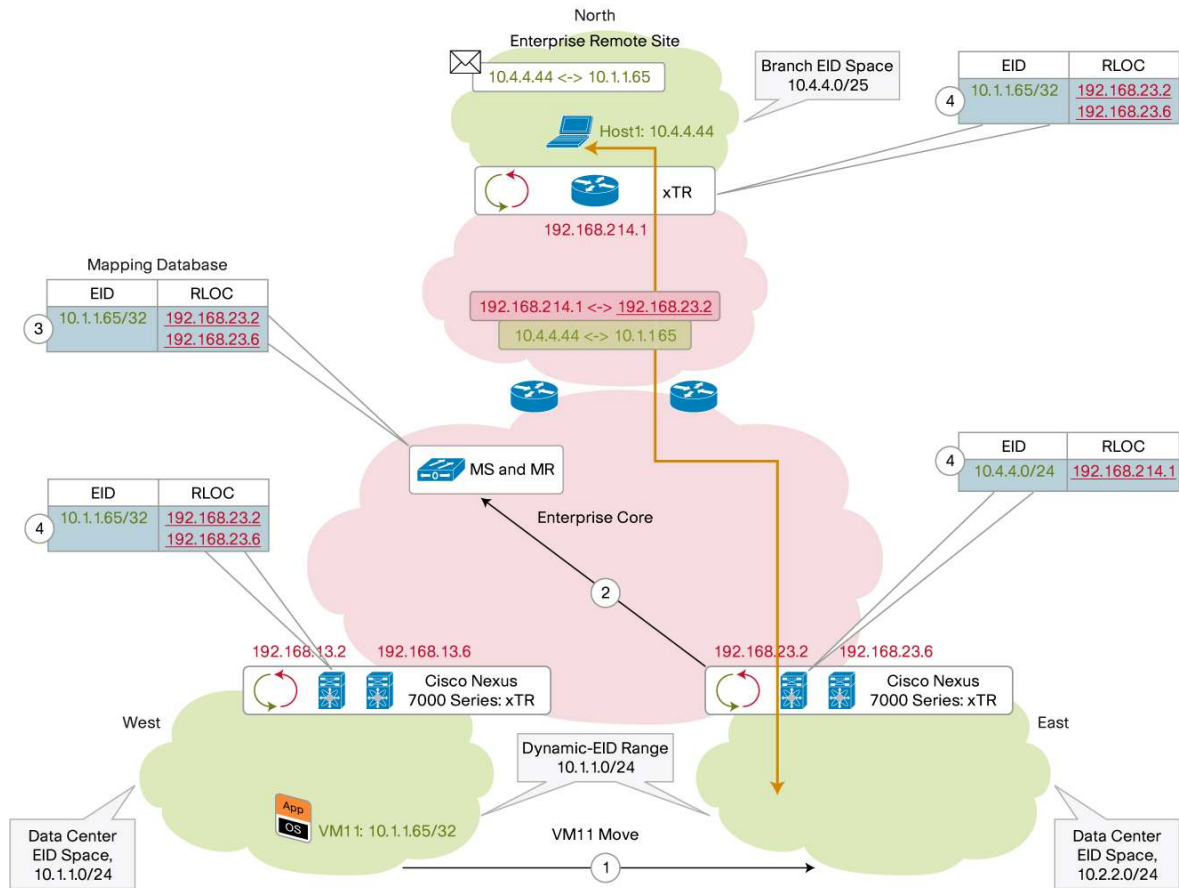
0.0.0.0/0, uptime: 01:34:31, expires: never, via static
  Negative cache entry, action: send-map-request
10.1.1.0/24, uptime: 16:03:20, expires: 07:56:39, via map-reply, auth
  Locator    Uptime    State      Priority/  Data      Control
              Weight    in/out    in/out
192.168.13.2 16:03:20  up         1/10      149838    1/1
192.168.13.6 16:03:20  up         1/10      574546    0/0

10.1.1.65/32 uptime: 00:10:23, expires: 23:55:02, via map-reply, auth
  Locator    Uptime    State      Priority/  Data      Control
              Weight    in/out    in/out
192.168.23.2 00:04:57  up         1/10      0/0*      0/0
192.168.23.6 00:04:57  up         1/10      0/0*      0/0
BR-3825-E-R214#
```

Use the previous network diagram to verify that the locators are updated to reflect the current VM1 location.

A new entry, 10.1.1.65/32, is added to the map cache with its current location. Also note that a 10.1.1.0/24 map cache still is present, and this map cache will be used to send traffic to other unmoved hosts in West data center. The final traffic path should look as shown in Figure 23.

Figure 23. LISP VM-Mobility Extended Subnet Final Traffic Path



LISP VM-Mobility Across Subnets Summary

- LISP VM-Mobility across subnets provides automated move detection, map cache update, and a direct data path to the mobile virtual machine's current location.
- Off-subnet connections are maintained across moves.
- Preserving on-subnet connections across moves would require a refresh of the ARP cache on the moving workload. Because of this, the across-subnet deployment model is currently targeted for cold workload migration use cases, such as disaster recovery scenarios.
- No routing reconvergence is required during a move.
- No DNS updates are required.
- No host protocol stack changes, OS changes, or configuration changes are required.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C11-693627-00 12/11