Note  This Cisco GETVPN+LISP Configuration Example is subject to change. The commands and their usage, configuration examples, and detailed outputs are provided as the best representation available at the time of this writing. This document will eventually be replaced with the formal version formatted and published in the same way as all other Cisco configuration guides and documentation.
Table of Contents

PURPOSE OF THIS DOCUMENT .............................................................................................................3
PREREQUISITES FOR CONFIGURING GETVPN+LISP ........................................................................3
RESTRICTIONS FOR CONFIGURING GETVPN+LISP ........................................................................3
LISP AND ENCRYPTION OVERVIEW ................................................................................................4
GETVPN + LISP EXAMPLE CONFIGURATION ....................................................................................5
  Reference LISP VPN Architecture ..................................................................................................5
LISP AND ENCRYPTION CONCLUSIONS .........................................................................................18
REFERENCES .....................................................................................................................................18
APPENDIX A – FULL CONFIGURATIONS FOR REFERENCE EXAMPLE ................................................19
Purpose of This Document

The purpose of this document is to provide configurations for a notional Enterprise VPN deployment that incorporates LISP and GETVPN. In this example, the Enterprise VPN deployment includes IPv4 and IPv6 “endpoint identifiers” (EIDs) at each Enterprise site, with virtualization (departmental VPNs - three in this example), all running over a common IPv4 core. GETVPN is added on a per-VRF and per-address family basis (i.e. IPv4 and IPv6 associated with each VRF is encrypted separately), and with redundant Key Servers. Multihoming is also included in this notional Enterprise VPN deployment model.

Other GETVPN+LISP deployment models are possible, and this document (hopefully) provides sufficient detail to permit extension to other VPN topologies and architectures also incorporating LISP, or GETVPN+LISP.

Prerequisites for Configuring GETVPN+LISP

This document provides configuration examples for deploying GETVPN+LISP. Knowledge of GETVPN configuration and deployment, separate from LISP, as well as LISP configuration and deployment, separate from GETVPN are assumed. This document does not cover the basics for either GETVPN or LISP.

- LISP configuration and deployment background information can be found in References [1] and [2], or here: http://lisp.cisco.com or www.cisco.com/go/lisp
- GETVPN configuration and deployment background information can be found in Reference [3], or here: http://www.cisco.com/go/getvpn

Restrictions for Configuring GETVPN+LISP

The configurations provided in this document are all based on Cisco IOS Release 15.2(3)T, which provides LISP support and GETVPN support. Other Cisco IOS and IOS-XE releases also support LISP and GETVPN. Be sure to check the release notes for specific platforms to be used in your network, and always confirm correct operational behavior for any deployed solutions.
**LISP and Encryption Overview**

The inherent properties of LISP give it support for multi-homing, virtualization, and host/VM mobility for both IPv4 and IPv6 address families make it an ideal architecture for creating highly efficient, AF-agnostic, Virtual Private Networks (VPNs). Existing IOS encryption support provided by the IPsec and GETVPN features can be used directly (in a “bolt-on” manner) with LISP to build encrypted VPNs.

Because LISP separates locators and endpoint identifiers, encryption can be added using IPsec or GETVPN by applying the crypto map to either the EID side (LISP0 virtual interface), or to the locator side (RLOC interface(s)), as illustrated in Figure 1.

*Figure 1. Crypto Map application points available to “bolt-on” GETVPN with LISP.*

Depending on where the crypto map is applied (as per Figure 1), the resulting configuration details change, as does the resultant packet handling and encrypted packet format. This document focuses solely on the GETVPN+LISP solution that applies the crypto map to the LISP0 virtual interface. This is the most common architecture and provides the most flexibility for applying unique security policies within the resultant VPN environment. When applied to **LISP0**, GETVPN encryption occurs first, followed by LISP encapsulation. The packet construction process is illustrated in Figure 2 below.

*Figure 2. LISP with GETVPN applied to LISP0 results in GETVPN and then LISP encapsulation.*
Recalling that LISP implements “Locator/ID” separation to create two namespaces - EIDs and RLOCs, it is easy to see that LISP can consider both EID and RLOC namespaces for virtualization. Either or both can be virtualized.

- Associating a LISP Instance-ID to an EID VRF enables EID virtualization. Instance-IDs are numerical tags defined in the LISP Canonical Address Format (LCAF) draft, and are used to maintain EID address space segmentation in both the control plane and data plane. EID namespace virtualization is referred to in LISP as “shared model,” because multiple, distinct EID namespaces, as segmented by VRFs and instance-ids, are “sharing” a common RLOC namespace. Shared model virtualization is illustrated in Figure 3 below. Notice in Figure 3 that a “LISP0” virtual interface is automatically created for each Instance-ID, but in this case, each new virtual interface is referenced to the Instance-ID. Thus, as shown in Figure 3, IID 1 is associated with LISP0.1, IID2 is associated with LISP0.2, and IID3 is associated with LISP0.3. (This will be important when crypto-maps are added to the configuration.)

- When multiple RLOC namespaces exist (and associated mapping services), the RLOC namespace can be virtualized. This is referred to in LISP as “parallel model” virtualization, because multiple, distinct RLOC namespaces, as segmented by VRFs, are used in “parallel.” In this model, one or more EID namespaces is associated to a specific RLOC namespace, and multiple RLOC namespaces are configured.

Additional details on LISP virtualization details can be found in Reference [2].

Figure 3. LISP shared model virtualization showing three separate EID namespaces, segmented by LISP instance-ids associated with EID VRFs, and sharing a single, IPv4 RLOC namespace.

GETVPN + LISP Example Configuration

Reference LISP VPN Architecture

The notional Enterprise VPN architecture used as an example here incorporates LISP with shared model virtualization and GETVPN for encryption. This notional topology, which is illustrated in Figure 4, includes the following elements.

- The topology includes a “Head Quarters” site and three “Remote Office” sites.
  - The HQ site is multihomed using two CPE routers, each with a single WAN connection to the IPv4 core network. These CPE routers function as LISP xTRs, as well as MS/MRs for the entire VPN. In addition, these CPE routers are also GETVPN GMs. The HQ site also hosts two separate CPE routers that function as redundant GETVPN Key Servers.
  - One Remote site is also multihomed and uses a single CPE router, and the other two Remote sites are single homed to the IPv4 core network. All CPE routers at these remote sites function as LISP xTRs, as well as GETVPN GMs.
- The core network is running IPv4. (Note that if the core network were instead running IPv6, only a single configuration change would be required on each site – that of the RLOC address. No other changes to other configurations, including the GETVPN configuration, would be necessary.)

- Three “departmental VPNs” are configured at all four sites; each of these VPNs includes both IPv4 and IPv6 site prefixes (EIDs).

- GETVPN is added on a per-VRF and per-address family basis (i.e. IPv4 and IPv6 associated with each VRF is encrypted separately). Redundant Key Servers are also deployed.

Figure 4. Reference LISP VPN architecture incorporating a Head Quarters site and three Remote sites.

Specific details about each CPE router illustrated in Figure 4 follow.

**HQ Site**

**RTR14 – xTR/MS/MR/GM**

RTR14 is a LISP xTR, LISP MS/MR, and GETVPN GM. It is connected to the IPv4 core with a single WAN connection of this own, but forms part of a multi-homed site. RTR18, one of the GETVPN Key Servers also is directly connected to RTR14 in default IPv4 EID space.

RLOC: 10.0.14.2/30
Loopback 0: Default/IID 0/ (ipv4) 192.168.255.14/32 (management)
VRF DeptA/IID 1/(ipv4) 192.168.14.0/24 (ipv6) 1:1:14::/64
VRF DeptB/IID 2/(ipv4) 192.168.14.0/24 (ipv6) 2:2:14::/64
VRF DeptC/IID 3/(ipv4) 192.168.14.0/24 (ipv6) 3:3:14::/64

**RTR15 – xTR/MS/MR/GM**

RTR15 is a LISP xTR, LISP MS/MR, and GETVPN GM. It is connected to the IPv4 core with a single WAN connection of this own, but forms part of a multi-homed site. RTR19, one of the GETVPN Key Servers also is directly connected to RTR15 in default IPv4 EID space.

RLOC: 10.0.15.2/30
Loopback 0: Default/IID 0/ (ipv4) 192.168.255.15/32 (management)
VRF DeptA/IID 1/(ipv4) 192.168.14.0/24 (ipv6) 1:1:14::/64

© 1992-2012 Cisco Systems, Inc. All rights reserved.
VRF DeptB/IID 2/ (ipv4) 192.168.14.0/24 (ipv6) 2:2:14::/64
VRF DeptC/IID 3/ (ipv4) 192.168.14.0/24 (ipv6) 3:3:14::/64

**RTR18 – Key Server 1**
RTR18 is one of two GETVPN Key Servers (RTR19 is the other one). It is directly connected to RTR14 in default IPv4 EID space.

- Eth0/0: Default/IID 0/ (ipv4) 192.168.18.2/24 (Eth0/0)

**RTR19 – Key Server 2**
RTR19 is one of two GETVPN Key Servers (RTR18 is the other one). It is directly connected to RTR15 in default IPv4 EID space.

- Eth0/0: Default/IID 0/ (ipv4) 192.168.19.2/24 (Eth0/0)

**Remote Site 11**
**RTR11 – xTR/GM**
RTR11 is a LISP xTR and GETVPN GM. It is connected to the IPv4 core with a single WAN connection and forms its own site.

- RLOC: 10.0.11.2/30
- Loopback 0: Default/IID 0/ (ipv4) 192.168.255.11/32 (management)
- VRF DeptA/IID 1/ (ipv4) 192.168.11.0/24 (ipv6) 1:1:11::/64
- VRF DeptB/IID 2/ (ipv4) 192.168.11.0/24 (ipv6) 2:2:11::/64
- VRF DeptC/IID 3/ (ipv4) 192.168.11.0/24 (ipv6) 3:3:11::/64

**Remote Site 16**
**RTR16 – xTR/GM**
RTR16 is a LISP xTR and GETVPN GM. It is multihomed to the IPv4 core with two WAN connections and forms its own site.

- RLOC: 10.0.16.2/30
- RLOC: 10.0.16.6/30
- Loopback 0: Default/IID 0/ (ipv4) 192.168.255.11/32 (management)
- VRF DeptA/IID 1/ (ipv4) 192.168.11.0/24 (ipv6) 1:1:11::/64
- VRF DeptB/IID 2/ (ipv4) 192.168.11.0/24 (ipv6) 2:2:11::/64
- VRF DeptC/IID 3/ (ipv4) 192.168.11.0/24 (ipv6) 3:3:11::/64

**Remote Site 13**
**RTR13 – xTR/GM**
RTR13 is a LISP xTR and GETVPN GM. It is connected to the IPv4 core with a single WAN connection and forms its own site.

- RLOC: 10.0.13.2/30
- Loopback 0: Default/IID 0/ (ipv4) 192.168.255.13/32 (management)
- VRF DeptA/IID 1/ (ipv4) 192.168.13.0/24 (ipv6) 1:1:13::/64
- VRF DeptB/IID 2/ (ipv4) 192.168.13.0/24 (ipv6) 2:2:13::/64
- VRF DeptC/IID 3/ (ipv4) 192.168.13.0/24 (ipv6) 3:3:13::/64

The remainder of this document provides detailed descriptions of the LISP and GETVPN configurations used to implement the architecture shown in Figure 4 and addressing listed above. Three areas are highlighted in each configuration (as appropriate to the device): (1) the general configuration, including RLOC connectivity to the IPv4 core, (2) the LISP configuration to implement multihoming, IPv4 and IPv6 enterprise prefixes, and virtualization, and (3) the GETVPN configuration to implement encryption for each VPN. Verification steps are also shown, providing procedures to validate successful deployment. Full configurations for each router are also provided in Appendix A. (Note that the configuration for RTR12, shown in outline in the IPv4 core network in Figure 4, is also provided in Appendix A.)
Configurations Explanations

The full configurations for all routers in this GETVPN+LISP example are provide in Appendix A. The following sections provide explanatory notes for the architectural philosophy used in the example, and the major configuration sections used to implement that philosophy.

1. **General Configurations**
   - All routers are configured with IPv4 WAN connections. LISP uses this connection and IP address as its RLOCs for encapsulation. Only a default route is used. For example, RTR14 is configured as follows:

```
interface Ethernet0/0
  ip address 10.0.14.2 255.255.255.252
  ip route 0.0.0.0 0.0.0.0 10.0.14.1
```

All routers are configured in a similar manner.

   - For the purposes of this example, all LISP EIDs are attached to Loopback interfaces. This simply holds the prefixes and provides ping targets for each prefix. For example, RTR11 is configured as follows:

```
interface Loopback0
  ip address 192.168.255.11 255.255.255.255
  ipv6 address 1::11/128

interface Loopback1
  vrf forwarding DeptA
  ip address 192.168.11.1 255.255.255.0
  ipv6 address 1:1:11::1/64

interface Loopback2
  vrf forwarding DeptB
  ip address 192.168.11.1 255.255.255.0
  ipv6 address 2:2:11::1/64

interface Loopback3
  vrf forwarding DeptC
  ip address 192.168.11.1 255.255.255.0
  ipv6 address 3:3:11::1/64
```

(Note that RTR14 and RTR15 are exceptions since both routers are connecting the same EID prefixes and so the EIDs are associated with Eth0/0.) In a real deployment, these EID prefixes would be associated with VLANs or networks attached to the router, with possibly some routing protocol (IGP) running as well.

3. **LISP Configurations**

The LISP VPN configuration can be added first. This establishes the Departmental VPNs for each address-family. This requires the configuration of the LISP xTRs, and MS/MRs.

   - LISP xTRs configurations on RTR14, RTR15, RTR11, RTR16, and RTR13 have entries for the default EID table, associated with IID0, as well as the three Departmental VPNs (VRF DeptA, VRF DeptB, and VRF DeptC, associated with IID 1, 2, and 3 respectively.) For example, RTR14 is configured as follows:

```
router lisp
  locator-set HQ-RLOC
    10.0.14.2 priority 1 weight 50
    10.0.15.2 priority 1 weight 50
  exit
  eid-table default instance-id 0
  database-mapping 192.168.18.0/24 10.0.14.2 priority 1 weight 1
  database-mapping 192.168.255.14/32 10.0.14.2 priority 1 weight 1
```

© 1992-2012 Cisco Systems, Inc. All rights reserved.
The use of the `locator-set` command (above) simplifies the `database-mapping` command definition by summarizing all RLOCs and policies associated with this Site under a single locator-set name. Notice, however, in the multihomed HQ site that for RTR14 and RTR15, the management loopback, configured under `eid-table default`, only includes the `local` RLOC interface in the `database-mapping` command and not the RLOC of the other router at the site. This is shown as an example, meaning, in this case, that access to the /32 management EID is through the `local` RLOC only and not via the other xTR at the same site.

RTR14 and RTR15 also have EID prefixes configured for use by the GETVPN Key Servers. These are 192.168.18.0/24 and 192.168.19.0/24 respectively. These EID prefixes are also configured in the default table with access through the `local` RLOC only and not via the other router at the same site. All GMs reach these KSs using LISP encapsulation in these default EID spaces.

- On Site 11 and Site 13, notice that LISP has been configured to pick up the IPv4 RLOC address automatically. This accommodates sites where DHCP is required, such as on most broadband connections. RTR 11 is show as an example:

```plaintext
! router lisp
  eid-table default instance-id 0
  database-mapping 192.168.255.11/32 IPv4-interface Ethernet0/0 priority 1 weight 1
  !
  exit
  !
  etc...
```

- The Map-Server configuration is integrated with the Hub site routers RTR14 and RTR15. For example, RTR14 is configured as follows:

```plaintext
! site HQ
  authentication-key hq-pswd
  eid-prefix 192.168.18.0/24
  eid-prefix 192.168.19.0/24
```
Notice that the EID prefixes configured without an instance-id are associated with the default table, and those configured with an instance-id are associated with that particular VPN. (See LISP shared model details in [2].)

3. LISP Verification
- You can verify that all sites are correctly configured for their own EID prefixes by looking at the output of the `show ip lisp data` command, or `show ipv6 lisp data` command – for each instance-id configured.

RTR14 is shown here as an example:

```
RTR14-xTR# show ip lisp data instance-id 0
LISP ETR IPv4 Mapping Database for EID-table default (IID 0), LSBs: 0x1, 2 entries
192.168.18.0/24
 Locator Pri/Wgt Source     State
  10.0.14.2  1/1    cfg-addr site-self, reachable
192.168.255.14/32
 Locator Pri/Wgt Source     State
  10.0.14.2  1/1    cfg-addr site-self, reachable
```
And...

RTR14-xTR# show ip lisp data instance-id 1
LISP ETR IPv4 Mapping Database for EID-table vrf DeptA (IID 1), LSBs: 0x3, 1 entries

Locator  Pri/Wgt  Source     State
10.0.14.2    1/50   cfg-addr site-self, reachable
10.0.15.2    1/50   cfg-addr site-other, report-reachable

RTR14-xTR# show ip lisp data instance-id 2
LISP ETR IPv4 Mapping Database for EID-table vrf DeptB (IID 2), LSBs: 0x3, 1 entries

Locator  Pri/Wgt  Source     State
10.0.14.2    1/50   cfg-addr site-self, reachable
10.0.15.2    1/50   cfg-addr site-other, report-reachable

RTR14-xTR# show ip lisp data instance-id 3
LISP ETR IPv4 Mapping Database for EID-table vrf DeptC (IID 3), LSBs: 0x3, 1 entries

Locator  Pri/Wgt  Source     State
10.0.14.2    1/50   cfg-addr site-self, reachable
10.0.15.2    1/50   cfg-addr site-other, report-reachable

RTR14-xTR# show ipv6 lisp data instance-id 0
% No local database entries configured.

RTR14-xTR# show ipv6 lisp data instance-id 1
LISP ETR IPv6 Mapping Database for EID-table vrf DeptA (IID 1), LSBs: 0x3, 1 entries

1:1:14::/64, locator-set HQ-LROC

Locator  Pri/Wgt  Source     State
10.0.14.2    1/50   cfg-addr site-self, reachable
10.0.15.2    1/50   cfg-addr site-other, report-reachable

RTR14-xTR# show ipv6 lisp data instance-id 2
LISP ETR IPv6 Mapping Database for EID-table vrf DeptB (IID 2), LSBs: 0x3, 1 entries

2:2:14::/64, locator-set HQ-LROC

Locator  Pri/Wgt  Source     State
10.0.14.2    1/50   cfg-addr site-self, reachable
10.0.15.2    1/50   cfg-addr site-other, report-reachable

RTR14-xTR# show ipv6 lisp data instance-id 3
LISP ETR IPv6 Mapping Database for EID-table vrf DeptC (IID 3), LSBs: 0x3, 1 entries

3:3:14::/64, locator-set HQ-LROC

Locator  Pri/Wgt  Source     State
10.0.14.2    1/50   cfg-addr site-self, reachable
10.0.15.2    1/50   cfg-addr site-other, report-reachable

RTR14-xTR#

- All LISP Site ETRs register to both Map-Servers (RTR14 and RTR15) – including RTR14 and RTR15 (which essentially means the ETR function on RTR14 and RTR15 registers to the MS function on RTR14 and RTR15). You can verify that all sites are correctly registering by looking at the output of the show lisp site command on RTR14 or RTR15, shown here on RTR14 as an example:

RTR14-xTR# show lisp site
LISP Site Registration Information

<table>
<thead>
<tr>
<th>Site Name</th>
<th>Last Register</th>
<th>Up</th>
<th>Who Last Registered</th>
<th>Inst ID</th>
<th>EID Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>HQ</td>
<td>00:00:46</td>
<td>yes</td>
<td>10.0.14.2</td>
<td>0</td>
<td>192.168.18.0/24</td>
</tr>
<tr>
<td></td>
<td>00:00:05</td>
<td>yes</td>
<td>10.0.15.2</td>
<td>0</td>
<td>192.168.19.0/24</td>
</tr>
<tr>
<td></td>
<td>00:00:46</td>
<td>yes</td>
<td>10.0.14.2</td>
<td>0</td>
<td>192.168.255.14/32</td>
</tr>
<tr>
<td></td>
<td>00:00:05</td>
<td>yes</td>
<td>10.0.15.2</td>
<td>0</td>
<td>192.168.255.15/32</td>
</tr>
<tr>
<td></td>
<td>00:00:09</td>
<td>yes</td>
<td>10.0.14.2</td>
<td>1</td>
<td>1:1:14::/64</td>
</tr>
<tr>
<td></td>
<td>00:00:56</td>
<td>yes</td>
<td>10.0.14.2</td>
<td>1</td>
<td>1:1:14::/64</td>
</tr>
<tr>
<td></td>
<td>00:00:32</td>
<td>yes</td>
<td>10.0.15.2</td>
<td>2</td>
<td>192.168.14.0/24</td>
</tr>
<tr>
<td></td>
<td>00:00:23</td>
<td>yes</td>
<td>10.0.15.2</td>
<td>2</td>
<td>2:2:14::/64</td>
</tr>
<tr>
<td></td>
<td>00:00:54</td>
<td>yes</td>
<td>10.0.15.2</td>
<td>3</td>
<td>192.168.14.0/24</td>
</tr>
<tr>
<td></td>
<td>00:00:43</td>
<td>yes</td>
<td>10.0.14.2</td>
<td>3</td>
<td>3:3:14::/64</td>
</tr>
<tr>
<td>Site11</td>
<td>00:00:07</td>
<td>yes</td>
<td>10.0.11.2</td>
<td>0</td>
<td>192.168.255.11/32</td>
</tr>
</tbody>
</table>
At this point, connectivity between all LISP sites across default EID space and virtualized EID space (IIDs) should be available. This can be verified by “source pinging” a few (or all) of the available EID prefixes. For example, the output of various ping commands in shown for RTR11 next, in default EID space, to each of the other site xTRs.

```
RTR11-xTR#ping 192.168.255.13 source 192.168.255.11 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.255.13, timeout is 2 seconds:
Packet sent with a source address of 192.168.255.11
!!!!!!!!
Success rate is 80 percent (8/10), round-trip min/avg/max = 1/1/1 ms
```

```
RTR11-xTR#ping 192.168.255.16 source 192.168.255.11 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.255.16, timeout is 2 seconds:
Packet sent with a source address of 192.168.255.11
!!!!!!!!
Success rate is 80 percent (8/10), round-trip min/avg/max = 1/1/1 ms
```

```
RTR11-xTR#ping 192.168.255.14 source 192.168.255.11 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.255.14, timeout is 2 seconds:
Packet sent with a source address of 192.168.255.11
!!!!!!!!
Success rate is 80 percent (8/10), round-trip min/avg/max = 2/5/6 ms
```

```
RTR11-xTR#ping 192.168.255.15 source 192.168.255.11 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.255.15, timeout is 2 seconds:
Packet sent with a source address of 192.168.255.11
!!!!!!!!
Success rate is 90 percent (9/10), round-trip min/avg/max = 1/5/7 ms
```

And the resultant LISP map-cache for the default IPv4 EID space follows:

```
RTR11-xTR#show ip lisp map-cache instance-id 0
LISP IPv4 Mapping Cache for EID-table default (IID 0), 5 entries
  0.0.0.0/0, uptime: 00:02:41, expires: never, via static send map-request
  Negative cache entry, action: send-map-request
  192.168.255.13/32, uptime: 00:01:36, expires: 23:58:26, via map-reply, complete
    Locator Uptime State Pri/Wgt
    10.0.13.2 00:01:36 up 1/1
  192.168.255.14/32, uptime: 00:00:43, expires: 23:59:18, via map-reply, complete
    Locator Uptime State Pri/Wgt
    10.0.14.2 00:00:43 up 1/1
  192.168.255.15/32, uptime: 00:00:34, expires: 23:59:26, via map-reply, complete
    Locator Uptime State Pri/Wgt
    10.0.15.2 00:00:34 up 1/1
  192.168.255.16/32, uptime: 00:00:58, expires: 23:59:03, via map-reply, complete
    Locator Uptime State Pri/Wgt
    10.0.16.6 00:00:58 up 1/1
```
The above process can be repeated for each Departmental VPN. Here, the output of the ping command in shown for RTR11 again, this time in the DeptA VPN, for both IPv4 and IPv6 EIDs, to each of the other site xTRs. Other VPNs will be similar.

RTR11-xTR#ping vrf DeptA 192.168.13.1 source 192.168.11.1 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.13.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
....
Success rate is 80 percent (8/10), round-trip min/avg/max = 1/1/1 ms
RTR11-xTR#ping vrf DeptA 192.168.14.1 source 192.168.11.1 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.14.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
....
Success rate is 80 percent (8/10), round-trip min/avg/max = 1/1/1 ms
RTR11-xTR#ping vrf DeptA 192.168.16.1 source 192.168.11.1 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.16.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
....
Success rate is 80 percent (8/10), round-trip min/avg/max = 1/1/1 ms
RTR11-xTR#
RTR11-xTR#ping vrf DeptA 1:1:13::1 source 1:1:11::1 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 1:1:13::1, timeout is 2 seconds:
Packet sent with a source address of 1:1:11::1%DeptA
....
Success rate is 80 percent (8/10), round-trip min/avg/max = 1/1/1 ms
RTR11-xTR#ping vrf DeptA 1:1:14::1 source 1:1:11::1 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 1:1:14::1, timeout is 2 seconds:
Packet sent with a source address of 1:1:11::1%DeptA
....
Success rate is 80 percent (8/10), round-trip min/avg/max = 1/1/1 ms
RTR11-xTR#ping vrf DeptA 1:1:16::1 source 1:1:11::1 rep 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 1:1:16::1, timeout is 2 seconds:
Packet sent with a source address of 1:1:11::1%DeptA
....
Success rate is 80 percent (8/10), round-trip min/avg/max = 1/1/1 ms
RTR11-xTR#

And the resultant LISP map-cache for the default IPv4 EID space follows:

RTR11-xTR#show ip lisp map-cache instance-id 1
LISP IPv4 Mapping Cache for EID-table vrf DeptA (IID 1), 4 entries
0.0.0.0/0, uptime: 00:11:15, expires: never, via static send map-request
   Negative cache entry, action: send-map-request
192.168.13.0/24, uptime: 00:01:49, expires: 23:58:14, via map-reply, complete
   Locator    Uptime    State      Pri/Wgt
   10.0.13.2  00:01:49 up           1/1
192.168.14.0/24, uptime: 00:01:38, expires: 23:58:25, via map-reply, complete
   Locator    Uptime    State      Pri/Wgt
   10.0.14.2  00:01:38 up           1/50
10.0.15.2  00:01:38 up           1/50
192.168.16.0/24, uptime: 00:01:29, expires: 23:58:34, via map-reply, complete
   Locator    Uptime    State      Pri/Wgt
   10.0.16.2  00:01:29 up           1/50
10.0.16.6  00:01:29 up           1/50
RTR11-xTR#
RTR11-xTR#show ipv6 lisp map-cache instance-id 1
LISP IPv6 Mapping Cache for EID-table vrf DeptA (IID 1), 4 entries
::/0, uptime: 00:11:14, expires: never, via static send map-request
   Negative cache entry, action: send-map-request
- Notice that the IPv4 EID prefix 192.168.14.0/24 and IPv6 EID prefix 1:1:14::/64 each have two RLOC addresses indicated. These prefixes a associated with mulithomed LISP sites.

4. GETVPN Configurations

Of course, the data planes for the LISP VPNs configured above are not encrypted. The following section adds GETVPN configurations to provide encryption for each VPN and each address-family separately.

- The Key Servers, RTR18 and RTR19, are configured as redundant pairs. The Key Server addresses, 192.168.18.2 and 192.168.19.2 respectively, are reachable as EID addresses in the default table. This means that each GM uses LISP encapsulation (in the default table) to reach the Key Servers. Although not illustrated in this example, running the Key Servers in IPv4 LISP EID space allows the use of these GETVPN KSs, even if the core is an IPv6-only network. (This example uses an IPv4 core, but if an IPv6 core were used as RLOC space, no changes whatsoever would be need on the KSs or LISP devices.

- The crypto configurations defined on the Key Servers create three separate IPv4 and three separate IPv6 gdoi groups, each with their own identity number and “match address” ACLs. This permits the attachment of unique crypto policies to each Departmental VPN, and for each Address-Family. This is an example of the IPv4 policy:

```plaintext
crypto gdoi group V4GROUP-0001
  identity number 10001
  server local
  rekey retransmit 60 number 2
  rekey authentication mypubkey rsa GET-KEYS1
  rekey transport unicast
  sa ipsec 1
  profile GDOI-PROFILE
  match address ipv4 GETVPN-0001
  replay time window-size 5
  address ipv4 192.168.10.2
  redundancy
  local priority 100
  peer address ipv4 192.168.19.2

! ip access-list extended GETVPN-0001
  permit ip any any
```

And this is an example of an IPv6 policy:

```plaintext
crypto gdoi group ipv6 V6GROUP-0001
  identity number 20001
  server local
  rekey retransmit 60 number 2
  rekey authentication mypubkey rsa GET-KEYS1
  rekey transport unicast
  sa ipsec 1
  profile GDOI-PROFILE
  match address ipv6 GETVPN6-0001
  replay time window-size 5
  address ipv4 192.168.18.2
  redundancy

! ip access-list extended GETVPN6-0001
  permit ip any any
```
The GETVPN crypto configuration applied to ALL GMs is IDENTICAL. (This is one of the nice features of GETVPN – that all GM configurations are just “cut and paste” without any differences.) Once the GM crypto configuration is added (see full configs above), it is simply a matter of applying the correct crypto map command to each LISP0.x interface. Here’s an example:

```
! interface LISP0
! interface LISP0.1
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0001
  crypto map MAP-V4-0001
! interface LISP0.2
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0002
  crypto map MAP-V4-0002
! interface LISP0.3
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0003
  crypto map MAP-V4-0003
!
```

The LISP process automatically creates each LISP0.x virtual interfaces once an IID is configured. Notice above that the LISP0 (default table) does not have a crypto map and thus incurs no encryption. Only the LISP0.x interfaces associated with the Departmental VPNs are encrypted – each with its own policy, and on a per address-family basis as well. Also notice above that the IPv4 and IPv6 MTU have been adjusted to alert the crypto process to the additional overhead for LISP encapsulation.

5. GETVPN Verification

- You can verify that all GMs are associated to the Key Servers using the the show ip show crypto gdoi ks members command. By adding a specific group member address, information can be restricted to a single site. For example, here is the output from RTR18-KS1 for RTR16. Notice that six separate groups are registered – one for each VPN and one for each address-family:

```
RTR18-KS1#show crypto gdoi ks members 192.168.255.16
Number of rekeys sent for group V4GROUP-0001 : 0

  Group Member ID : 192.168.255.16  GM Version: 1.0.4
  Group ID        : 10001
  Group Name      : V4GROUP-0001
  Key Server ID   : 192.168.19.2
  Rekeys sent     : 0
  Rekeys retries  : 0
  Rekey Acks Rcvd : 0
  Rekey Acks missed : 0
  Sent seq num   : 0 0 0 0 0
  Rcvd seq num   : 0 0 0 0 0

Number of rekeys sent for group V4GROUP-0002 : 0

  Group Member ID : 192.168.255.16  GM Version: 1.0.4
  Group ID        : 10002
  Group Name      : V4GROUP-0002
  Key Server ID   : 192.168.19.2
```

© 1992-2012 Cisco Systems, Inc. All rights reserved.
- On the GMs, the standard “show crypto” commands are available and can be used to validate ISAKMP and IPSEC parameters. For example, useful commands might include `show crypto isakmp sa` and `show crypto ipsec sa` amongst others.
To validate that encryption is occurring, repeat the pings from item #3 (LISP verification) above and then check the output from the show crypto engine connection active command. Here's an example from RTR11:

```
RTR11-xTR#ping vrf DeptA 192.168.13.1 source 192.168.11.1 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.13.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
RTR11-xTR#sh cry eng conn ac
Crypto Engine Connections

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Algorithm</th>
<th>Encrypt</th>
<th>Decrypt</th>
<th>LastSeqN</th>
<th>IP-Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>137</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>FE80::A8BB:CCFF:FE00:B00</td>
</tr>
<tr>
<td>138</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>FE80::A8BB:CCFF:FE00:B00</td>
</tr>
<tr>
<td>139</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>FE80::A8BB:CCFF:FE00:B00</td>
</tr>
<tr>
<td>140</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>FE80::A8BB:CCFF:FE00:B00</td>
</tr>
<tr>
<td>141</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>FE80::A8BB:CCFF:FE00:B00</td>
</tr>
<tr>
<td>142</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>FE80::A8BB:CCFF:FE00:B00</td>
</tr>
<tr>
<td>143</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>192.168.11.1</td>
</tr>
<tr>
<td>144</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>192.168.11.1</td>
</tr>
<tr>
<td>145</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>192.168.11.1</td>
</tr>
<tr>
<td>146</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>192.168.11.1</td>
</tr>
</tbody>
</table>

Notice the encrypt/decrypt packet count. The associated SA IDs are for the VPN (DeptA in this case) and Address-Family (IPv4 in this case). Other VPNS and AFs will use a different IPSec SA pair. For example, again on RTR11, here is the result for another VPN and for IPv6:

```
RTR11-xTR#ping vrf DeptB 2::2:13::1 source 2::2:11::1 rep 1000
Type escape sequence to abort.
Sending 1000, 100-byte ICMP Echos to 2::2:13::1, timeout is 2 seconds:
Packet sent with a source address of 2::2:11::1%DeptB
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
RTR11-xTR#sh cry eng conn ac
Crypto Engine Connections

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Algorithm</th>
<th>Encrypt</th>
<th>Decrypt</th>
<th>LastSeqN</th>
<th>IP-Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>137</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>FE80::A8BB:CCFF:FE00:B00</td>
</tr>
<tr>
<td>138</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>FE80::A8BB:CCFF:FE00:B00</td>
</tr>
<tr>
<td>139</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>FE80::A8BB:CCFF:FE00:B00</td>
</tr>
<tr>
<td>140</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>FE80::A8BB:CCFF:FE00:B00</td>
</tr>
<tr>
<td>141</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>998</td>
<td>0</td>
<td>0</td>
<td>192.168.11.1</td>
</tr>
<tr>
<td>142</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>192.168.11.1</td>
</tr>
<tr>
<td>143</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>192.168.11.1</td>
</tr>
<tr>
<td>144</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>100</td>
<td>0</td>
<td>0</td>
<td>192.168.11.1</td>
</tr>
<tr>
<td>145</td>
<td>IPsec</td>
<td>AES256+SHA512</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>192.168.11.1</td>
</tr>
</tbody>
</table>
```
LISP and Encryption Conclusions

The inherent properties of LISP give it support for multi-homing, virtualization, and host/VM mobility for both IPv4 and IPv6 address families make it an ideal architecture for creating highly efficient, AF-agnostic, Virtual Private Networks (VPNs). Existing IOS encryption support provided by the IPsec and GETVPN features can be used directly (in a “bolt-on” manner) with LISP to build encrypted VPNs. This document describes the application of GETVPN to LISP EIDs.

- Overall, LISP configuration is simple in terms of creating scalable VPNs and for IPv4 and IPv6 address families. In addition, deployment details such as multihoming and dynamic RLOC addressing assignment are also handled seamlessly. The underlying routing core can also be IPv4 or IPv6.
- Adding GETVPN encryption is also simple and straightforward. Using multiple groups permits the application of separate, distinct encryption policies to multiple VPNs and on a per-address family basis.

References

http://lisp.cisco.com/LISP-cfg_gde_IOS_1514XB.pdf


APPENDIX A – Full Configurations For Reference Example

RTR12 – Core Router (provided for lab testing purposes)

```plaintext
! hostname RTR12-core
! no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
! interface Ethernet0/0
  ip address 10.0.11.1 255.255.255.252
! interface Ethernet0/1
  ip address 10.0.13.1 255.255.255.252
! interface Ethernet0/2
  ip address 10.0.14.1 255.255.255.252
! interface Ethernet0/3
  ip address 10.0.15.1 255.255.255.252
! interface Ethernet1/0
  ip address 10.0.16.1 255.255.255.252
! interface Ethernet1/1
  ip address 10.0.16.5 255.255.255.252
! interface Ethernet1/2
  no ip address
  shutdown
! interface Ethernet1/3
  no ip address
  shutdown
! ip forward-protocol nd
! no ip http server
no ip http secure-server
! control-plane
! line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
line vty 0 4
  exec-timeout 0 0
  privilege level 15
password cisco
login
  transport input all
end
```

RTR18 – KS-1

```plaintext
! hostname RTR18-KS1
! no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
```
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 16
crypto isakmp key FOO address 0.0.0.0
crypto isakmp keepalive 15 periodic

! crypto ipsec transform-set GDOI-TRANS esp-aes 256 esp-sha512-hmac
! crypto ipsec profile GDOI-PROFILE
  set transform-set GDOI-TRANS
!
crypto gdoi group V4GROUP-0001
  identity number 10001
  server local
  rekey retransmit 60 number 2
  rekey authentication mypubkey rsa GET-KEYS1
  rekey transport unicast
  sa ipsec 1
    profile GDOI-PROFILE
    match address ipv4 GETVPN-0001
    replay time window-size 5
    address ipv4 192.168.18.2
  redundancy
    local priority 100
    peer address ipv4 192.168.19.2
!!
crypto gdoi group V4GROUP-0002
  identity number 10002
  server local
  rekey retransmit 60 number 2
  rekey authentication mypubkey rsa GET-KEYS2
  rekey transport unicast
  sa ipsec 1
    profile GDOI-PROFILE
    match address ipv4 GETVPN-0002
    replay time window-size 5
    address ipv4 192.168.18.2
  redundancy
    local priority 100
    peer address ipv4 192.168.19.2
!!
crypto gdoi group V4GROUP-0003
  identity number 10003
  server local
  rekey retransmit 60 number 2
  rekey authentication mypubkey rsa GET-KEYS3
  rekey transport unicast
  sa ipsec 1
    profile GDOI-PROFILE
    match address ipv4 GETVPN-0003
    replay time window-size 5
    address ipv4 192.168.18.2
  redundancy
    local priority 100
    peer address ipv4 192.168.19.2
!!
crypto gdoi group ipv6 V6GROUP-0001
  identity number 20001
  server local
  rekey retransmit 60 number 2
  rekey authentication mypubkey rsa GET-KEYS1
  rekey transport unicast
  sa ipsec 1
    profile GDOI-PROFILE
    match address ipv6 GETVPN6-0001
    replay time window-size 5
    address ipv4 192.168.18.2
  redundancy
    local priority 100
peer address ipv4 192.168.19.2
!
crypto gdoi group ipv6 V6GROUP-0002
  identity number 20002
  server local
  rekey retransmit 60 number 2
  rekey authentication mypubkey rsa GET-KEYS2
  rekey transport unicast
  sa ipsec 1
  profile GDOI-PROFILE
  match address ipv6 GETVPN6-0002
  replay time window-size 5
  address ipv4 192.168.18.2
  redundancy
  local priority 100
  peer address ipv4 192.168.19.2
!
crypto gdoi group ipv6 V6GROUP-0003
  identity number 20003
  server local
  rekey retransmit 60 number 2
  rekey authentication mypubkey rsa GET-KEYS3
  rekey transport unicast
  sa ipsec 1
  profile GDOI-PROFILE
  match address ipv6 GETVPN6-0003
  replay time window-size 5
  address ipv4 192.168.18.2
  redundancy
  local priority 100
  peer address ipv4 192.168.19.2
!
interface Ethernet0/0
  ip address 192.168.18.2 255.255.255.0
  !
  no ip http server
  no ip http secure-server
  ip route 0.0.0.0 0.0.0.0 192.168.18.1
  !
ip access-list extended GETVPN-0001
  permit ip any any
  ip access-list extended GETVPN-0002
  permit ip any any
  ip access-list extended GETVPN-0003
  permit ip any any
  !
ipv6 access-list GETVPN6-0001
  permit ipv6 any any
  !
ipv6 access-list GETVPN6-0002
  permit ipv6 any any
  !
ipv6 access-list GETVPN6-0003
  permit ipv6 any any
  !
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  line aux 0
  line vty 0 4
  exec-timeout 0 0
  privilege level 15
  password cisco
  login
  transport input all
  !
end
hostname RTR19-KS2
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
crypto isakmp policy 10
enccr aes 256
authentication pre-share
group 16
crypto isakmp key FOO address 0.0.0.0
crypto isakmp keepalive 15 periodic

crypto ipsec transform-set GDOI-TRANS esp-aes 256 esp-sha512-hmac

crypto ipsec profile GDOI-PROFILE
set transform-set GDOI-TRANS

crypto gdoi group V4GROUP-0001
identity number 10001
server local
rekey retransmit 60 number 2
rekey authentication mypubkey rsa GET-KEYS1
rekey transport unicast
sa ipsec 1
profile GDOI-PROFILE
match address ipv4 GETVPN-0001
replay time window-size 5
address ipv4 192.168.19.2
redundancy
local priority 100
peer address ipv4 192.168.18.2
!
crypto gdoi group V4GROUP-0002
identity number 10002
server local
rekey retransmit 60 number 2
rekey authentication mypubkey rsa GET-KEYS2
rekey transport unicast
sa ipsec 1
profile GDOI-PROFILE
match address ipv4 GETVPN-0002
replay time window-size 5
address ipv4 192.168.19.2
redundancy
local priority 100
peer address ipv4 192.168.18.2
!
crypto gdoi group V4GROUP-0003
identity number 10003
server local
rekey retransmit 60 number 2
rekey authentication mypubkey rsa GET-KEYS3
rekey transport unicast
sa ipsec 1
profile GDOI-PROFILE
match address ipv4 GETVPN-0003
replay time window-size 5
address ipv4 192.168.19.2
redundancy
local priority 100
peer address ipv4 192.168.18.2
!
crypto gdoi group ipv6 V6GROUP-0001
identity number 20001
server local
rekey retransmit 60 number 2
rekey authentication mypubkey rsa GET-KEYS1
rekey transport unicast
  sa ipsec 1
    profile GDOI-PROFILE
    match address ipv6 GETVPN6-0001
    replay time window-size 5
    address ipv4 192.168.19.2
    redundancy
      local priority 100
      peer address ipv4 192.168.18.2

! crypto gdoi group ipv6 V6GROUP-0002
  identity number 20002
  server local
    rekey retransmit 60 number 2
    rekey authentication mypubkey rsa GET-KEYS2
    rekey transport unicast
      sa ipsec 1
        profile GDOI-PROFILE
        match address ipv6 GETVPN6-0002
        replay time window-size 5
        address ipv4 192.168.19.2
        redundancy
          local priority 100
          peer address ipv4 192.168.18.2

! crypto gdoi group ipv6 V6GROUP-0003
  identity number 20003
  server local
    rekey retransmit 60 number 2
    rekey authentication mypubkey rsa GET-KEYS3
    rekey transport unicast
      sa ipsec 1
        profile GDOI-PROFILE
        match address ipv6 GETVPN6-0003
        replay time window-size 5
        address ipv4 192.168.19.2
        redundancy
          local priority 100
          peer address ipv4 192.168.18.2

! interface Ethernet0/0
  ip address 192.168.19.2 255.255.255.0

! no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.19.1

! ip access-list extended GETVPN-0001
  permit ip any any
ip access-list extended GETVPN-0002
  permit ip any any
ip access-list extended GETVPN-0003
  permit ip any any

! ipv6 access-list GETVPN6-0001
  permit ipv6 any any

! ipv6 access-list GETVPN6-0002
  permit ipv6 any any

! ipv6 access-list GETVPN6-0003
  permit ipv6 any any

! line con 0
  exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
line vty 0 4
exec-timeout 0 0
RTR14 – xTR/GM

! hostname RTR14-xTR
! vrf definition DeptA
  ! address-family ipv4
  ! exit-address-family
  ! address-family ipv6
  ! exit-address-family
! vrf definition DeptB
  ! address-family ipv4
  ! exit-address-family
  ! address-family ipv6
  ! exit-address-family
! vrf definition DeptC
  ! address-family ipv4
  ! exit-address-family
  ! address-family ipv6
  ! exit-address-family
! no ip domain lookup
! ip cef
! ipv6 unicast-routing
! ipv6 cef
! crypto isakmp policy 10
  enacr aes 256
  authentication pre-share
  group 16
! crypto isakmp key FOO address 192.168.18.2
! crypto isakmp key FOO address 192.168.19.2
! crypto gdoi group V4GROUP-0001
  identity number 10001
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
! crypto gdoi group V4GROUP-0002
  identity number 10002
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
! crypto gdoi group V4GROUP-0003
  identity number 10003
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
! crypto gdoi group ipv6 V6GROUP-0001
  identity number 20001
  server address ipv4 192.168.18.2
server address ipv4 192.168.19.2
client registration interface Loopback0
!
crypto gdoi group ipv6 V6GROUP-0002
  identity number 20002
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
client registration interface Loopback0
!
crypto gdoi group ipv6 V6GROUP-0003
  identity number 20003
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
client registration interface Loopback0
!
crypto gdoi group ipv6 V6GROUP-0002
set group V6GROUP-0002
!
crypto map MAP-V4-0001 10 gdoi
set group V4GROUP-0001
!
crypto map MAP-V4-0002 10 gdoi
set group V4GROUP-0002
!
crypto map MAP-V4-0003 10 gdoi
set group V4GROUP-0003
!
crypto map ipv6 MAP-V6-0001 10 gdoi
set group V6GROUP-0001
!
crypto map ipv6 MAP-V6-0002 10 gdoi
set group V6GROUP-0002
!
crypto map ipv6 MAP-V6-0003 10 gdoi
set group V6GROUP-0003
!
interface Loopback0
  ip address 192.168.255.14 255.255.255.255
!
interface LISP0.1
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0001
  crypto map MAP-V4-0001
!
interface LISP0.2
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0002
  crypto map MAP-V4-0002
!
interface LISP0.3
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0003
  crypto map MAP-V4-0003
!
interface Ethernet0/0
  ip address 10.0.14.2 255.255.255.252
!
interface Ethernet0/1
  no ip address
!
interface Ethernet0/1.1
  encapsulation dot1Q 1 native
  vrf forwarding DeptA
  ip address 192.168.14.1 255.255.255.0
  ipv6 address 1:1:14::1/64
!
interface Ethernet0/1.2
  encapsulation dot1Q 2
  vrf forwarding DeptB
ip address 192.168.14.1 255.255.255.0
ipv6 address 2:2:14::1/64
!
interface Ethernet0/1.3
encapsulation dot1Q 3
vrf forwarding DeptC
ip address 192.168.14.1 255.255.255.0
ipv6 address 3:3:14::1/64
!
interface Ethernet0/2
ip address 192.168.18.1 255.255.255.0
!
interface Ethernet0/3
no ip address
shutdown
!
router lisp
locator-set HQ-RLOC
  10.0.14.2 priority 1 weight 50
  10.0.15.2 priority 1 weight 50
!
eid-table default instance-id 0
database-mapping 192.168.18.0/24 10.0.14.2 priority 1 weight 1
database-mapping 192.168.255.14/32 10.0.14.2 priority 1 weight 1
exit
!
eid-table vrf DeptA instance-id 1
database-mapping 192.168.14.0/24 locator-set HQ-RLOC
database-mapping 1:1:14::/64 locator-set HQ-RLOC
exit
!
eid-table vrf DeptB instance-id 2
database-mapping 192.168.14.0/24 locator-set HQ-RLOC
database-mapping 2:2:14::/64 locator-set HQ-RLOC
exit
!
eid-table vrf DeptC instance-id 3
database-mapping 192.168.14.0/24 locator-set HQ-RLOC
database-mapping 3:3:14::/64 locator-set HQ-RLOC
exit
!
site HQ
authentication-key hq-pswd
eid-prefix 192.168.18.0/24
eid-prefix 192.168.19.0/24
eid-prefix 192.168.255.14/32
eid-prefix 192.168.255.15/32
eid-prefix instance-id 1 192.168.14.0/24
eid-prefix instance-id 1 1:1:14::/64
eid-prefix instance-id 2 192.168.14.0/24
eid-prefix instance-id 2 2:2:14::/64
eid-prefix instance-id 3 192.168.14.0/24
eid-prefix instance-id 3 3:3:14::/64
exit
!
site Site11
authentication-key site11-pswd
eid-prefix 192.168.255.11/32
eid-prefix instance-id 1 192.168.11.0/24
eid-prefix instance-id 1 1:1:11::/64
eid-prefix instance-id 2 192.168.11.0/24
eid-prefix instance-id 2 2:2:11::/64
eid-prefix instance-id 3 192.168.11.0/24
eid-prefix instance-id 3 3:3:11::/64
exit
!
site Site13
authentication-key site13-pswd
eid-prefix 192.168.255.13/32
eid-prefix instance-id 1 192.168.13.0/24
eid-prefix instance-id 1 1::13::/64
eid-prefix instance-id 2 192.168.13.0/24
eid-prefix instance-id 2 2::2::13::/64
eid-prefix instance-id 3 192.168.13.0/24
eid-prefix instance-id 3 3::3::13::/64
exit

site Site16
  authentication-key site16-pswd
  eid-prefix 192.168.255.16/32
  eid-prefix instance-id 1 1::1:16::/64
  eid-prefix instance-id 2 192.168.16.0/24
  eid-prefix instance-id 2 2::2:16::/64
  eid-prefix instance-id 3 192.168.16.0/24
  eid-prefix instance-id 3 3::3:16::/64
exit

ipv4 map-server
ipv4 map-resolver
no ipv4 map-cache-persistent
ipv4 itr map-resolver 10.0.14.2
ipv4 itr map-resolver 10.0.15.2
ipv4 itr
ipv4 etr map-server 10.0.14.2 key hq-pswd
ipv4 etr map-server 10.0.15.2 key hq-pswd
ipv4 etr
ipv6 map-server
ipv6 map-resolver
no ipv6 map-cache-persistent
ipv6 itr map-resolver 10.0.14.2
ipv6 itr map-resolver 10.0.15.2
ipv6 itr
ipv6 etr map-server 10.0.14.2 key hq-pswd
ipv6 etr map-server 10.0.15.2 key hq-pswd
ipv6 etr
exit

no ip http server
no ip http secure-server
ip route 10.0.0.0 255.0.0.0 10.0.14.1
! line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
line vty 0 4
  exec-timeout 0 0
  privilege level 15
  password cisco
  login
  transport input all
!
end

RTR15–xTR/GM

! hostname RTR15-xTR
!
! vrf definition DeptA
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
vrf definition DeptB
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
vrf definition DeptC
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 16
crypto isakmp key FOO address 192.168.18.2
crypto isakmp key FOO address 192.168.19.2
!
crypto gdoi group V4GROUP-0001
  identity number 10001
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
crypto gdoi group V4GROUP-0002
  identity number 10002
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
crypto gdoi group V4GROUP-0003
  identity number 10003
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
crypto gdoi group ipv6 V6GROUP-0001
  identity number 20001
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
crypto gdoi group ipv6 V6GROUP-0002
  identity number 20002
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
crypto gdoi group ipv6 V6GROUP-0003
  identity number 20003
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
crypto map MAP-V4-0001 10 gdoi
  set group V4GROUP-0001
!
crypto map MAP-V4-0002 10 gdoi
  set group V4GROUP-0002
!
crypto map MAP-V4-0003 10 gdoi
set group V4GROUP-0003
! crypto map ipv6 MAP-V6-0001 10 gdoi
  set group V6GROUP-0001
! crypto map ipv6 MAP-V6-0002 10 gdoi
  set group V6GROUP-0002
! crypto map ipv6 MAP-V6-0003 10 gdoi
  set group V6GROUP-0003
! interface Loopback0
  ip address 192.168.255.15 255.255.255.255
! interface LISP0
! interface LISP0.1
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0001
  crypto map MAP-V4-0001
! interface LISP0.2
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0002
  crypto map MAP-V4-0002
! interface LISP0.3
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0003
  crypto map MAP-V4-0003
! interface Ethernet0/0
  ip address 10.0.15.2 255.255.255.252
! interface Ethernet0/1
  no ip address
! interface Ethernet0/1.1
  encapsulation dot1Q 1 native
  vrf forwarding DeptA
  ip address 192.168.14.2 255.255.255.0
  ipv6 address 1:1:14::2/64
! interface Ethernet0/1.2
  encapsulation dot1Q 2
  vrf forwarding DeptB
  ip address 192.168.14.2 255.255.255.0
  ipv6 address 2:2:14::2/64
! interface Ethernet0/1.3
  encapsulation dot1Q 3
  vrf forwarding DeptC
  ip address 192.168.14.2 255.255.255.0
  ipv6 address 3:3:14::2/64
! interface Ethernet0/2
  ip address 192.168.19.1 255.255.255.0
! interface Ethernet0/3
  no ip address
  shutdown
! router lisp
  locator-set HQ-RLOC
  10.0.14.2 priority 1 weight 50
  10.0.15.2 priority 1 weight 50
  exit
!
<table>
<thead>
<tr>
<th>Table</th>
<th>Default Instance-ID</th>
<th>Database Mapping</th>
<th>Priority</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>192.168.19.0/24</td>
<td>10.0.15.2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>192.168.255.15/32</td>
<td>10.0.15.2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table</th>
<th>VRF DeptA Instance-ID</th>
<th>Database Mapping</th>
<th>Locator</th>
<th>RLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>192.168.14.0/24</td>
<td>HQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1:1:14::/64</td>
<td>set HQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table</th>
<th>VRF DeptB Instance-ID</th>
<th>Database Mapping</th>
<th>Locator</th>
<th>RLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
<td>192.168.14.0/24</td>
<td>HQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2:2:14::/64</td>
<td>set HQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table</th>
<th>VRF DeptC Instance-ID</th>
<th>Database Mapping</th>
<th>Locator</th>
<th>RLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>192.168.14.0/24</td>
<td>HQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3:3:14::/64</td>
<td>set HQ</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Site</th>
<th>Authentication-Name</th>
<th>Prefixes</th>
<th>Instance-ID</th>
<th>Locator</th>
<th>RLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>HQ</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Site11</td>
<td></td>
<td></td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Site13</td>
<td></td>
<td></td>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Site16</td>
<td></td>
<td></td>
<td>16</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ipv4 Map-Server</th>
<th>Ipv4 Map-Resolver</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 1992-2012 Cisco Systems, Inc. All rights reserved.
ipv4 itr map-resolver 10.0.15.2
ipv4 itr
ipv4 etr map-server 10.0.14.2 key hq-pswd
ipv4 etr map-server 10.0.15.2 key hq-pswd
ipv4 etr
ipv6 map-server
ipv6 map-resolver
no ipv6 map-cache-persistent
ipv6 itr map-resolver 10.0.14.2
ipv6 itr map-resolver 10.0.15.2
ipv6 itr
ipv6 etr map-server 10.0.14.2 key hq-pswd
ipv6 etr map-server 10.0.15.2 key hq-pswd
ipv6 etr
exit
!
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.0.15.1
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
line vty 0 4
  exec-timeout 0 0
  privilege level 15
  password cisco
  login
  transport input all
  !
end
!

RTR11 – xTR/GM
!
hostname RTR11-xTR
!
vrf definition DeptA
!
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
!
vrf definition DeptB
!
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
!
vrf definition DeptC
!
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 16
crypto isakmp key FOO address 192.168.18.2
crypto isakmp key FOO address 192.168.19.2

! crypto gdoi group V4GROUP-0001
  identity number 10001
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
! crypto gdoi group V4GROUP-0002
  identity number 10002
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
! crypto gdoi group V4GROUP-0003
  identity number 10003
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
! crypto gdoi group ipv6 V6GROUP-0001
  identity number 20001
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
! crypto gdoi group ipv6 V6GROUP-0002
  identity number 20002
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
! crypto gdoi group ipv6 V6GROUP-0003
  identity number 20003
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
! crypto map MAP-V4-0001 10 gdoi
  set group V4GROUP-0001
!
! crypto map MAP-V4-0002 10 gdoi
  set group V4GROUP-0002
!
! crypto map MAP-V4-0003 10 gdoi
  set group V4GROUP-0003
!
! crypto map ipv6 MAP-V6-0001 10 gdoi
  set group V6GROUP-0001
!
! crypto map ipv6 MAP-V6-0002 10 gdoi
  set group V6GROUP-0002
!
! crypto map ipv6 MAP-V6-0003 10 gdoi
  set group V6GROUP-0003
!
interface Loopback0
  ip address 192.168.255.11 255.255.255.255
  ipv6 address 1::11/128
!
interface Loopback1
  vrf forwarding DeptA
  ip address 192.168.11.1 255.255.255.0
  ipv6 address 1:1:11::1/64
!
interface Loopback2
  vrf forwarding DeptB
ip address 192.168.11.1 255.255.255.0
ipv6 address 2:2:11::1/64
!
interface Loopback3
vrf forwarding DeptC
ip address 192.168.11.1 255.255.255.0
ipv6 address 3:3:11::1/64
!
interface LISP0
!
interface LISP0.1
ip mtu 1456
ipv6 mtu 1436
ipv6 crypto map MAP-V6-0001
crypto map MAP-V4-0001
!
interface LISP0.2
ip mtu 1456
ipv6 mtu 1436
ipv6 crypto map MAP-V6-0002
crypto map MAP-V4-0002
!
interface LISP0.3
ip mtu 1456
ipv6 mtu 1436
ipv6 crypto map MAP-V6-0003
crypto map MAP-V4-0003
!
interface Ethernet0/0
ip address 10.0.11.2 255.255.255.252
!
interface Ethernet0/1
no ip address
shutdown
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
routing lisp
eid-table default instance-id 0
database-mapping 192.168.255.11/32 IPv4-interface Ethernet0/0 priority 1 weight 1
exit
!
eid-table vrf DeptA instance-id 1
database-mapping 192.168.11.0/24 IPv4-interface Ethernet0/0 priority 1 weight 1
database-mapping 1:1:11::/64 IPv4-interface Ethernet0/0 priority 1 weight 1
exit
!
eid-table vrf DeptB instance-id 2
database-mapping 192.168.11.0/24 IPv4-interface Ethernet0/0 priority 1 weight 1
database-mapping 2:2:11::/64 IPv4-interface Ethernet0/0 priority 1 weight 1
exit
!
eid-table vrf DeptC instance-id 3
database-mapping 192.168.11.0/24 IPv4-interface Ethernet0/0 priority 1 weight 1
database-mapping 3:3:11::/64 IPv4-interface Ethernet0/0 priority 1 weight 1
exit
!
no ipv4 map-cache-persistent
ipv4 itr map-resolver 10.0.14.2
ipv4 itr map-resolver 10.0.15.2
ipv4 itr
ipv4 etr map-server 10.0.14.2 key site11-pswd
ipv4 etr map-server 10.0.15.2 key site11-pswd
ipv4 etr
ipv6 map-server
ipv6 map-resolver
no ipv6 map-cache-persistent
ipv6 itr map-resolver 10.0.14.2
ipv6 itr map-resolver 10.0.15.2
ipv6 itr
ipv6 etr map-server 10.0.14.2 key site11-pswd
ipv6 etr map-server 10.0.15.2 key site11-pswd
ipv6 etr
exit

no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.0.11.1
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
line vty 0 4
  exec-timeout 0 0
  privilege level 15
  password cisco
  login
  transport input all
!
end

RTR13 – xTR/GM

! hostname RTR13-xTR
!
  vrf definition DeptA
  !
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
!
  vrf definition DeptB
  !
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
!
  vrf definition DeptC
  !
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
group 16
crypto isakmp key FOO address 192.168.18.2
crypto isakmp key FOO address 192.168.19.2
!
crypto gdoi group V4GROUP-0001
  identity number 10001
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0

crypto gdoi group V4GROUP-0002
  identity number 10002
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0

crypto gdoi group V4GROUP-0003
  identity number 10003
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0

crypto gdoi group ipv6 V6GROUP-0001
  identity number 20001
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0

crypto gdoi group ipv6 V6GROUP-0002
  identity number 20002
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0

crypto gdoi group ipv6 V6GROUP-0003
  identity number 20003
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0

crypto map MAP-V4-0001 10 gdoi
  set group V4GROUP-0001

crypto map MAP-V4-0002 10 gdoi
  set group V4GROUP-0002

crypto map MAP-V4-0003 10 gdoi
  set group V4GROUP-0003

crypto map ipv6 MAP-V6-0001 10 gdoi
  set group V6GROUP-0001

crypto map ipv6 MAP-V6-0002 10 gdoi
  set group V6GROUP-0002

crypto map ipv6 MAP-V6-0003 10 gdoi
  set group V6GROUP-0003

interface Loopback0
  ip address 192.168.255.13 255.255.255.255

interface Loopback1
  vrf forwarding DeptA
  ip address 192.168.13.1 255.255.255.0
  ipv6 address 1:1:13::/64

interface Loopback2
  vrf forwarding DeptB
  ip address 192.168.13.1 255.255.255.0
  ipv6 address 2:2:13::/64

interface Loopback3
  vrf forwarding DeptC
  ip address 192.168.13.1 255.255.255.0
  ipv6 address 3:3:13::/64
! interface LISP0
! interface LISP0.1
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0001
  crypto map MAP-V4-0001
! interface LISP0.2
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0002
  crypto map MAP-V4-0002
! interface LISP0.3
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0003
  crypto map MAP-V4-0003
! interface Ethernet0/0
  ip address 10.0.13.2 255.255.255.252
! interface Ethernet0/1
  no ip address
  shutdown
! interface Ethernet0/2
  no ip address
  shutdown
! interface Ethernet0/3
  no ip address
  shutdown
! router lisp
  eid-table default instance-id 0
    database-mapping 192.168.255.13/32 IPv4-interface Ethernet0/0 priority 1 weight 1
    exit
  !
  eid-table vrf DeptA instance-id 1
    database-mapping 192.168.13.0/24 IPv4-interface Ethernet0/0 priority 1 weight 1
    database-mapping 1:1:13::/64 IPv4-interface Ethernet0/0 priority 1 weight 1
    exit
  !
  eid-table vrf DeptB instance-id 2
    database-mapping 192.168.13.0/24 IPv4-interface Ethernet0/0 priority 1 weight 1
    database-mapping 2:2:13::/64 IPv4-interface Ethernet0/0 priority 1 weight 1
    exit
  !
  eid-table vrf DeptC instance-id 3
    database-mapping 192.168.13.0/24 IPv4-interface Ethernet0/0 priority 1 weight 1
    database-mapping 3:3:13::/64 IPv4-interface Ethernet0/0 priority 1 weight 1
    exit
  !
  no ipv4 map-cache-persistent
  ipv4 itr map-resolver 10.0.14.2
  ipv4 itr map-resolver 10.0.15.2
  ipv4 itr
  ipv4 etr map-server 10.0.14.2 key site13-pswd
  ipv4 etr map-server 10.0.15.2 key site13-pswd
  ipv4 etr
  ipv6 map-server
  ipv6 map-resolver
  no ipv6 map-cache-persistent
  ipv6 itr map-resolver 10.0.14.2
  ipv6 itr map-resolver 10.0.15.2
  ipv6 itr
  ipv6 etr map-server 10.0.14.2 key site13-pswd
  ipv6 etr map-server 10.0.15.2 key site13-pswd
ipv6 etr
exit
!
o no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.0.13.1
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
line vty 0 4
  exec-timeout 0 0
  privilege level 15
password cisco
login
  transport input all
!
end
!

RTR16 – xTR/GM
!
hostname RTR16-xTR
!
vrf definition DeptA
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
vrf definition DeptB
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
vrf definition DeptC
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
!
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
group 16
crypto isakmp key FOO address 192.168.18.2
crypto isakmp key FOO address 192.168.19.2
!
crypto gdoi group V4GROUP-0001
  identity number 10001
  server address ipv4 192.168.18.2
  server address ipv4 192.168.19.2
  client registration interface Loopback0
!
crypto gdoi group V4GROUP-0002
identity number 10002
server address ipv4 192.168.18.2
server address ipv4 192.168.19.2
client registration interface Loopback0
!
crypto gdoi group V4GROUP-0003
identity number 10003
server address ipv4 192.168.18.2
server address ipv4 192.168.19.2
client registration interface Loopback0
!
crypto gdoi group ipv6 V6GROUP-0001
identity number 20001
server address ipv4 192.168.18.2
server address ipv4 192.168.19.2
client registration interface Loopback0
!
crypto gdoi group ipv6 V6GROUP-0002
identity number 20002
server address ipv4 192.168.18.2
server address ipv4 192.168.19.2
client registration interface Loopback0
!
crypto gdoi group ipv6 V6GROUP-0003
identity number 20003
server address ipv4 192.168.18.2
server address ipv4 192.168.19.2
client registration interface Loopback0
!
crypto map MAP-V4-0001 10 gdoi
set group V4GROUP-0001
!
crypto map MAP-V4-0002 10 gdoi
set group V4GROUP-0002
!
crypto map MAP-V4-0003 10 gdoi
set group V4GROUP-0003
!
crypto map ipv6 MAP-V6-0001 10 gdoi
set group V6GROUP-0001
!
crypto map ipv6 MAP-V6-0002 10 gdoi
set group V6GROUP-0002
!
crypto map ipv6 MAP-V6-0003 10 gdoi
set group V6GROUP-0003
!
interface Loopback0
ip address 192.168.255.16 255.255.255.255
!
interface Loopback1
vrft forwarding DeptA
ip address 192.168.16.1 255.255.255.0
ipv6 address 1:1:16::1/64
!
interface Loopback2
vrft forwarding DeptB
ip address 192.168.16.1 255.255.255.0
ipv6 address 2:2:16::1/64
!
interface Loopback3
vrft forwarding DeptC
ip address 192.168.16.1 255.255.255.0
ipv6 address 3:3:16::1/64
!
interface LISP0
!
interface LISP0.1
ip mtu 1456
ipv6 mtu 1436
ipv6 crypto map MAP-V6-0001
crypto map MAP-V4-0001
!
interface LISP0.2
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0002
  crypto map MAP-V4-0002
!
interface LISP0.3
  ip mtu 1456
  ipv6 mtu 1436
  ipv6 crypto map MAP-V6-0003
  crypto map MAP-V4-0003
!
interface Ethernet0/0
  ip address 10.0.16.2 255.255.255.252
!
interface Ethernet0/1
  ip address 10.0.16.6 255.255.255.252
!
interface Ethernet0/2
  no ip address
  shutdown
!
interface Ethernet0/3
  no ip address
  shutdown
!
routing lisp
  locator-set Site16-RLOC
    10.0.16.2 priority 1 weight 50
    10.0.16.6 priority 1 weight 50
  exit
!
edid-table default instance-id 0
  database-mapping 192.168.255.16/32 locator-set Site16-RLOC
  exit
!
edid-table vrf DeptA instance-id 1
  database-mapping 192.168.16.0/24 locator-set Site16-RLOC
  database-mapping 1:1:16::/64 locator-set Site16-RLOC
  exit
!
edid-table vrf DeptB instance-id 2
  database-mapping 192.168.16.0/24 locator-set Site16-RLOC
  database-mapping 2:2:16::/64 locator-set Site16-RLOC
  exit
!
edid-table vrf DeptC instance-id 3
  database-mapping 192.168.16.0/24 locator-set Site16-RLOC
  database-mapping 3:3:16::/64 locator-set Site16-RLOC
  exit
!
no ipv4 map-cache-persistent
ipv4 itr map-resolver 10.0.14.2
ipv4 itr map-resolver 10.0.15.2
ipv4 itr
ipv4 etr map-server 10.0.14.2 key site16-pswd
ipv4 etr map-server 10.0.15.2 key site16-pswd
ipv4 etr
ipv4 map-server
ipv4 map-resolver
no ipv6 map-cache-persistent
ipv6 itr map-resolver 10.0.14.2
ipv6 itr map-resolver 10.0.15.2
ipv6 itr
ipv6 etr map-server 10.0.14.2 key site16-pswd
ipv6 etr map-server 10.0.15.2 key site16-pswd
ipv6 etr
exit
no ip http server
no ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.0.16.1
ip route 0.0.0.0 0.0.0.0 10.0.16.5
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line aux 0
line vty 0 4
  exec-timeout 0 0
  privilege level 15
  password cisco
  login
  transport input all
!
end
!