Cisco IOS LISP Application Note Series: Network Address Translation

Version 1.1 (28 April 2011)

Background

The LISP Application Note Series provides targeted information that focuses on the integration and configuration of relevant Cisco IOS features in conjunction with the deployment of LISP.

LISP (Locator/ID Separation Protocol) is not a feature, but rather is a next-generation routing architecture which implements a new semantic for IP addressing that creates two namespaces: Endpoint Identifiers (EIDs), which are assigned to end-hosts, and Routing Locators (RLOCs), which are assigned to devices (primarily routers) that make up the global routing system. Creating separate namespaces for EIDs and RLOCs creates a *level of indirection* that yields many advantages over a single namespace (i.e. the current IP address concept) including: improved scalability of the routing system through greater aggregation of RLOCs, improved multi-homing efficiency, ingress traffic engineering, and the ability to move EIDs without breaking sessions (mobility). LISP also was designed at the outset to be Address Family agnostic, and thus handles multiple AF's seamlessly making its use ideal in IPv6 transition solutions.

This and other LISP Application Notes in this series assume a working knowledge of LISP and are not intended to provide basic information on its use-cases, or guidelines on configuration and deployment. These details can be found in the *Cisco LISP Command Reference Guide*, *Cisco LISP Configuration Guide*, (Reference [1]) and other information available at **http:// lisp.cisco.com**.

Application Note Organization

Like all Application Notes in the LISP series, this application note is organized into three main sections.

1. Concept Overview – This section provides a brief description of the feature or technology being addressed in this Application Note in the context of a LISP implementation.
2. Concept Details – This section provides a detailed description of the feature or technology and its interaction with LISP, and a description of its (typical) usage in deployment.
3. Concept Examples – This section provides detailed testing of the feature or technology. This provides verification of the detailed descriptions, and also allows network administrators to set up a similar LISP environment and repeat the feature test.

Comments and corrections are welcome. Please direct all queries to: **lisp-support@cisco.com**.

Concept Overview: Cisco IOS Network Address Translation and LISP

Network Address Translation (NAT) enables private networks that use non-global or private addresses to connect to the Internet. NAT capable devices translate these private addresses into global and routable addresses before forwarding the packets out. It can be used at the enterprise edge to allow enterprise users Internet access and to allow Internet access of internal devices such as web servers. NAT can also be used for advertising of a single address to the Internet for the entire private network, such as is the case for web servers when located behind a Server Load Balance (SLB).

When LISP is deployed, the hosts within a LISP site generally have IP addresses assigned from LISP EID namespace, which is not part of the global Internet routing table (or the upstream provider routing table). Without additional support then, conversations between a host at a LISP site and a host at a non-LISP site would fail. In this case, the LISP site xTR would forward packets natively, and they would reach the non-LISP site, but the return packets cannot reach the host at the LISP site since the EID-prefix is not contained in the global routing Internet table. Therefore, to address LISP-to-Non-LISP communications then, the LISP Interworking draft (Reference [2]) defines two approaches, as follows:

- **Proxy Ingress Tunnel Router (PITR)** – A PITR is a LISP device that provides connectivity between non-LISP sites and LISP sites by advertising a highly aggregated prefix covering LISP EID namespace into the global routing table, this attracting non-LISP traffic destined to LISP sites and encapsulating this traffic to LISP sites.
- **Network Address Translation (NAT)** – The NAT approach relies on the LISP xTR to perform NAT translations from LISP EID source addresses to globally routable addresses before forwarding them natively. Once translated to a globally routable address, return traffic from the non-LISP site will be able to reach the LISP site.

Both approaches have valid use-cases. For example, the use of a PITR is beneficial when LISP benefits such as multi-homing and ingress traffic engineering are useful. Also, NAT is beneficial when private host addresses require translation to LISP EIDs, or when local control of packets is desired.

This application note describes the main use-cases for NAT integration (References [3], [4]), with certain LISP deployments, and provides details the specific deployment requirements and configurations.

Concept Details: Cisco IOS Network Address Translation and LISP

There are two main use-cases for NAT integration with LISP:

1. Hosts at LISP sites talking to non-LISP sites
2. Hosts at LISP sites with private (or overlapping) addresses talking to other LISP sites

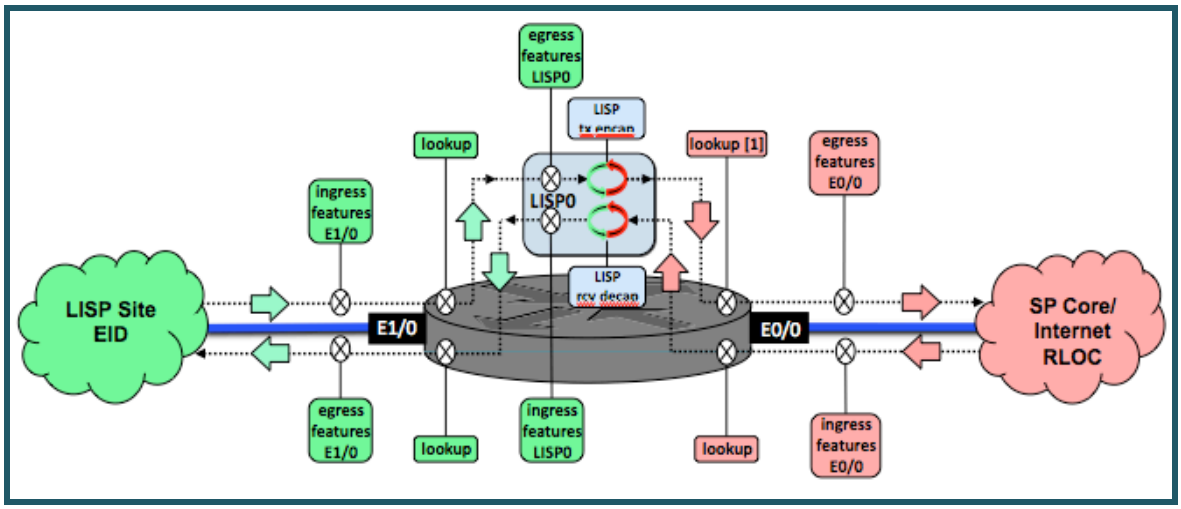
This application note covers both of the above topics in detail.

LISP0 interface

Before discussing the details of NAT, it is first useful to discuss the internal processing behavior of LISP within the Cisco IOS router. The LISP process in IOS creates the LISP0 virtual interface, as illustrated in Figure 1, as a reference point for encapsulation and decapsulation operations. This LISP0 virtual interface, described in detail in the Application Note available at Reference [1], serves as the natural boundary between the EID and RLOC namespaces for the xTR. Egress features are applied to packets that are leaving the router via LISP, just prior to LISP encapsulation. Similarly, ingress features are applied to

packets that are arriving from LISP, just after LISP decapsulation. Note that in both cases, the LISP0 ingress and egress feature application points are in the EID namespace.

Figure 1. Conceptual interfaces and feature application points with LISP



NAT configurations include the use of the **ip nat** {**inside** | **outside**} command on various interfaces to indicate directionality of packet flows in association with the defined NAT policy. Referring to Figure 1, NAT can be applied to site-facing interface **E1/0**, core-facing interface **E0/0**, and the **LISP0** interface. The specific use-case will determine the interfaces and direction of NAT application. The two use-cases covered here provide specific examples. (All interfaces and directions may not have use-cases with NAT).

LISP sites talking to non-LISP sites

When hosts at a LISP site wants to talk to a hosts at non-LISP sites using NAT, the LISP xTR must be configured to translate the source EID address to a routable address. This allows the return traffic from the non-LISP site to find its way back to the LISP router, where the reverse NAT process can be taken. This use case is referred to as "EID-to-Global" address translation, and is covered in example #1 below.

Generally, packets going from a LISP site to a non-LISP site do not undergo LISP encapsulation. (The exception is when a Proxy Egress Tunnel Router (PETR) is used.) In this case, **ip nat inside** is configured on the site-facing interface(s), and **ip nat outside** is configured on the core-facing interface(s). This scheme and translation policy is exactly the same as how NAT is traditionally used.

LISP sites with private addresses talking to other LISP sites

When a site already has its hosts configured to use private RFC1918 IPv4 addresses and then adds LISP, the LISP xTR must be configured to use NAT to translate the private addresses to addresses from the LISP EID-prefix range when talking to other LISP sites. (The alternative is to re-number the hosts from the new LISP EID namespace, which avoids having to use NAT.) Thus, when the destination LISP site does the EID-to-RLOC map resolution, it will properly encapsulate the return traffic back to this originating LISP router, where the reverse NAT process can happen. This use case is referred to as "private-to-EID" address translation, and is covered in example #2 below.

In this case, packets going from a LISP site to another LISP site undergo LISP encapsulation and so NAT must convert the private source addresses into LISP EID addresses just prior to LISP encapsulation.

Therefore, **ip nat inside** is configured on the site-facing interface(s), and **ip nat outside** is configured on the LISP0 interface.

In this second use-case, it is also likely that hosts within the LISP site will also need to talk to non-LISP sites, adding the requirements of the first use-case. To achieve this, two NAT policies are required, i.e. a combination of both example #1 and example #2, and this is demonstrated in example #3.

Caveats and Notes Related to NAT

The following caveats and notes are applicable to NAT for use with LISP:

1. NAT should only be deployed in conjunction with LISP when both ITR and ETR functionality are enabled on the same device. Otherwise, the return packets may hit a different device than the one that performed the outbound NAT translation, meaning that that inbound device does not have the NAT state table for reverse translation for return packets.

In general, normal Cisco IOS NAT rules and configuration procedures are applicable should be followed.

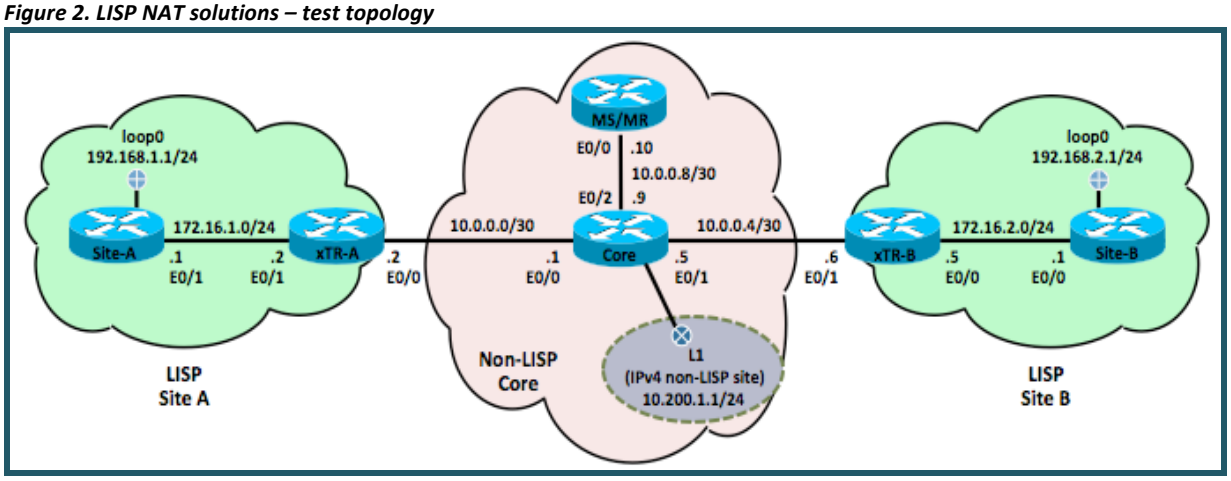
Concept Examples: Cisco IOS Network Address Translation and LISP

Initial LISP Configuration

The test network topology for this Application Note is illustrated in Figure 2, with the following elements:

- LISP Site A is assigned the LISP IPv4 EID-prefix **192.168.1.0/24**. Cisco IOS router **xTR-A** is site's xTR, and it registers with the map-server located at 10.0.0.10. Router **Site-A** provides a convenient host for sourcing traffic during the NAT testing. NAT is applied only to **xTR-A**.
- LISP Site B is assigned the LISP IPv4 EID-prefix **192.168.2.0/24**. The Cisco IOS router **xTR-B** is the LISP SITE B's xTR, and it registers with the Map-Server located at 10.0.0.10.
- The Non-LISP/Core includes the router **Core** and represents the public (RLOC) space through which the LISP sites communicate. A loopback on **Core** with address 10.200.1.1 is used as the non-LISP site with which the LISP sites communicate during validation testing.
- MS/MR is the Map-Server/Map-Resolver that provides mapping-resolution services for the LISP sites. The Cisco ISO router **MS/MR** is deployed for this purpose.

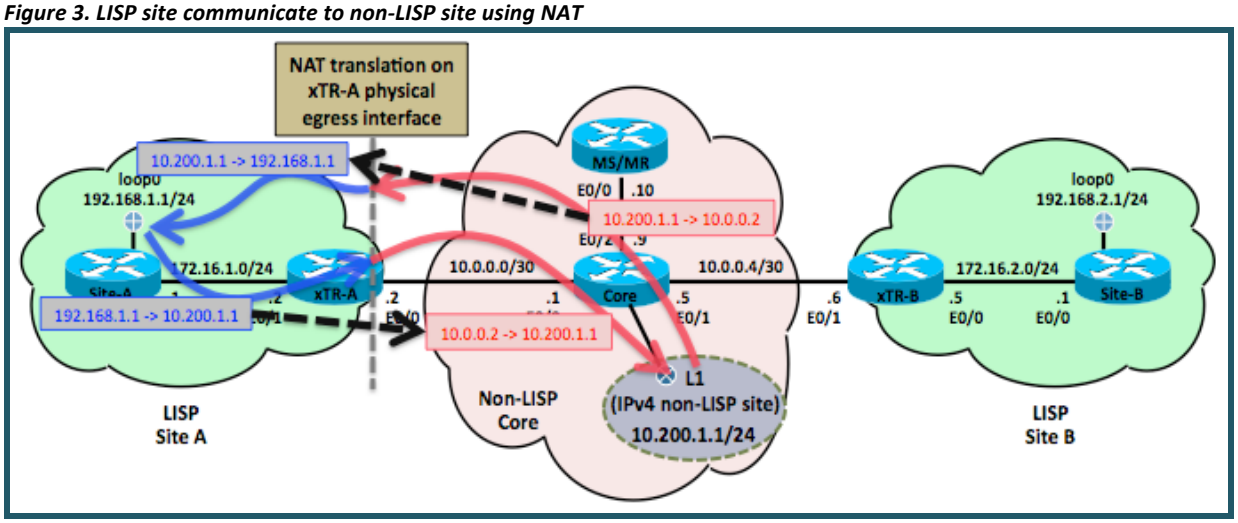
Figure 2. LISP NAT solutions – test topology



Example 1 – LISP sites talking to non-LISP sites using NAT (EID-to-Global)

Example 1 validates the use case of LISP hosts talking to non-LISP hosts using NAT. Figure 3 illustrates the packet flow for this use case, as demonstrated in the configuration and output samples below.

Figure 3. LISP site communicate to non-LISP site using NAT



As shown in Figure 3, a source-ping is initiated from the LIST host 192.168.1.1 and destined for the non-LISP host 10.200.1.1 (in the non-LISP core network). Figure 3 illustrates the packet headers are various steps in the flow. The following steps provide NAT configuration details and validation for this example.

Step 1. Configure NAT on LISP router xTR-A

NAT is configured on **xTR-A** and translates the 192.168.1.1 source address to the RLOC address 10.0.0.2, which is global and known to the non-LISP Core.

```
!
ip nat pool eid-to-global 10.0.0.2 10.0.0.2 prefix-length 24
ip nat inside source route-map routemap_eid-to-global pool eid-to-global
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
route-map routemap_eid-to-global permit 10
 match ip address 1
!
interface Ethernet0/1
ip nat inside
!
interface Ethernet0/0
ip nat outside
!
```

In the above configuration, a NAT pool is created (called **eid-to-global**), and it is associated with the NAT policy (**ip nat inside source**). The standard ACL (**access-list 1**) identifies LISP EIDs as candidates for NAT. The NAT inside and outside interfaces are identified as the physical interfaces E0/1 (site-facing) and E0/0 (core-facing). (Note that this is just one method of configuring NAT. Refer to Cisco IOS NAT configuration guidelines for other methods.)

Step 2. Test the NAT configuration using a source-ping

Next, initiate a source-ping from **Site-A** (192.168.1.1) to the non-LISP host (10.200.1.1), and enable **debug ip icmp** on the router **Core** (which is where the non-LISP host is implemented as a Loopback interface).

```
Site-A#ping 10.200.1.1 source 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Site-A#
```

You can see that the ping was successful.

And (enable prior to the ping):

```
Core#debug ip icmp
Oct 11 10:06:14.895 PDT: ICMP: echo reply sent, src 10.200.1.1, dst
10.0.0.2, topology BASE, dscp 0 topoid 0
<snip>
```

You can see that an ICMP echo-reply was sent to 10.0.0.2 from 10.200.1.1 as expected.

Step 3. Review the NAT translation table.

Finally, review the NAT state table using **show ip nat** commands for translation and statistics on **xTR-A**.

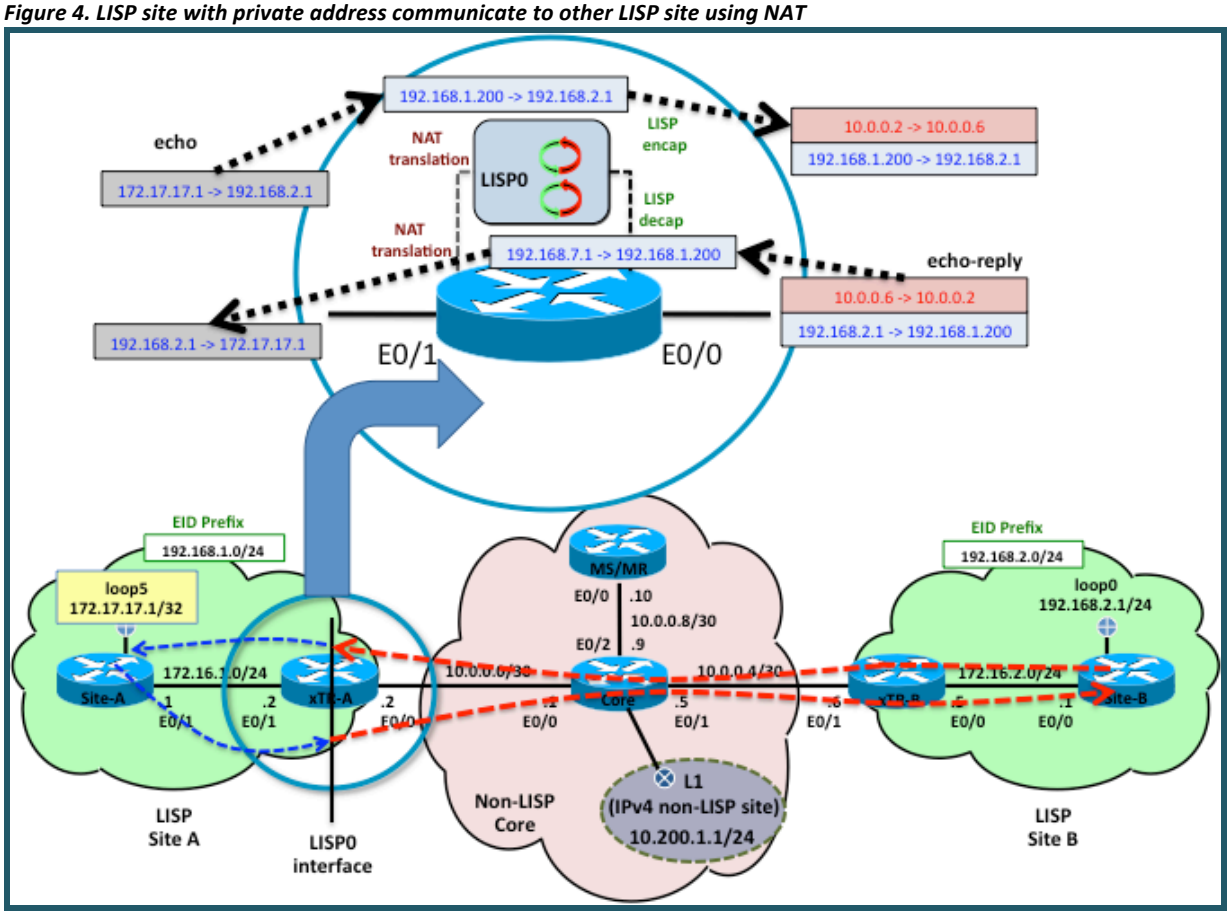
```
xTR-A#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 10.0.0.2:34       192.168.1.1:34     10.200.1.1:34      10.200.1.1:34

xTR-A#show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:00:01 ago
Outside interfaces:
  Ethernet0/0
Inside interfaces:
  Ethernet0/1
Hits: 10  Misses: 0
CEF Translated packets: 10, CEF Punted packets: 0
<snip>
```

In the first show output it is clear that xTR-A has translated the inside local IP 192.168.1.1 to the global IP 10.0.0.2 as expected. Note also that the **show ip nat statistics** output shows cumulative statistics of both directions, hence 10 packets.

Example 2 – LISP sites with private addresses talking to other LISP sites using NAT (Private-to-EID)

Example 2 validates the use case of private hosts within LISP sites talking to other LISP sites using NAT to translate the private IP addresses into LISP EID addresses. Figure 4 illustrates the packet flow for this use case, as demonstrated in the configuration and output samples below.

Figure 4. LISP site with private address communicate to other LISP site using NAT



As shown in Figure 4, a source-ping is initiated from the private host 172.17.17.1 in Site-A and destined for the LISP host 192.168.2.1 in Site-B. Figure 4 illustrates the packet headers are various steps in the flow, including the NAT translation from private address of 172.17.17.1 to LISP EID address 192.168.1.200, LISP encapsulation of this packet for transport from Site-A to Site-B, and the reverse process for return traffic. The following steps provide NAT configuration details and validation for this example.

Step 1. Modify LISP and configure NAT on LISP router xTR-A

Cisco IOS only considers packets to be eligible for LISP encapsulation when the source IP address is identified as a LISP EID through its inclusion in a **lisp database-mapping** command. In this example, the 172.17.17.0/24 private prefix is not recognized as a LISP EID and so LISP encapsulation would normally not be invoked. In order to change this behavior, a *dummy* lisp database-mapping command must be configured on xTR-A for the private prefix 172.17.17.0/24 – making it eligible for LISP encapsulation processing. In addition, **ip nat outside** is configured on the LISP0 interface to enable the private-to-EID address translation prior to LISP encapsulation, and **ip nat inside** remains configured on E0/1 (the site-facing interface).

```
!
ip lisp database-mapping 172.17.17.0/24 10.0.0.2 priority 1 weight 100
!
interface LISP0
 ip nat outside
!
interface Ethernet0/1
```

```
ip nat inside
!
ip nat pool pvt-to-eid 192.168.1.200 192.168.1.200 prefix-length 24
ip nat inside source route-map routemap-pvt-to-eid pool pvt-to-eid
!
access-list 2 permit 172.17.17.0 0.0.0.255
!
route-map routemap-pvt-to-eid permit 10
 match ip address 2
!
```

Note: Configuring the dummy **lisp database-mapping** command causes the private prefix (172.17.17.0/24 in this case) to be included in the map-register message with the map-server. This private prefix will not be registered, however, since the map-server is not configured to accept the prefix. This does not affect any other LISP operations and does not break anything. Using a dummy **lisp database-mapping** command entry is a temporary workaround for enabling private-to-EID NAT translation prior to LISP encapsulation. A future release of Cisco IOS LISP will include a mechanism for identifying private-to-EID NAT eligible prefixes without the need for this dummy entry.

Step 2. Test the NAT configuration using a source-ping

Next, initiate a source-ping from the private host in Site-A (172.17.17.1) to the Site-B 192.168.2.1 address.

```
Site-A#ping 192.168.2.1 source 172.17.17.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.17.17.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Site-A#
```

Step 3. Review the NAT table and statistics

Check NAT show outputs for the translation and the statistics.

```
xTR-A#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.1.200:46  172.17.17.1:46     192.168.2.1:46     192.168.2.1:46

xTR-A#show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:00:06 ago
Outside interfaces:
  LISP0
Inside interfaces:
  Ethernet0/1
Hits: 10  Misses: 0
CEF Translated packets: 10, CEF Punted packets: 0
<snip>
```

Step 4. Review the MR/MS LISP site information.

For completeness, review the LISP database on xTR-A, and the LISP Map-Server details and show that no new prefixes have been registered (that is, the dummy prefix has not been added).

```
xTR-A# show ip lisp database
LISP ETR IPv4 Mapping Database, LSBs: 0x3, 2 entries

EID-prefix: 172.17.17.0/24
  10.0.0.2, priority: 1, weight: 100, state: site-self, reachable
EID-prefix: 192.168.1.0/24
  10.0.0.2, priority: 1, weight: 100, state: site-self, reachable
xTR-A#
```

And:

```
MRMS#show lisp site
LISP Site Registration Information

Site Name      Last      Up   Who Last             Inst     EID Prefix
               Register       Registered           ID
Site-A          00:00:13  yes  10.0.0.2                      192.168.1.0/24
Site-B          00:00:24  yes  10.0.0.6                      192.168.2.0/24
MRMS#
```

Note that the Map-Server does not register the dummy prefix.

Example 3 – Combining both the NAT translation techniques

If a site wishes to deploy LISP with private addresses and be able to speak to other LISP as well as non-LISP sites without use of a PITR, it is possible to apply NAT on both LISP0 (for speaking with LISP sites) and egress physical interface (for speaking with non-LISP sites). This is simply a combination of the two previous examples.

Step 1. Review NAT configuration

Both route-map configurations from example 1 and example 2 are included here, as well as the **ip nat inside** configuration on the site-facing interface E0/1 and **ip nat outside** configuration on both LISP0 and the core-facing interface E0/0.

```
!
interface LISP0
 ip nat outside
!
interface Ethernet0/1
ip nat inside
!
interface Ethernet0/0
ip nat outside
!
access-list 1 permit 192.168.1.0 0.0.0.255
!
access-list 2 permit 172.17.17.0 0.0.0.255
!
route-map routemap-pvt-to-eid permit 10
 match ip address 2
!
route-map routemap-eid-to-global permit 10
 match ip address 1
!
route-map routemap-pvt-to-eid permit 10
 match ip address 2
!
```

Step 2. Test the NAT configuration using a source-ping

Next, initiate a source-ping to check that both translation types are working. Source-ping from the private host in Site-A (172.17.17.1) to the Site-B 192.168.2.1 address.

```
Site-A#ping 10.200.1.1 source 192.168.1.1 rep 5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.200.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Site-A#
```

And:

```
Site-A#ping 192.168.2.1 source 172.17.17.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.17.17.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
Site-A#
```

Step 3. Review the NAT table and statistics

```
xTR-A#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.1.200:49  172.17.17.1:49     192.168.2.1:49     192.168.2.1:49
icmp 10.0.0.2:50       192.168.1.1:50     10.200.1.1:50      10.200.1.1:50

xTR-A#show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:03:12 ago
Outside interfaces:
  Ethernet0/0, LISP0
Inside interfaces:
  Ethernet0/1
Hits: 20  Misses: 0
CEF Translated packets: 20, CEF Punted packets: 0
<snip>
```

As you can see, both NAT operations are successful.

Conclusions

This application note described the use of NAT with LISP implementations. The interaction of NAT with LISP operations was described, showing that NAT can be deployed with LISP to enable LISP EIDs to talk to non-LISP sites, and to enable private hosts within a LISP site to talk to other LISP sites.

LISP Resources

1. LISP Documentation, including the LISP Command Reference Guide, LISP Configuration Guide, and LISP Lab Test Guide can be found here: http://lisp.cisco.com
2. "Interworking LISP with IPv4 and IPv6, draft-ietf-lisp-interworking," http://tools.ietf.org/wg/lisp/

3. “Configuring Network Address Translation: Getting Started,” http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml
4. “NAT Support for Multiple Pools Using Route-Maps,” http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080093fca.shtml
5. Cisco Marketing Information about LISP can be found here: http://www.cisco.com/go/lisp
6. LISP Beta Network information can be found here: http://www.lisp4.net and http://www.lisp6.net

Comments and corrections are welcome. Please direct all queries to: **lisp-support@cisco.com**.

Appendix: Test Network Router Configurations

Site-A

```
hostname Site-A
!
ip cef
!
interface Loopback1
 ip address 192.168.1.1 255.255.255.255
!
interface Loopback5
 ip address 172.17.17.1 255.255.255.255
!
interface Ethernet0/0
 ip address 172.16.1.1 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 network 172.16.1.1 0.0.0.0 area 0
 network 172.17.17.1 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
```

xTR-A

```
hostname xTR-A
!
ip cef
!
interface LISP0
 ip nat outside
 ip virtual-reassembly
!
interface Ethernet0/0
 ip address 10.0.0.2 255.255.255.252
 ip nat outside
 ip virtual-reassembly
!
interface Ethernet0/1
 ip address 172.16.1.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
router lisp
 database-mapping 172.17.17.0/24 10.0.0.2 priority 1 weight 100
 database-mapping 192.168.1.0/24 10.0.0.2 priority 1 weight 100
 ipv4 lisp itr map-resolver 10.0.0.10
 ipv4 lisp itr
 ipv4 lisp etr map-server 10.0.0.10 key site-a-s3cr3t
 ipv4 lisp etr
 exit
!
router ospf 1
 log-adjacency-changes
 network 172.16.1.2 0.0.0.0 area 0
 default-information originate
!
ip nat pool pvt-to-eid 192.168.1.200 192.168.1.200 prefix-length 24
ip nat pool eid-to-global 10.0.0.2 10.0.0.2 prefix-length 24
ip nat inside source route-map routemap-pvt-to-eid pool pvt-to-eid
ip nat inside source route-map routemap-eid-to-global pool eid-to-global
```

```
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.1.0 255.255.255.0 Null0
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 2 permit 172.17.17.0 0.0.0.255
!
route-map routemap-eid-to-global permit 10
 match ip address 1
!
route-map routemap-pvt-to-eid permit 10
 match ip address 2
!
```

Core

```
hostname Core
!
ip cef
!
interface Loopback1
 ip address 10.200.1.1 255.255.255.0
!
interface Ethernet1/0
 description To xTR-A
 ip address 10.0.0.1 255.255.255.252
!
interface Ethernet1/1
 description To xTR-B
 ip address 10.0.0.5 255.255.255.252
!
interface Ethernet0/2
 description To MSMR
 ip address 10.0.0.9 255.255.255.252
!
```

MR/MS

```
hostname MRMS
!
vrf definition lisp
!
 address-family ipv4
 exit-address-family
!
ip cef
!
router lisp
 site Site-A
  description LISP Site A
  authentication-key site-a-s3cr3t
  eid-prefix 192.168.1.0/24
  exit
 !
 site Site-B
  description LISP Site B
  authentication-key site-b-s3cr3t
  eid-prefix 192.168.2.0/24
  exit
 !
 ipv4 lisp map-server
 ipv4 lisp map-resolver
```

```
 ipv4 lisp alt-vrf lisp
!
interface LISP0
!
interface Ethernet0/0
 description To Core
 ip address 10.0.0.10 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 10.0.0.9
```

xTR-B

```
hostname xTR-B
!
ip cef
!
interface Loopback0
 no ip address
!
interface LISP0
!
interface Ethernet0/0
 ip address 172.16.2.2 255.255.255.0
!
interface Ethernet0/1
 description To Core
 ip address 10.0.0.6 255.255.255.252
!
router lisp
 database-mapping 192.168.2.0/24 10.0.0.2 priority 1 weight 100
 ipv4 lisp itr map-resolver 10.0.0.10
 ipv4 lisp itr
 ipv4 lisp etr map-server 10.0.0.10 key site-b-s3cr3t
 ipv4 lisp etr
 exit
!
router ospf 1
 log-adjacency-changes
 network 172.16.2.2 0.0.0.0 area 0
 default-information originate
!
ip route 0.0.0.0 0.0.0.0 10.0.0.5
```

Site-B

```
hostname SiteB
!
ip cef
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/0
 ip address 172.16.2.1 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 passive-interface Loopback0
 network 172.16.2.1 0.0.0.0 area 0
 network 192.168.2.1 0.0.0.0 area 0
!
```

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.**

Printed in the USA C11-617390-00 08/10