LISP Data Plane Security

The Locator/ID Separation Protocol (LISP) Data Plane Security feature ensures that only traffic from within a LISP VPN can be decapsulated into the VPN. The feature is enforced when LISP packets are decapsulated by a tunnel router at the destination. Egress tunnel routers (ETRs) and proxy egress tunnel routers (PETRs) validate that the source Routing Locator (RLOC) address carried by the data packet is a member of the LISP VPN.

The solution relies on Unicast Reverse Path Forwarding (uRPF) being implemented in the RLOC network to ensure that the RLOC source addresses in LISP encapsulated data packets cannot be spoofed. Packets from outside the LISP VPN carry invalid source RLOCs that are blocked during decapsulation by ETRs and PETRs.

The advantages of implementing the LISP Data Plane Security feature are given below:

- Enhanced security due to validation by ETRs and PETRs during decapsulation.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for LISP Data Plane Security

- Understanding of LISP concepts, including the concept of virtual routing and forwarding (VRF) instances bound to instance IDs (IIDs). These concepts are explained in the chapters *LISP Overview*, *Configuring LISP*, and *LISP Shared Model Virtualization*.
- uRPF implementation in the RLOC network.

Restrictions for LISP Data Plane Security

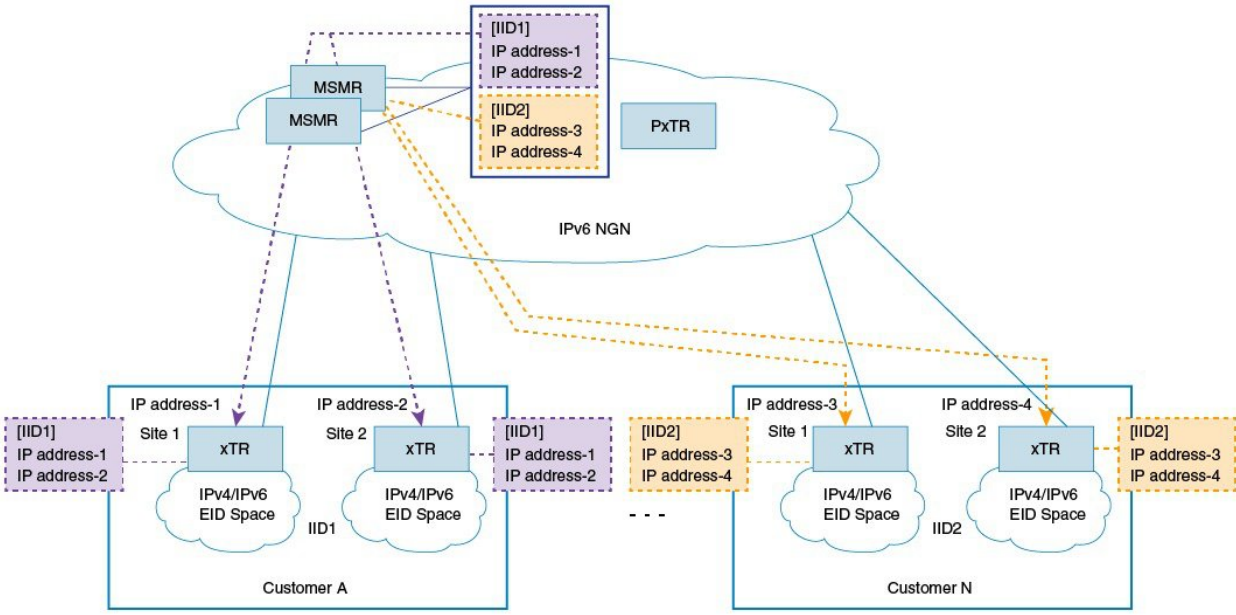
- All sites within a given LISP VPN must register to one or a common set of Map-Servers. That is, all IP prefixes associated with a specific instance ID must be delegated from common a Map-Server to ensure that these Map-Servers can construct a complete RLOC set for the given LISP VPN.

Information About LISP Data Plane Security

Source RLOC Decapsulation Filtering

This feature enhances data plane security by monitoring LISP packets during the decapsulation stage, when the packets are sent from an ingress tunnel router (ITR) or proxy ingress tunnel router (PITR) to an ETR or PETR. To protect LISP VPN end sites from decapsulating LISP packets that do not belong to the VPN, whether the result of misconfiguration or an attack, the source address in the incoming LISP packets are compared with a dynamically distributed set of source RLOC addresses corresponding to valid LISP VPN end sites. LISP packet decapsulation by ETRs and PETRs validate that a source RLOC address of an incoming LISP data packet is a member of the VPN. Note that this solution requires that source RLOC addresses are not spoofed, and hence unicast RPF or ingress anti-spoofing access control lists (ACLs) are required within the RLOC core network.

Consider the scenario in the image below:



1. Customer A has 2 LISP sites, site1 and site2, each having an xTR (a device performing the role of ETR and ITR). Site 1 and Site 2 register with the Map-Servers (of the Map-Server/Map-Resolver [MSMR] devices) supporting the LISP control plane for the LISP VPN with instance ID 1. The Map-Server automatically records the registration RLOCs for both sites, and dynamically pushes this list of valid RLOCs to both sites. In this way, site 1 and site 2 of the customer A LISP VPN can send traffic between each other. No other LISP encapsulated traffic is permitted, as the source RLOC will not match the valid source RLOC list.
2. Customer N also has 2 LISP sites, site1 and site2, and both register to the Map-Servers supporting the LISP control plane for this LISP VPN with instance ID 2. The Map-Server automatically records the registration RLOCs for both sites, and dynamically pushes this list of valid RLOCs to both sites. In this way, site 1 and site 2 of the customer N LISP VPN can send traffic between each other. No other LISP encapsulated traffic is permitted, as the source RLOC will not match the valid source RLOC list.

In addition to the automatically learned source RLOCs of registering LISP sites, the per-IID (instance ID) membership list can be extended to include specific source RLOCs of valid devices that do no register, such as PxTRs. When this feature is deployed, the source RLOCs of the PxTR is made available with the xTRs.

Some pointers for implementing source RLOC decapsulation filtering are given below :

- For Map-Servers to be able to construct the complete list of members for an EID instance ID, they must receive registrations from all the xTRs participating in the customer VPN.
- Map-Servers construct the EID instance ID-RLOC membership list using the RLOC information in the received mapping records in map-register messages.
- All IP prefixes associated with a specific instance ID must be delegated from a common Map-Server to ensure that these Map-Servers can construct a complete RLOC set for the given LISP VPN.
- All xTRs within a VPN must register with a common set of Map-Servers.

- PxTRs do not (normally) register with the Map-Servers, such that the Map-Servers could discover the PxTR RLOC, and that the Map-Servers could distribute learned RLOCs to the PxTRs. Thus, PxTR RLOCs need to be manually configured on the Map-Server.
- The EID instance membership lists built by Map-Servers are communicated only to xTRs and PxTRs that are members of the VPN.

TCP-based Sessions for LISP Packet Transport

The LISP data plane security mechanism requires the automated distribution and updating of RLOC filter lists to VPN members. This automated distribution is accomplished through a TCP-based session established between the xTRs and Map-Servers after the normal registration process has completed.

For example, xTRs periodically transmit map register messages and process the resulting map notify messages issued by the Map-Server. The Map-Servers process map register messages, update corresponding registration state, and transmit matching map notify messages.

To implement a more reliable, secure, and scalable transport option, TCP-based sessions are provided for LISP-related communication between xTRs and Map-Servers.

Some pointers regarding TCP-based sessions are given below:

- The UDP-based registration mechanism is conducted, and then a TCP-based session is established and used for the distribution of EID-instance RLOC membership lists. The number of xTRs that a Map-Server can support is limited by the number of TCP sessions that the Map-Server can establish and maintain. This determines the number of VPN customers that a Map-Server can host.
- The xTRs belonging to the same VPN must register with the same Map-Servers. This limits the number of sites within a VPN to the number of TCP sessions that a Map-Server can support.

How to Configure LISP Data Plane Security

Configuring MSMR

To configure the MSMR devices, perform the steps given below:

Note Steps 5 to 10 are optional. You can use those to modify the list of RLOC addresses (filter list) discovered by the Map-Server.

Before You Begin

- Ensure that you have available any RLOCs associated with PxTRs serving within the LISP VPN.

SUMMARY STEPS

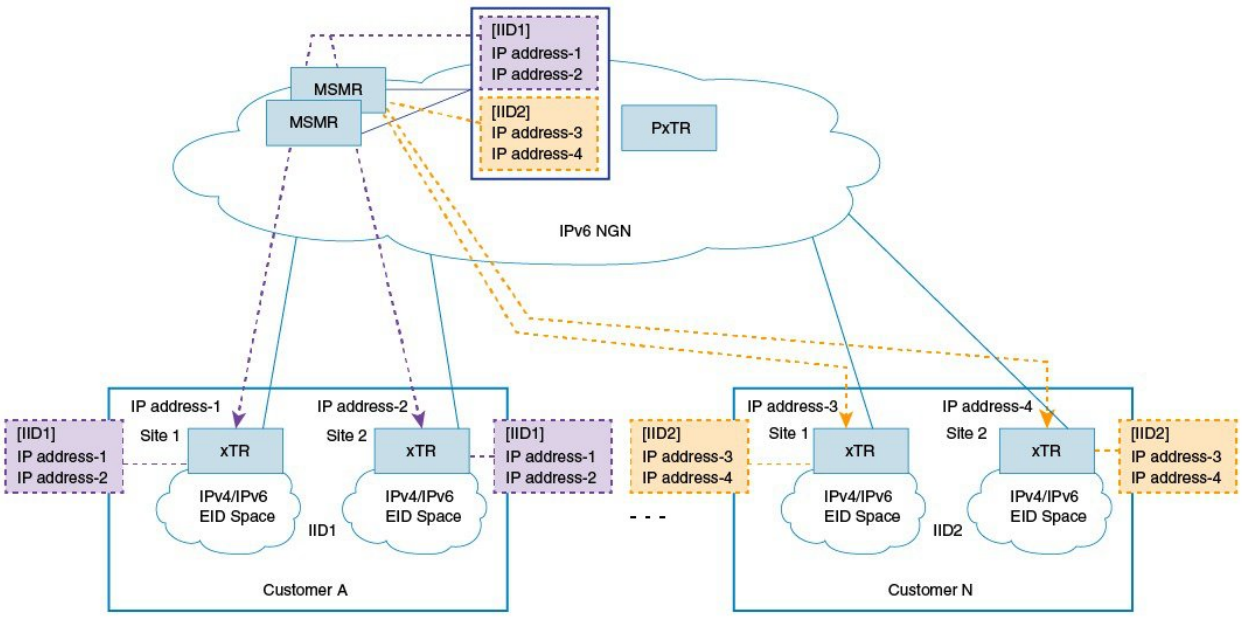
1. **enable**
2. **configure terminal**
3. **router lisp**
4. **map-server rloc members distribute**
5. **locator-set** *locator-set-name*
6. *ipv4-address* **priority** *value* **weight** *value*
7. **exit**
8. **eid-table vrf** *vrf-name* **instance-id** *iid*
9. **map-server rloc members modify-discovered add locator-set** *locator-set-name*
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router lisp** **Example:** `Device(config)# router lisp`	Enters LISP configuration mode.
Step 4	**map-server rloc members distribute** **Example:** `Device(config-router-lisp)# map-server rloc members distribute`	Enables distribution of the list of EID prefixes to xTRs at the customer end.
Step 5	**locator-set** *locator-set-name* **Example:** `Device(config-router-lisp)# locator-set PTR_set`	(Optional) Specifies a locator set for the PxTR and enters LISP locator set configuration mode.
Step 6	*ipv4-address* **priority** *value* **weight** *value* **Example:** `Device(config-router-lisp-locator-set)# 10.10.10.1 priority 1 weight 1`	(Optional) Configures the LISP locator set. You can configure each locator address by creating a locator entry with an assigned priority and weight

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-router-lisp-locator-set)# exit`	(Optional) Exits LISP locator set configuration mode and enters LISP configuration mode.
Step 8	**eid-table vrf** *vrf-name* **instance-id** *iid* **Example:** `Device(config-router-lisp)# eid-table vrf cust-A instance-id 1`	(Optional) Configures an association between a VRF table and a LISP instance ID, and enters eid-table configuration submode.
Step 9	**map-server rloc members modify-discovered add locator-set** *locator-set-name* **Example:** `Device(config-router-lisp-eid-table)# map-server rloc members modify-discovered add locator-set PTR_set`	(Optional) Adds RLOC addresses in the specified locator set to the list of *discovered* RLOC addresses. **Note** The updated list will be sent to the xTRs at the customer end when the distribution option is enabled.
Step 10	**exit** **Example:** `Device(config-router-lisp-eid-table)# exit`	(Optional) Exits eid-table configuration submode and enters LISP configuration mode.

Configuring the xTRs



To enable data plane security on the xTRs belonging to customer A (as shown in the image), configure the xTR at site1, as shown below:

Before You Begin

- Ensure that you have configured the MSMR devices.
- Ensure that uRPF is implemented in the RLOC network.
- Ensure that you have identified EIDs and the LISP device acting as an xTR.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router lisp**
4. **decapsulation filter rloc source member**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router lisp** **Example:** `Device(config)# router lisp`	Enters LISP configuration mode.
Step 4	**decapsulation filter rloc source member** **Example:** `Device(config-router-lisp)# decapsulation filter rloc source member`	Enables source RLOC address validation of LISP packets.
Step 5	**exit** **Example:** `Device(config-router-lisp)# exit`	Exits LISP configuration mode and returns to global configuration mode.

What to Do Next

- The above steps enable data plane security for the xTR at one of customer A's sites, 'site1'. You need to repeat the steps to enable RLOC decapsulation filtering for customer A's second site, 'site2'.

Configuring PxTR

To configure the PxTR, perform the steps given below:

Before You Begin

- Ensure that the MSMR devices and xTRs at the customer sites are configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router lisp**
4. **decapsulation filter rloc source members**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router lisp** **Example:** `Device(config)# router lisp`	Enters LISP configuration mode.
Step 4	**decapsulation filter rloc source members** **Example:** `Device(config-router-lisp)# decapsulation filter rloc source members`	Enables source RLOC address validation of LISP packets.
Step 5	**exit** **Example:** `Device(config-router-lisp)# exit`	Exits LISP configuration mode and returns to global configuration mode.

What to Do Next

- Configure any other PxTR as needed.

Verifying LISP Data Plane Security On a Map-Server

Verify the LISP Data Plane Security feature on a Map-Server by using the commands given below:

SUMMARY STEPS

1. **show lisp** [**session** [**established**] | **vrf** [*vrf-name* [**session** [*peer-address*]]]]
2. **show lisp site rloc members** [**instance-id** *iid*]

DETAILED STEPS

Step 1 **show lisp** [**session** [**established**] | **vrf** [*vrf-name* [**session** [*peer-address*]]]]

Example:

```
Device# show lisp session

Sessions for VRF default, total: 8, established: 7
Peer                            State      Up/Down        In/Out    Users
2001:DB8:A:1::2                 Up         00:04:13        2/7      2
2001:DB8:A:2::2                 Up         00:04:13        2/7      2
2001:DB8:A:3::2                 Up         00:03:53        2/7      2
2001:DB8:B:1::2                 Up         00:04:04        2/6      2
2001:DB8:B:2::2                 Init       never           0/0      1
2001:DB8:C:1::2                 Up         00:03:55        2/6      2
2001:DB8:C:2::2                 Up         00:03:54        2/6      2
2001:DB8:E:F::2                 Up         00:04:04        6/19     4
```

This command displays reliable transport session information. If there is more than one transport session, the corresponding information will be displayed.

Step 2 **show lisp site rloc members** [**instance-id** *iid*]

Example:

```
Device# show lisp site rloc members

LISP RLOC membership for EID table default (IID 0), 5 entries

RLOC                          Origin                    Valid
10.0.1.2                      registration               Yes
10.0.2.2                      config & registration      Yes
```

The **Origin** column displays configuration details of the RLOC member – whether the RLOC member is manually configured, automatically gleaned from received registrations, or both. The **Valid** column shows whether the RLOC is a valid member that is distributed to (P)xTRs. A listed RLOC may not be valid if it is gleaned from registrations but the 'override' option is used in the 'modify-discovered' configuration, and the specified locator-set does not include the RLOC.

Verifying and Troubleshooting LISP Data Plane Security on an xTR or PxTR

Verify the LISP Data Plane Security feature on an xTR or PxTR by using the commands given below:

SUMMARY STEPS

1. **show lisp** [**session** [**established**] | **vrf** [*vrf-name* [**session** [*peer-address*]]]]
2. **show lisp decapsulation filter** [*IPv4-rloc-address* | *IPv6-rloc-address*] [**eid-table** *eid-table-vrf* | **instance-id** *iid*]
3. **show cef source-filter table**
4. **debug lisp control-plane eid-membership**
5. **debug lisp control-plane session**

DETAILED STEPS

Step 1 **show lisp** [**session** [**established**] | **vrf** [*vrf-name* [**session** [*peer-address*]]]]

Example:

```
Device# show lisp session

Sessions for VRF default, total: 8, established: 7
Peer                          State      Up/Down        In/Out    Users
2001:DB8:A:1::2               Up         00:04:13        2/7      2
2001:DB8:A:2::2               Up         00:04:13        2/7      2
2001:DB8:A:3::2               Up         00:03:53        2/7      2
2001:DB8:B:1::2               Up         00:04:04        2/6      2
2001:DB8:B:2::2               Init       never           0/0      1
2001:DB8:C:1::2               Up         00:03:55        2/6      2
2001:DB8:C:2::2               Up         00:03:54        2/6      2
2001:DB8:E:F::2               Up         00:04:04        6/19     4
```

This command displays reliable transport session information. If there is more than one transport session, the corresponding information will be displayed.

Step 2 **show lisp decapsulation filter** [*IPv4-rloc-address* | *IPv6-rloc-address*] [**eid-table** *eid-table-vrf* | **instance-id** *iid*]

Example:

```
Device# show lisp decapsulation filter instance-id 0

LISP decapsulation filter for EID-table default (IID 0), 3 entries

Source RLOC     Added by
10.0.0.1         Config
10.0.0.5         209.165.200.230 209.165.200.232
10.0.0.6         Config 209.165.200.230
```

The RLOC address configuration details (whether it is manually configured or discovered) on a (P)xTR is displayed in the above table.

Step 3 **show cef source-filter table**

Example:

```
Device# show cef source-filter table

[lisp:0:0:IPv4] state [enabled, active], 0 entries, refcount 3, flags [], action [drop]
```

```
Database epoch 0
Hits 0, misses 0, fwd 0, drop 0
```

This command displays Cisco Express Forwarding (CEF) source-filter tables.

Step 4 **debug lisp control-plane eid-membership**

Example:

```
Device# debug lisp control-plane eid-membership

LISP control plane EID membership debugging is on
```

Displays debugging information for EID membership discovery.

Step 5 **debug lisp control-plane session**

Example:

```
Device# debug lisp control-plane session

LISP control plane session debugging is on
```

Displays detailed session establishment debugging information.

Configuration Examples for LISP Data Plane Security

Example: Configuring MSMR

Note Steps for adding the locator set and the RLOC address are optional. You can use those steps to modify the list of RLOC addresses (filter list) discovered by the Map-Server.

```
Device> enable
Device# configure terminal
Device(config)# router lisp
Device(config-router-lisp)# map-server rloc members distribute
Device(config-router-lisp)# locator-set PTR_set
Device(config-router-lisp-locator-set)# 10.10.10.1 priority 1 weight 1
Device(config-router-lisp-locator-set)# exit
Device(config-router-lisp)# eid-table vrf cust-A instance-id 1
Device(config-router-lisp-eid-table)# map-server rloc members modify-discovered add
locator-set PTR_set
Device(config-router-lisp-eid-table)# exit
```

Repeat the above steps to configure one or more map servers, as needed

Example: Configuring the xTRs

```
Device> enable
Device# configure terminal
Device(config)# router lisp
```

```
Device(config-router-lisp)# decapsulation filter rloc source member
Device(config-router-lisp)# exit
```

The above steps enable data plane security for the xTR at one of customer sites. You must repeat the steps to enable RLOC decapsulation filtering for other sites.

Example: Configuring PxTR

```
Device> enable
Device# configure terminal
Device(config)# router lisp
Device(config-router-lisp)# decapsulation filter rloc source member
Device(config-router-lisp)# exit
```

Additional References for LISP Data Plane Security

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Locator/ID Separation Protocol (LISP) commands	Cisco IOS IP Routing: LISP Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 6830	*Locator/ID Separation Protocol (LISP)*
RFC 6832	*Interworking between Locator/ID Separation Protocol (LISP) and Non-LISP Sites*
RFC 6833	*Locator/ID Separation Protocol (LISP) Map-Server Interface*

MIBs

MIB	MIBs Link
• CISCO-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for LISP Data Plane Security

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for LISP Data Plane Security

Feature Name	Releases	Feature Information
LISP Data Plane Security	Cisco IOS XE Release 3.14S	The LISP Data Plane Security feature ensures that only traffic from within a LISP VPN can be decapsulated into the VPN. The following commands were introduced by this feature: **clear lisp vrf**, **decapsulation filter rloc source**, **debug lisp control-plane eid-membership**, **debug lisp control-plane session**, **map-server rloc members distribute**, **map-server rloc members modify-discovered**, **show lisp decapsulation filter**, **show lisp site rloc members**, **show lisp session** .