CISCO

Cisco NX-OS LISP Command Reference, Nexus 7000 Series
Cisco NX-OS Release 5.2(1.lisp-r7-39)

July 14, 2012

Note This Cisco NX-OS LISP Command Reference Guide is preliminary and subject to change. The commands and their usage, examples, and detailed outputs are provided as the best representation available at the time of this writing. This document will be replaced with the formal version that will be formatted and published in the same way as all other Cisco NX-OS guides and documentation.

CONTENTS

New and Changed Information

This chapter provides release-specific information for each new and changed feature in the Cisco NX-OS LISP Command Reference, Nexus 7000 Series, Cisco NX-OS Release 5.2(1.lisp-r7-39). The latest version of this document is available at the following Cisco website: http://lisp.cisco.com. To check for additional information about the Cisco NX-OS LISP Command Reference, Nexus 7000 Series, Cisco NX-OS Release 5.2(1.lisp-r7-39), see the latest version of the release notes referenced at the following Cisco website: http://lisp.cisco.com.

Table 1 summarizes the new and changed features for the Cisco NX-OS LISP Command Reference, Nexus 7000 Series, Cisco NX-OS Release 5.2(1.lisp-r7-39).

Table 1   New and Changed Information for Cisco NX-OS LISP Command Reference, Nexus 7000 Series, Cisco NX-OS Release 5.2(1.lisp-r7-39).

Date Introduced	Change Description	Changed in Release	Where Documented
31 Mar 2010	Added global LISP configuration command. Added LISP interface configuration commands. Added LISP show commands. Added LISP site configuration commands. Added LISP debug commands. Added LISP clear commands. Added other LISP-related commands.	Cisco NX-OS Release 5.0(1.13)	LISP Global Configuration, Show, and Debug Commands
09 Aug 2010	Added LISP VM-Mobility global, interface, and VM-Mobility configuration commands. Added LISP VM-Mobility configuration commands Added LISP VM-Mobility show, debug, and clear commands.	Cisco NX-OS Release 5.0(1.13) August Rel.	LISP Global Configuration, Show, and Debug Commands
04 Nov 2010	Added LISP Instance-ID global and LISP Site configuration commands. Added LISP Instance-ID show, debug, and clear commands.	Cisco NX-OS Release 5.0(3.lisp)	LISP Global Configuration, Show, and Debug Commands
21 Feb 2011	Updated LISP VM-Mobility configuration commands.	Cisco NX-OS Release 5.0(3.lisp-80)	LISP Global Configuration, Show, and Debug Commands
30 June 2011	Added new commands **lisp security**, **ip|ipv6 lisp ntr**, and **ip|ipv6 lisp use-bgp-locators**. Removed **lisp beta** command. Updated LISP VM-Mobility configuration commands.	Cisco NX-OS Release 5.2(0.266.lisp-52)	LISP Global Configuration, Show, and Debug Commands
28 July 2011	Documentation update for Release 5.2(0.266.lisp-58).	Cisco NX-OS Release 5.2(0.266.lisp-58)	Show Commands
06 Oct 2011	Added **secure-handoff** subcommand to **lisp dynamic-eid** mode.	Cisco NX-OS Release 5.2(1.lisp-r5-20)	LISP Dynamic-EID Configuration Commands
13 April 2012	Added **LISP-DDT** configuration, show, debug, and clear commands. Added **rig** command.	Cisco NX-OS Release 5.2(1.lisp-r7-39)	LISP DDT Configuration, Show, Debug, and Clear Commands

Cisco LISP Commands

This chapter describes the Cisco NX-OS LISP Command Reference, Nexus 7000 Series, Cisco NX-OS Release 5.2(1.lisp-r7-39). These commands are used to configure and monitor the following Locator/ID Separation Protocol (LISP) capabilities and features:

- LISP Ingress Tunnel Router (ITR)/Egress Tunnel Router (ETR) functionality
- LISP Proxy Ingress Tunnel Router (PITR)/Proxy Egress Tunnel Router (PETR) functionality
- LISP Map Server (MS) functionality
- LISP Map Resolver (MR) functionality
- LISP-ALT functionality
- LISP VM-Mobility functionality
- LISP Instance ID functionality for LISP MS/MR, xTR, and PxTR virtualization
- LISP Network Address Translation (NAT) Tunnel Router (LISP-NTR) functionality
- LISP Security (LISP-SEC) functionality
- LISP On Demand Forwarding (LISP-ODF) functionality
- LISP Delegated Database Tree (LISP-DDT) functionality

This *Cisco NX-OS LISP Command Reference* is organized into the following categories:

- LISP Global Configuration Commands
- LISP Interface Configuration Commands
- LISP Site Configuration Commands
- LISP VM-Mobility Configuration Commands
- LISP DDT Configuration Commands
- Other LISP Configuration Commands
- LISP Show Commands
- LISP Debug Commands
- LISP Clear Commands
- Other LISP-Related Commands

This document only describes the LISP commands, syntax, and usage for Cisco NX-OS. For information on how to configure Cisco LISP features, as well as configuration examples using the commands in this document, refer to the *Cisco LISP Configuration Guide*.

LISP Global Configuration Commands

ip lisp alt-vrf

To configure an alternate virtual routing and forwarding (VRF) instance supporting the IPv4 address-family for LISP to use for resolving IPv4 EID-to-RLOC mappings, use the **ip lisp alt-vrf** command in global configuration mode. To remove this reference to a VRF, use the **no** form of this command.

> **[no] ip lisp alt-vrf** *vrf-name*

Syntax Description

vrf-name	Name assigned to the LISP-ALT VRF.

Defaults

By default, a LISP-ALT VRF is not referenced by LISP.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use the command **ip lisp alt-vrf** to configure which virtual routing and forwarding (VRF) instance supporting the IPv4 address-family the LISP device should use for control plane mapping resolution functions.

The **ip lisp alt-vrf** command is required for all LISP devices connected to the LISP Alternative Logical Topology (ALT) for exchange of LISP control plane messages for mapping resolution. Primarily this includes LISP Map-Server (MS), Map-Resolver (MR), and Proxy Ingress Tunnel Router (PITR) devices. This can also include directly ALT-connected xTRs.

> ✎
>
> **Note** When the **ip lisp alt-vrf** command is used, the referenced VRF must already have been created using the **vrf context** command. In addition, any other corresponding configurations necessary for connecting the LISP device to the ALT, including the GRE tunnel interface(s) and any routing associated with the VRF (static and/or dynamic) must also have been created.

The LISP ALT does not support virtualization. Thus, the following must be considered when deploying LISP with ALT functionality.

- A Map-Request containing an instance-id cannot be forwarded over the LISP ALT. When a LISP device is configured for virtualization, the **ip lisp alt-vrf** command must not be configured.
- When instance-ID's are configured on a MS (see LISP Site **eid-prefix** command), the MS **must be** configured stand-alone or to use LISP-DDT since virtualization of the LISP ALT is not support.
- When a router is configured as a stand-alone MS/MR without virtualization (i.e. when it is not connected to any ALT and it has full knowledge of the LISP Mapping System for a private LISP deployment for example), the use of the **ip lisp alt-vrf** command is not required.

- A PITR can be configured to send a Map-Request to a configured Map-Resolver for EID-to-RLOC mapping resolution. When configured to use a Map-Resolver instead of the ALT, the **ip lisp alt-vrf** command is not required. A LISP PITR should only be configured with the **ip lisp alt-vrf** command if it is directly using the ALT for EID-to-RLOC mapping resolution.

- When using a PITR in a virtualized LISP deployment, the PITR **must be** configured to use a Map-Resolver for EID-to-RLOC mapping resolution and not the LISP ALT since the LISP ALT does not support virtualization. In this case, the **ip lisp alt-vrf** command is not used.

Examples

The following example configures the VRF named **lisp**, and then configures LISP to use this VRF when resolving IPv4 EID-to-RLOC mappings.

```
Router(config)# vrf context lisp
Router(config-vrf)# exit
Router(config)# ip lisp alt-vrf lisp
```

Related Commands

Command	Description
ip lisp itr	Configure the router to act as an IPv4 LISP Ingress Tunnel Router (ITR)
ip lisp proxy-itr	Configures the router to act as an IPv4 LISP Proxy Ingress Tunnel Router (PITR)

ip lisp database-mapping

To configure an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy use the **ip lisp database-mapping** command in global configuration mode. To remove the configured database mapping, use the **no** form of this command.

[no] ip lisp database-mapping *EID-prefix* {*locator* | **dynamic** *interface-name*} **priority** *priority* **weight** *weight*

Syntax Description

EID-prefix/prefix-length	The IPv4 EID prefix and length to be advertised by this router.
locator	The IPv4 or IPv6 Routing Locator (RLOC) associated with this EID-prefix
dynamic *interface-name*	Allow the Routing Locator (RLOC) associated with this EID to be learned dynamically in coordination with the LISP interface command **ip nat-traversal** by sending a LISP Echo-Request message to the configured Map-Server via the interface specified by *interface-name*.
priority *priority*	The priority (value between 0 and 255) assigned to the RLOC. When multiple locators have the same priority they may be used in load-shared fashion. A lower value indicates a higher priority.
weight *weight*	The weight (value between 0 and 100) assigned to the locator. Used in order to determine how to load-share traffic between multiple locators when the priorities assigned to multiple locators are the same. The value represents the percentage of traffic to be load-shared.

Defaults

No LISP database entries are defined by default.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command configures the LISP database parameters for the specified IPv4 EID-prefix block, including its associated locator, priority and weight. The IPv4 EID-prefix/prefix-length is a LISP IPv4 EID-prefix block for which this ETR registers as being authoritative for with a Map-Server. The locator is the IPv4 or IPv6 address of a loopback interface or physical WAN interface used as the Routing Locator (RLOC) address for the EID-prefix assigned to the site.

Associated with the locator address are a priority and weight used to define traffic policies when multiple RLOCs apply to the same EID-prefix block. When a router is configured as an ETR, these LISP database-mapping parameters are advertised within a Map-Reply message to indicate the ingress traffic preferences of the site for the associated EID-prefix block. An ITR then selects a locator (outer header) address for encapsulating packets destined to the EID-prefix based on these advertised parameters.

When a LISP site has multiple locators associated with the same EID-prefix block, multiple **ip lisp database-mapping** commands are used to configure all of the locators for a given EID-prefix block. Each locator may be assigned the same or a different priority value between 0 and 255. When multiple locators are assigned different priority values, the priority value alone is used by an ITR to determine which locator to prefer. A lower value indicates a more preferable path. A value of 255 indicates that the locator must not be used for unicast traffic forwarding. When multiple locators have the same priority, this indicates they may be used in a load-sharing manner. In this case, for a given priority, the weight given to each locator is used to determine how to load-balance unicast packets between them. Weight is a value between 0 and 100 and represents the percentage of traffic to be load-shared to that locator. A weight value of zero indicates to an ITR receiving the Map-Reply that it may decide how to load-share traffic destined to that EID-prefix block. If a non-zero weight value is assigned to any locator for a given EID-prefix block, then all locators with the same priority for that same EID-prefix block must also be assigned a non-zero weight value and the sum of all weight values must equal 100. If a weight value of zero is assigned to any locator for a given EID-prefix block, then all locators with the same priority for that same EID-prefix block must also be assigned a weight value of zero.

When a LISP site is assigned multiple IPv4 EID-prefixes, the **ip lisp database-mapping** command is configured for each IPv4 EID-prefix assigned to the site and for each locator by which the IPv4 EID-prefix is reachable.

Note NX-OS limits the number of **ip lisp database-mapping** commands configured on an ETR to four (4) entries per EID Address Family, per vrf context.

When multiple ETRs are used at a LISP site, the **ip lisp database-mapping** command must be configured identically on all ETRs for all locators by which an IPv4 EID-prefix block is reachable, even when the locator is not local to the specific ETR being configured. For example, if a site uses two ETRs and each has a single locator, both ETRs must configure the **ip lisp database-mapping** command for the assigned IPv4 EID-prefix block for its own locator as well as the locator of the other ETR.

If the ETR is sited behind an upstream NAT device, the RLOC to be associated with EID prefixes may not be know. In addition, the local interface of the ETR (what would typically be its routing locator) could belong to the private address space for example, that the NAT device translates to a public globally routed address. In this case it may not be possible to specify a locator in the **ip lisp database-mapping** entry. The **dynamic** keyword can be configured with the **ip lisp database-mapping** command in this case so to dynamically determine the RLOC rather than being statically defined in each **ip lisp database-mapping** entry.

✎

Note When the **dynamic** keyword is used because an ETR is sited behind NAT in order to find dynamically the public global locator address for use in Map-Register and Map-Reply messages, the command {**ip** | **ipv6**} **lisp nat-traversa**l must also be configured under the interface connecting the ETR to the core. The command {**ip** | **ipv6**} **lisp nat-traversa**l performs the actual process of determining the global NAT'ed routing locator address. See the {**ip** | **ipv6**} **lisp nat-traversa**l commands for further details.

Examples

The following example configures LISP database-mapping entries for a single IPv4 EID-prefix block and two locators associated with the EID-prefix block. Each locator is assigned the same priority (1) and weight (50), indicating that ingress traffic is expected to be load-shared equally across both paths.

```
Router(config)# ip lisp database-mapping 192.168.1.0/24 10.1.1.1 priority 1 weight 50
Router(config)# ip lisp database-mapping 192.168.1.0/24 10.1.2.1 priority 1 weight 50
```

Related Commands

Command	Description
ip lisp etr map-server	Configures the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv4 EID prefixes.
ip lisp map-cache	Configures a static IPv4 EID-prefix to locator map-cache entry.
ip lisp nat-transversal	To configure an ETR with a private locator that is sited behind a NAT device to dynamically determine its NAT-translated public globally routed locator address for the applied interface.

---

ip lisp etr

To configure a router to act as an IPv4 LISP Egress Tunnel Router (ETR), use the **ip lisp etr** command in global configuration mode. To remove LISP ETR functionality, use the **no** form of this command.

> **[no] ip lisp etr**

Syntax Description

This command has no arguments or keywords.

Defaults

The router does not provide LISP ETR services.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable the router to perform IPv4 LISP Egress Tunnel Router (ETR) functionality. When a router is configured as an IPv4 ETR, it is typically also configured with **ip lisp database-mapping** commands so

LISP-11

that the ETR knows what EID-prefix blocks and corresponding locators are used for its LISP site. In addition, the ETR is also configured to register with a Map-Server by using the **ip lisp etr map-server** command, or to use static LISP EID-to-RLOC mappings with the **ip lisp map-cache** command to participate in LISP networking.

✎ **Note** When an ETR is handling packets with mixed Address Families between EIDs and RLOCs (i.e. IPv4 EIDs and IPv6 RLOCs, or IPv6 EIDs and IPv4 RLOCs), it is required to configure both the **ip lisp etr** command as well as the **ipv6 lisp etr** command.

✎ **Note** It is common for a device configured as an ETR to also be configured as an ITR. However, the LISP architecture does not require this and ETR and ITR functionality can occur in different devices. When configuring a device as both an ITR and an ETR, using the command **ip lisp itr-etr** to enable both capabilities in one command is recommended.

Examples

The following example configures IPv4 LISP ETR functionality on the router.

```
Router(config)# ip lisp etr
```

Related Commands

Command	Description
ip lisp database-mapping	Configures an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy.
ip lisp etr map-server	Configures the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv4 EID prefixes.
ip lisp itr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR)
ip lisp itr-etr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR) and an IPv4 LISP Egress Tunnel Router (ETR) with one command.
ip lisp map-cache	Configures a static IPv4 EID-prefix to locator map-cache entry.

---

ip lisp etr accept-map-request-mapping

To configure an ETR to cache IPv4 mapping data contained in a Map-Request message, use the **ip lisp etr accept-map-request-mapping** command in global configuration mode. To remove this functionality, use the **no** form of this command.

> **[no] ip lisp etr accept-map-request-mapping** [**verify**]

Syntax Description

verify	(Optional) Specifies that mapping data should be cached but not used for forwarding packets until the ETR can send its own Map-Request to one of the locators from the mapping data record and receive a Map-Reply with the same data in response.

Defaults

The router does not cache mapping data contained in a Map-Request message.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When an ETR receives a Map-Request message, this message may contain mapping data for the invoking IPv4 source-EID's packet. By default, the ETR will ignore mapping data included in Map-Request messages. However, by configuring the **ip lisp etr accept-map-request-mapping** command, the ETR will cache the mapping data in its map-cache and immediately use it for forwarding packets.

When the optional **verify** keyword is configured, the ETR will still cache the mapping data but will not use it for forwarding packets until the ETR can send its own Map-Request to one of the locators from the mapping data record, and receives the same data in a Map-Reply message.

✎
Note For security purposes, it is recommended that the **verify** keyword be configured. Unless the ETR and ITR are deployed in a trusted environment, using the optional **verify** keyword is considered a best practice. In a trusted environment it may be considered acceptable for verification to not be configured, in which case the new mapping will occur in one-half round-trip-time (RTT) as compared with the normal Map-Request/Map-Reply exchange process.

When the **ip lisp etr accept-map-request-mapping** command is enabled and then later disabled, issuing the command **clear ip lisp map-cache** is required to clear any map-cache entries that are currently in the "tentative" state. Map-cache entries can remain in the "tentative" state for up to one minute and thus it may be desirable to clear these entries manually when this command is removed.

Examples

The following example configures the ETR to cache IPv4 mapping data included in Map-Request messages but to verify its accuracy prior to using this data to forward packets.

```
Router(config)# ip lisp etr accept-map-request-mapping verify
```

Related Commands

Command	Description
ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR).
clear ip lisp map-cache	Clear the LISP IPv4 map-cache on the local router.

---

ip lisp etr glean-mapping

To configure an ETR to add inner header (EID) source address to outer header (RLOC) source address mappings it to its EID-to-RLOC cache (map-cache), use the **ip lisp etr glean-mapping** command in global configuration mode. To remove this functionality, use the **no** form of this command.

> **[no] ip lisp etr glean-mapping** [**verify**]

Syntax Description

verify	(Optional) Specifies that gleaned EID-to-RLOC mapping data should be cached but not used for forwarding packets until the ETR can send its own Map-Request to the originating ITR and receive a Map-Reply with the same data in response.

Defaults

The router does not cache gleaned EID-to-RLOC mapping data in its map-cache.

LISP-13

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When an ETR receives LISP encapsulated packets, the inner header (EID) source address and outer header (RLOC) source address should match an entry found in the map-cache as determined by the results of a Map-Request/Map-Reply exchange. In certain circumstances, for example when a host moves from one ITR to another ITR, it is possible for the EID-to-RLOC mapping to change since the new ITR can encapsulate packets to the ETR using a different locator. By configuring the **ip lisp etr glean-mapping** command, the ETR will recognize the new locator information for the moved host's EID and update the map-cache with this information.

✎

Note Gleaned EID-to-RLOC map-cache entries are stored with a priority of 1 and a weight of 100.

When the optional **verify** keyword is configured, the ETR will cache the gleaned EID-to-RLOC mapping data but it will not be used for forwarding packets until the ETR can send its own Map-Request to the originating ITR and receive a Map-Reply with the same nonce included in the Map-Request. The gleaned locator will then be used. When the **verify** keyword is specified, the gleaned locator will not be used to forward traffic and all packets will be dropped until the Map-Reply is returned.

✎

Note For security purposes, it is recommended that the **verify** keyword be configured. Unless the ETR and ITR are deployed in a trusted environment, using the optional **verify** keyword is considered a best practice. In a trusted environment it may be considered acceptable for verification to not be configured, in which case the new mapping will occur in one-half round-trip-time (RTT) as compared with the normal Map-Request/Map-Reply exchange process.

Examples

The following example configures the ETR to cache IPv4 mapping data included in Map-Request messages but to verify its accuracy prior to using this data to forward packets.

```
Router(config)# ip lisp etr glean-mapping verify
```

Related Commands

Command	Description
ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR).

---

ip lisp etr map-cache-ttl

To configure the TTL value to be inserted into LISP IPv4 Map-Reply messages, use the **ip lisp etr map-cache-ttl** command in global configuration mode. To remove the configured TTL value and return to the default value, use the **no** form of this command.

[no] ip lisp etr map-cache-ttl *time-to-live*

Syntax Description

time-to-live	A value, in minutes, to be inserted in the TTL field in Map-Reply messages. Valid entries are between 60 minutes (1 hour) and 10080 minutes (1 week).

Defaults

The default TTL value is 1440 minutes (24 hours).

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to change the default value associated with the Time-to-Live (TTL) field in IPv4 Map-Reply messages. This may be useful when you wish to change the default TTL that remote ITRs will cache and use for your sites IPv4 EID prefix. The default value is 1440 minutes (24 hours), the minimum value cannot be less than 60 minutes, and the maximum cannot be greater than 10080 minutes (one week).

Examples

The following example configures the ETR to use a TTL of 120 minutes in its IPv4 Map-Reply messages.

```
Router(config)# ip lisp etr map-cache-ttl 120
```

Related Commands

Command	Description
ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR).

---

ip lisp etr map-server

To configure the IPv4 or IPv6 locator address of the LISP Map-Server to be used by the ETR when registering for IPv4 EIDs, use the **ip lisp etr map-server** command in global configuration mode. To remove the configured locator address of the LISP Map-Server, use the **no** form of this command.

> [no] ip lisp etr map-server *map-server-address* {[**key** *key-type password*] | **proxy-reply**}

Syntax Description

map-server-address	Specifies the IPv4 or IPv6 locator addresses of the Map-Server.
key *key-type*	Specifies how the following SHA-1 password (key) is encoded. Type (0) indicates that a cleartext password follows; Type (3) indicates that a 3DES encrypted key follows; Type (7) indicates that a Cisco Type 7 encrypted password follows.
password	Specifies the password used for computing the SHA-1 HMAC hash that is included in the header of the Map-Register message.

LISP-15

proxy-reply	(Optional) Indicates to the Map-Server via a Map-Register message that the Map-Server should send Map-Replies on behalf of the ETR (this site) to requesting ITRs.

Defaults

No LISP Map-Server locator addresses are configured by default.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.0(1.13) August Release	This command was modified.

Usage Guidelines

Use the **ip lisp etr map-server** command to configure the IPv4 or IPv6 locator of the Map-Server to which the ETR will register for its IPv4 EID(s). A password used in the calculation of a SHA-1 HMAC hash that is included in the header of the Map-Register message must also be provided. You can configure the ETR to register with at most two Map-Servers per EID address family. Once the ETR registers with the Map-Server(s), the Map-Server(s) will begin to advertise the EID-prefix block(s) and RLOC(s) for the LISP site.

The SHA-1 HMAC password may be entered in unencrypted (cleartext) form or encrypted form. To enter an unencrypted password, specify a key-type value of 0. To enter a 3DES-encrypted password, specify a key-type value of 3. To enter a Cisco-encrypted password, specify a key-type value of 7.

⚠ **Caution** A Map-Server authentication key entered in cleartext form will automatically be converted to Type 3 (encrypted) form.

✎ **Note** The Map-Server must also be configured with IPv4 EID prefixes that match the IPv4 EID-prefixes configured on this ETR using the **ip lisp database-mapping** command, as well as a password matching the one provided with the **key** keyword on this ETR.

When the keyword **proxy-reply** is used with this command, the ETR is indicating to the Map-Server via a Map-Register message that the Map-Server should send non-authoritative Map-Replies on behalf of the ETR (this LISP site) to ITRs requesting EID-to-RLOC mapping resolutions for an EID prefix at this LISP site. On the Map-Server, the **show lisp site** *site-name* command indicates whether proxy-reply is enabled or not.

✎ **Note** If the command **ip lisp itr map-resolver** is not configured, then the locator address used in the command **ip lisp etr map-server** will automatically be used for a Map-Resolver locator (without the need to explicityly configure one). This allows for the minimum LISP configuration on an NX-OS xTR of:

```
feature lisp
ip lisp itr-etr
ip lisp database-mapping ....
ip lisp etr map-server ...
```

The output of the command **show ip lisp** indicates whether the Map-Server locator is also used as a Map-Resolver locator.

Examples

The following example configures the ETR to register to two Map-Servers, one with the locator 10.1.1.1 and another with the locator 172.16.1.7.

```
Router(config)# ip lisp etr map-server 10.1.1.1 key some-password
Router(config)# ip lisp etr map-server 172.16.1.7 key some-password
```

The following example configures the ETR to register to the Map-Server with the locator 10.1.1.1 and requests that the Map-Server proxy-reply for the site.

```
Router(config)# ip lisp etr map-server 10.1.1.1 key some-password
Router(config)# ip lisp etr map-server 10.1.1.1 proxy-reply
```

Related Commands

Command	Description
ip lisp alt-vrf	Configures which VRF supporting the IPv4 address-family LISP should use when sending Map Requests for an IPv4 EID-to-RLOC mapping directly over the ALT.
ip lisp database-mapping	Configures an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy.
ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR)
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server

---

ip lisp hardware-forwarding

To enable hardware-forwarding specifically on the Nexus 7000 when at least one 32x10GE line card is installed, use the **ip lisp hardware-forwarding** command in global configuration mode. To disable this functionality, use the **no** form of this command.

    [no] ip lisp hardware-forwarding

Syntax Description

This command has no arguments or keywords.

Defaults

By default, hardware forwarding is enabled on the Nexus 7000 when at least one 32x10GE line card is installed.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command is **ONLY** applicable to the Nexus 7000. Hardware forwarding for LISP is only supported on the following Line Cards:

- N7K-M132XP-12 Cisco Nexus 7000 Series 32-Port 10Gb Ethernet Module
- N7K-M132XP-12L Cisco Nexus 7000 Series 32-Port 10Gb Ethernet Module with XL Option

LISP input and output interfaces MUST be on the above Line Cards in order for hardware-based LISP encapsualtion and decapsulation to be performed.

By default, hardware forwarding of LISP packets is enabled on the Nexus 7000 when at least one 32x10GE line card is installed. In certain debugging operations, however, it may be useful to disable hardware forwarding. This is accomplished by using the **no ip lisp hardware-forwarding** command. When the **no** form of this command is used, software-based supervisor LISP forwarding is enabled on the Nexus 7000.

⚠

Caution   Disabling hardware forwarding should only be used in diagnostic situations. Configuring the **no ip lisp hardware-forwarding** command will cause a full map-cache download to the Nexus 7000 hardware.

✎

Note   Configuring the **no ip lisp hardware-forwarding** command for debugging purposes is best used in conjunction with the **debug lisp ufdm detail** command. Be sure to re-enable hardware-forwarding when debugging operations are completed by invoking the **ip lisp hardware-forwarding** command.

Examples

The following example disables IPv4 LISP hardware forwarding on the Nexus 7000 and then enables UFDM debugging.

```
Router(config)# no ip lisp hardware-forwarding
Router(config)# exit
Router# debug lisp ufdm detail
```

Related Commands

Command	Description
lisp beta	Enable LISP functionality on the Nexus 7000 router.
debug lisp ufdm	Display debug messages related to activities between the LISP process and the UFDM process and which program the EARL8 on the Nexus 7000 only.

---

ip lisp itr

To configure a router to act as an IPv4 LISP Ingress Tunnel Router (ITR), use the **ip lisp itr** command in global configuration mode. To remove LISP ITR functionality, use the **no** form of this command.

> **[no] ip lisp itr**

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not provide ITR functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable the router to perform IPv4 LISP Ingress Tunnel Router (ITR) functionality.

When a router is configured as an ITR, it must decide how to handle the packets it receives. This decision process is summarized as follows:

1. If the packet destination matches an existing route in the routing table, the packet is forwarded natively (regardless of the packet source IP address).

2. If the packet destination matches a DEFAULT ROUTE or NO ROUTE in the routing table, then the packet source IP address is checked against configured **ip lisp database-mapping** commands to determine if the source is a LISP EID.

   a. If the packet source IP address **is not** a configured EID, then the packet **is not** LISP-eligible. If the destination matches a DEFAULT ROUTE, the packet is forwarded natively. If there is no route to the destination, the packet is dropped.

   b. If the packet source IP address **is** a configured EID, then the packet **is** LISP-eligible. In this case, the ITR checks the existing map-cache and does one of the following actions:

      - If a map-cache entry exists with an action of LISP encapsulation, as would be the case for a destination that is another valid LISP site, then the packet is LISP-encapsulated and forwarded.

      - If a map-cache entry exists with an action of "forward-native," as would be the case when the destination is not another LISP site and the map-cache entry is added by a Negative-Map-Reply, then the packet is forwarded natively. If the **ip lisp use-petr** command is also configured, then the packet is LISP-encapsulated to the configured PETR.

      - If a map-cache entry exists with an action of "drop," as would be the case when a static map-cache entry is added with this action, then the packet is dropped.

      - If a map-cache entry exists with an action of "send-requst," as would be the case when a static map-cache entry is added (such as in the case of a PITR) or when it matches no entry, then a Map-Request is sent to the configured Map-Resolver and the packet is silently dropped. Subsequent packets to the same destination should be covered by any new map-cache entry added as a result of the Map-Request.

The ITR may use one of two methods to send a Map-Request to obtain an IPv4 EID-to-RLOC mapping:

- When a Map-Resolver is configured via the **ip lisp itr map-resolve**r command, the ITR will send its Map-Request in a LISP Encapsulated Control Message (ECM) to the Map-Resolver.
- When the ITR is directly attached to the ALT using the **ip lisp alt-vrf** command, the ITR will send its Map-Request directly on the alternate LISP Alternate Logical Topology (ALT).

The ITR caches the resultant IPv4 EID-to-RLOC mapping information returned by the associated Map-Reply in its map-cache. Subsequent packets destined to the same IPv4 EID-prefix are then LISP-encapsulated according to this IPv4 EID-to-RLOC mapping entry.

Note When instance-ID's are used to support LISP virtualization, an ITR must be configured to use a Map-Resolver (MR) (configured via the **ip lisp itr map-resolve**r command) to obtain IPv4 EID-to-RLOC mappings. It **must not** be configured to directly attach to the ALT (using the **ip lisp alt-vrf** command) since the ALT does not support LISP virtualization.

Note It is common for a device configured as an ITR to also be configured as an ETR. However, the LISP architecture does not require this and the functionality can occur in a different device. When configuring a device as both an ITR and an ETR, using the command **ip lisp itr-etr** to enable both capabilities in one command is recommended.

Examples

The following example configures IPv4 LISP ITR functionality on the router.

```
Router(config)# ip lisp itr
```

Related Commands

Command	Description
ip lisp alt-vrf	Configures which VRF supporting the IPv4 address-family LISP should use when sending Map Requests for an IPv4 EID-to-RLOC mapping directly over the ALT.
ip lisp database-mapping	Configures an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy.
lp lisp itr-etr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR) and an IPv4 LISP Egress Tunnel Router (ETR) with one command.
ip lisp itr map-resolver	Configures the IPv4 or IPv6 locator address of the LISP Map-Resolver to which the ITR sends IPv4 Map-Request messages
ip lisp map-cache	Configure a static IPv4 EID-prefix to locator map-cache entry.

ip lisp itr map-resolver

To configure the IPv4 or IPv6 locator address of the LISP Map-Resolver to be used by the ITR or PITR when sending Map-Requests for IPv4 EID-to-RLOC mapping resolution, use the **ip lisp itr map-resolver** command in global configuration mode. To remove the configured locator address of the LISP Map-Resolver, use the **no** form of this command.

[no] ip lisp itr map-resolver *map-resolver-address*

Syntax Description

map-resolver-address	Specifies the IPv4 or IPv6 locator addresses of the Map-Resolver.

Defaults

No LISP Map-Resolver locator address is configured by default.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command configures the locator to be used by a LISP ITR or PITR to reach the configured Map-Resolver when sending a map request for IPv4 EID-to-RLOC mapping resolution. Up to two Map-Resolvers can be configured per ITR or PITR within a site, for each address-family. The locator of the Map-Resolver may be reachable via IPv4 or IPv6 RLOC addresses.

When a LISP ITR or PITR needs to resolve an IPv4 EID-to-RLOC mapping for a destination EID, it can be configured to send a map request message either to a Map Resolver configured using the **ip lisp itr map-resolver** command, or directly over the LISP ALT using the **ip lisp alt-vrf** command. When a Map Resolver is used, map requests are sent to the Map Resolver as a LISP Encapsulated Control Message (ECM). When the ALT is used, map requests sent over the ALT directly to the EID being queried.

Note When the **ip lisp itr map-resolver** command is entered, the **ip lisp alt-vrf** command is not used (and may be removed).

Note When instance-ID's are used to support LISP virtualization, an ITR or PITR **must** be configured to use a configured Map-Resolver (MR) (configured via the **ip lisp itr map-resolve**r command) to obtain IPv4 EID-to-RLOC mappings. The LISP-ALT mapping system does not support LISP virtualization.

Note If the command **ip lisp etr map-resolver** is not configured, then the locator address used in the command **ip lisp etr map-server** will automatically be used for a Map-Resolver locator (without the need to explicityly configure one). This allows for the minimum LISP configuration on an NX-OS xTR of:

```
feature lisp
ip lisp itr-etr
ip lisp database-mapping ....
ip lisp etr map-server ...
```

The output of the command **show ip lisp** indicates whether the Map-Server locator is also used as a Map-Resolver locator.

Examples

The following example configures an ITR to use the Map-Resolver located at 10.1.1.1 when sending its Map-Request messages.

```
Router(config)# ip lisp itr map-resolver 10.1.1.1
Router(config)# ip lisp itr map-resolver 2001:DB8:0A::1
```

Related Commands

Command	Description
ip lisp alt-vrf	Configures which VRF supporting the IPv4 address-family LISP should use when sending Map Requests for an IPv4 EID-to-RLOC mapping directly over the ALT.
ip lisp itr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR)
ip lisp map-request-source	Configures the source IPv4 or IPv6 address to be used in IPv4 LISP Map-Request messages.

ip lisp itr send-data-probe

To configure an ITR or PITR to find an IPv4 EID-to-RLOC mapping for a packet it needs to encapsulate by sending a Data Probe rather than by sending a Map-Request message, use the **ip lisp itr send-data-probe** command in global configuration mode. To remove this functionality, use the **no** form of this command.

[no] ip lisp itr send-data-probe

Syntax Description

This command has no arguments or keywords.

Defaults

By default, an ITR does not send data-probes to determine IPv4 EID-to-RLOC mappings.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

⚠

Caution The **ip lisp itr send-data-probe** command is deprecated and no longer supported and should not be used. Its inclusion in this document is solely for legacy purposes. The use of the LISP Data Probe is strongly discouraged as this mechanism forwards data plane traffic over the LISP-ALT. The LISP-ALT is intended to function solely as a control plane mechanism for LISP and its use for carrying data plane traffic consumers potentially scarce resources, as well as potentially subjects it to denial of service attacks.

When a LISP ITR or PITR gets a map-cache miss and needs to resolve an IPv4 EID-to-RLOC mapping for a destination EID, it is typically configured to send a Map-Request message either in a LISP Encapsulate Control Message (ECM) to the Map Resolver configured using the **ip lisp itr map-resolver** command, or directly over the LISP ALT referred to by the **ip lisp alt-vrf** command. In either case, the first packet of the flow that caused the map-cache miss is dropped. Once the Map-Reply populates the map-cache, subsequent packets to the same destination are forwarded directly by LISP.

A **deprecated** method for determining EID-to-RLOC mappings that does not drop the first packet of a flow is implemented using a LISP Data Probe technique. When using the LISP Data Probe technique, rather than dropping the first data packet and sending a Map-Request message, the data packet is LISP-encapsulated where the inner header destination address equals the outer header destination address and forwarded directly over the LISP-ALT to the decapsulating ETR. This Data Probe packet triggers a Map-Reply by the ETR, which then returns a Map-Reply directly back to the ITR.

✎

Note When an ITR or PITR is configured with the **ip lisp itr send-data-probe** command the ITR or PITR must also be configured to use the LISP-ALT (using the **ip lisp alt-vrf** command) since the Data-Probe is sent over the LISP-ALT.

Examples

The following example configures a LISP ITR to send Data Probes to determine IPv4 EID-to-RLOC mappings.

```
Router(config)# ip lisp itr send-data-probe
```

Related Commands

Command	Description
ip lisp alt-vrf	Configures which VRF supporting the IPv4 address-family that LISP should use when sending Map Requests for an IPv4 EID-to-RLOC mapping directly over the ALT.
ip lisp itr map-resolver	Configured the IPv4 or IPv6 locator address of the LISP Map-Resolver to which the ITR sends IPv4 Map-Request messages

---

ip lisp itr-etr

To configure a router to act as both an IPv4 LISP Ingress Tunnel Router (ITR) and Egress Tunnel Router (ETR), use the **ip lisp itr-etr** command in global configuration mode. To remove LISP ITR functionality, use the **no** form of this command.

> **[no] ip lisp itr-etr**

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not provide ITR or ETR functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13) (August update)	This command was introduced.

Usage Guidelines

Use this command to enable the router to perform both IPv4 LISP Ingress Tunnel Router (ITR) and Egress Tunnel Router (ETR) functionality simultaneously, via a single command.

For usage guidelines for IPv4 LISP Ingress Tunnel Router (ITR) functionality, refer to the **ip lisp itr** command.
For usage guidelines for IPv4 LISP Egress Tunnel Router (ETR) functionality, refer to the **ip lisp etr** command.

Note If this command is used and either of the **ip lisp itr** or **ip lisp etr** commands have already been configured, they will be automatically removed from the configuration file.

Note It is common for a device configured as an ITR to also be configured as an ETR. However, the LISP architecture does not require this and the functionality can occur in a different device. When configuring a device as both an ITR and an ETR, using the command **ip lisp itr-etr** to enable both capabilities in one command is recommended.

Examples

The following example configures IPv4 LISP ITR and ETR functionality on the router.

```
Router(config)# ip lisp itr-etr
```

Related Commands

Command	Description
ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR)
ip lisp itr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR)

---

ip lisp locator-down

To configure a locator from a locator-set associated with an IPv4 EID-prefix database-mapping to be unreachable (down), use the **ip lisp locator-down** hidden command in global configuration mode. To return the locator to be reachable (up), remove the configuration using the **no** form of this command.

> **[no] ip lisp locator-down** *EID-prefix/prefix-length locator*

Syntax Description

EID-prefix/prefix-length	The IPv4 EID prefix and length advertised by this router.
locator	The IPv4 or IPv6 Routing Locator (RLOC) associated with this EID-prefix.

Defaults

An IPv4 or IPv6 locator associated with a configured IPv4 EID-prefix block is considered reachable (up) unless an IGP routing protocol indicates it is down.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When LISP database parameters are configured on an ITR for specified IPv4 EID-prefix blocks using the **ip lisp database-mapping** command or **ip lisp map-cache** command, the locators associated with these IPv4 EID-prefix blocks are considered as reachable (up) by default. The hidden command **ip lisp locator-down** command can be used to configure a locator from a locator-set associated with the EID-prefix database mapping to be down.

When this command is configured, the Locator Status Bits (LSB) for the configured locator will be cleared (set to zero) when encapsulating packets to remote sites. ETRs at remote sites look for changes in the LSBs when decapsulating LISP packets, and when the LSB indicates that a specific locator is down, the ETR, also acting as an ITR, will refrain from encapsulating packets using the 'down' locator to reach the local site.

LISP-24

> ✎
>
> **Note** If this command is configured on an ITR to indicate that a locator is unreachable (down) and the LISP site includes multiple ITRs, this command must be configured on all ITRs at the site to ensure that the site consistently tells remote sites that the configured locator is not reachable.

Examples

The following example configures the locator 10.1.1.1 to a down state for the EID-prefix block 192.168.1.0/24.

```
Router(config)# ip lisp locator-down 192.168.1.0/24 10.1.1.1
```

Related Commands

Command	Description
ip lisp database-mapping	Configures an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy.
ip lisp itr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR)
ip lisp map-cache	Configures a static IPv4 EID-prefix to locator map-cache entry.

---

ip lisp locator-vrf

To configure a non-default virtual routing and forwarding (VRF) table to be referenced by any IPv4 locators, use the **ip lisp locator-vrf** command in global configuration mode. To return to using the default routing table for locator address references, use the **no** form of this command.

   [no] ip lisp locator-vrf {*vrf-name* | **default**}

Syntax Description

vrf-name	The name of the VRF to be referenced by IPv4 locator addresses.
default	Specifies that the **default** VRF should be referenced by the IPv4 locator addresses.

Defaults

IPv4 locator addresses are associated with the default (global) routing table.

Command Modes

VRF configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(3.lisp)	This command was introduced.

Usage Guidelines

By default, LISP is configured to consider both EIDs and locators to be reachable from the default VRF (i.e. the global routing table). When it is desired to configure LISP to associate locator addresses with a VRF other than the default VRF, the **ip lisp locator-vrf** command is used to specify the IPv4 VRF to be associated with these locator addresses.

When the **ip lisp locator-vrf** command is configured, the locator addresses in any subsequent LISP commands are referenced to the specified VRF. For example, the locator addresses in the **ip lisp itr map-resolver** and **ip lisp etr map-server** commands would refer to the VRF configured by the **ip lisp locator-vrf** command when configured. Note that the map-server(s) and map-resolver(s) must also share the configuration from the locator-VRF and be reachable within that address space.

✎

Note When mixed address families are configured for EIDs and/or locators (i.e. IPv4 EIDs and IPv6 locators or IPv6 EIDs and IPv4 locators), this command must be configured for both address families.

Example

In the following example, a LISP xTR is configured with one EID VRF context named **PURPLE**, and one locator VRF context named **BLUE**. That is, the EID prefixes 192.168.1.0/24 and 2001:db8:a::/64 are reachable via the VRF context **PURPLE**. The locator used for encapsulation (i.e. 10.0.0.2), and the locators of the Map-Server and Map-resolver (i.e. 10.0.2.2) are reachable via the VRF context BLUE.

```
Router(config)# feature lisp
Router(config)# vrf context PURPLE
Router(config-vrf)# lisp instance-id 101
Router(config-vrf)# ip lisp locator-vrf BLUE
Router(config-vrf)# ipv6 lisp locator-vrf default
Router(config-vrf)# ip lisp itr-etr
Router(config-vrf)# ipv6 lisp itr-etr
Router(config-vrf)# ip lisp database-mapping 192.168.1.0/24 10.0.0.2 priority 1 weight 100
Router(config-vrf)# ipv6 lisp database-mapping 2001:db8:a::/64 10.0.0.2 priority 1 weight 100
Router(config-vrf)# ip lisp etr map-server 10.0.2.2 key PURPLE-key
Router(config-vrf)# ipv6 lisp etr map-server 10.0.2.2 key PURPLE-key
Router(config-vrf)# ip lisp itr map-resolver 10.0.2.2
Router(config-vrf)# ipv6 lisp itr map-resolver 10.0.2.2
Router(config-vrf)# exit
Router(config)# vrf context BLUE
Router(config-vrf)# ip lisp itr-etr
Router(config-vrf)# ipv6 lisp itr-etr
Router(config-vrf)# ip route 0.0.0.0/0 10.0.0.1
Router(config-vrf)# exit
Router(config)#
```

Related Commands

Command	Description
ip lisp etr map-server	Configured the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv4 EID prefixes
ip lisp itr map-resolver	Configured the locator address of the LISP Map-Resolver to which the ITR sends Map-Request messages

ip lisp map-cache

To configure a static IPv4 EID-to-RLOC mapping relationship and its associated traffic policy, or to statically configure the packet handling behavior associated with a destination IPv4 EID-prefix, use the **ip lisp map-cache** command in global configuration mode. To remove the configuration, use the **no** form of this command.

> **[no] ip lisp map-cache** *destination-EID-prefix/prefix-length* {*locator* **priority** *priority* **weight** *weight*}

> **[no] ip lisp map-cache** *destination-EID-prefix/prefix-length* {**drop | map-request | native-forward**}

Syntax Description

destination-EID-prefix/prefix-length	Destination IPv4 EID-prefix/prefix-length.
locator	The IPv4 or IPv6 Routing Locator (RLOC) associated with this EID-prefix/prefix-length
priority *priority*	The priority (value between 0 and 255) assigned to the RLOC. When multiple locators

LISP-26

	have the same priority they may be used in load-shared fashion. A lower value indicates a higher priority.
weight *weight*	The weight (value between 0 and 100) assigned to the locator. Used in order to determine how to load-share traffic between multiple locators when the priorities assigned to multiple locators are the same. The value represents the percentage of traffic to be load-shared.
drop	(Optional) Drop packets that match this map-cache entry
map-request	(Optional) Send a Map-Request for packets that match this map-cache entry
native-forward	(Optional) Natively forward packets that match this map-cache entry

Defaults

No IPv4 EID-to-RLOC mapping relationships or static IPv4 EID-to-RLOC mapping destinations are configured by default.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The first use of this command is to configure an ITR with a static IPv4 EID-to-RLOC mapping relationship and its associated traffic policy. For each entry, a destination IPv4 EID-prefix block and its associated locator, priority and weight are entered. The IPv4 EID-prefix/prefix-length is the LISP EID-prefix block at the destination site. The locator is an IPv4 or IPv6 address of the remote site where the IPv4 EID-prefix can be reached. Associated with the locator address is a priority and weight that are used to define traffic policies when multiple RLOCs are defined for the same EID-prefix block. This command can be entered up to four (4) times for a given EID-prefix. Static IPv4 EID-to-RLOC mapping entries configured using this command take precedence over dynamic mappings learned through Map-Request/Map-Reply exchanges.

The second, optional use of this command is to statically configure the packet handling behavior associated with a specified destination IPv4 EID-prefix. For each entry, a destination IPv4 EID-prefix block is associated with a configured forwarding behavior. When a packet's destination address matches the EID-prefix, one of the following packet handling options can be configured:

drop – Packets matching the destination IPv4 EID-prefix are dropped. For example, this action may be useful when administrative policies define that packets should be prevented from reaching a site.

native-forward – Packets matching the destination IPv4 EID-prefix are natively forwarded without LISP encapsulation. This action may be useful when the destination site is known to always be reachable natively and LISP encapsulation should never be used.

map-request – Packets matching the destination IPv4 EID-prefix cause a Map-Request to be sent. It is implied that the Map-Reply returned by this request will allow subsequent packets matching this EID-prefix to be LISP-encapsulated. This action may be useful for troubleshooting map-request activities and other diagnostic actions.

Examples

The following example configures a destination EID-to-RLOC mapping and associated traffic policy for the IPv4 EID-prefix block 192.168.1.0/24. In this example, the locator for this EID-prefix block is 10.1.1.1 and the traffic policy for this locator has a priority of 1 and a weight of 100.

LISP-27

```
Router(config)# ip lisp map-cache 192.168.1.0/24 10.1.1.1 priority 1 weight 100
```

The following example configures a destination EID-to-RLOC mapping and associated traffic policy for the IPv4 EID-prefix block 192.168.2.0/24 to **drop**. No traffic will be forwarded to this destination as a result.

```
Router(config)# ip lisp map-cache 192.168.2.0/24 drop
```

Related Commands

Command	Description
ip lisp database-mapping	Configures an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy.
ip lisp itr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR)
ip lisp map-cache-limit	Configures the maximum number of IPv4 LISP map-cache entries allowed to be stored by the router.

ip lisp map-cache-limit

To configure the maximum number of IPv4 LISP map-cache entries allowed to be stored by the router, use the **ip lisp map-cache-limit** command in global configuration mode. To remove the configured map-cache limit, use the **no** form of this command.

> **[no] ip lisp map-cache-limit** *cache-limit* [**reserve-list** *list*]

Syntax Description

cache-limit	The maximum number of IPv4 LISP map-cache entries allowed to be stored on the router. The valid range is from 0 to 10000.
reserve-list *list*	(Optional) Specifies a set of IPv4 EID-prefixes in the referenced prefix-list for which dynamic map-cache entries shall always be stored.

Defaults

The default map-cache limit is 1000 entries.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to control the maximum number of IPv4 LISP map-cache entries that are allowed to be stored on the router. An optional **reserve-list** can be configured to guarantee that the router always stores the referenced IPv4 EID-prefixes.

LISP IPv4 map-cache entries are added in one of two ways – dynamically or statically. Dynamic entries are added when a valid Map-Reply message is returned for a Map-Request message generated in response to a

LISP-28

cache-miss lookup. Static entries are added via the **ip lisp map-cache** command. Whether a new map-cache entry is stored depends on the following conditions.

- Dynamic map-cache entries are always added until the default or configured cache-limit is reached. After the default or configured cache-limit is reached, unless the optional **reserve-list** is configured, no further dynamic entries are added and no further Map-Requests are generated in response to cache-miss lookups until a free position is available.
  - When the optional **reserve-list** is not configured, dynamic entries are added on a first-in-first-added basis until the configured map-cache limit is reached. After that time, no new dynamic entries can be added. If the **reserve-list** is configured but the prefix-list to which it refers is not configured, the results are the same as if the **reserve-list** was not configured.
  - When the optional **reserve-list** is configured, a Map-Request will be generated and a new dynamic map-cache entry may be added only for IP v4 EID-prefixes that are permitted by the prefix-list referenced by the **reserve-list**. In this case, the new entry must be able to replace an existing dynamic entry such that the cache-limit is maintained. The dynamic entry deleted will be either a non-reserve idle map-cache entry or non-reserve active map-cache entry. Idle map-cache entries are those that have seen no activity in the last 10 minutes. If all current dynamic entries are also permitted by the prefix-list referenced by the **reserve-list**, no further dynamic entries can be added.
  - Existing dynamic IPv4 map-cache entries can time-out due to inactivity or can be removed by the administrator via the **clear ip lisp map-cache** command to create a free position in the map-cache.
- Static map-cache entries are always added, until the default or configured cache-limit is reached. After the default or configured cache-limit is reached, unless the optional **reserve-list** is configured, no further static entries are added.
  - When the optional **reserve-list** is not configured, static entries are added on a first-in-first-added basis until the configured map-cache limit is reached. After that time, no new static entries can be added. If the **reserve-list** is configured but the prefix-list to which it refers is not configured, the results are the same as if the **reserve-list** was not configured.
  - When the optional **reserve-list** is configured, a static entry matching the **reserve-list** prefix-list may be added, but only if it can replace an existing static entry or dynamic entry that does not-match the **reserve-list** prefix-list.

⚠ **Caution** When the optional **reserve-list** is used, once the configured cache-limit is reached, if all existing entries also match the prefix-list and are not candidates for deletion, no new dynamic or static entries will be added, even if a new dynamic or static entry also matches the **reserve-list** prefix-list.

📝 **Note** When the **reserve-list** command is used, be sure that the prefix-list includes entries that match all expected prefixes in any Map-Reply, including the more-specifics. This can be ensured by appending **le 32** to the end of all prefix-list entries for IPv4 prefixes. For example, if you want to match 153.16.0.0/16 and any of the more specifics, you should specify **ip prefix-list lisp-list seq 5 permit 153.16.0.0/16 le 32** in order to cover all replies within this range.

The addition and deletion of dynamic and static IPv4 map-cache entries can be observed by enabling the **debug ip lisp mapping control** command. As with all debugging commands, exercise caution when using this command on a production system.

Examples

The following example configures a lisp cache-limit of 2000 entries and a reserve-list referencing the IPv4 prefix-list LISP-v4-always.

```
Router(config)# ip lisp map-cache-limit 2000 reserve-list LISP-v4-always
Router(config)# ip prefix-list LISP-v4-always seq 20 permit 172.16.0.0/16 le 32
```

Related Commands

Command	Description
ip lisp map-cache	Configures a static IPv4 EID-prefix to locator map-cache entry.
clear ip lisp map-cache	Clear the LISP IPv4 map-cache on the local router.
debug ip lisp mapping control	Display logs for Map-Request, Map-Reply, and other LISP IPv4 mapping activities

---

ip lisp map-request-source

To configure an IPv4 or IPv6 address to be used as the source address for LISP IPv4 Map-Request messages, use the **ip lisp map-request-source** command in global configuration mode. To remove the configured Map-Request source address and return to the default behavior, use the **no** form of this command.

> **[no] ip lisp map-request-source** *source-address*

Syntax Description

source-address	The IPv4 or IPv6 source address to be used in LISP IPv4 Map-Request messages.

Defaults

The router uses one of the locator addresses configured in the **ip lisp database-mapping** command as the default source address for LISP Map-Request messages.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Typically, a locator address configured in the **ip lisp database-mapping** command is used as the source address for LISP IPv4 Map-Request messages. There are cases, however, where it may be necessary or useful to configure the specified source address for these Map-Request messages. For example, when the ITR is behind a NAT device it may be necessary to specify a source address that matches the NAT configuration to properly allow for return traffic.

When the **ip lisp map-request-source** command is configured on an ITR, the specified IPv4 or IPv6 locator is used by an ITR as the source address for Map-Request messages. When this command configured on a Map-Server, this locator is used as the source address in the Encapsulated Control Message carrying a Map-Request to an ETR.

Examples

The following example configures an ITR to use the source IP address 172.16.1.7 in its IPv4 Map-Request messages.

```
Router(config)# ip lisp map-request-source 172.16.1.7
```

Related Commands

Command	Description
ip lisp database-mapping	Configures an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy.

---

ip lisp map-resolver

To configure a router to act as an IPv4 LISP Map-Resolver (MR), use the **ip lisp map-resolver** command in global configuration mode. To remove LISP Map-Resolver functionality, use the **no** form of this command.

[no] ip lisp map-resolver

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not provide Map-Resolver functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable the router to perform IPv4 LISP Map-Resolver (MR) functionality. A LISP Map-Resolver is deployed as a LISP Infrastructure component.

A Map-Resolver receives a LISP Encapsulated Control Messages (ECM) containing a Map-Request from a LISP ITR directly over the underlying locator-based network. The Map-Resolver decapsulates this message and handles it according to other configurations and conditions as follows.

- When a Map-Resolver is concurrently configured as a standalone Map-Resolver/Map-Server, registered EID prefixes are maintained directly in its own database. In this case, the Map-Resolver component knows if the EID being queried for is available, as the authoritative ETR would be registering the EID prefix. If an ETR is registering the EID prefix, the Map-Server forwards the Map-Request as a LISP Encapsulated Control Messages (ECM) to the authoritative ETR. If the EID prefix being queried is not available, the Map-Resolvers sends a Negative Map-Reply directly back to an ITR in response to queries for non-LISP addresses.

- When a Map-Resolver is configured to use LISP-DDT, it is also configured with ddt root and delegation commands. In this case, the Map-Resolver checks its referral-cache and if nothing is found sends a Negative Map-Reply directly back to an ITR in response to queries for non-LISP addresses. If an entry is found, the Map-Resolver creates a DDT Map-Request and forwards it to to one of the RLOCs in the chosen referral cache entry. (See the LISP-DDT commands for additional details.)

- When a Map-Resolver is configured to use the LISP ALT for EID-to-RLOC mapping resolution, the Map-Resolver configuration must include the **ip lisp alt-vrf** command. In this case, the Map-Resolver knows if the EID being queried for is available, as the EID prefix will exist in the ALT. If the EID prefix is available, the Map-Resolver forwards the Map-Request directly over the ALT, where it is then delivered either to the Map-Server that is injecting EID-prefixes into the LISP-ALT on behalf of the authoritative ETR, and then from that Map-Server as an LISP ECM to the authoritative ETR. If the EID prefix being queried is not available, the Map-Resolvers sends a Negative Map-Reply directly back to an ITR in response to queries for non-LISP addresses.

✎

Note When a Map-Resolver supports a LISP deployment that is configured for virtualization, the Map-Resolver must be concurrently configured as a Map-Server, or to use LISP-DDT. A Map-Resolver cannot forward a Map-Request with an instance-id over the LISP ALT.

Examples

The following example configures IPv4 LISP Map-Resolver functionality on the router.

```
Router(config)# ip lisp map-resolver
```

Related Commands

Command	Description
ip lisp alt-vrf	Configures which VRF supporting the IPv4 address-family LISP should use when sending Map Requests for an IPv4 EID-to-RLOC mapping directly over the ALT.

ip lisp map-server

To configure a router to act as an IPv4 LISP Map-Server (MS), use the **ip lisp map-server** command in global configuration mode. To remove LISP Map-Server functionality, use the **no** form of this command.

> **[no] ip lisp map-server**

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not provide Map-Server functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable the router to perform IPv4 LISP Map-Server (MS) functionality. A LISP Map-Server is deployed as a LISP Infrastructure component.

LISP-32

LISP site commands are configured on the Map Server for a LISP ETR that registers to it, including an authentication key, which must match the one also configured on the ETR. A Map Server receives Map-Register control packets from ETRs.

A Map-Server may be configured concurrently configured as a standalone Map-Resolver/Map-Server, or as part of an infrastructure device in a LISP-DDT or LISP-ALT hierarchy. In general, Map-Server functions pertaining to these configurations are as follows.

- When a Map-Server is concurrently configured as a standalone Map-Resolver/Map-Server, registered EID prefixes are maintained directly in its own database. In this case, the Map-Resolver component knows if the EID being queried for is available, as the authoritative ETR would be registering the EID prefix. If an ETR is registering the EID prefix, the Map-Server forwards the Map-Request as a LISP Encapsulated Control Messages (ECM) to the authoritative ETR. If the EID prefix being queried is not available, the Map-Resolvers sends a Negative Map-Reply directly back to an ITR in response to queries for non-LISP addresses.

- When a Map-Server is configured as a LISP-DDT device, it is also configured with ddt root and delegation commands. In this case, when a Map-Server receives a DDT Map-Request, if the requested EID matches a registered EID-prefix, then the Map-Request is forwarded to one of the destination ETR RLOCs (as a LISP ECM). If the request EID is not found, the Map-Server sends a Negative Map Referral back to the requesting Map-Resolver (who then sends a Negative Map-Reply directly back to an ITR in response to queries for non-LISP addresses). (See the LISP-DDT commands for additional details.)

- When a Map-Server is configured to use the LISP ALT for EID-to-RLOC mapping resolution, the Map-Server configuration must include the **ip lisp alt-vrf** command. In this case, the Map-Server receives the Map-Request from the ALT for an EID it has advertised. The Map-Server should only advertise an EID if the site is registered and the EID is avialble. In this case, the Map-Server forwards the Map-Request as an LISP ECM to the authoritative ETR.

Note When a Map-Server supports a LISP deployment that is configured for virtualization, the Map-Server must be concurrently configured as a Map-Resovler, or to use LISP-DDT. A Map-Server cannot recieve a Map-Request with an instance-id over the LISP ALT.

Examples

The following example configures IPv4 LISP Map-Server functionality on the router.

```
Router(config)# ip lisp map-server
```

Related Commands

Command	Description
ip lisp alt-vrf	Configure which VRF supporting the IPv4 address-family LISP should use when sending Map Requests for an IPv4 EID-to-RLOC mapping directly over the ALT.

ip lisp ntr

To configure a device to act as an IPv4 LISP Network Address Translation (NAT) Tunnel Router (NTR), use the **ip lisp ntr** command in global configuration mode. To remove LISP NTR functionality, use the **no** form of this command.

[no] ip lisp ntr *local-locator-address*

Syntax Description

local-locator-address	The IPv4 local address to be used by the NTR in its proxy-reply to a LISP-MN.

Defaults

By default, LISP NTR functionality is not enabled.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was introduced.

Usage Guidelines

LISP Network Address Translation (NAT) Tunnel Router (NTR) functionality enables a LISP device, typically a Map-Server/Map-Resolver, to be a re-encapsulating router and is intended to support LISP Mobile Node (LISP-MN) deployments where NAT is a potential issue for LISP-MNs.

When a LISP Mobile Node (LISP-MN) roams, the locator that it receives can potentially be a publicly accessible address, a private address behind a Network Address Translation (NAT) device that is then translated to a public address, or even a LISP EID if it lands behind a LISP network. For any possible locator-set, the LISP-MN registers with its configured Map-Server (MS) and provides this locator-set and EIDs to the MS. When the LISP-MN receives a public locator, the Map-Register message source address and reported locator-set match. However, when a LISP-MN locator is behind a NAT device somewhere between itself and the MS, NAT is applied to the locator. In this case, the Map-Register message source address and reported locator-set will not match. Without LISP NTR functionality enabled, the MS does a simple proxy-reply for the LISP MN and includes the LISP MN locator-set to Map-Requests. When the **ip lisp ntr** command is configured, the MS instead sends a proxy Map-Reply with its own locators to a Map-Request it receives for a registered LISP-MN. The LISP-MN encapsulates packet to the NTR; the NTR decapsulates packets destined to the LISP-MN EID.

NTR functionality is enabled on the MS/MR to which the LISP-MN registers by configuring the **ip lisp ntr** command. This solves the NAT problem for LISP-MN devices by enabling the following behavior:

- The NTR-enabled MS/MR (refered to below as simply an NTR) observes that the locator by which the LISP-MN registered differs from the locator included within the Map-Register message.

- If a LISP-MN roams and changes its locator, the Map-Register message will indicate this new locator to the MS. Again, differences between the source address of the message and the locator reported within the message will be noted.

- The NTR-enabled MS/MR proxy-replies to Map-Requests for the LISP-MN mapping from other LISP-MN devices with its own locator address, not the locator of the requested LISP-MN. Other LISP devices, including another LISP-MN that may also be located behind NAT, encapsulate then to the NTR locator instead of directly referencing the LISP-MN locator. Since the NTR knows the NAT'ed locator of the LISP-MN, it decapsulates these LISP packets and re-encapsulates them to this LISP-MN locator.

In this way, a LISP-MN can roam from one public hotspot to another, and still be found by other LISP devices. Using the NTR *local-locator-address* in a proxy-reply keeps NAT state to a minimum (2 entries per LISP-MN regardless of the number of its EID traffic flows).

Use command **ip lisp ntr** to enable an MS/MR to perform LISP Network Address Translation (NAT) Tunnel Router (NTR) functionality. The LISP NTR functionality, when added to the MS/MR functionality, that provides LISP re-encapsulating in support of LISP Mobile Node (LISP-MN) devices that need to send and receive packets through a stateful NAT firewall.

> **Note** Only a device configured as a combined Map-Server (MS) and Map-Resolver (MR) can be configured to provide LISP NTR support. The MS and MR cannot be configured separately. In addition, for LISP NTR to work, it must be configured on the MS/MR device to which the LISP-MN registers.

> **Note** LISP Mobile Node (LISP-MN) functionality is described in **draft-meyer-lisp-mn**, the most current version of which is available here: https://datatracker.ietf.org/wg/lisp/.

When LISP NTR functionality is enabled on an MS/MR, the following concepts and caveats must be considered.

- When LISP NTR functionality is enabled on an MS/MR, the MS/MR becomes a re-encapsualting tunnel router for LISP-MN-to-LISP-MN packets. Because the NTR-enabled MS/MR proxy-replies to Map-Requests for registered LISP-MNs when NTR is enabled, LISP-MN-to-LISP-MN traffic always traverses the NTR. When other LISP-MN sites encapsulate traffic to the NTR, the NTR must decapsulate these packets, and then re-encapsulate them to the locator of the destination LISP-MN. Traffic between a LISP-MN and normal LISP sites or to non-LISP sites is not affected by NTR functionality. Encapsulation and decapsulation functions are normally those provided by LISP ITR, ETR, PITR, and PETR devices. However, when **ip lisp ntr** is configured, none of these other capabilities need be enabled in order to provide encapsulation/decapsulation functions. Note also that the capabilities of the device indicated by the output of the **show ip lisp** command only indicate that the NAT Tunnel Router (NTR) feature is enabled, as shown here:

```
MS-MR# show ip lisp
LISP IP Configuration Information for VRF "default" (iid 0)
  Ingress Tunnel Router (ITR):    disabled
  Egress Tunnel Router (ETR):     disabled
  Proxy-ITR Router (PTR):         disabled
  Proxy-ETR Router (PETR):        disabled
  Map Resolver (MR):              enabled
  Map Server (MS):                enabled
  NAT Tunnel Router (NTR):        enabled
---<skip>---ip lisp ntr 10.1.1.1
```

- Because the LISP-NTR provides re-encapsulation functionality, the MS/MR now contains a map-cache for maintaining EID-to-RLOC mappings. The **show ip lisp map-cache** command indicates the contents of the map-cache on the MS/MR enabled as an NTR.

When LISP NTR functionality is enabled on an MS/MR, the following concepts and caveats must be considered.

Examples

The following example configures IPv4 LISP Map-Resolver functionality on the router.

```
Router(config)# ip lisp ntr 10.1.1.1
```

Related Commands

Command	Description
ip lisp map-resolver	Configure a device to function as an IPv4 LISP Map-Resolver.
ip lisp map-server	Configure a device to function as an IPv4 LISP Map-Server.
show ip lisp	Displays the current IPv4 LISP configuration status.
show ip lisp map-cache	Displays the current dynamic and static IPv4 EID-to-RLOC map-cache entries.

ip lisp proxy-etr

To configure a router to act as an IPv4 LISP Proxy Egress Tunnel Router (PETR), use the **ip lisp proxy-etr** command in global configuration mode. To remove LISP PETR functionality, use the **no** form of this command.

> **[no] ip lisp proxy-etr**

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not provide PETR functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable IPv4 LISP Proxy Egress Tunnel Router (PETR) functionality on the router. PETR functionality is a special case of ETR functionality where the router accepts LISP-encapsulated packets from an ITR or PITR that are destined to non-LISP sites, de-encapsulates them, and then forwards them natively toward their non-LISP destination.

PETR services may be necessary in several cases.

1) By default when a LISP sites forwards packets to a non-LISP site natively (not LISP encapsulated), the source IP address of the packet is that of a site EID(s). When the provider side of the access network is configured with strict unicast reverse path forwarding (uRPF) it may consider these packets to be spoofed and drop them since EIDs are not advertised in the provider core network. In this case, instead of natively forwarding packets destined to non-LISP sites, the ITR encapsulates these packets using its site locator(s) as the source address and the PETR as the destination address. The assumption and necessity here is that the native connectivity of the PETR is not configured with the same uRPF or anti-spoofing restrictions as the ITR. (Note that packets destined for LISP sites will follow normal LISP forwarding processes and be sent directly to the destination ETR as normal.)

2) When a LISP IPv6 (EID) site wishes to talk to a non-LISP IPv6 site and some portion of the intermediate network does not support IPv6 (it is IPv4 only), the PETR can be used to "hop over" the address family incompatibility, assuming that the PETR has both IPv4 and IPv6 connectivity. The ITR in this case can LISP-encapsulate the IPv6 EIDs with IPv4 locators destined for the PETR, which de-encapsulates the packets and forwards them natively to the non-LISP IPv6 site over its IPv6 connection. In this case, the use of the PETR effectively allows the LISP sites packets to traverse (hop over) the IPv4 portion of network using the LISP mixed protocol encapsulation support. This use-case also assumes the availability of a dual-stack PITR for return traffic flows.

Note An NX-OS router can be configured to perform ETR and PETR functions at the same time. A router that is configured as an ETR performs a check to verify that the LISP packet inner header destination address is within the address range of a local EID prefix, whereas a router configured as a PETR does not perform this check.

Note When an ITR or PITR requires the use of IPv4 PETR services, it must be configured to forward IPv4 EID packets to the PETR by using the **ip lisp use-petr** command.

Examples

The following example configures IPv4 LISP PETR functionality on the router.

```
Router(config)# ip lisp proxy-etr
```

Related Commands

Command	Description
ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR)
ip lisp use-petr	Configures an ITR or PITR to use the PETR for traffic destined to non-LISP IPv4 destinations.

ip lisp proxy-itr

To configure a router to act as an IPv4 LISP Proxy Ingress Tunnel Router (PITR), use the **ip lisp proxy-itr** command in global configuration mode. To remove LISP PITR functionality, use the **no** form of this command.

> **[no] ip lisp proxy-itr** *ipv4-local-locator* [*ipv6-local-locator*]

Syntax Description

ipv4-local-locator	The IPv4 locator address used as a source address for encapsulation of data packets, a Data Probe, or a Map-Request message.
ipv6-local-locator	(Optional) The IPv6 locator address used to as a source address for encapsulation of data packets, a Data Probe, or a Map-Request message when the locator-hash function returns a destination RLOC in the IPv6 address-family.

Defaults

By default, the router does not provide PITR functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable IPv4 LISP Proxy Ingress Tunnel Router (PITR) functionality on the router. PITR functionality is za special case of ITR functionality where the router receives native packets from non-LISP sites that are destined for LISP sites, encapsulates them, and forwards them to the ETR that is authoritative for the destination LISP site EID.

PITR services are required to provide interworking between non-LISP sites and LISP sites. For example, when connected to the Internet, a PITR acts as a gateway between the legacy Internet and the LISP enabled network. To accomplish this, the PITR must advertise one or more highly aggregated EID prefixes on behalf of LISP sites into the underlying DFZ (i.e. Internet) and act as an ITR for traffic received from the public Internet.

Any packet received by the PITR then that does not match a route from the routing table (associated with the VRF of the packet's incoming interface) or that matches the default route (0.0.0.0/0) or more-specific prefix with a null0 next-hop from the routing table (associated with the VRF for the packet's incoming interface), may be LISP encapsulated – provided the destination is a LISP destintion. Thus, in addition to configuring the **ip lisp itr map-resolve**r command, a PITR must also be configured to know the EID-prefix space it is acting on behalf of. This can be accomplished in one of two ways (only one can be configured at any time).

1) When the PITR is ALT-connected, it has direct knowledge of all EID-prefix space. (See the **ip lisp alt-vrf** command for details.) In this case, the PITR sends Map-Request directly on the ALT to obtain an IPv4 EID-to-RLOC mapping.

2) When the PITR is configured to use a Map-Resolver via the **ip lisp itr map-resolve**r command, it must also be configured with one or more static map-cache entries indicating the EID-prefix space and with an action of **map-request**. (See the **ip lisp map-cache** command for details.) In this case, the PITR sends a LISP Encapsulated Control Message (ECM) to the configured Map-Resolver to obtain an IPv4 EID-to-RLOC mapping.

The PITR caches the resultant IPv4 EID-to-RLOC mapping information returned by the associated Map-Reply in its map-cache. Subsequent packets destined to the same IPv4 EID-prefix block are then LISP-encapsulated according to this IPv4 EID-to-RLOC mapping entry. A Negative Map-Reply indicates that the destination is not a LISP site and the PITR forwards these packets natively.

Note A PITR may also be concurrently configured on the same device as a stand-alone MR/MS device, simplifying the overall LISP architecture.

Note An NX-OS router can be configured to perform ITR and PITR functions at the same time. (An IOS router cannot be configured to perform both ITR and PITR functions at the same time). A router that is configured as an ITR performs a check to verify that the source of any packet intended for LISP encapsulation is within the address range of a local EID prefix, whereas a router configured as a PITR does not perform this check. If a router is configured as an ITR and as a PITR, preference goes to PITR functionality for packet processing.

When PITR services are enabled using the **ip lisp proxy-itr** command, the PITR LISP-encapsulated packets when it sends a data packet to a LISP site. The outer (LISP encapsulation) header address-family and source address are determined as follows:

- When the locator-hash function returns a destination RLOC within the IPv4 address-family, the address *ipv4-local-locator* is used as the source address from the locator namespace, and
- When the locator-hash function returns a destination RLOC within the IPv6 address-family (assuming the optional address *ipv6-local-locator* is entered), it will be used as a source locator for encapsulation.

Examples

The following example configures LISP PITR functionality on the router, and to encapsulate packets using an IPv4 source locator of 10.1.1.1 and an IPv6 source locator of 2001:db8:bb::1.

```
Router(config)# ip lisp proxy-itr 10.1.1.1 2001:db8:bb::1
```

Related Commands

Command	Description
ip lisp alt-vrf	Configures which VRF supporting the IPv4 address-family LISP should use when sending Map Requests for an IPv4 EID-to-RLOC mapping directly over the ALT.
ip lisp itr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR)
ip lisp map-cache	Configures a static IPv4 EID-prefix to locator map-cache entry.

ip lisp shortest-eid-prefix-length

To configure the shortest IPv4 EID-prefix mask-length that is acceptable to an ITR or PITR in a received Map-Reply message or to an ETR in the mapping-data record of a received Map-Request, use the **ip lisp shortest-eid-prefix-length** command in global configuration mode. To return to the default configuration, use the **no** form of this command.

> **[no] ip lisp shortest-eid-prefix-length** *IPv4-EID-prefix-length*

Syntax Description

IPv4-EID-prefix-length	The shortest IPv4 EID prefix-length accepted from a Map-Reply or data record in a Map-Request. (0 to 32)

Defaults

By default, the shortest IPv4 EID prefix length accepted is a /16.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When an ITR or PITR receives a Map-Reply message, the mapping data it contains includes the EID mask-length for the returned EID prefix. By default, the shortest EID prefix mask-length accepted by an ITR or PITR for an IPv4 EID prefix is a /16. The global command **ip lisp shortest-eid-prefix-length** can be used to change this default when it is advantageous to do so. For example, it may be necessary for a PITR to accept a shorter (coarser) prefix if one exists.

Similarly, when an ETR receives a Map-Request message, it may contain a mapping data record that the ETR can cache and possible use to forward traffic, depending on the configuration of the **ip lisp etr accept-map-request-mapping** command. The global command **ip lisp shortest-eid-prefix-length** can also be used to change the shortest prefix length accepted by the ETR. In this case, the check for the shortest EID-prefix mask-length is done prior to the verifying Map-Request, if also configured. That is, if the EID-prefix mask-length is less than the configured value, the verifying Map-Request will not be sent and the mapping data will not be accepted.

Examples

The following example configures the router to accept a minimum IPv4 EID-prefix length of /12.

```
Router(config)# ip lisp shortest-eid-prefix-length 12
```

Related Commands

Command	Description
ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR).
ip lisp itr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR).
ip lisp proxy-itr	Configures the router to act as an IPv4 LISP Proxy Ingress Tunnel Router (PITR)

ip lisp translate

To configure IPv4 LISP translation mapping, use the **ip lisp translate** command in global configuration mode. To remove IPv4 LISP translation mappings and return to the default value, use the **no** form of this command.

[no] ip lisp translate inside *IPv4-inside-EID* **outside** *IPv4-outside-EID*

Syntax Description

inside	Indicates that the inside (non-routable) IPv4 EID prefix follows.
IPv4-inside-EID	The non-routable IPv4 address associated with an inside EID prefix.
outside	Indicates that the outside (routable) IPv4 EID prefix follows.
IPv4-outside-EID	The routable IPv4 address associated with an outside EID prefix.

Defaults

By default, a LISP device does not perform address translation.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When a LISP ITR or ETR is configured with a non-routable EID prefix and it is desired to replace it with a routable EID prefix, this can be accomplished by configuring the **ip lisp translate** command. When this command is configured, a LISP device acting as an ITR and detecting a non-routable EID in the source IPv4 address field, as referred to by the **inside** keyword, will replace it with the routable EID referred to by the **outside** keyword. In the opposite direction when acting as an ETR, it will replace the routable EID referred to by the **outside** keyword with the non-routable EID referred to by the **inside** keyword.

Note The outside EID address may be assigned to the router itself, in which case it responds to ARP requests, ICMP echo-requests (ping) and any other packet sent to this address. When the outside EID is not assigned to the device, the address does not answer ARP requests.

This feature may be useful when a site upgrades to LISP but wishes to continue to communicate with non-LISP sites. An alternative approach for providing communications between LISP and non-LISP sites is to use Proxy-ITR services. Refer to the **ip lisp proxy-itr** command for further details. Both proxy-ITR and NAT translation services, commonly referred to as Interworking services, are described in *draft-ietf-lisp-interworking-00*.

Examples

The following example configures LISP to translate the inside address 192.168.10.1 to the outside address 10.1.10.1.

```
Router(config)# ip lisp translate inside 192.168.10.1 outside 10.1.10.1
```

Related Commands

Command	Description
ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR).

ip lisp itr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR).
ip lisp proxy-itr	Configures the router to act as an IPv4 LISP Proxy Ingress Tunnel Router (PITR)

ip lisp use-bgp-locators

To configure LISP to use iBGP routes as EID-prefixes and their BGP RIB next-hop addresses as locators to dynamically create map-cache entries, use the **ip lisp use-bgp-locators** command in global configuration mode. To remove this functionality, use the **no** form of this command.

[no] ip lisp use-bgp-locators [**route-map** *route-map-name*]

Syntax Description

route-map *route-map-name*	(Optional) Specifies the route-map supplying the match criteria for identifying which iBGP routes are EID-prefixes and that should use BGP RIB next-hop addresses.

Defaults

By default, the router does not enable this functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was introduced.

Usage Guidelines

In most cases, running BGP is not needed or even desirable when deploying LISP sites. The LISP mapping system provides all necessary information for performing EID forwarding, and the added complexity of BGP is typically not useful. There are cases, however, where adding BGP be advantageous and can simplify LISP deployments and operations. One example is the case where BGP running on an edge router in a private core has knowledge of EID prefixes at other sites. Since the BGP next-hops for theses EID prefixes represent their RLOCs, LISP simply needs to use these BGP-known EID prefixes and next-hops in order to encapsulate packets between sites. This functionality is called LISP On Demand Forwarding (LISP-ODF).

To configure LISP-ODF, which enables the device to dynamically create map-cache entries use iBGP routes as EID-prefixes and their BGP RIB next-hop addresses as locators, use the **ip lisp use-bgp-locators** command. When implementing this functionality, the following design details should be considered:

- When an architeture implements LISP-ODF, it no longer is required to register EID prefixes with an mapping system (Map-Server), as would typically be the case since all EID prefixes and their locators are available directly in BGP. LISP map-cache entries are dynamically built using BGP information by configuring the **ip lisp use-bgp-locators** command.
- Because a LISP device is not configured with database-mapping entries for its own EID prefixes or configured to register these EID prefixes with a Map-Server, it is not necessary to configure it as an ETR or ITR. The LISP device must simply be configured as a Proxy ITR (PITR) to encapsulate LISP packets and as a Proxy ETR (PETR) to decapsulate LISP packets.
- Map-cache entries dynamically created via LISP-ODF automatically have a priority of 1 and weight of 100 in all cases.

Note A LISP-ODF router (i.e. one using **ip lisp use-bgp-locators**) does not register any EID-prefixes to a Map-Server unless it is also doing ITR/ETR services for configured database-mappings.

Use the **route-map** *route-map-name* command to specifiy a route-map with match criteria for identifying which iBGP routes are EID-prefixes and that should be included, along with their BGP next-hop addresses, as dynamically created map-cache entries. LISP will then only encapsulate packets to these prefixes. Other remaining iBGP prefixes are assumed to be non-LISP and packets to these will be forwarded natively.

Note Because BGP next-hop addresses are used as locators, BGP may need to be configured with **next-hop-self** to ensure that the proper addresses are available to be used as locators.

Examples

The following example configures IPv4 LISP Map-Resolver functionality on the router.

```
Router(config)# feature bgp
Router(config)# feature lisp
Router(config)# router bgp 65001
Router(config-router)# router-id 10.10.10.10
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)# exit
Router(config-router)# neighbor 172.31.1.1 remote-as 65002
Router(config-router-neighbor)# address-family ipv4 unicast
Router(config-router-neighbor-af)# exit
Router(config-router-neighbor)# exit
Router(config-router)# exit
Router(config)# feature lisp
Router(config)# ip lisp proxy-itr 172.16.1.1
Router(config)# ip lisp proxy-etr
Router(config)# ip lisp use-bgp-locators
```

Related Commands

Command	Description
ip lisp proxy-itr	Configures the router to act as an IPv4 LISP Proxy Ingress Tunnel Router (PITR)
ip lisp proxy-etr	Configures the router to act as an IPv4 LISP Proxy Egress Tunnel Router (PETR)
ipv6 lisp proxy-itr	Configures the router to act as an IPv4 LISP Proxy Ingress Tunnel Router (PITR)
ipv6 lisp proxy-etr	Configures the router to act as an IPv6 LISP Proxy Ingress Tunnel Router (PETR)

---

ip lisp use-petr

To configure a router to use an IPv4 LISP Proxy Egress Tunnel Router (PETR), use the **ip lisp use-petr** command in global configuration mode. To remove the use of a LISP PETR, use the **no** form of this command.

[no] ip lisp use-petr *locator-address*

Syntax Description

locator-address	IPv4 or IPv6 locator address of the PETR.

Defaults

By default, the router does not use PETR services.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable the router to use IPv4 Proxy Egress Tunnel Router (PETR) services. When the use of PETR services is enabled, instead of natively forwarding packets destined to non-LISP sites, these packets are LISP-encapsulated and forwarded to the PETR, where these packets are then de-encapsulated, and then forwarded natively toward the non-LISP destination. An ITR or PITR can be configured to use PETR services.

PETR services may be necessary in several cases.

1) By default when a LISP sites forwards packets to a non-LISP site natively (not LISP encapsulated), the source IP address of the packet is that of a site EID(s). When the provider side of the access network is configured with strict unicast reverse path forwarding (uRPF) it may consider these packets to be spoofed and drop them since EIDs are not advertised in the provider core network. In this case, instead of natively forwarding packets destined to non-LISP sites, the ITR encapsulates these packets using its site locator(s) as the source address and the PETR as the destination address. The assumption and necessity here is that the native connectivity of the PETR is not configured with the same uRPF or anti-spoofing restrictions as the ITR. (Note that packets destined for LISP sites will follow normal LISP forwarding processes and be sent directly to the destination ETR as normal.)

2) When a LISP IPv6 (EID) site wishes to talk to a non-LISP IPv6 site and some portion of the intermediate network does not support IPv6 (it is IPv4 only), the PETR can be used to "hop over" the address family incompatibility, assuming that the PETR has both IPv4 and IPv6 connectivity. The ITR in this case can LISP-encapsulate the IPv6 EIDs with IPv4 locators destined for the PETR, which de-encapsulates the packets and forwards them natively to the non-LISP IPv6 site over its IPv6 connection. In this case, the use of the PETR effectively allows the LISP sites packets to traverse (hop over) the IPv4 portion of network using the LISP mixed protocol encapsulation support. This use-case also assumes the availability of a dual-stack PITR for return traffic flows.

Note Because LISP supports mixed protocol encapsulations, the locator specified for the PETR in this case can either be an IPv4 or IPv6 address. Up to eight PETRs can be configured per address-family.

Examples

The following example configures an ITR to use the PETR with the IPv4 locator of 10.1.1.1. In this case, LISP site IPv4 EIDs destined to non-LISP IPv4 sites will be encapsulated in an IPv4 LISP header destined to the PETR located at 10.1.1.1.

```
Router(config)# ip lisp use-petr 10.1.1.1
```

Related Commands

Command	Description
ip lisp proxy-etr	Configures the router to act as an IPv4 LISP Proxy Egress Tunnel Router (PETR)

ipv6 lisp alt-vrf

To configure an alternate virtual routing and forwarding (VRF) instance supporting the IPv4 address-family for LISP to use for resolving IPv6 EID-to-RLOC mappings, use the **ipv6 lisp alt-vrf** command in global configuration mode. To remove this reference to a VRF, use the **no** form of this command.

> **[no] ipv6 lisp alt-vrf** *vrf-name*

Syntax Description

vrf-name	Name assigned to the LISP ALT VRF.

Defaults

By default, a LISP-ALT VRF is not referenced by LISP.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use the command **ipv6 lisp alt-vrf** to configure which virtual routing and forwarding (VRF) instance supporting the IPv6 address-family that the LISP device should use for control plane mapping resolution functions.

The **ipv6 lisp alt-vrf** command is required for all LISP devices that are connected to the LISP Alternative Logical Topology (ALT) for exchange of LISP control plane messages for mapping resolution. Primarily this includes LISP Map-Server (MS), Map-Resolver (MR), and Proxy Ingress Tunnel Router (PITR) devices. This can also include directly ALT-connected xTRs.

> **Note** When the **ipv6 lisp alt-vrf** command is used, the referenced VRF must already have been created using the **vrf context** command. In addition, any other corresponding configurations necessary for connecting the LISP device to the ALT, including the GRE tunnel interface(s) and any routing associated with the VRF (static and/or dynamic) must also have been created.

The LISP ALT does not support virtualization. Thus, the following must be considered when deploying LISP with ALT functionality.

- A Map-Request containing an instance-id cannot be forwarded over the LISP ALT. When a LISP device is configured for virtualization, the **ipv6 lisp alt-vrf** command must not be configured.
- When instance-ID's are configured on a MS (see LISP Site **eid-prefix** command), the MS **must be** configured stand-alone or to use LISP-DDT since virtualization of the LISP ALT is not support.
- When a router is configured as a stand-alone MS/MR without virtualization (i.e. when it is not connected to any ALT and it has full knowledge of the LISP Mapping System for a private LISP deployment for example), the use of the **ipv6 lisp alt-vrf** command is not required.
- A PITR can be configured to send a Map-Request to a configured Map-Resolver for EID-to-RLOC mapping resolution. When configured to use a Map-Resolver instead of the ALT for EID-to-RLOC mapping resolution, the **ipv6 lisp alt-vrf** command is not required. A LISP PITR may be configured with the **ipv6 lisp alt-vrf** command if it is directly using the ALT for EID-to-RLOC mapping resolution as an alternative.

LISP-44

- When using a PITR in a virtualized LISP deployment, the PITR must be configured to use a Map-Resolver for EID-to-RLOC mapping resolution and not the LISP ALT since the LISP ALT does not support virtualization. In this case, the **ipv6 lisp alt-vrf** command is not used.

Examples

The following example configures the VRF named 'lisp' and then configures LISP to use this VRF when resolving IPv6 EID-to-RLOC mappings.

```
Router(config)# vrf context lisp
Router(config-vrf)# exit
Router(config)# ipv6 lisp alt-vrf lisp
```

Related Commands

Command	Description
ipv6 lisp itr	Configure the router to act as a LISP Ingress Tunnel Router (ITR)
ipv6 lisp pitr	Configures the router to act as a LISP Proxy Ingress Tunnel Router (PITR)

---

ipv6 lisp database-mapping

To configure an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy use the **ipv6 lisp database-mapping** command in global configuration mode. To remove the configured database mapping, use the **no** form of this command.

> **[no] ipv6 lisp database-mapping** *EID-prefix* {*locator* | **dynamic** *interface-name*} **priority** *priority* **weight** *weight*

Syntax Description

EID-prefix	The IPv6 EID prefix and length to be advertised by this router.
locator	The IPv4 or IPv6 Routing Locator (RLOC) associated with this EID-prefix
dynamic *interface-name*	Allow the Routing Locator (RLOC) associated with this EID to be learned dynamically in coordination with the LISP interface command **ip nat-traversal** by sending a LISP Echo-Request message to the configured Map-Server via the interface specified by *interface-name*.
dynamic *interface-name*	Allow the Routing Locator (RLOC) associated with this EID to be determined dynamically by using the address for the interface specified by *interface-name*.
priority *priority*	The priority (value between 0 and 255) assigned to the RLOC. When multiple locators have the same priority they may be used in load-shared fashion. A lower value indicates a higher priority.
weight *weight*	The weight (value between 0 and 100) assigned to the locator. Used in order to determine how to load-share traffic between multiple locators when the priorities assigned to multiple locators are the same. The value represents the percentage of traffic to be load-shared.

Defaults

No LISP database entries are defined by default.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command configures the LISP database parameters for the specified IPv6 EID-prefix block, including its associated locator, priority and weight. The IPv6 EID-prefix/prefix-length is a LISP IPv6 EID-prefix block for which this ETR registers as being authoritative for with a Map-Server. The locator is the IPv4 or IPv6 address of a loopback interface or physical WAN interface used as the Routing Locator (RLOC) address for the EID-prefix assigned to the site.

Associated with the locator address are a priority and weight used to define traffic policies when multiple RLOCs apply to the same EID-prefix block. When a router is configured as an ETR, these LISP database-mapping parameters are advertised within a Map-Reply message to indicate the ingress traffic preferences of the site for the associated EID-prefix block. An ITR then selects a locator (outer header) address for encapsulating packets destined to the EID-prefix based on these advertised parameters.

When a LISP site has multiple locators associated with the same EID-prefix block, multiple **ipv6 lisp database-mapping** commands are used to configure all of the locators for a given EID-prefix block. Each locator may be assigned the same or a different priority value between 0 and 255. When multiple locators are assigned different priority values, the priority value alone is used by an ITR to determine which locator to prefer. A lower value indicates a more preferable path. A value of 255 indicates that the locator must not be used for unicast traffic forwarding. When multiple locators have the same priority, this indicates they may be used in a load-sharing manner. In this case, for a given priority, the weight given to each locator is used to determine how to load-balance unicast packets between them. Weight is a value between 0 and 100 and represents the percentage of traffic to be load-shared to that locator. A weight value of zero indicates to an ITR receiving the Map-Reply that it may decide how to load-share traffic destined to that EID-prefix block. If a non-zero weight value is assigned to any locator for a given EID-prefix block, then all locators with the same priority for that same EID-prefix block must also be assigned a non-zero weight value and the sum of all weight values must equal 100. If a weight value of zero is assigned to any locator for a given EID-prefix block, then all locators with the same priority for that same EID-prefix block must also be assigned a weight value of zero.

When a LISP site is assigned multiple IPv6 EID-prefixes, the **ipv6 lisp database-mapping** command is configured for each IPv6 EID-prefix assigned to the site and for each locator by which the IPv6 EID-prefix is reachable.

Note NX-OS limits the number of **ip lisp database-mapping** commands configured on an ETR to four (4) entries per EID Address Family, per vrf context.

When multiple ETRs are used at a LISP site, the **ipv6 lisp database-mapping** command must be configured identically on all ETRs for all locators by which an IPv6 EID-prefix block is reachable, even when the locator is not local to the specific ETR being configured. For example, if a site uses two ETRs and each has a single locator, both ETRs must configure the **ipv6 lisp database-mapping** command for the assigned IPv6 EID-prefix block for its own locator as well as the locator of the other ETR.

If the ETR is sited behind an upstream NAT device, the RLOC to be associated with EID prefixes may not be know. In addition, the local interface of the ETR (what would typically be its routing locator) could belong to the private address space for example, and that the NAT device translates to a public globally routed address. In this case it may not be possible to specify a locator in the **ipv6 lisp database-mapping** entry. The **dynamic** keyword can be configured with the **ipv6 lisp database-mapping** command in this case so to dynamically determine the RLOC rather than being statically defined in each **ipv6 lisp database-mapping** entry.

Note When the **dynamic** keyword is used because an ETR is sited behind NAT in order to find dynamically the public global locator address for use in Map-Register and Map-Reply messages, the command {**ip** | **ipv6**} **lisp nat-traversa**l must also be configured under the interface connecting the ETR to the core. The

LISP-46

command {**ip** | **ipv6**} **lisp nat-traversa**l performs the actual process of determining the global NAT'ed routing locator address. See the {**ip** | **ipv6**} **lisp nat-traversa**l commands for further details.

Examples

The following example configures LISP database-mapping entries for a single IPv6 EID-prefix block and two IPv4 locators associated with the EID-prefix block. Each locator is assigned the same priority (1) and weight (50), indicating that ingress traffic is expected to be load-shared equally across both paths.

```
Router(config)# ipv6 lisp database-mapping 2001:DB8:BB::/48 10.1.1.1 priority 1 weight 100
Router(config)# ipv6 lisp database-mapping 2001:DB8:BB::/48 10.1.2.1 priority 1 weight 100
```

Related Commands

Command	Description
ipv6 lisp etr map-server	Configures the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv6 EID prefixes.
ipv6 lisp map-cache	Configures a static IPv6 EID-prefix to locator map-cache entry.
Ipv6 lisp nat-transversal	To configure an ETR with a private locator that is sited behind a NAT device to dynamically determine its NAT-translated public globally routed locator address for the applied interface.

ipv6 lisp etr

To configure a router to act as an IPv6 LISP Egress Tunnel Router (ETR), use the **ipv6 lisp etr** command in global configuration mode. To remove LISP ETR functionality, use the **no** form of this command.

> **[no] ipv6 lisp etr**

Syntax Description

This command has no arguments or keywords.

Defaults

The router does not provide LISP ETR services.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable the router to perform IPv6 LISP Egress Tunnel Router (ETR) functionality. When a router is configured as an IPv6 ETR, it is typically also configured with **ipv6 lisp database-mapping** commands so that the ETR knows what IPv6 EID-prefix blocks and corresponding locators are used for its LISP site. In addition, the ETR is also configured to register with a Map-Server by using the **ipv6 lisp etr map-server** command, or to use static LISP EID-to-RLOC mappings with the **ipv6 lisp map-cache** command to participate in LISP networking.

✎

Note When an ETR is handling packets with mixed Address Families between EIDs and RLOCs (i.e. IPv4 EIDs and IPv6 RLOCs, or IPv6 EIDs and IPv4 RLOCs), it is required to configure both the **ip lisp etr** command as well as the **ipv6 lisp etr** command.

✎

Note It is common for a device configured as an ETR to also be configured as an ITR. However, the LISP architecture does not require this and ETR and ITR functionality can occur in different devices. When configuring a device as both an ITR and an ETR, using the command **ipv6 lisp itr-etr** to enable both capabilities in one command is recommended.

Examples

The following example configures IPv6 LISP ETR functionality on the router.

```
Router(config)# ipv6 lisp etr
```

Related Commands

Command	Description
ipv6 lisp database-mapping	Configures an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy.
ipv6 lisp etr map-server	Configures the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv6 EID prefixes.
ipv6 lisp itr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR)
ipv6 lisp itr-etr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR) and an IPv6 LISP Egress Tunnel Router (ETR) with one command.
ipv6 lisp map-cache	Configures a static IPv6 EID-prefix to locator map-cache entry.

---

ipv6 lisp etr accept-map-request-mapping

To configure an ETR to cache IPv6 mapping data contained in a Map-Request message, use the **ipv6 lisp etr accept-map-request-mapping** command in global configuration mode. To remove this functionality, use the **no** form of this command.

[no] ipv6 lisp etr accept-map-request-mapping [**verify**]

Syntax Description

verify	(Optional) Specifies that mapping data should be cached but not used for forwarding packets until the ETR can send its own Map-Request to one of the locators from the mapping data record and receive a Map-Reply with the same data in response.

Defaults

The router does not cache mapping data contained in a Map-Request message.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When an ETR receives a Map-Request message, this message may contain mapping data for the invoking IPv6 source-EID's packet. By default, the ETR will ignore mapping data included in Map-Request messages. However, by configuring the **ipv6 lisp etr accept-map-request-mapping** command, the ETR will cache the mapping data in its map-cache and immediately use it for forwarding packets.

When the optional **verify** keyword is configured, the ETR will still cache the mapping data but will not use it for forwarding packets until the ETR can send its own Map-Request to one of the locators from the mapping data record, and receives the same data in a Map-Reply message.

✎

Note For security purposes, it is recommended that the **verify** keyword be configured. Unless the ETR and ITR are deployed in a trusted environment, using the optional **verify** keyword is considered a best practice. In a trusted environment it may be considered acceptable for verification to not be configured, in which case the new mapping will occur in one-half round-trip-time (RTT) as compared with the normal Map-Request/Map-Reply exchange process.

When the **ipv6 lisp etr accept-map-request-mapping** command is enabled and then later disabled, issuing the command **clear ipv6 lisp map-cache** is required to clear any map-cache entries that are currently in the "tentative" state. Map-cache entries can remain in the "tentative" state for up to one minute and thus it may be desirable to clear these entries manually when this command is removed.

Examples

The following example configures the ETR to accept and cache IPv6 mapping data included in Map-Request messages but to verify its accuracy prior to using this data to forward packets.

```
Router(config)# ipv6 lisp etr accept-map-request-mapping verify
```

Related Commands

Command	Description
ipv6 lisp etr	Configures the router to act as an IPv6 LISP Egress Tunnel Router (ETR).
clear ipv6 lisp map-cache	Clear the LISP IPv6 map-cache on the local router.

---

ipv6 lisp etr glean-mapping

To configure an ETR to add inner header (EID) source address to outer header (RLOC) source address mappings it to its EID-to-RLOC cache (map-cache), use the **ipv6 lisp etr glean-mapping** command in global configuration mode. To remove this functionality, use the **no** form of this command.

   [no] ipv6 lisp etr glean-mapping [**verify**]

Syntax Description

Verify	(Optional) Specifies that gleaned EID-to-RLOC mapping data should be cached but not used for forwarding packets until the ETR can send its own Map-Request to the originating ITR and receive a Map-Reply with the same data in response.

Defaults

The router does not cache gleaned EID-to-RLOC mapping data in its map-cache.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When an ETR receives LISP encapsulated packets, the inner header (EID) source address and outer header (RLOC) source address should match an entry found in the map-cache as determined by the results of a Map-Request/Map-Reply exchange. In certain circumstances, for example when a host moves from one ITR to another, it is possible for the EID-to-RLOC mapping to change since the new ITR can encapsulate packets to the ETR using a different locator. By configuring the **ipv6 lisp etr glean-mapping** command, the ETR will recognize the new locator information for the moved host's EID and update the map-cache with this information.

Note Gleaned EID-to-RLOC map-cache entries are stored with a priority of 1 and a weight of 100.

When the optional **verify** keyword is configured, the ETR will cache the gleaned EID-to-RLOC mapping data but it will not be used for forwarding packets until the ETR can send its own Map-Request to the originating ITR and receive a Map-Reply with the same nonce included in the Map-Request. The gleaned locator will then be used. When the **verify** keyword is specified, the gleaned locator will not be used to forward traffic and all packets will be dropped until the Map-Reply is returned.

Note For security purposes, it is recommended that the **verify** keyword be configured. Unless the ETR and ITR are deployed in a trusted environment, using the optional **verify** keyword is considered a best-practice. In a trusted environment it may be considered acceptable for verification to not be configured, in which case the new mapping will occur in one-half round-trip-time (RTT) as compared with the normal Map-Request/Map-Reply exchange process.

Examples

The following example configures the ETR to glean and cache IPv6 mapping data included in Map-Request messages but to verify its accuracy prior to using this data to forward packets.

```
Router(config)# ipv6 lisp etr glean-mapping verify
```

Related Commands

Command	Description
ipv6 lisp etr	Configures the router to act as an IPv6 LISP Egress Tunnel Router (ETR).

ipv6 lisp etr map-cache-ttl

To configure the TTL value to be inserted into LISP IPv6 Map-Reply messages, use the **ipv6 lisp etr map-cache-ttl** command in global configuration mode. To remove the configured TTL value and return to the default value, use the **no** form of this command.

[no] ipv6 lisp etr map-cache-ttl *time-to-live*

Syntax Description

time-to-live	A value, in minutes, to be inserted in the TTL field in Map-Reply messages. Valid entries are between 60 minutes (1 hour) and 10080 minutes (1 week).

Defaults

The default TTL value is 1440 minutes (24 hours).

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to change the default value associated with the Time-to-Live (TTL) field in IPv6 Map-Reply messages. This may be useful when you wish to change the default TTL that remote ITRs will cache and use for your sites IPv6 EID prefix. The default value is 1440 minutes (24 hours), the minimum value cannot be less than 60 minutes, and the maximum cannot be greater than 10080 minutes (one week).

Examples

The following example configures the ETR to use a TTL of 120 minutes in its IPv6 Map-Reply messages.

```
Router(config)# ipv6 lisp etr map-cache-ttl 120
```

Related Commands

Command	Description
ipv6 lisp etr	Configures the router to act as an IPv6 LISP Egress Tunnel Router (ETR).

---

ipv6 lisp etr map-server

To configure the IPv4 or IPv6 locator address of the LISP Map-Server to be used by the ETR when registering for IPv6 EIDs, use the **ipv6 lisp etr map-server** command in global configuration mode. To remove the configured locator address of the LISP Map-Server, use the **no** form of this command.

[no] ipv6 lisp etr map-server *map-server-address* {[**key** *key-type password*] | **proxy-reply**}

Syntax Description

map-server-address	Specifies the IPv4 or IPv6 locator addresses of the Map-Server.
key *key-type*	Specifies how the following SHA-1 password (key) is encoded. Type (0) indicates that a cleartext password follows; Type (3) indicates that a 3DES encrypted key follows; Type (7) indicates that a Cisco Type 7 encrypted password follows.

password	Specifies the password used for computing the SHA-1 HMAC hash that is included in the header of the Map-Register message.
proxy-reply	(Optional) Indicates to the Map-Server via a Map-Register message that the Map-Server should send Map-Replies on behalf of the ETR (this site) to requesting ITRs.

Defaults

No LISP Map-Server locator addresses are configured by default.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.0(1.13) (August update)	This command was modified.

Usage Guidelines

Use the **ipv6 lisp etr map-server** command to configure the IPv4 or IPv6 locator of the Map-Server to which the ETR will register for its IPv6 EID(s). A password used for in the calculation of a SHA-1 HMAC hash that is included in the header of the Map-Register message must also be provided. You can configure the ETR to register with at most two Map-Servers per EID address family. Once the ETR registers with the Map-Server(s), the Map-Server(s) will begin to advertise the IPv6 EID-prefix block(s) and RLOC(s) for the LISP site.

The SHA-1 HMAC password may be entered in unencrypted (cleartext) form or encrypted form. To enter an unencrypted password, specify a key-type value of 0. To enter a 3DES-encrypted password, specify a key-type value of 3. To enter a Cisco-encrypted password, specify a key-type value of 7.

⚠ **Caution** A Map-Server authentication key entered in cleartext form will automatically be converted to Type 3 (encrypted) form.

✎ **Note** The Map-Server must also be configured with IPv6 EID prefixes that match the IPv6 EID-prefixes configured on this ETR using the **ipv6 lisp database-mapping** command, as well as a password matching the one provided with the **key** keyword on this ETR.

When the keyword **proxy-reply** is used with this command, the ETR is indicating to the Map-Server via a Map-Register message that the Map-Server should send non-authoritative Map-Replies on behalf of the ETR (this LISP site) to ITRs requesting EID-to-RLOC mapping resolutions for an EID prefix at this LISP site. On the Map-Server, the **show lisp site** *site-name* command indicates whether proxy-reply is enabled or not.

✎ **Note** If the command**ipv6 lisp itr map-resolver** is not configured, then the locator address used in the command **ipv6 lisp etr map-server** will automatically be used for a Map-Resolver locator (without the need to explicityly configure one). This allows for the minimum LISP configuration on an NX-OS xTR of:

```
feature lisp
ipv6 lisp itr-etr
ipv6 lisp database-mapping ....
ipv6 lisp etr map-server ...
```

The output of the command **show ipv6 lisp** indicates whether the Map-Server locator is also used as a Map-Resolver locator.

Examples

The following example configures the ETR to register to two Map-Servers, one with the locator 2001:DB8:0A::1 and another with the locator 2001:DB8:0B::1.

```
Router(config)# ipv6 lisp etr map-server 2001:db8:0a::1 key some-password
Router(config)# ipv6 lisp etr map-server 2001:db8:0b::1 key some-password
```

The following example configures the ETR to register to the Map-Server with the locator 2001:DB8:0A::1 and requests that the Map-Server proxy-reply for the site.

```
Router(config)# ipv6 lisp etr map-server 2001:db8:0a::1 key some-password
Router(config)# ipv6 lisp etr map-server 2001:db8:0a::1 proxy-reply
```

Related Commands

Command	Description
ipv6 lisp alt-vrf	Configure which VRF supporting the IPv6 address-family LISP should use when sending Map Requests for an IPv6 EID-to-RLOC mapping directly over the ALT.
ipv6 lisp database-mapping	Configure an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy.
ipv6 lisp etr	Configures the router to act as an IPv6 LISP Egress Tunnel Router (ETR)
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server

---

ipv6 lisp hardware-forwarding

To enable hardware-forwarding specifically on the Nexus 7000 when at least one 32x10GE line card is installed, use the **ipv6 lisp hardware-forwarding** command in global configuration mode. To disable this functionality, use the **no** form of this command.

[no] ipv6 lisp hardware-forwarding

Syntax Description

This command has no arguments or keywords.

Defaults

By default, hardware forwarding is enabled on the Nexus 7000 when at least one 32x10GE line card is installed.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command is **ONLY** applicable to the Nexus 7000. Hardware forwarding for LISP is only supported on the following Line Cards:

- N7K-M132XP-12 Cisco Nexus 7000 Series 32-Port 10Gb Ethernet Module
- N7K-M132XP-12L Cisco Nexus 7000 Series 32-Port 10Gb Ethernet Module with XL Option

LISP input and output interfaces MUST be on the above Line Cards in order for hardware-based LISP encapsualtion and decapsulation to be performed.

By default, hardware forwarding of LISP packets is enabled on the Nexus 7000 when at least one 32x10GE line card is installed. In certain debugging operations, however, it may be useful to disable hardware forwarding. This is accomplished by using the **no ipv6 lisp hardware-forwarding** command. When the **no** form of this command is used, software-based supervisor LISP forwarding is enabled on the Nexus 7000.

⚠️

Caution Disabling hardware forwarding should only be used in diagnostic situations. Configuring the **no ipv6 lisp hardware-forwarding** command will cause a full map-cache download to the Nexus 7000 hardware.

✎

Note Configuring the **no ipv6 lisp hardware-forwarding** command for debugging purposes is best used in conjunction with the **debug lisp ufdm detail** command. . Be sure to re-enable hardware-forwarding when debugging operations are completed by invoking the **ipv6 lisp hardware-forwarding** command.

Examples

The following example disables IPv6 LISP hardware forwarding on the Nexus 7000 and then enables UFDM debugging.

```
Router(config)# no ipv6 lisp hardware-forwarding
Router(config)# exit
Router# debug lisp ufdm detail
```

Related Commands

Command	Description
lisp beta	Enable LISP functionality on the Nexus 7000 router.
debug lisp ufdm	Display debug messages related to activities between the LISP process and the UFDM process and which program the EARL8 on the Nexus 7000 only.

---

ipv6 lisp itr

To configure a router to act as an IPv6 LISP Ingress Tunnel Router (ITR), use the **ipv6 lisp itr** command in global configuration mode. To remove LISP ITR functionality, use the **no** form of this command.

    [no] ipv6 lisp itr

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not provide ITR functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable the router to perform IPv6 LISP Ingress Tunnel Router (ITR) functionality.

When a router is configured as an ITR, it must decide how to handle the packets it receives. This decision process is summarized as follows:

3. If the packet destination matches an existing route in the routing table, the packet is forwarded natively (regardless of the packet source IP address).

4. If the packet destination matches a DEFAULT ROUTE or NO ROUTE in the routing table, then the packet source IP address is checked against configured **ipv6 lisp database-mapping** commands to determine if the source is a LISP EID.

   a. If the packet source IP address **is not** a configured EID, then the packet **is not** LISP-eligible. If the destination matches a DEFAULT ROUTE, the packet is forwarded natively. If there is no route to the destination, the packet is dropped.

   b. If the packet source IP address **is** a configured EID, then the packet **is** LISP-eligible. In this case, the ITR checks the existing map-cache and does one of the following actions:

   - If a map-cache entry exists with an action of LISP encapsulation, as would be the case for a destination that is another valid LISP site, then the packet is LISP-encapsulated and forwarded.

   - If a map-cache entry exists with an action of "forward-native," as would be the case when the destination is not another LISP site and the map-cache entry is added by a Negative-Map-Reply, then the packet is forwarded natively. If the **ipv6 lisp use-petr** command is also configured, then the packet is LISP-encapsulated to the configured PETR.

   - If a map-cache entry exists with an action of "drop," as would be the case when a static map-cache entry is added with this action, then the packet is dropped.

   - If a map-cache entry exists with an action of "send-requst," as would be the case when a static map-cache entry is added (such as in the case of a PITR) or when it matches no entry, then a Map-Request is sent to the configured Map-Resolver and the packet is silently dropped. Subsequent packets to the same destination should be covered by any new map-cache entry added as a result of the Map-Request.

The ITR may use one of two methods to send a Map-Request to obtain an IPv4 EID-to-RLOC mapping:

- When a Map-Resolver is configured via the **ipv6 lisp itr map-resolve**r command, the ITR will send its Map-Request in a LISP Encapsulated Control Message (ECM) to the Map-Resolver.
- When the ITR is directly attached to the ALT using the **ipv6 lisp alt-vrf** command, the ITR will send its Map-Request directly on the alternate LISP Alternate Logical Topology (ALT).

The ITR caches the resultant IPv6 EID-to-RLOC mapping information returned by the associated Map-Reply in its map-cache. Subsequent packets destined to the same IPv6 EID-prefix are then LISP-encapsulated according to this IPv6 EID-to-RLOC mapping entry.

Note When instance-ID's are used to support LISP virtualization, an ITR must be configured to use a Map-Resolver (MR) (configured via the **ipv6 lisp itr map-resolve**r command) to obtain IPv4 EID-to-RLOC mappings. It **must not** be configured to directly attach to the ALT (using the **ipv6 lisp alt-vrf** command) since the ALT does not support LISP virtualization.

Note It is common for a device configured as an ITR to also be configured as an ETR. However, the LISP architecture does not require this and the functionality can occur in a different device. When configuring a device as both an ITR and an ETR, using the command **ipv6 lisp itr-etr** to enable both capabilities in one command is recommended.

Examples

The following example configures IPv6 LISP ITR functionality on the router.

```
Router(config)# ipv6 lisp itr
```

Related Commands

Command	Description
ipv6 lisp alt-vrf	Configures which VRF supporting the IPv6 address-family that LISP should use when sending Map Requests for an IPv6 EID-to-RLOC mapping directly over the ALT.
ipv6 lisp database-mapping	Configures an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy.
Ipv6 lisp itr-etr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR) and an IPv6 LISP Egress Tunnel Router (ETR) with one command.
ipv6 lisp itr map-resolver	Configures the IPv4 or IPv6 locator address of the LISP Map-Resolver to which the ITR sends IPv6 Map-Request messages
ipv6 lisp map-cache	Configures a static IPv6 EID-prefix to locator map-cache entry.

---

ipv6 lisp itr map-resolver

To configure the IPv4 or IPv6 locator address of the LISP Map-Resolver to be used by the ITR or PITR when sending Map-Requests for IPv6 EID-to-RLOC mapping resolution, use the **ipv6 lisp itr map-resolver** command in global configuration mode. To remove the configured locator address of the LISP Map-Resolver, use the **no** form of this command.

[no] ip lisp itr map-resolver *map-resolver-address*

Syntax Description

map-resolver-address	Specifies the IPv4 or IPv6 locator addresses of the Map-Resolver.

Defaults

No LISP Map-Resolver locator address is configured by default.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command configures the locator to be used by a LISP ITR or PITR to reach the configured Map-Resolver when sending a map request for IPv6 EID-to-RLOC mapping resolution. Only a single Map-Resolver can be configured per ITR or PITR within a site, for each address-family. The locator of the Map-Resolver may be reachable via IPv4 or IPv6 RLOC addresses.

When a LISP ITR or PITR needs to resolve an IPv4 EID-to-RLOC mapping for a destination EID, it can be configured to send a map request message either to a Map Resolver configured using the **ip lisp itr map-resolver** command, or directly over the LISP ALT using the **ip lisp alt-vrf** command. When a Map Resolver is used, map requests are sent to the Map Resolver as a LISP Encapsulated Control Message (ECM). When the ALT is used, map requests sent over the ALT directly to the EID being queried.

✎
Note When the **ipv6 lisp itr map-resolver** command is entered, the **ipv6 lisp alt-vrf** command is not used (and may be removed).

✎
Note When instance-ID's are used to support LISP virtualization, an ITR or PITR **must** be configured to use a configured Map-Resolver (MR) (configured via the **ipv6 lisp itr map-resolve**r command) to obtain IPv6 EID-to-RLOC mappings. The LISP-ALT mapping system does not support LISP virtualization.

✎
Note If the command **ip lisp etr map-resolver** is not configured, then the locator address used in the command **ip lisp etr map-server** will automatically be used for a Map-Resolver locator (without the need to explicityly configure one). This allows for the minimum LISP configuration on an NX-OS xTR of:

```
feature lisp
ip lisp itr-etr
ip lisp database-mapping ....
ip lisp etr map-server ...
```

The output of the command **show ip lisp** indicates whether the Map-Server locator is also used as a Map-Resolver locator.

Examples

The following example configures an ITR to use the Map-Resolver located at 2001:DB8:0A::1 when sending its Map-Request messages.

```
Router(config)# ipv6 lisp itr map-resolver 2001:DB8:0A::1
Router(config)# ipv6 lisp itr map-resolver 10.1.1.1
```

Related Commands

Command	Description
ipv6 lisp alt-vrf	Configures which VRF supporting the IPv6 address-family LISP should use when sending Map Requests for an IPv6 EID-to-RLOC mapping directly over the ALT.
ipv6 lisp itr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR)
ipv6 lisp map-request-source	Configures the source IPv4 or IPv6 address to be used in IPv6 LISP Map-Request messages.

ipv6 lisp itr send-data-probe

To configure an ITR or PITR to find an IPv6 EID-to-RLOC mapping for a packet it needs to encapsulate by sending a Data Probe rather than by sending a Map-Request message, use the **ipv6 lisp itr send-data-probe** hidden command in global configuration mode. To remove this functionality, use the **no** form of this command.

[no] ipv6 lisp itr send-data-probe

Syntax Description

This command has no arguments or keywords.

Defaults

By default, an ITR does not send data-probes to determine IPv6 EID-to-RLOC mappings.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

⚠️

Caution The **ipv6 lisp itr send-data-probe** command is deprecated and no longer supported and should not be used. Its inclusion in this document is solely for legacy purposes. The use of the LISP Data Probe is strongly discouraged as this mechanism forwards data plane traffic over the LISP-ALT. The LISP-ALT is intended to function solely as a control plane mechanism for LISP and its use for carrying data plane traffic consumers potentially scarce resources, as well as potentially subjects it to denial of service attacks.

When a LISP ITR or PITR gets a map-cache miss and needs to resolve an IPv6 EID-to-RLOC mapping for a destination EID, it is typically configured to send a Map-Request message either in a LISP Encapsulate Control Message (ECM) to the Map Resolver configured using the **ipv6 lisp itr map-resolver** command, or directly over the LISP ALT referred to by the **ipv6 lisp alt-vrf** command. In either case, the first packet of the flow that caused the map-cache miss is dropped. Once the Map-Reply populates the map-cache, subsequent packets to the same destination are forwarded directly by LISP.

A **deprecated** method for determining EID-to-RLOC mappings that does not drop the first packet of a flow is implemented using a LISP Data Probe technique. When using the LISP Data Probe technique, rather than dropping the first data packet and sending a Map-Request message, the data packet is LISP-encapsulated where the inner header destination address equals the outer header destination address and forwarded directly over the LISP-ALT to the decapsulating ETR. This Data Probe packet triggers a Map-Reply by the ETR, which then returns a Map-Reply directly back to the ITR.

✎

Note When an ITR or PITR is configured with the **ipv6 lisp itr send-data-probe** command, the ITR or PITR must also be configured to use the LISP-ALT (using the **ipv6 lisp alt-vrf** command) since the Data-Probe is sent over the LISP-ALT.

Examples

The following example configures a LISP ITR to send Data Probes to determine IPv6 EID-to-RLOC mappings.

```
Router(config)# ipv6 lisp itr send-data-probe
```

Related Commands

Command	Description
ipv6 lisp alt-vrf	Configures which VRF supporting the IPv6 address-family LISP should use when sending Map Requests for an IPv6 EID-to-RLOC mapping directly over the ALT.
ipv6 lisp itr map-resolver	Configured the IPv4 or IPv6 locator address of the LISP Map-Resolver to which the ITR sends IPv6 Map-Request messages

---

ipv6 lisp itr-etr

To configure a router to act as both an IPv6 LISP Ingress Tunnel Router (ITR) and Egress Tunnel Router (ETR), use the **ipv6 lisp itr-etr** command in global configuration mode. To remove LISP ITR functionality, use the **no** form of this command.

[no] ipv6 lisp itr-etr

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not provide ITR functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13) (August update)	This command was introduced.

Usage Guidelines

Use this command to enable the router to perform both IPv6 LISP Ingress Tunnel Router (ITR) and Egress Tunnel Router (ETR) functionality simultaneously, via a single command.

For usage guidelines for IPv6 LISP Ingress Tunnel Router (ITR) functionality, refer to the **ipv6 lisp itr** command. For usage guidelines for IPv6 LISP Egress Tunnel Router (ETR) functionality, refer to the **ipv6 lisp etr** command.

Note If this command is used and either of the **ipv6 lisp itr** or **ipv6 lisp etr** commands have already been configured they will be automatically removed from the configuration file.

✎

Note It is common for a device configured as an ITR to also be configured as an ETR. However, the LISP architecture does not require this and the functionality can occur in a different device. When configuring a device as both an ITR and an ETR, using the command **ipv6 lisp itr-etr** to enable both capabilities in one command is recommended.

Examples

The following example configures IPv6 LISP ITR and ETR functionality on the router.

```
Router(config)# ipv6 lisp itr-etr
```

Related Commands

Command	Description
ipv6 lisp etr	Configures the router to act as an IPv6 LISP Egress Tunnel Router (ETR)
ipv6 lisp itr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR)

ipv6 lisp locator-down

To configure a locator from a locator-set associated with an IPv6 EID-prefix database-mapping to be unreachable (down), use the **ipv6 lisp locator-down** hidden command in global configuration mode. To return the locator to be reachable (up), remove the configuration using the **no** form of this command.

> **[no] ipv6 lisp locator-down** *EID-prefix/prefix-length locator*

Syntax Description

EID-prefix/prefix-length	The IPv6 EID prefix and length advertised by this router.
locator	The IPv4 or IPv6 Routing Locator (RLOC) associated with this EID-prefix

Defaults

An IPv4 or IPv6 locator associated with a configured IPv6 EID-prefix block is considered reachable (up) unless an IGP routing protocol indicates it is down.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When LISP database parameters are configured on an ITR for specified IPv6 EID-prefix blocks using the **ipv6 lisp database-mapping** command or **ipv6 lisp map-cache** command, the locators associated with these IPv6 EID-prefix blocks are considered as reachable (up) by default. The **ipv6 lisp locator-down** hidden command can be used to configure a locator from a locator-set associated with the IPv6 EID-prefix database mapping to be down.

LISP-60

When this command is configured, the Locator Status Bits (LSB) for the configured locator will be cleared (set to zero) when encapsulating packets to remote sites. ETRs at remote sites look for changes in the LSBs when decapsulating LISP packets, and when the LSB indicates that a specific locator is down, the ETR, also acting as an ITR, will refrain from encapsulating packets using the 'down' locator to reach the local site.

✎

Note If this command is configured on an ITR to indicate that a locator is unreachable (down) and the LISP site includes multiple ITRs, this command must be configured on all ITRs at the site to ensure that the site consistently tells remote sites that the configured locator is not reachable.

Examples

The following example configures the locator 2001:DB8:0A::1 to a down state for the IPv6 EID-prefix block 2001:DB8:BB::/48.

```
Router(config)# ipv6 lisp locator-down 2001:DB8:BB::/48 2001:DB8:0A::1
```

Related Commands

Command	Description
ipv6 lisp database-mapping	Configures an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy.
ipv6 lisp itr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR)
ipv6 lisp map-cache	Configures a static IPv6 EID-prefix to locator map-cache entry.

Ipv6 lisp locator-vrf

To configure a non-default virtual routing and forwarding (VRF) table to be referenced by any IPv6 locator addresses, use the **ipv6 lisp locator-vrf** command in global configuration mode. To return to using the default routing table for locator address references, use the **no** form of this command.

> [no] ipv6 lisp locator-vrf {*vrf-name* | **default**}

Syntax Description

vrf-name	The name of the VRF to be referenced by IPv6 locator addresses instead of the default table.
default	Specifies that the **default** VRF should be referenced by the IPv4 locator addresses.

Defaults

IPv6 locator addresses are associated with the default (global) routing table.

Command Modes

VRF configuration mode

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(3.lisp)	This command was introduced.

Usage Guidelines

By default, LISP is configured to consider both EIDs and locators to be reachable from the default VRF (i.e. the global routing table). When it is desired to configure LISP to associate locator addresses with a VRF other than the default VRF, the **ipv6 lisp locator-vrf** command is used to specify the IPv6 VRF to be associated with these locator addresses.

When the **ipv6 lisp locator-vrf** command is configured, the locator addresses in any subsequent LISP commands are referenced to the specified VRF. For example, the locator addresses in the **ipv6 lisp itr map-resolver** and **ipv6 lisp etr map-server** commands would refer to the VRF configured by the **ipv6 lisp locator-vrf** command when configured. Note that the map-server(s) and map-resolver(s) must also share the configuration from the locator-VRF and be reachable within that address space.

✎

Note When mixed address families are configured for EIDs and/or locators (i.e. IPv4 EIDs and IPv6 locators or IPv6 EIDs and IPv4 locators), this command must be configured for both address families.

Example

In the following example, a LISP xTR is configured with one EID VRF context named **PURPLE**, and one locator VRF context named **BLUE**. That is, the EID prefixes 192.168.1.0/24 and 2001:db8:a::/64 are reachable via the VRF context **PURPLE**. The locator used for encapsulation (i.e. 10.0.0.2), and the locators of the Map-Server and Map-resolver (i.e. 10.0.2.2) are reachable via the VRF context BLUE.

```
Router(config)# feature lisp
Router(config)# vrf context PURPLE
Router(config-vrf)# lisp instance-id 101
Router(config-vrf)# ip lisp locator-vrf BLUE
Router(config-vrf)# ipv6 lisp locator-vrf default
Router(config-vrf)# ip lisp itr-etr
Router(config-vrf)# ipv6 lisp itr-etr
Router(config-vrf)# ip lisp database-mapping 192.168.1.0/24 10.0.0.2 priority 1 weight 100
Router(config-vrf)# ipv6 lisp database-mapping 2001:db8:a::/64 10.0.0.2 priority 1 weight 100
Router(config-vrf)# ip lisp etr map-server 10.0.2.2 key PURPLE-key
Router(config-vrf)# ipv6 lisp etr map-server 10.0.2.2 key PURPLE-key
Router(config-vrf)# ip lisp itr map-resolver 10.0.2.2
Router(config-vrf)# ipv6 lisp itr map-resolver 10.0.2.2
Router(config-vrf)# exit
Router(config)# vrf context BLUE
Router(config-vrf)# ip lisp itr-etr
Router(config-vrf)# ipv6 lisp itr-etr
Router(config-vrf)# ip route 0.0.0.0/0 10.0.0.1
Router(config-vrf)# exit
Router(config)#
```

Related Commands

Command	Description
Ipv6 lisp etr map-server	Configured the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv6 EID prefixes
Ipv6 lisp itr map-resolver	Configured the locator address of the LISP Map-Resolver to which the ITR sends Map-Request messages

ipv6 lisp map-cache

To configure a static IPv6 EID-to-RLOC mapping relationship and its associated traffic policy, or to statically configure the packet handling behavior associated with a specified destination IPv6 EID-prefix, use the **ip lisp**

map-cache command in global configuration mode. To remove the configuration, use the **no** form of this command.

> **[no] ipv6 lisp map-cache** *destination-EID-prefix/prefix-length* {*locator* **priority** *priority* **weight** *weight* | {**drop | map-request | native-forward**}}

Syntax Description

destination-EID-prefix/prefix-length	Destination IPv6 EID-prefix/prefix-length.
locator	The IPv4 or IPv6 Routing Locator (RLOC) associated with this EID-prefix/prefix-length
priority *priority*	The priority (value between 0 and 255) assigned to the RLOC. When multiple locators have the same priority they may be used in load-shared fashion. A lower value indicates a higher priority.
weight *weight*	The weight (value between 0 and 100) assigned to the locator. Used in order to determine how to load-share traffic between multiple locators when the priorities assigned to multiple locators are the same. The value represents the percentage of traffic to be load-shared.
drop	(Optional) Drop packets that match this map-cache entry
map-request	(Optional) Send a Map-Request for packets that match this map-cache entry
native-forward	(Optional) Natively forward packets that match this map-cache entry

Defaults

No IPv6 EID-to-RLOC mapping relationships or static IPv6 EID-to-RLOC mapping destinations are configured by default.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The first use of this command is to configure an ITR with a static IPv6 EID-to-RLOC mapping relationship and its associated traffic policy. For each entry, a destination EID-prefix block and its associated locator, priority and weight are entered. The EID-prefix/prefix-length is the LISP EID-prefix block at the destination site. The locator is an IPv4 or IPv6 address of the remote site where the IPv6 EID-prefix can be reached. Associated with the locator address is a priority and weight that are used to define traffic policies when multiple RLOCs are defined for the same EID-prefix block. This command can be entered up to four (4) times for a given EID-prefix. Static IPv6 EID-to-RLOC mapping entries configured using this command take precedence over dynamic mappings learned through Map-Request/Map-Reply exchanges.

The second, optional use of this command is to statically configure the packet handling behavior associated with a specified destination IPv6 EID-prefix. For each entry, a destination IPv6 EID-prefix block is associated with a configured forwarding behavior. When a packet's destination address matches the EID-prefix, one of the following packet handling options can be configured:

> **drop** – Packets matching the destination IPv6 EID-prefix are dropped. For example, this action may be useful when administrative policies define that packets should be prevented from reaching a site.

LISP-63

native-forward – Packets matching the destination IPv6 EID-prefix are natively forwarded without LISP encapsulation. This action may be useful when the destination site is known to always be reachable natively and LISP encapsulation should never be used.

map-request – Packets matching the destination IPv6 EID-prefix cause a Map-Request to be sent. It is implied that the Map-Reply returned by this request will allow subsequent packets matching this EID-prefix to be LISP-encapsulated. This action may be useful for troubleshooting map-request activities and other diagnostic actions.

Examples

The following example configures a destination EID-to-RLOC mapping and associated traffic policy for the IPv6 EID-prefix block 2001:DB8:BB::/48. In this example, the locator for this EID-prefix block is 2001:DB8:0A::1 and the traffic policy for this locator has a priority of 1 and a weight of 100.

```
Router(config)# ipv6 lisp map-cache 2001:DB8:BB::/48 2001:DB8:0A::1 priority 1 weight 100
```

The following example configures a destination EID-to-RLOC mapping and associated traffic policy for the IPv6 EID-prefix block 2001:db8:aa::0/64 to **drop**. No traffic will be forwarded to this destination as a result.

```
Router(config)# ip lisp map-cache 2001:DB8:AA::/64 drop
```

Related Commands

Command	Description
ipv6 lisp database-mapping	Configures an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy.
ipv6 lisp itr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR)
ipv6 lisp map-cache-limit	Configures the maximum number of IPv6 LISP map-cache entries allowed to be stored by the router.

---

ipv6 lisp map-cache-limit

To configure the maximum number of IPv6 LISP map-cache entries allowed to be stored by the router, use the **ipv6 lisp map-cache-limit** command in global configuration mode. To remove the configured map-cache limit, use the **no** form of this command.

> **[no] ipv6 lisp map-cache-limit** *cache-limit* [**reserve-list** *list*]

Syntax Description

cache-limit	The maximum number of IPv6 LISP map-cache entries allowed to be stored on the router. The valid range is from 0 to 10000.
reserve-list *list*	(Optional) Specifies a set of IPv6 EID-prefixes in the referenced prefix-list for which dynamic map-cache entries shall always be stored.

Defaults

The default map-cache limit is 1000 entries.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to control the maximum number of IPv6 LISP map-cache entries that are allowed to be stored on the router. An optional **reserve-list** can be configured to guarantee that the router always stores the referenced IPv6 EID-prefixes.

LISP IPv6 map-cache entries are added in one of two ways – dynamically or statically. Dynamic entries are added when a valid Map-Reply message is returned for a Map-Request message generated in response to a cache-miss lookup. Static entries are added via the **ipv6 lisp map-cache** command. Whether a new map-cache entry is stored depends on the following conditions.

- Dynamic map-cache entries are always added until the default or configured cache-limit is reached. After the default or configured cache-limit is reached, unless the optional **reserve-list** is configured, no further dynamic entries are added and no further Map-Requests are generated in response to cache-miss lookups until a free position is available.
    - o When the optional **reserve-list** is not configured, dynamic entries are added on a first-in-first-added basis until the configured map-cache limit is reached. After that time, no new dynamic entries can be added. If the **reserve-list** is configured but the prefix-list to which it refers is not configured, the results are the same as if the **reserve-list** was not configured.
    - o When the optional **reserve-list** is configured, a Map-Request will be generated and a new dynamic map-cache entry may be added only for IP v6 EID-prefixes that are permitted by the prefix-list referenced by the **reserve-list**. In this case, the new entry must be able to replace an existing dynamic entry such that the cache-limit is maintained. The dynamic entry deleted will be either a non-reserve idle map-cache entry or non-reserve active map-cache entry. Idle map-cache entries are those that have seen no activity in the last 10 minutes. If all current dynamic entries are also permitted by the prefix-list referenced by the **reserve-list**, no further dynamic entries can be added.
    - o Existing dynamic IPv6 map-cache entries can time-out due to inactivity or can be removed by the administrator via the **clear ipv6 lisp map-cache** command to create a free position in the map-cache.
- Static map-cache entries are always added, until the default or configured cache-limit is reached. After the default or configured cache-limit is reached, unless the optional **reserve-list** is configured, no further static entries are added.
    - o When the optional **reserve-list** is not configured, static entries are added on a first-in-first-added basis until the configured map-cache limit is reached. After that time, no new static entries can be added. If the **reserve-list** is configured but the prefix-list to which it refers is not configured, the results are the same as if the **reserve-list** was not configured.
    - o When the optional **reserve-list** is configured, a static entry matching the **reserve-list** prefix-list may be added, but only if it can replace an existing static entry or dynamic entry that does not-match the **reserve-list** prefix-list.

⚠ **Caution** When the optional **reserve-list** is used, once the configured cache-limit is reached, if all existing entries also match the prefix-list and are not candidates for deletion, no new dynamic or static entries will be added, even if a new dynamic or static entry also matches the **reserve-list** prefix-list.

✎ **Note** When the **reserve-list** command is used, be sure that the prefix-list includes entries that match all expected prefixes in any Map-Reply, including the more-specifics. This can be ensured by appending **le 128** to the end of all prefix-list entries for IPv6 prefixes. For example, if you want to match 2001:DDB8:BB::/48 and any of the more specifics, you should specify **ipv6 prefix-list lisp-list seq 5 permit 2001:DDB8:BB::/48 le 128** in order to cover all replies within this range.

The addition and deletion of dynamic and static IPv6 map-cache entries can be observed by enabling the **debug ipv6 lisp mapping control** command. As with all debugging commands, exercise caution when using this command on a production system.

Examples

The following example configures a lisp cache-limit of 2000 entries and a reserve-list referencing the IPv6 prefix-list LISP-v6-always.

```
Router(config)# ipv6 lisp map-cache-limit 2000 reserve-list LISP-v6-always
Router(config)# ip prefix-list LISP-always seq 10 permit 2001:DB8:BA::/46 le 128
```

Related Commands

Command	Description
ipv6 lisp map-cache	Configures a static IPv6 EID-prefix to locator map-cache entry.
clear ipv6 lisp map-cache	Clear the LISP IPv6 map-cache on the local router.
debug ipv6 lisp mapping control	Display logs for Map-Request, Map-Reply, and other LISP IPv6 mapping activities

---

ipv6 lisp map-request-source

To configure an IPv4 or IPv6 address to be used as the source address for LISP IPv6 Map-Request messages, use the **ipv6 lisp map-request-source** command in global configuration mode. To remove the configured Map-Request source address and return to the default behavior, use the **no** form of this command.

> [no] ipv6 lisp map-request-source *source-address*

Syntax Description

source-address	The IPv4 or IPv6 source address to be used in LISP IPv6 Map-Request messages.

Defaults

The router uses one of the locator addresses configured in the **ipv6 lisp database-mapping** command as the default source address for LISP Map-Request messages.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Typically, a locator address configured in the **ipv6 lisp database-mapping** command is used as the source address for LISP IPv6 Map-Request messages. There are cases, however, where it may be necessary or useful to configure the specified source address for these Map-Request messages. For example, when the ITR is

behind a NAT device it may be necessary to specify a source address that matches the NAT configuration to properly allow for return traffic.

When the **ipv6 lisp map-request-source** command is configured on an ITR, the specified IPv4 or IPv6 locator is used by an ITR as the source address for Map-Request messages. When this command configured on a Map-Server, this locator is used as the source address in the Encapsulated Control Message carrying a Map-Request to an ETR.

Examples

The following example configures an ITR to use the source IPv6 address 2001:DB8:0A::1 in its IPv6 Map-Request messages.

```
Router(config)# ipv6 lisp map-request-source 2001:DB8:0A::1
```

Related Commands

Command	Description
ipv6 lisp database-mapping	Configures an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy.

---

ipv6 lisp map-resolver

To configure a router to act as an IPv6 LISP Map-Resolver (MR), use the **ipv6 lisp map-resolver** command in global configuration mode. To remove LISP Map-Resolver functionality, use the **no** form of this command.

[no] ipv6 lisp map-resolver

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not provide Map-Resolver functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable the router to perform IPv6 LISP Map-Resolver (MR) functionality. A LISP Map-Resolver is deployed as a LISP Infrastructure component.

A Map-Resolver receives a LISP Encapsulated Control Messages (ECM) containing a Map-Request from a LISP ITR directly over the underlying locator-based network. The Map-Resolver decapsulates this message and handles it according to other configurations and conditions as follows.

- When a Map-Resolver is concurrently configured as a standalone Map-Resolver/Map-Server, registered EID prefixes are maintained directly in its own database. In this case, the Map-Resolver component knows if the EID being queried for is available, as the authoritative ETR would be registering the EID prefix. If an ETR is registering the EID prefix, the Map-Server forwards the Map-Request as a LISP Encapsulated Control Messages (ECM) to the authoritative ETR. If the EID prefix being queried is not available, the Map-Resolvers sends a Negative Map-Reply directly back to an ITR in response to queries for non-LISP addresses.

- When a Map-Resolver is configured to use LISP-DDT, it is also configured with ddt root and delegation commands. In this case, the Map-Resolver checks its referral-cache and if nothing is found sends a Negative Map-Reply directly back to an ITR in response to queries for non-LISP addresses. If an entry is found, the Map-Resolver creates a DDT Map-Request and forwards it to to one of the RLOCs in the chosen referral cache entry. (See the LISP-DDT commands for additional details.)

- When a Map-Resolver is configured to use the LISP ALT for EID-to-RLOC mapping resolution, the Map-Resolver configuration must include the **ip lisp alt-vrf** command. In this case, the Map-Resolver knows if the EID being queried for is available, as the EID prefix will exist in the ALT. If the EID prefix is available, the Map-Resolver forwards the Map-Request directly over the ALT, where it is then delivered either to the Map-Server that is injecting EID-prefixes into the LISP-ALT on behalf of the authoritative ETR, and then from that Map-Server as an LISP ECM to the authoritative ETR. If the EID prefix being queried is not available, the Map-Resolvers sends a Negative Map-Reply directly back to an ITR in response to queries for non-LISP addresses.

Note When a Map-Resolver supports a LISP deployment that is configured for virtualization, the Map-Resolver must be concurrently configured as a Map-Server, or to use LISP-DDT. A Map-Resolver cannot forward a Map-Request with an instance-id over the LISP ALT.

Examples

The following example configures IPv6 LISP Map-Resolver functionality on the router.

```
Router(config)# ipv6 lisp map-resolver
```

Related Commands

Command	Description
ipv6 lisp alt-vrf	Configures which VRF supporting the IPv4 address-family LISP should use when sending Map Requests for an IPv4 EID-to-RLOC mapping directly over the ALT.

---

ipv6 lisp map-server

To configure a router to act as an IPv6 LISP Map-Server (MS), use the **ipv6 lisp map-server** command in global configuration mode. To remove LISP Map-Server functionality, use the **no** form of this command.

> **[no] ipv6 lisp map-server**

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not provide Map-Server functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable the router to perform IPv6 LISP Map-Server (MS) functionality. A LISP Map-Server is deployed as a LISP Infrastructure component.

LISP site commands are configured on the Map Server for a LISP ETR that registers to it, including an authentication key, which must match the one also configured on the ETR. A Map Server receives Map-Register control packets from ETRs.

A Map-Server may be configured concurrently configured as a standalone Map-Resolver/Map-Server, or as part of an infrastructure device in a LISP-DDT or LISP-ALT hierarchy. In general, Map-Server functions pertaining to these configurations are as follows.

- When a Map-Server is concurrently configured as a standalone Map-Resolver/Map-Server, registered EID prefixes are maintained directly in its own database. In this case, the Map-Resolver component knows if the EID being queried for is available, as the authoritative ETR would be registering the EID prefix. If an ETR is registering the EID prefix, the Map-Server forwards the Map-Request as a LISP Encapsulated Control Messages (ECM) to the authoritative ETR. If the EID prefix being queried is not available, the Map-Resolvers sends a Negative Map-Reply directly back to an ITR in response to queries for non-LISP addresses.

- When a Map-Server is configured as a LISP-DDT device, it is also configured with ddt root and delegation commands. In this case, when a Map-Server receives a DDT Map-Request, if the requested EID matches a registered EID-prefix, then the Map-Request is forwarded to one of the destination ETR RLOCs (as a LISP ECM). If the request EID is not found, the Map-Server sends a Negative Map Referral back to the requesting Map-Resolver (who then sends a Negative Map-Reply directly back to an ITR in response to queries for non-LISP addresses). (See the LISP-DDT commands for additional details.)

- When a Map-Server is configured to use the LISP ALT for EID-to-RLOC mapping resolution, the Map-Server configuration must include the **ip lisp alt-vrf** command. In this case, the Map-Server receives the Map-Request from the ALT for an EID it has advertised. The Map-Server should only advertise an EID if the site is registered and the EID is avialble. In this case, the Map-Server forwards the Map-Request as an LISP ECM to the authoritative ETR.

✎

Note When a Map-Server supports a LISP deployment that is configured for virtualization, the Map-Server must be concurrently configured as a Map-Resovler, or to use LISP-DDT. A Map-Server cannot recieve a Map-Request with an instance-id over the LISP ALT.

Examples

The following example configures IPv6 LISP Map-Server functionality on the router.

```
Router(config)# ipv6 lisp map-server
```

Related Commands

Command	Description
ipv6 lisp alt-vrf	Configure which VRF supporting the IPv6 address-family LISP should use when sending Map Requests for an IPv6 EID-to-RLOC mapping directly over the ALT.

---

ipv6 lisp proxy-etr

To configure a router to act as an IPv6 LISP Proxy Egress Tunnel Router (PETR), use the **ipv6 lisp proxy-etr** command in global configuration mode. To remove LISP PETR functionality, use the **no** form of this command.

[no] ipv6 lisp proxy-etr

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not provide PETR functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable IPv6 LISP Proxy Egress Tunnel Router (PETR) functionality on the router. PETR functionality is a special case of ETR functionality where the router accepts LISP-encapsulated packets from an ITR or PITR that are destined to non-LISP sites, de-encapsulates them, and then forwards them natively toward their non-LISP destination.

PETR services may be necessary in several cases.

1) By default when a LISP sites forwards packets to a non-LISP site natively (not LISP encapsulated), the source IP address of the packet is that of a site EID(s). When the provider side of the access network is configured with strict unicast reverse path forwarding (uRPF) it may consider these packets to be spoofed and drop them since EIDs are not advertised in the provider core network. In this case, instead of natively forwarding packets destined to non-LISP sites, the ITR encapsulates these packets using its site locator(s) as the source address and the PETR as the destination address. The assumption and necessity here is that the native connectivity of the PETR is not configured with the same uRPF or anti-spoofing restrictions as the ITR. (Note that packets destined for LISP sites will follow normal LISP forwarding processes and be sent directly to the destination ETR as normal.)

2) When a LISP IPv6 (EID) site wishes to talk to a non-LISP IPv6 site and some portion of the intermediate network does not support IPv6 (it is IPv4 only), the PETR can be used to "hop over" the address family incompatibility, assuming that the PETR has both IPv4 and IPv6 connectivity. The ITR in this case can LISP-encapsulate the IPv6 EIDs with IPv4 locators destined for the PETR, which de-

encapsulates the packets and forwards them natively to the non-LISP IPv6 site over its IPv6 connection. In this case, the use of the PETR effectively allows the LISP sites packets to traverse (hop over) the IPv4 portion of network using the LISP mixed protocol encapsulation support. This use-case also assumes the availability of a dual-stack PITR for return traffic flows.

✎

Note An NX-OS router can be configured to perform ETR and PETR functions at the same time. A router that is configured as an ETR performs a check to verify that the LISP packet inner header destination address is within the address range of a local EID prefix, whereas a router configured as a PETR does not perform this check.

✎

Note When an ITR or PITR requires the use IPv6 PETR services, it must be configured to forward IPv6 EID packets to the PETR by using the **ipv6 lisp use-petr** command.

Examples

The following example configures IPv6 LISP PETR functionality on the router.

```
Router(config)# ipv6 lisp proxy-etr
```

Related Commands

Command	Description
ipv6 lisp etr	Configures the router to act as an IPv6 LISP Egress Tunnel Router (ETR)
ipv6 lisp use-petr	Configures an ITR or PITR to use the PETR for traffic destined to non-LISP IPv6 destinations.

ipv6 lisp proxy-itr

To configure a router to act as an IPv6 LISP Proxy Ingress Tunnel Router (PITR), use the **ipv6 lisp proxy-itr** command in global configuration mode. To remove LISP PITR functionality, use the **no** form of this command.

> **[no] ipv6 lisp proxy-itr** *ipv6-local-locator* [*ipv4-local-locator*]

Syntax Description

ipv6-local-locator	The IPv6 locator address used as a source address for encapsulation of data packets, a Data Probe, or a Map-Request message.
ipv4-local-locator	(Optional) The IPv4 locator address used to as a source address for encapsulation of data packets, a Data Probe, or a Map-Request message when the locator-hash function returns a destination RLOC in the IPv4 address-family.

Defaults

By default, the router does not provide PITR functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable IPv6 LISP Proxy Ingress Tunnel Router (PITR) functionality on the router. PITR functionality is a special case of ITR functionality where the router receives native packets from non-LISP sites that are destined for LISP sites, encapsulates them, and forwards them to the ETR that is authoritative for the destination LISP site EID.

PITR services are required to provide interworking between non-LISP sites and LISP sites. For example, when connected to the Internet, a PITR acts as a gateway between the legacy Internet and the LISP enabled network. To accomplish this, the PITR must advertise one or more highly aggregated EID prefixes on behalf of LISP sites into the underlying DFZ (i.e. Internet) and act as an ITR for traffic received from the public Internet.

Any packet received by the PITR then that does not match a route from the routing table (associated with the VRF of the packet's incoming interface) or that matches the default route (0.0.0.0/0) or more-specific prefix with a null0 next-hop from the routing table (associated with the VRF for the packet's incoming interface), may be LISP encapsulated – provided the destination is a LISP destintion. Thus, in addition to configuring the **ipv6 lisp itr map-resolve**r command, a PITR must also be configured to know the EID-prefix space it is acting on behalf of. This can be accomplished in one of two ways (only one can be configured at any time).

1) When the PITR is ALT-connected, it has direct knowledge of all EID-prefix space. (See the **ipv6 lisp alt-vrf** command for details.) In this case, the PITR sends Map-Request directly on the ALT to obtain an IPv4 EID-to-RLOC mapping.

2) When the PITR is configured to use a Map-Resolver via the **ipv6 lisp itr map-resolve**r command, it must also be configured with one or more static map-cache entries indicating the EID-prefix space and with an action of **map-request**. (See the **ipv6 lisp map-cache** command for details.) In this case, the PITR sends a LISP Encapsulated Control Message (ECM) to the configured Map-Resolver to obtain an IPv4 EID-to-RLOC mapping.

The PITR caches the resultant IPv6 EID-to-RLOC mapping information returned by the associated Map-Reply in its map-cache. Subsequent packets destined to the same IPv6 EID-prefix block are then LISP-encapsulated according to this IPv6 EID-to-RLOC mapping entry. A Negative Map-Reply indicates that the destination is not a LISP site and the PITR forwards these packets natively.

Note A PITR may also be concurrently configured on the same device as a stand-alone MR/MS device, simplifying the overall LISP architecture.

Note An NX-OS router can be configured to perform ITR and PITR functions at the same time. (An IOS router cannot be configured to perform both ITR and PITR functions at the same time). A router that is configured as an ITR performs a check to verify that the source of any packet intended for LISP encapsulation is within the address range of a local EID prefix, whereas a router configured as a PITR does not perform this check. If a router is configured as an ITR and as a PITR, preference goes to PITR functionality for packet processing.

When PITR services are enabled using the **ipv6 lisp proxy-itr** command, the PITR LISP-encapsulated packets when it sends a data packet to a LISP site. The outer (LISP encapsulation) header address-family and source address are determined as follows:

- When the locator-hash function returns a destination RLOC within the IPv4 address-family, the address *ipv4-local-locator* is used as the source address from the locator namespace, and
- When the locator-hash function returns a destination RLOC within the IPv6 address-family (assuming the optional address *ipv6-local-locator* is entered), it will be used as a source locator for encapsulation.

Examples

The following example configures LISP PITR functionality on the router, and to encapsulate packets using an IPv6 source locator of 2001:db8:bb::1 and an IPv4 source locator of 10.1.1.1.

```
Router(config)# ipv6 lisp proxy-itr 2001:db8:bb::1 10.1.1.1
```

Related Commands

Command	Description
ipv6 lisp alt-vrf	Configures which VRF supporting the IPv6 address-family LISP should use when sending Map Requests for an IPv6 EID-to-RLOC mapping directly over the ALT.
ipv6 lisp itr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR)

ipv6 lisp shortest-eid-prefix-length

To configure the shortest IPv6 EID-prefix mask-length that is acceptable to an ITR or PITR in a received Map-Reply message or to an ETR in the mapping-data record of a received Map-Request, use the **ipv6 lisp shortest-eid-prefix-length** command in global configuration mode. To return to the default configuration, use the **no** form of this command.

> [no] ipv6 lisp shortest-eid-prefix-length *IPv6-EID-prefix-length*

Syntax Description

IPv6-EID-prefix-length	The shortest IPv6 EID prefix-length accepted from a Map-Reply or data record in a Map-Request. (0 to 128)

Defaults

By default, the shortest IPv6 EID prefix length accepted is a /48.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When an ITR or PITR receives a Map-Reply message, the mapping data it contains includes the EID mask-length for the returned EID prefix. By default, the shortest EID prefix mask-length accepted by an ITR or PITR for an IPv6 EID prefix is a /48. The global command **ip lisp shortest-eid-prefix-length** can be used to change this default when it is advantageous to do so. For example, it may be necessary for a PITR to accept a shorter (coarser) prefix if one exists.

Similarly, when an ETR receives a Map-Request message, it may contain a mapping data record that the ETR can cache and possible use to forward traffic, depending on the configuration of the **ip lisp etr accept-map-request-mapping** command. The global command **ip lisp shortest-eid-prefix-length** can also be used in this case to change the shortest prefix length accepted by the ETR. In this case, the check for the shortest EID-prefix mask-length is done prior to the verifying Map-Request, if also configured. That is, if the EID-prefix mask-length

is less than the configured value, the verifying Map-Request would not be sent and the mapping data would not be accepted.

Examples

The following example configures the router to accept a minimum IPv6 EID-prefix length of /40.

```
Router(config)# ipv6 lisp shortest-eid-prefix-length 40
```

Related Commands

Command	Description
ipv6 lisp etr	Configures the router to act as an IPv6 LISP Egress Tunnel Router (ETR).
ipv6 lisp itr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR).
ipv6 lisp proxy-itr	Configures the router to act as an IPv6 LISP Proxy Ingress Tunnel Router (PITR)

ipv6 lisp translate

To configure IPv6 LISP translation mapping, use the **ipv6 lisp translate** command in global configuration mode. To remove IPv6 LISP translation mappings and return to the default value, use the **no** form of this command.

> **[no] ipv6 lisp translate inside** *IPv6-inside-EID* **outside** *IPv6-outside-EID*

Syntax Description

inside	Indicates that the inside (non-routable) IPv6 EID prefix follows.
IPv6-inside-EID	The non-routable IPv6 address associated with an inside EID prefix.
outside	Indicates that the outside (routable) IPv6 EID prefix follows.
IPv6-outside-EID	The routable IPv6 address associated with an outside EID prefix.

Defaults

By default, a LISP device does not perform address translation.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When a LISP ITR or ETR is configured with a non-routable EID prefix and it is desired to replace it with a routable EID prefix, this can be accomplished by configuring the **ipv6 lisp translate** command. When this command is configured, a LISP device acting as an ITR and detecting a non-routable EID in the source IPv6 address field, as referred to by the **inside** keyword, will replace it with the routable EID referred to by the **outside** keyword. In the opposite direction when acting as an ETR, it will replace the routable EID referred to by the **outside** keyword with the non-routable EID referred to by the **inside** keyword.

✎

Note The outside EID address may be assigned to the router itself, in which case it responds to ARP requests, ICMP echo-requests (ping) and any other packet sent to this address. When the outside EID is not assigned to the device, the address does not answer ARP requests.

This feature may be useful when a site upgrades to LISP but wishes to continue to communicate with non-LISP sites. An alternative approach for providing communications between LISP and non-LISP sites is to use Proxy-ITR services. Refer to the **ipv6 lisp proxy-itr** command for further details. Both proxy-ITR and NAT translation services, commonly referred to as Interworking services, are described in *draft-ietf-lisp-interworking-00*.

Examples

The following example configures LISP to translate the inside address 2001:db8:aa::1 to the outside address 2001:db8:bb::1.

```
Router(config)# ipv6 lisp translate inside 2001:db8:aa::1 outside 2001:db8:bb::1
```

Related Commands

Command	Description
ipv6 lisp etr	Configures the router to act as an IPv6 LISP Egress Tunnel Router (ETR).
ipv6 lisp itr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR).
ipv6 lisp proxy-itr	Configures the router to act as an IPv6 LISP Proxy Ingress Tunnel Router (PITR)

---

ipv6 lisp use-bgp-locators

To configure LISP to use iBGP routes as EID-prefixes and their BGP RIB next-hop addresses as locators to dynamically create map-cache entries, use the **ipv6 lisp use-bgp-locators** command in global configuration mode. To remove this functionality, use the **no** form of this command.

> **[no] ipv6 lisp use-bgp-locators** [**route-map** *route-map-name*]

Syntax Description

route-map *route-map-name*	(Optional) Specifies the route-map supplying the match criteria for identifying which iBGP routes are EID-prefixes and that should use BGP RIB next-hop addresses.

Defaults

By default, the router does not enable this functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was introduced.

Usage Guidelines

In most cases, running BGP is not needed or even desirable when deploying LISP sites. The LISP mapping system provides all necessary information for performing EID forwarding, and the added complexity of BGP is typically not useful. There are cases, however, where adding BGP be advantageous and can simplify LISP deployments and operations. One example is the case where BGP running on an edge router in a private core has knowledge of EID prefixes at other sites. Since the BGP next-hops for theses EID prefixes represent their RLOCs, LISP simply needs to use these BGP-known EID prefixes and next-hops in order to encapsulate packets between sites. This functionality is called LISP On Demand Forwarding (LISP-ODF).

To configure LISP-ODF, which enables the device to dynamically create map-cache entries use iBGP routes as EID-prefixes and their BGP RIB next-hop addresses as locators, use the **ipv6 lisp use-bgp-locators** command. When implementing this functionality, the following design details should be considered:

- When an architeture implements LISP-ODF, it no longer is required to register EID prefixes with an mapping system (Map-Server), as would typically be the case since all EID prefixes and their locators are available directly in BGP. LISP map-cache entries are dynamically built using BGP information by configuring the **ipv6 lisp use-bgp-locators** command.
- Because a LISP device is not configured with database-mapping entries for its own EID prefixes or configured to register these EID prefixes with a Map-Server, it is not necessary to configure it as an ETR or ITR. The LISP device must simply be configured as a Proxy ITR (PITR) to encapsulate LISP packets and as a Proxy ETR (PETR) to decapsulate LISP packets.
- Map-cache entries dynamically created via LISP-ODF automatically have a priority of 1 and weight of 100 in all cases.

✎

Note A LISP-ODF router (i.e. one using **ipv6 lisp use-bgp-locators**) does not register any EID-prefixes to a Map-Server unless it is also doing ITR/ETR services for configured database-mappings.

Use the **route-map** *route-map-name* command to specifiy a route-map with match criteria for identifying which iBGP routes are EID-prefixes and that should be included, along with their BGP next-hop addresses, as dynamically created map-cache entries. LISP will then only encapsulate packets to these prefixes. Other remaining iBGP prefixes are assumed to be non-LISP and packets to these will be forwarded natively.

✎

Note Because BGP next-hop addresses are used as locators, BGP may need to be configured with **next-hop-self** to ensure that the proper addresses are available to be used as locators.

Examples

The following example configures IPv4 LISP Map-Resolver functionality on the router.

```
Router(config)# feature bgp
Router(config)# feature lisp
Router(config)# router bgp 65001
Router(config-router)# router-id 10.10.10.10
Router(config-router)# address-family ipv6 unicast
Router(config-router-af)# exit
Router(config-router)# neighbor 2001:db8:ff::f remote-as 65002
Router(config-router-neighbor)# address-family ipv6 unicast
Router(config-router-neighbor-af)# exit
Router(config-router-neighbor)# exit
Router(config-router)# exit
Router(config)# feature lisp
Router(config)# ipv6 lisp proxy-itr 2001:db8:ff::1
Router(config)# ipv6 lisp proxy-etr
Router(config)# ipv6 lisp use-bgp-locators
```

Related Commands

Command	Description
ip lisp proxy-itr	Configures the router to act as an IPv4 LISP Proxy Ingress Tunnel Router (PITR)
ip lisp proxy-etr	Configures the router to act as an IPv4 LISP Proxy Egress Tunnel Router (PETR)

ipv6 lisp proxy-itr	Configures the router to act as an IPv4 LISP Proxy Ingress Tunnel Router (PITR)
ipv6 lisp proxy-etr	Configures the router to act as an IPv6 LISP Proxy Ingress Tunnel Router (PETR)

ipv6 lisp use-petr

To configure a router to use an IPv6 LISP Proxy Egress Tunnel Router (PETR), use the **ipv6 lisp use-petr** command in global configuration mode. To remove the use of a LISP PETR, use the **no** form of this command.

      [no] ipv6 lisp use-petr *locator-address*

Syntax Description

locator-address	IPv4 or IPv6 locator address of the PETR.

Defaults

By default, the router does not use PETR services.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable the router to use IPv6 Proxy Egress Tunnel Router (PETR) services. When the use of PETR services is enabled, instead of natively forwarding packets destined to non-LISP sites, these packets are LISP-encapsulated and forwarded to the PETR, where these packets are then de-encapsulated, and then forwarded natively toward the non-LISP destination. An ITR or PITR can be configured to use PETR services.

PETR services may be necessary in several cases.

1) By default when a LISP sites forwards packets to a non-LISP site natively (not LISP encapsulated), the source IP address of the packet is that of a site EID(s). When the provider side of the access network is configured with strict unicast reverse path forwarding (uRPF) it may consider these packets to be spoofed and drop them since EIDs are not advertised in the provider core network. In this case, instead of natively forwarding packets destined to non-LISP sites, the ITR encapsulates these packets using its site locator(s) as the source address and the PETR as the destination address. The assumption and necessity here is that the native connectivity of the PETR is not configured with the same uRPF or anti-spoofing restrictions as the ITR. (Note that packets destined for LISP sites will follow normal LISP forwarding processes and be sent directly to the destination ETR as normal.)

2) When a LISP IPv6 (EID) site wishes to talk to a non-LISP IPv6 site and some portion of the intermediate network does not support IPv6 (it is IPv4 only), the PETR can be used to "hop over" the address family incompatibility, assuming that the PETR has both IPv4 and IPv6 connectivity. The ITR in this case can LISP-encapsulate the IPv6 EIDs with IPv4 locators destined for the PETR, which de-encapsulates the packets and forwards them natively to the non-LISP IPv6 site over its IPv6 connection. In this case, the use of the PETR effectively allows the LISP sites packets to traverse (hop over) the IPv4 portion of network using the LISP mixed protocol encapsulation support. This use-case also assumes the availability of a dual-stack PITR for return traffic flows.

LISP-77

✎

Note Because LISP supports mixed protocol encapsulations, the locator specified for the PETR in this case can either be an IPv4 or IPv6 address. Up to eight PETRs can be configured per address-family.

Examples

The following example configures an ITR to use the PETR with the IPv4 locator of 10.1.1. In this case, LISP site IPv6 EIDs destined for IPv6 non-LISP sites will be encapsulated in an IPv4 LISP header to the PETR located at 10.1.1.1. When it receives these packets, the PETR will strip the IPv4 LISP encapsulation and natively forward the IPv6 packets toward their IPv6 non-LISP destination. (This assumes that the PETR supports dual-stack connectivity.)

```
Router(config)# ipv6 lisp use-petr 10.1.1.1
```

Related Commands

Command	Description
ipv6 lisp proxy-etr	Configures the router to act as an IPv6 LISP Proxy Egress Tunnel Router (PETR)

---

lisp instance-id

To configure an instance-id to be associated with EID-prefixes for a LISP xTR, use the **lisp instance-id** command in global configuration mode. To disable this functionality, use the **no** form of this command.

   [no] lisp {instance-id *iid*}

Syntax Description

instance-id *iid*	Configure the instance-id for this xTR (value between 1 and 16777215).

Defaults

By default, an xTR is not configured to use an instance-id.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(3.lisp)	This command was introduced.

Usage Guidelines

Virtualization support is currently is available in LISP ITR/ETRs (xTRs), PITRs, and MS/MRs. The instance-id has been added to LISP to support virtualization.

Use this command to configure the instance-id associated with EID prefixes within the default VRF or specified VRF context on this xTR. Only one instance-id can be configured per EID VRF context. When an instance-id is configured, this instance-id will be included with the EID-prefixes when they are registered with the Map-Server.

The Map-Server must also include the same instance-id within the EID-prefix configurations for this LISP site. Instance-ID's are configured on the MS using the **eid-prefix** command within the **lisp site** command mode.

✎

Note Virtualization support is not currently available for the LISP ALT, which means that it is also not supported on LISP PITRs.

Examples

The following example configures an instance-ID of 123 in the default VRF on this xTR.

```
Router(config)# vrf context default
Router(config-vrf)# lisp instance-id 123
Router(config)# ipv6 lisp database-mapping 2001:db8:a::/48 10.10.10.1 priority 1 weight 1
```

The following example configures an instance-id 111 in the VRF context named **red** on this xTR.

```
Router(config)# vrf context red
Router(config-vrf)# lisp instance-id 111
Router(config-vrf)# ipv6 lisp database-mapping 2001:db8:a::/48 10.10.10.1 priority 1 weight 1
```

Related Commands

Command	Description
EID-prefix	LISP Map-Server site configuration mode subcommand for configuring the EID-prefix and associated instance-id for a LISP Site.

lisp loc-reach-algorithm

To configure a LISP locator reachability algorithm, use the **lisp loc-reach-algorithm** command in global configuration mode. To disable this functionality, use the **no** form of this command.

> **[no] lisp loc-reach-algorithm** {**count-tcp | echo-nonce | rloc-probing**}

Syntax Description

tcp-count	Enable the tcp-count locator reachability algorithm.
echo-nonce	Enable the echo-nonce locator reachability algorithm.
rloc-probing	Enable the rloc-probing locator reachability algorithm.

Defaults

The locator reachability algorithm rloc-probing is disabled by default by LISP.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Use this command to enable or disable the selected LISP locator reachability algorithms. When a LISP site communicates with a remote LISP site, it maintains EID-to-RLOC mapping information in its local map-cache. In order for a LISP site to maintain an accurate status of locators at remote LISP sites with which it is communicating, the xTR can be configured to use three different locator reachability algorithms, **tcp-count**, **echo-nonce**, and **rloc-probing**. Certain algorithms can only be enabled on certain devices. In addition, each algorithm has beneficial effects in certain applications but perhaps not for others. The following locator reachability algorithms and their descriptions follow:

- The **tcp-count** algorithm is most useful when the traffic between the sites is asymmetric (but also works for symmetric traffic patterns). The **count-tcp** algorithm can only be enabled on ITR and PITR devices. An ETR does not need to participate. The **count-tcp** algorithm is particularly useful in PITRs since encapsulated traffic is not returned to a PITR. When **count-tcp** is configured, an ITR will count SYN and ACK TCP packets per locator to which it encapsulates packets. Over a one-minute period, if SYNs-seen are non-zero and ACKs-seen are zero, the ITR assumes the locator is no longer reachable; the locator is marked to the down status and a switchover is made to another locator if one is available. After three minutes, the locator is brought back up and counting resumes.

- The **echo-nonce** algorithm only works when traffic is flowing in both directions between locators. The **echo-nonce** algorithm must be enabled on both an ITR and ETR to have it operate correctly. The **echo-nonce** algorithm must not be used on a PITR since the **echo-nonce** algorithm requires bidirectional traffic flows between locators and encapsulated traffic is not returned to the PITR. When **echo-nonce** is configured, every one minute, an ITR will request that the nonce it is using in encapsulated packets be echoed back from the locator it is using. If data is still arriving from the locator but the nonce is not being echoed, the ITR then assumes that the forward-path is unreachable; the locator is marked to the down status and a switchover is made to another locator if one is available. After three minutes and if data is arriving from the locator, the ITR marks the locator up and will start sending nonce requests again.

- The **rloc-probing** algorithm is the most flexible in that it works in most environments. The **rloc-probing** algorithm can be used on ITR, ETR, and PITR devices. When the **rloc-probing** algorithm is configured, the ITR sends a Map-Request to an ETR with the Probe-bit set. This solicits a Map-Reply with the Probe-bit from the ETR. The **rloc-probing** algorithm should only be used when the **tcp-count** and **echo-nonce** cannot determine the up/down status of the forwarding path, and is particularly useful for unidirectional traffic flows between two sites. In this case, an ETR that receives a Map-Request rloc-probe from an ITR can use the mapping data if supplied and if the ETR has **accept-map-request-data** configured. An ITR that receives a Map-Reply rloc-probe from an ETR can use the mapping data from the ETR's site. This can allow fast mapping data updates.

Multiple algorithms may be enabled concurrently, subject to the dependencies listed above with each algorithm.

The status associated with each locator reachability algorithm can be viewed using the **show ip lisp map-cache** or **show ipv6 lisp map-cache** commands.

Examples

The following example configures the locator reachability algorithm rloc-probing functionality on the router.

```
Router(config)# lisp loc-reach-algorithm rloc-probing
```

Related Commands

Command	Description
ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR)
ip lisp itr	Configures the router to act as an IPv4 LISP Ingress Tunnel Router (ITR)
ipv6 lisp etr	Configures the router to act as an IPv6 LISP Egress Tunnel Router (ETR)
ipv6 lisp itr	Configures the router to act as an IPv6 LISP Ingress Tunnel Router (ITR)
show ip lisp map-cache	Display the current dynamic and static IPv4 EID-to-RLOC map-cache entries.
show ipv6 lisp map-cache	Display the current dynamic and static IPv6 EID-to-RLOC map-cache entries.

lisp security

To configure an xTR or PITR to enable LISP-SEC security functionality, use the **lisp security** command in global configuration mode. To remove LISP-SEC security functionality, use the **no** form of this command.

[no] lisp security [**strong**]

Syntax Description

strong	(Optional) Indicates that LISP security should use the strong mode.

Defaults

By default, the router does not enable LISP-SEC functionality.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was introduced.

Usage Guidelines

When an ITR or PITR is configured to use a Map-Resolver for the resolution of EID-to-RLOC mappings (using the **ip lisp itr map-resolver** and **ipv6 lisp itr map-resolver** commands), the ITR or PITR will send its Map-Request in a LISP Encapsulated Control Message (ECM) to the Map-Resolver. The Map-Resolver will forward the Map-Request to the Map-Server that is authoritative for the queried EID, and the Map-Server will forward the Map-Request in a LISP Encapsulated Control Message (ECM) to the ETR. The ETR will then reply back directly to the ITR with a Map-Reply message. Normally, these EID-to-RLOC mapping resolution exchanges, carried through Map-Request and Map-Reply messages, are transmitted without integrity protection.

The LISP-SEC feature enables a set of security mechanisms that provide origin authentication, integrity, and anti-replay protection to these mapping resolution exchanges, as defined in draft-ietf-lisp-sec-00.txt. The LISP-SEC functionality also enables verification of EID prefix claims, ensuring that the entity that provides the location for the EID prefix(es) for which it is entitled to do so for.

LISP-SEC functionality is enabled by configuring the **lisp security** command on xTRs, and PITRs. Even though the command **lisp security** is not configured on a Map-Resolver (MR) or Map-Server (MS), all MRs and MSs participating within a mapping system supporting LISP-SEC must be running LISP-SEC capable software.

When the **lisp security** command is configured, the following things occur:

- An ETR registers as being "LISP-SEC capable" with its configured Map-Server(s). (This is why the Map-Server must also be running LISP-SEC capable software.)

- An ITR and PITR include the LISP-SEC security fields in the Encapsulated Control Message (ECM) header of Map-Requests sent to their configured Map-Resolver. (This is why the Map-Resolver must also be running LISP-SEC capable software.)

Note An ALT-connected ITR or PITR cannot include the LISP-SEC security fields in Map-Requests send over the ALT. At present, a LISP-SEC header can only be included when the ITR or PITR

uses a Map-Resolver. (The ability to include the LISP-SEC fields in Map-Requests send over the ALT will be included in the next NX-OS release.)

- The Map-Resolver receiving the LISP-SEC enabled ECM Map-Request from the ITR or PITR strips the ECM, adds a new ECM header referencing its own RLOC as the source address, and forwards it to the Map-Server that is authoritative for the EID being queried.

- The Map-Server receiving the LISP-SEC enabled ECM Map-Request from the Map-Resolver strips the ECM, adds a new ECM header referencing its own RLOC as the source address, and forwards it to the ETR that owns the EID being queried.

- The ETR strips the ECM, processes the Map-Request, and sends a LISP-SEC enabled Map-Reply directly to the originating ITR.

The **lisp security** command has two modes of operation known as strong-mode and weak-mode. The mode determines how an ITR or PITR handles incoming Map-Replies. The follwing describes how Map-Replies are handled by each mode:

- Use the keyword **strong** when configuring LISP-SEC (**lisp security strong**) to enable strong mode. When strong mode is enabled, the ITR/PITR requires the responding Map-Reply to be signed by the ETR. If the Map-Reply is not signed, or if the signature is not verifiable, the Map-Reply is rejected.

- Do not use the keyword **strong** when configuring LISP-SEC (**lisp security**) to enable weak mode. When weak mode is enables, the ITR/PITR will accept a Map-Reply that is signed or not signed.

Weak mode provides a transitional capability for use in networks where LISP-SEC functionality is not supported by all devices. This allows LISP-SEC enabled ITRs and PITRs to interoperate with both LISP-SEC and non LISP-SEC ETRs devices.

Note   The Map-Resolver (MR) and Map-Server (MS) do not need have a LISP-SEC configuration. However, all MR and MS devices that participate within a LISP mapping system that supports LISP-SEC must be running LISP-SEC capable software.

When interoperability with both LISP-SEC and non LISP-SEC ETR devices is required, the following considerations are important to understand:

- ETRs register if they are LISP-SEC capable with the MS. (From the perspective of the ETR, the output of the command **show [ip|ipv6] lisp** indicates whether LISP-SEC is enabled and its mode. From the perspective of the MS, the output of the command **show lisp site detail** indicates the control plane security capabilities of registered sites.) Thus, when a MS receives a LISP-SEC enabled ECM Map-Request, it will do the following:

  - When the EID being queried is located at a LISP-SEC capable ETR, the MS will forward a LISP-SEC enabled ECM Map-Request to this ETR. The ETR sends a LISP-SEC enabled Map-Reply back to the ITR.
  - When the EID being queried is located at a non-LISP-SEC capable ETR, the MS will forward a standard ECM Map-Request to this ETR. The ETR sends a standard Map-Reply back to the ITR.

- At present, when an ETR registers with the **proxy-reply** capability set (see **ip lisp etr map-server** command), the Map-Server will only send a standard Map-Reply back to the ITR, regardless of whether the ETR is LISP-SEC capable or not. When the **proxy-reply** capability is used, ITRs should be configured for weak-mode so that they accept unsigned Map-Replies.

Note   The LISP-SEC functionality is introduced in the Cisco NX-OS 5.2(0.266.lisp-52) release. The LISP-SEC functionality is not yet available in any IOS releases at the time of this writing. For further information and updates, be sure to check all appropriate release notes.

Examples

The following example configures LISP-SEC strong mode functionality on the router.

```
Router(config)# lisp security strong
```

Related Commands

Command	Description
show ip lisp	Displays the IPv4 LISP configuration status.
show ipv6 lisp	Displays the IPv6 LISP configuration status.
show lisp site	On a LISP Map-Server, displays the status of configured LISP sites.

---

lisp smr-locators

To configure an ITR to send Solicit Map Request (SMR) messages to each locator in a locator set when a dynamic-EID moves, use the **lisp smr-locators** command in global configuration mode. To remove this functionality, use the **no** form of the command.

    [no] lisp smr-locators

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not send SMR's to each locator in a locator set when a dynamic-EID moves.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r5-20)	This command was modified from hidden to visible.

Usage Guidelines

When a dynamic-EID moves to a new xTR and sends data packets to an EID at a destination LISP site, it is possible that the destination LISP site may already have a map-cache entry for the dynamic-EID that is based on its prior location. By default, normal LISP data-driven mechanisms (such as piggybacking mappings in Map-Requests) will cause the destination xTR to update its map-cache.

When the destination LISP site is multi-homed (with multiple xTRs), however, data packets may not reach all xTRs in the LISP site. When the command **lisp smr-locators** is configured, the ITR to which a dynamic-EID has moved sends Solicit Map Request (SMR) messages to each locator in a locator set (that is in an "up" state) for a destination LISP site. In this way, all xTRs at a destination LISP site will update their map-cache for the new location of the dynamic-EID.

⚠️
Caution Enabling **lisp smr-locators** can result in the generation of numerous LISP control messages, especially during numerous dynamic-EID roaming events. Use care when enabling this command.

Examples

The following example configures an ITR to send SMR's to each locator that is in an "up" state within in a locator set for a destination LISP site to which it is sending data.

```
Router(config)# lisp smr-locators
```

Related Commands

Command	Description
lisp dynamic-eid	Configures a LISP dynamic-EID roaming policy.
lisp mobility	Configure an interface on an ITR to participate in LISP VM-mobility.

LISP Interface Configuration Commands

ip lisp nat-transversal

To configure an ETR with a private locator that is sited behind a NAT device to dynamically determine its NAT-translated public locator for use in Map-Register and Map-Reply messages, use the **ip lisp nat-transversal** command in interface configuration mode. To remove this functionality, use the **no** form of this command.

> **[no] ip lisp nat-transversal**

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not dynamically determine its public global routing locator address.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When an ETR is sited behind a NAT device, its routing locator belongs to the private address space that the NAT device translates to a public globally routed address. The ETR needs to know this public global locator address since this is the address that is required for use in Map-Register and Map-Reply messages.

When the **ip lisp nat-transversal** command is configured, the ETR determines its own public global locator dynamically by sending a LISP Echo-Request message to the configured Map-Server out the interface under which this command is configured. The Map-Server replies with an Echo-Reply message that includes the source address from the Echo-Request – which is the NAT-Translated public global locator address.

✎

Note The **ip lisp nat-transversal** command **MUST** be used when the **dynamic** keyword is used with the [**ip | ipv6**] **lisp database-mapping** command in order to dynamically determine the routing locator rather than statically defining it. Configuring the **ip lisp nat-transversal** command is what actually performs the process of determining the global NAT'ed routing locator address when an IPv4 routing locator is defined.

Examples

The following example configures the ETR to dynamically determine its public global routing locator when it is behind a NAT device.

```
Router(config)# interface Ethernet2/0
Router(config-if)# ip lisp nat-transversal
```

Related Commands

Command	Description
ip lisp database-mapping	Configure an IPv6 EID-to-RLOC mapping relationship and traffic policy.

ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR).

ip lisp source-locator

To configure a source locator to be used for IPv4 LISP encapsulated packets, use the **ip lisp source-locator** command in interface configuration mode. To remove the configured source locator, use the **no** form of this command.

> **[no] ip lisp source-locator** *interface*

Syntax Description

interface	The name of the interface whose IPv4 address should be used as the source locator address for outbound LISP encapsulated packets.

Defaults

The IPv4 address of the outbound interface is used by default as the source locator address for outbound LISP encapsulated packets.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When sending a LISP encapsulated packet (data or control message), a destination lookup is done to determine the appropriate outgoing interface. By default, the IPv4 address of this outgoing interface is used as the source locator for the outbound LISP encapsulated packet.

In some circumstances it may be necessary to use the IPv4 address of a different interface as the source locator for the outbound LISP encapsulated packets rather than that of the outgoing interface. For example, when an ITR has multiple egress interfaces you may configure a loopback interface for stability purposes and instruct the ITR to use the address of this loopback interface as the source locator for the outbound LISP encapsulated packets rather than one or both of the physical interface addresses. The use of this command is also important for maintaining locator consistency between the two xTRs when **rloc-probing** is used.

Examples

The following example configures the ITR to use the IPv4 address of interface Loopback0 as the source-locator when sending LISP encapsulated packets out interfaces Ethernet2/0 and Ethernet2/1.

```
Router(config)# interface Ethernet2/0
Router(config-if)# ip lisp source-locator Loopback0
Router(config-if)# interface Ethernet2/1
Router(config-if)# ip lisp source-locator Loopback0
```

Related Commands

Command	Description
ip lisp itr	Configure the router to act as an IPv4 LISP Ingress Tunnel Router (ITR)

---

ipv6 lisp nat-transversal

To configure an ETR with a private locator that is sited behind a NAT device to dynamically determine its NAT-translated public locator for use in Map-Register and Map-Reply messages, use the **ip lisp nat-transversal** command in interface configuration mode. To remove this functionality, use the **no** form of this command.

[no] ipv6 lisp nat-transversal

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the router does not dynamically determine its public global routing locator address.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When an ETR is sited behind a NAT device, its routing locator belongs to the private address space that the NAT device translates to a public globally routed address. The ETR needs to know this public global locator address since this is the address that is required for use in Map-Register and Map-Reply messages.

When the **ipv6 lisp nat-transversal** command is configured, the ETR determines its own public global locator dynamically. When configured, the ETR sends a LISP Echo-Request message to the configured Map-Server out the interface under which this command is configured. The Map-Server replies with an Echo-Reply message that includes the source address from the Echo-Request – which is the NAT-Translated public global locator address.

✎

Note The **ipv6 lisp nat-transversal** command **MUST** be used when the **dynamic** keyword is used with the [**ip | ipv6] lisp database-mapping** command in order to dynamically determine the routing locator rather than statically defining it. Configuring the **ipv6 lisp nat-transversal** command is what actually performs the process of determining the global NAT'ed routing locator address when an IPv6 routing locator is defined.

Examples

The following example configures the ETR to dynamically determine its public global routing locator when it is behind a NAT device.

```
Router(config)# interface Ethernet2/0
Router(config-if)# ipv6 lisp nat-transversal
```

Related Commands

Command	Description
ipv6 lisp database-mapping	Configure an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy.
ipv6 lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR).

ipv6 lisp source-locator

To configure a source locator to be used for IPv6 LISP encapsulated packets, use the **ipv6 lisp source-locator** command in interface configuration mode. To remove the configured source locator, use the **no** form of this command.

> **[no] ipv6 lisp source-locator** *interface*

Syntax Description

interface	The name of the interface whose IPv6 address should be used as the source locator address for outbound LISP encapsulated packets.

Defaults

The IPv6 address of the outbound interface is used by default as the source locator address for outbound LISP encapsulated packets.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When sending a LISP encapsulated packet (data or control message), a destination lookup is done to determine the appropriate outgoing interface. By default, the IPv6 address of this outgoing interface is used as the source locator for the outbound LISP encapsulated packet.

In certain circumstances it may be necessary to use the IPv6 address of a different interface as the source locator for the outbound LISP encapsulated packets rather than that of the outgoing interface. For example, when an ITR has multiple egress interfaces you may configure a loopback interface for stability purposes and instruct the ITR to use the address of this loopback interface as the source locator for the outbound LISP encapsulated packets rather than one or both of the physical interface addresses. The use of this command is also important for maintaining locator consistency between the two xTRs when **rloc-probing** is used.

Examples

The following example configures the ITR to use the IPv6 address of interface Loopback0 as the source-locator when sending LISP encapsulated packets out interfaces Ethernet2/0 and Ethernet2/1.

```
Router(config)# interface Ethernet2/0
Router(config-if)# ipv6 lisp source-locator Loopback0
Router(config-if)# interface Ethernet2/1
Router(config-if)# ipv6 lisp source-locator Loopback0
```

Related Commands

Command	Description
ipv6 lisp itr	Configure the router to act as an IPv6 LISP Ingress Tunnel Router (ITR)

---

lisp extended-subnet-mode

To configure an interface to create dynamic-EID state for hosts attached on their own subnet in order to track the movement of EIDs from one part of its subnet to another part of the same subnet, use the **lisp extend-subnet-mode** command in interface configuration mode. To remove this functionality, use the **no** form of this command.

   [no] lisp extended-subnet-mode

Syntax Description

This command has no arguments or keywords.

Defaults

By default, this command is disabled.

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(3.lisp-80)	This command was introduced.

Usage Guidelines

This command is used when a subnet is extended across a layer-3 cloud where layer-2 connectivity is maintained by a mechanism other than LISP (i.e. OTV or VPLS). This command enables dynamic-EID state to be created for hosts attached on their own subnet so remote ITRs/PITRs can track the movement of EIDs from one part of its subnet to another part of the same subnet (by LISP encapsulating to the current locator-set for the roaming dynamic-EID). The default setting for this command is disabled.

✎

Note When **lisp extended-subnet-mode** is configured on an interface, any dynamic-EID prefixes configured using **lisp mobility** commands on the same interface must be more specific prefixes than any overlapping subnet prefixes. For example, if **lisp extended-subnet-mode** is configured on an interface that has a base subnet of a /24, then when **lisp mobility** *dyn-eid-name* is configured, the EID-prefix for dynamic-EID *dyn-eid-name* must be /25 or greater.

Examples

The following example configures the interface Ethernet2/0 to use the **lisp extended-subnet-mode** command.

```
Router(config)# interface Ethernet2/0
Router(config-if)# lisp extended-subnet-mode
```

Related Commands

Command	Description
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
lisp dynamic-eid	Configures the LISP dynamic-EID roaming policy.
lisp mobility	Configures an interface on an ITR to participate in LISP VM-mobility (dynamic-EID roaming).

---

lisp mobility

To configure an interface on an ITR to participate in LISP VM-mobility (dynamic-EID roaming) for the referenced dynamic-EID policy, use the **lisp mobility** command in interface configuration mode. To remove this functionality, use the **no** form of this command.

> **[no] lisp mobility** *dynamic-EID-policy-name*

Syntax Description

dynamic-EID-policy-name	The name of the LISP dynamic-EID policy to apply to this interface.

Defaults

By default, the interface does not participate in LISP VM-mobility (dynamic-EID roaming).

Command Modes

Interface configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13) (August update)	This command was introduced.

Usage Guidelines

In order for an interface on an xTR to participate in LISP VM-mobility (dynamic-EID roaming), it must be associated by name with a specific LISP dynamic-EID roaming policy. A LISP dynamic-EID roaming policy is configured using the **lisp dynamic-eid** *dynamic-eid-policy-name* global command. This policy is then associated with an interface using the **lisp mobility** *dynamic-eid-policy-name* command, where the *dynamic-eid-policy-name* provides the association.

When a packet is received on an interface configured for LISP VM-mobility, the packet is considered a candidate for LISP VM-mobility (dynamic-EID roaming) and its source address is compared against the EID-prefix in the database-mapping entry (or entries) included as part of the referenced **lisp dynamic-eid** policy. If there is a match, the rules associated with LISP dynamic-EID roaming are applied. If there is no match, the packet is forwarded natively (i.e. not LISP-encapsulated).

LISP-90

Multiple **lisp mobility** commands referring to different *dynamic-EID-policy-name* instances can be applied to the same interface. Packets received on the interface will be compared against all policies until a match is found or the packet discarded.

⚠️

Caveats In this release of LISP VM-Mobility, the following caveats apply:

- When a dynamic-EID will be roaming across subnets, the dynamic-EID prefix must be "more-specific" than the subnet configured on the interface.
- All dynamic-EIDs must be configured with a common MAC address, and an interface route to the "default router." For example, for a linux/unix host, the following configuration will be used:

```
ifconfig eth0 <eid-address> netmask 255.255.255.255
route add default <any-router-address>
arp -s <any-router-address> 00:00:0e:1d:01:0c
```

- All LISP VM-Router interfaces (the interface the dynamic-EID will roam to) must have the same MAC address. Interfaces can be configured with the following command:
    ```
    mac-address 0000.0e1d.010c
    ```
    Note that any MAC address can be used; the MAC address in the example above, which approximates "EID" (0e1d) and "LOC" (010c), is used just an example.

✎

Note This feature is available for IPv4 only at this time. Support for IPv6, including necessary changes for IPv6 ND has not yet been implemented.

✎

Note When **lisp extended-subnet-mode** is configured on an interface, any dynamic-EID prefixes configured using **lisp mobility** commands on the same interface must be more specific prefixes than any overlapping subnet prefixes. For example, if **lisp extended-subnet-mode** is configured on an interface that has a base subnet of a /24, then when **lisp mobility** *dyn-eid-name* is configured, the EID-prefix for dynamic-EID *dyn-eid-name* must be /25 or greater.

Examples

The following example configures the interface Ethernet2/0 to use the **Roamer-1** policy defined under the LISP dynamic-EID configuration.

```
Router(config)# interface Ethernet2/0
Router(config-if)# lisp mobility Roamer-1
```

Related Commands

Command	Description
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
lisp dynamic-eid	Configures the LISP dynamic-EID roaming policy.
lisp extended-subnet-mode	Configures an interface to create dynamic-EID state for hosts attached on their own subnet to track EID movement from one part of the subnet to another part of the same subnet

LISP Site Configuration Commands

lisp site

To configure a LISP site and enter site configuration mode on a LISP Map-Server, use the **lisp site** command in global configuration mode. To remove the LISP site, use the **no** form of this command.

> **[no] lisp site** *site-name*

Syntax Description

site-name	Locally significant name assigned to a LISP site.

Defaults

By default, no LISP sites are configured.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

For a LISP ETR to properly register with a Map-Server, the Map-Server must already have been configured with certain LISP site attributes that match those of the ETR. At a minimum, this includes the EID-prefix(es) to be registered by the ETR, and a shared authentication key. On the ETR, these attributes are configured using the **[ip|ipv6] lisp database-mapping** and **[ip|ipv6] lisp etr map-server** commands.

When the **lisp site** command is entered, the referenced LISP site is created and you are placed in the site configuration mode. In this mode, all attributes associated with the referenced LISP site can be entered.

Examples

The following example configures the LISP site named 'Customer-1' and then enters the site command mode.

```
Router(config)# lisp site Customer-1
Router(config-lisp-site)#
```

Related Commands

Command	Description
ip lisp database-mapping	Configure an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy.
ip lisp etr map-server	Configured the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv4 EID prefixes.
ipv6 lisp database-mapping	Configure an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy.
ipv6 lisp etr map-server	Configured the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv6 EID prefixes.

allowed-locators

To configure a list of locators that are allowed in a Map-Register message sent by an ETR when registering to the Map-Server, use the **allowed-locator** command in site configuration mode. To remove the locators, use the **no** form of this command.

[no] allowed-locator {*rloc1* [*rloc2* [*rloc3* [*rloc4*]]]}

Syntax Description

rloc1	IPv4 or IPv6 Routing Locator (RLOC) allowed within Map-Registration message.
rloc2, rloc3, rloc4	(Optional) Additional IPv4 or IPv6 RLOCs allowed within Map-Registration message.

Defaults

By default, allowable locators are not defined and the Map-Server will accept any locators.

Command Modes

LISP site configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When a LISP ETR registers with a Map-Server, it sends a Map-Register message that contains, among other things, one or more EID-prefixes and routing locators that the ETR is configured to use. After verifying the authentication data, the Map-Server checks the presented EID-prefixes against those configured on the Map-Server. If they agree, the Map-Register is accepted and the ETR registration is completed.

The Map-Server default behavior can be further constrained such that the ETR can only register using specific routing locators. To enable this functionality, configure the **allowed-locator** command in LISP site configuration mode. When the **allowed-locator** command is used, the Map-Register message from the ETR must contain the same locators that are listed in the Map-Server lisp site configuration. If the list in the Map-Register does not match the one configured on the Map-Server, the Map-Register message is not accepted and the ETR is not registered. Up to four IPv4 or IPv6 routing locators (total) may be configured.

Note When **allowed-locators** is configured, an exact match for all locators or a subset of all locators listed on the Map-Server within the lisp site configuration **MUST** also appear in the Map-Register message sent by the ETR for it to be accepted.

Examples

The following example configures the IPv4 address 172.16.1.1 and IPv6 address 2001:db8:bb::1 as allowable locators for the LISP site Customer-1. When Customer-1 registers with this Map-Server, at least one or both of the configured locators must be included in the Map-Registration for the site to register.

```
Router(config)# lisp site Customer-1
Router(config-lisp-site)# allowed-locator 172.16.1.1 2001:db8:bb::1
```

Related Commands

Command	Description

LISP-93

lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
show lisp site	Display registered LISP sites on a Map Server.

authentication-key

To configure the password used to create the SHA-1 HMAC hash for authenticating the Map-Register message sent by an ETR when registering to the Map-Server, use the **authentication-key** command in site configuration mode. To remove the password, use the **no** form of this command.

> **[no] authentication-key** *key-type password*

Syntax Description

key-type	Specifies how the key-type that the following SHA-1 password (key) is encoded. Type (0) indicates that a cleartext password follows; Type (3) indicates that a 3DES encrypted key follows; Type (7) indicates that a Cisco Type 7 encrypted password follows.
password	The password used to create the SHA-1 HMAC hash when authenticating the Map-Register message sent by the ETR.

Defaults

By default, no LISP sites authentication key is configured.

Command Modes

LISP site configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When a LISP ETR registers with a Map-Server, the Map-Server must already have been configured with certain LISP site attributes that match those of the ETR. This includes a shared password that is used to create the SHA-1 HMAC hash that the Map-Server uses to validate the authentication data presented in the Map-Register message. On the ETR, this password is configured with the **[ip|ipv6] lisp etr map-server** command.

On the Map-Server, the password is configured as part of the lisp site configuration process. To enter the lisp site password, configure the **authentication-key** command in LISP site configuration mode. The SHA-1 HMAC password may be entered in unencrypted (cleartext) form or encrypted form. To enter an unencrypted password, specify a key-type value of 0. To enter a 3DES-encrypted password, specify a key-type value of 3. To enter a Cisco-encrypted password, specify a key-type value of 7.

⚠️

Caution Map-Server authentication keys entered in cleartext form will automatically be converted to Type 3 (encrypted) form.

✎

Note The Map-Server and ETR must be configured with matching passwords for the Map-Registration process to successfully complete. When a LISP site successfully completes the Map-Registration process, its

LISP-94

attributes will be displayed by the **show lisp site** command. If the Map-Registration process is unsuccessful, the site will not be display.

Examples

The following example configures the LISP site named 'Customer-1' and then enters the site command mode. The shared password *s0m3-s3cr3t-k3y* is then entered in cleartext form.

```
Router(config)# lisp site Customer-1
Router(config-lisp-site)# authentication-key 0 s0m3-s3cr3t-k3y
```

Related Commands

Command	Description
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
ip lisp etr map-server	Configured the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv4 EID prefixes.
ipv6 lisp etr map-server	Configured the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv6 EID prefixes.
show lisp site	Display registered LISP sites on a Map Server.

description

To configure a description to a LISP site configuration, use the **description** command in site configuration mode. To remove the reference to a LISP site, use the no form of this command.

> **[no] lisp site** *description*

Syntax Description

description	Description listed with the associated LISP site.

Defaults

By default, no LISP site description is defined.

Command Modes

LISP site configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

On the Map-Server, when the **lisp site** command is entered, you are placed in the site sub-command mode. In this mode, a description to be associated with the referenced LISP site can be entered using the **description** command. This description will be displayed by the **show lisp site** command.

Examples

The following example configures the description string for the LISP site named 'Customer-1'.

```
Router(config)# lisp site Customer-1
Router(config-lisp-site)# description Customer-1 Site Information
```

Related Commands

Command	Description
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
show lisp site	Display registered LISP sites on a Map Server.

---

eid-prefix

To configure a list of EID-prefixes that are allowed in a Map-Register message sent by an ETR when registering to the Map-Server, use the **eid-prefix** command in site configuration mode. To remove the locators, use the **no** form of this command.

[no] eid-prefix *EID-prefix* **[instance-id** *iid*] [**route-tag** *tag*] [**accept-more-specifics**]

Syntax Description

EID-prefix	IPv4 or IPv6 EID prefix associated with the LISP site.
instance-id *iid*	(Optional) EID instance-ID
route-tag *tag*	(Optional) Route tag associated with this EID-prefix.
accept-more-specifics	(Optional) Route tag associated with this EID-prefix.

Defaults

By default, EID-prefixes are not defined for a LISP site.

Command Modes

LISP site configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.0(1.13) (August update)	This command updated to include **accept-more-specifics**
Cisco NX-OS Release 5.0(3.lisp)	This command updated to include **instance-id**

Usage Guidelines

When a LISP ETR registers with a Map-Server, it sends a Map-Register message that contains, among other things, one or more EID-prefixes that the ETR is configured to be authoritative for. On the ETR, these EID-prefixes are configured using the **[ip|ipv6] lisp database-mapping** command. These same EID-prefixes must also be configured on the Map-Server in order for the ETR to properly register. On the Map-Server, these EID-prefixes are configured using the **eid-prefix** command in lisp site configuration mode.

When the registering ETR enables a LISP instance-id by using the **lisp instance-id** command, the Map-Server must also include this same instance-id within the EID-prefix configurations for this LISP site using the **instance-id** keyword and *iid* value as part of the **eid-prefix** command.

The same EID-prefix(es), and instance-id when applicable, must be configured on Map-Server and the ETR in order for the ETR to be registered, and for these EID-prefixes to be advertised by LISP. After verifying the

LISP-96

authentication data, the Map-Server compares the EID-prefixes within the Map-Register message against those configured on the Map-Server for the LISP site. If they agree, the Map-Register is accepted and the ETR registration is completed. If the EID-prefixes in the Map-Register message do not match those configured on the Map-Server, the Map-Register message is not accepted and the ETR is not registered.

> **Note** A Map-Register message sent by an ETR contains all of the EID prefixes that the ETR is authoritative for. All of these EID prefixes MUST be listed on the Map-Server within the lisp site configuration for the Map-Register message sent by the ETR to be accepted. If the list in the Map-Register does not match the one configured on the Map-Server, the Map-Register message is not accepted and the ETR is not registered.

When a LISP site successfully completes the Map-Registration process, its attributes will be displayed by the **show lisp site** command. If the Map-Registration process is unsuccessful, the site will not be display.

When **route-tag** keyword is used, a tag value is associated with the EID-prefix being configured. This tag value may be useful for simplifying processes that populate the URIB or U6RIB alt-vrf, as for example by means of a route-map policy defined to match this tag for BGP redistribution of these EID-prefixes into the vrf.

When the **accept-more-specifics** keyword is used, any EID-prefix that is more specific then the EID-prefix configured will be accepted and tracked. The **accept-more-specifics** keyword is mainly intended for LISP VM-Mobility (dynamic-EID roaming). When a dynamic-EID moves from one LISP-VM router to another, the registration of the dynamic-EID to a new locator is performed to the Map-Server. The use of this keyword in the configuration avoids the need to configure an EID-prefix for each dynamic-EID that is capable of roaming.

Examples

The following example configures the IPv4 EID-prefix 192.168.1.0/24 and the IPv6 EID-prefix 2001:db8:aa::/48, each with the route-tag 123, for the LISP site Customer-1.

```
Router(config)# lisp site Customer-1
Router(config-lisp-site)# eid-prefix 192.168.1.0/24 route-tag 123
Router(config-lisp-site)# eid-prefix 2001:db8:aa::/48 route-tag 123
```

The following example configures the IPv4 EID-prefix 192.168.2.0/24 for the LISP site Roamer-1 and adds the **accept-more-specific** keyword. In this case, the host-prefix 192.68.2.12/32, for example, could register according to this configuration.

```
Router(config)# lisp site Roamer-1
Router(config-lisp-site)# eid-prefix 192.168.2.0/24 accept-more-specifics
```

The following example configures the IPv4 EID-prefix 192.168.1.0/24 with the instance-id of 123 for the LISP site Customer-2.

```
Router(config)# lisp site Customer-2
Router(config-lisp-site)# eid-prefix 192.168.1.0/24 instance-id 123 route-tag 123
```

Related Commands

Command	Description
ip lisp etr map-server	Configured the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv4 EID prefixes.
ipv6 lisp etr map-server	Configured the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv6 EID prefixes.
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
lisp dynamic-eid	Configures the LISP dynamic-EID roaming policy.
lisp mobility	Associates a LISP dynamic-EID roaming policy to an interface.

LISP VM-Mobility Configuration Commands

lisp dynamic-eid

To configure a LISP VM-Mobility (dynamic-EID roaming) policy and enter dynamic-EID configuration mode on an xTR, use the **lisp dynamic-eid** command in global configuration mode. To remove the LISP dynamic-EID policy, use the **no** form of this command.

      [no] lisp dynamic-eid *dynamic-EID-policy-name*

Syntax Description

dynamic-EID-policy-name	The name of the LISP dynamic-EID policy.

Defaults

By default, no LISP dynamic-eid policies are configured.

Command Modes

Global configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13) (August update)	This command was updated.

Usage Guidelines

To configure LISP VM-Mobility, you must create a dynamic-EID roaming policy that can be referenced by the **lisp mobility** *dynamic-eid-policy-name* interface command. When the **lisp dynamic-eid** *dynamic-EID-policy-name* command is typed, the referenced LISP dynamic-EID policy is created and you are placed in the dynamic-EID configuration mode. In this mode, all attributes associated with the referenced LISP dynamic-EID policy can be entered.

⚠
Caveats In this release of LISP VM-Mobility, the following caveats apply:
- When a dynamic-EID will be roaming across subnets, the dynamic-EID prefix must be "more-specific" than the subnet configured on the interface.
- All dynamic-EIDs must be configured with a common MAC address, and an interface route to the "default router." For example, for a linux/unix host, the following configuration will be used:

```
ifconfig eth0 <eid-address> netmask 255.255.255.255
route add default <any-router-address>
arp -s <any-router-address> 00:00:0e:1d:01:0c
```

- All LISP VM-Router interfaces (the interface the dynamic-EID will roam to) must have the same MAC address. Interfaces can be configured with the following command:
  ```
  mac-address 0000.0e1d.010c
  ```
  Note that any MAC address can be used; the MAC address in the example above, which approximates "EID" (0e1d) and "LOC" (010c), is used just an example.

Note This feature is available for IPv4 only at this time. Support for IPv6, including necessary changes for IPv6 ND has not yet been implemented.

Note When **lisp extended-subnet-mode** is configured on an interface, any dynamic-EID prefixes configured using **lisp mobility** commands on the same interface must be more specific prefixes than any overlapping subnet prefixes. For example, if **lisp extended-subnet-mode** is configured on an interface that has a base subnet of a /24, then when **lisp mobility** *dyn-eid-name* is configured, the EID-prefix for dynamic-EID *dyn-eid-name* must be /25 or greater.

Examples

The following example configures the LISP dynamic-EID policy named **Roamer-1** and then enters dynamic-EID configuration mode.

```
Router(config)# lisp dynamic-eid Roamer-1
Router(config-lisp-dynamic-eid)#
```

Related Commands

Command	Description
lisp mobility	Configure an interface on an ITR to participate in LISP VM-mobility (dynamic-EID roaming)

---

database-mapping

To configure a IPv4 or IPv6 dynamic-EID-to-RLOC mapping relationship and its associated traffic policy use the **database-mapping** command in dynamic-EID configuration mode. To remove the configured database mapping, use the **no** form of this command.

> **[no] database-mapping** *dynamic-EID-prefix locator* **priority** *priority* **weight** *weight*

Syntax Description

dynamic-EID-prefix	The IPv4 or IPv6 dynamic-EID prefix and length to be registered as a roaming EID for this policy.
locator	The IPv4 or IPv6 Routing Locator (RLOC) associated with this EID-prefix
priority *priority*	The priority (value between 0 and 255) assigned to the RLOC. Since only a single locator can be specified for dynamic-EIDs, the priority should be set to 1 (but doesn't matter).
weight *weight*	The weight (value between 0 and 100) assigned to the locator. Since only a single locator can be specified for dynamic-EIDs, the priority should be set to 100 (but doesn't matter).

Defaults

No dynamic-EID database entries are defined by default.

Command Modes

Dynamic-EID configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13) (August update)	This command was updated.

Usage Guidelines

When a dynamic-EID policy is configured, you must specify the dynamic-EID-to-RLOC mapping relationship and its associated traffic policy to use for each permitted prefix. When a packet is received on an interface on which the **lisp mobility** command has been applied, the source address of the packet is compared against the EID configured in the **database-mapping** entry (or entries) of the referenced **lisp dynamic-eid** *dynamic-EID-policy-name* that matches the **lisp mobility** *dynamic-EID-policy-name*.

When a dynamic-EID match is discovered, the dynamic-EID will be registered to the Map-Server with a 3-tuple of (*locator*, *priority*, *weight*). Multiple **database-mapping** entry commands may be used to make up the locator-set for a *dynamic-EID-prefix*. Both *dynamic-EID-prefix* and *locator* can be an IPv4 or IPv6 addresses.

✎

Note   All **database-mapping** dynamic-EID subcommands must be consistent on all LISP-VM routers supporting the same roaming dynamic-EID.

Examples

The following example configures the LISP dynamic-EID policy named **Roamer-1**, enters dynamic-EID configuration mode, and then configures the IPv4 dynamic-EID prefix 172.16.1.1/32 with IPv4 locator 10.1.1.1 and a priority and weight of 1 and 100 respectively.

```
Router(config)# lisp dynamic-eid Roamer-1
Router(config-lisp-dynamic-eid)# database-mapping 172.16.1.1/32 10.1.1.1 priority 1 weight
100
```

Related Commands

Command	Description
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
lisp mobility	Configure an interface on an ITR to participate in LISP VM-mobility (dynamic-EID roaming)

---

instance-id

To configure an instance-id to be associated with EID-prefixes configured for this dynamic-EID policy, use the **instance-id** command in dynamic-EID configuration mode. To disable this functionality, use the **no** form of this command.

[no] instance-id *iid*

Syntax Description

iid	Configure the instance-id for this xTR (value between 1 and 16777215).

Defaults

By default, an instance-id is not configured for a dynamic-EID policy.

Command Modes

Dynamic-EID configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(3.lisp)	This command was introduced.

Usage Guidelines

Virtualization support is currently is available in LISP ITR/ETRs (xTRs), PITRs, and MS/MRs. The instance-id has been added to LISP to support virtualization.

Use this command to configure the instance-id associated with EID-prefixes within the default VRF or specified VRF context configured for this dynamic-EID policy. This allows ETRs to register multiple overlapping EID-prefixes in a segmented manner by using the instance-id as the distinguisher. Only one instance-id may be configured for each dynamic-EID policy. When an instance-id is configured, this instance-id will be included with the EID-prefixes when they are registered with the Map-Server. The Map-Server must also include the same instance-id within the EID-prefix configurations for this LISP site. Instance-ID's are configured on the MS using the **eid-prefix** command within the **lisp site** command mode.

✎
Note Virtualization support is not currently available for the LISP ALT, which means that it is also not supported on LISP PITRs.

Examples

The following example configures an instance-ID of 123 for the dynamic-EID policy Roamer-1.

```
Router(config)# lisp dynamic-eid Roamer-1
Router(config-lisp-dynamic-eid)# instance-id 123
```

Related Commands

Command	Description
EID-prefix	LISP Map-Server site configuration mode subcommand for configuring the EID-prefix and associated instance-id for a LISP Site.

---

map-notify-group

To configure a discovering LISP-VM router to send a Map-Notify message to other LISP-VM routers within the same Data Center site so that they can also determine the location of the dynamic-EID, use the **map-notify-group** command in dynamic-EID configuration mode. To remove this functionality, use the **no** form of this command.

> [no] **map-notify-group** *IPv4-group-address*

Syntax Description

IPv4-group-address	The IPv4 multicast group address used for both sending and receiving site-based Map-Notify multicast messages.

LISP-101

Defaults

By default, this command is disabled.

Command Modes

Dynamic-EID configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(3.lisp-80)	This command was introduced.

Usage Guidelines

This command is used when dynamic-EID discovery is necessary in a multi-homed Data Center. When a dynamic-EID has been configured with more than one locator in the locator-set, any locator can decapsulate LISP packets that enter the Data Center. Since unicast packets that egress the Data Center go out a single LISP-VM router, this router is the only one that can discover the location of a roaming dynamic-EID. By using this command, the discovering LISP-VM router will send Map-Notify messages to other LISP-VM routers (via the configured *IPv4-group-address* multicast group address) at the Data Center site, so that all LISP-VM routers can determine the location of the dynamic-EID.

The multicast group address is used for both sending and receiving site-based Map-Notify multicast messages. The interface for which this multicast Map-Notify messages are received on is the interface used to send decapsulated packets to the dynamic-EID.

Examples

The following example configures the LISP dynamic-EID policy named **Roamer-1**, enters dynamic-EID configuration mode, and then configures the **map-notify-group** command with the 239.1.1.254.

```
Router(config)# lisp dynamic-eid Roamer-1
Router(config-lisp-dynamic-eid)# map-notify-group 239.1.1.254
```

Related Commands

Command	Description
lisp mobility	Configure an interface on an ITR to participate in LISP VM-mobility (dynamic-EID roaming)

---

map-server

To configure the Map-Server to which the dynamic-EID registers to when this policy is invoked, use the **map-server** command in dynamic-EID configuration mode. To remove the configured reference to the Map-Server, use the **no** form of this command.

> **[no] map-server** *locator* **key** *key-type password*

> **[no] map-server** *locator* **proxy-reply**

Syntax Description

locator	IPv4 or IPv6 Routing Locator (RLOC) allowed within Map-Registration message.
key *key-type*	Specifies how the key-type that the following SHA-1 password (key) is encoded. Type

LISP-102

	(0) indicates that a cleartext password follows; Type (3) indicates that a 3DES encrypted key follows; Type (7) indicates that a Cisco Type 7 encrypted password follows.
password	The password used to create the SHA-1 HMAC hash when authenticating the Map-Register message sent by the ETR.
proxy-reply	Specifies that the Map-Register sent to the Map-Server requests that the Map-Server proxy map-reply on behalf of dynamic-EIDs included in this policy.

Defaults

By default, no Map-Server is configured within a dynamic-EID policy and the configured map-server on the LISP-VM router (from the {**ip|ipv6**} **lisp etr map-server** command) will be used to register the dynamic-EID.

Command Modes

Dynamic-EID configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13) (August update)	This command was updated.

Usage Guidelines

In LISP VM-Mobility, when a dynamic-EID roams to this LISP-VM router, the dynamic-EID must be registered to a Map-Server with its new attributes (the 3-tuple of (*locator*, *priority*, *weight*) according to the **database-mapping** dynamic-EID subcommand). This **map-server** dynamic-EID subcommand configures the Map-Server to which the dynamic-EID registers. The *locator* specified in the **map-server** command can be either an IPv4 or IPv6 address in locator space.

Multiple **map-server** commands can be configured so that registration can occur to different Map-Servers with either the same or different authentication keys.

Note Typically, the home Map-Server (i.e. the one that the dynamic-EID initially registered to) should be configured as the dynamic-EID Map-Server.

When the **map-server** dynamic-EID subcommand command is not configured, the configured map-server on the LISP-VM router (from the {**ip|ipv6**} **lisp etr map-server** command) will be used to register the dynamic-EID.

When the **proxy-reply** keyword is configured, the Map-Register sent to the Map-Server requests that the Map-Server proxy map-reply on behalf of dynamic-EIDs when it receives a Map-Request for the dynamic-EID prefix.

Examples

The following example configures the LISP dynamic-EID policy named **Roamer-1**, enters dynamic-EID configuration mode, and then configures the Map-Server with IPv4 locator 10.1.1.1 for dynamic-EIDs matching this policy to register to. The Map-Server is also specified to proxy-reply on behalf of the dynamic-EID.

```
Router(config)# lisp dynamic-eid Roamer-1
Router(config-lisp-dynamic-eid)# map-server 10.1.1.1 key some-password
Router(config-lisp-dynamic-eid)# map-server 10.1.1.1 proxy-reply
```

Related Commands

Command	Description
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
lisp mobility	Configure an interface on an ITR to participate in LISP VM-mobility (dynamic-EID roaming)

---

register-database-mapping

To configure the LISP VM-router to register the dynamic-EID prefix from the **database-mapping** dynamic-EID subcommand rather than a more-specific host-EID, use the optional **register-database-mapping** command in dynamic-EID configuration mode. To remove this optional functionality, use the **no** form of this command.

> **[no] register-database-mapping**

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the more-specific (typically host-EID) prefix is registered with the configured Map-Server.

Command Modes

Dynamic-EID configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13) (August update)	This command was updated.

Usage Guidelines

This optional command causes the LISP VM-router to register the dynamic-EID prefix from the **database-mapping** dynamic-EID subcommand rather than (more-specific) dynamic host-EIDs to the Map-Server. By default, host-based dynamic-EIDs are registered to the Map-Server.

This command can be used to support cloud applications. When a dynamic-EID matches the dynamic-EID-prefix from the **database-mapping** dynamic-EID subcommand, the entire dynamic-EID prefix is registered which moves all EIDs to the new locator-set.

Examples

The following example configures the LISP dynamic-EID policy named **Roamer-1**, enters dynamic-EID configuration mode, and then configures the policy to register the entire dynamic-EID prefix instead of individual dynamic host EIDs.

```
Router(config)# lisp dynamic-eid Roamer-1
Router(config-lisp-dynamic-eid)# register-database-mapping
```

Related Commands

Command	Description
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
lisp mobility	Configure an interface on an ITR to participate in LISP VM-mobility (dynamic-EID roaming)

---

roaming-eid-prefix

To configure an optional EID (or list of EIDs) to be considered as roaming dynamic-EIDs, use the optional **roaming-eid-prefix** command in dynamic-EID configuration mode. To remove this optional functionality, use the **no** form of this command.

[no] roaming-eid-prefix *eid-prefix*

Syntax Description

eid-prefix	IPv4 or IPv6 EID-prefix allowed to be considered as dynamic-EIDs (roaming).

Defaults

By default, more-specific (host-EID) prefixes within the *dynamic-EID-prefix* range specified in the **database-mapping** dynamic-EID subcommand are individually registered with the configured Map-Server.

Command Modes

Dynamic-EID configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13) (August update)	This command was updated.

Usage Guidelines

This optional command is used to apply further restrictions on deciding which EIDs are to be considered dynamic-EIDs and allowed to roam onto the interface(s) configured with the matching *dynamic-EID-policy-name* using the **lisp mobility** *dynamic-EID-policy-name* command.

When an EID is detected to be a candidate for dynamic-EID roaming and the optional **roaming-eid-prefix** command is used, the EID must be covered by the **roaming-eid-prefix** entry in order to be *discovered*. At such time, the EID-prefix listed in a **database-mapping** entry within the **lisp dynamic-eid** policy will be registered with the Map Server specified in the **map-server** command. That is, the **roaming-eid-prefix** command restricts the *discovery* aspect of LISP VM-Mobility (dynamic-EID roaming) for initiating Map-Server registration.

✎ **Note** Without this command, any EID within the EID-prefix range configured via the **database-mapping** entry will be *discovered* and be registered.

The EID referenced by the **roaming-eid-prefix** command can be either an IPv4 or IPv6 address in EID space.

LISP-105

Examples

The following example configures the LISP dynamic-EID policy named **Roamer-1**, enters dynamic-EID configuration mode, configures the IPv4 dynamic-EID prefix 172.16.1.1/32 with IPv4 locator 10.1.1.1 with the **database-mapping** command, and then configures the **roaming-eid-prefix** command with the more-specific EID of 172.16.1.12/32 as the only EID prefix that will invoke registration.

```
Router(config)# lisp dynamic-eid Roamer-1
Router(config-lisp-dynamic-eid)# database-mapping 172.16.1.0/24 10.1.1.1 priority 1 weight
100
Router(config-lisp-dynamic-eid)# roaming-eid-prefix 172.16.1.12/32
```

Related Commands

Command	Description
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
lisp mobility	Configure an interface on an ITR to participate in LISP VM-mobility (dynamic-EID roaming)

---

secure-handoff

To enable an ETR to perform roaming dynamic-EID verification prior to registering its move with the mapping system, configure the optional **secure-handoff** command in dynamic-EID configuration mode. To remove this optional functionality, use the **no** form of this command.

   [no] secure-handoff

Syntax Description

This command has no arguments or keywords.

Defaults

By default, **secure-handoff** is disabled.

Command Modes

Dynamic-EID configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r5-20)	This command was added.

Usage Guidelines

By default, when a dynamic-EID roams to an ETR, the ETR automatically registers this dynamic-EID move with the mapping system immediately upon discovery. However, if the dynamic-EID was being spoofed, this new registration should not be permitted. Configuring the optional **secure-handoff** command causes the ETR to perform a dynamic-EID verification process prior to registering the move with the mapping system. This command is disabled by default.

When **secure-handoff** is configured, the ETR performs a dynamic-EID verification process prior to registering the move with the mapping system. The operation of this verification process is based on the premise that if a dynamic-EID address is being spoofed, the real dynanmic-EID is likely to still be at its current location according to locator information in the mapping database system. Thus, when **secure-handoff** is configured, the following dynamic-EID verification process occurs.

- When the xTR initially discovers a dynamic-EID, it will attempt to establish a TCP connection to that dynamic-EID on destination port 4342 (the LISP control port). To do this, a TCP SYN packet is sent as a LISP-encapsulated data packet to locator currently registered in the mapping system for the EID.

- If the host representing the dynamic-EID is still located at the currently-registered locator – meaning it has not moved and is likely being spoofed, the host will respond back to with either a TCP reset packet or an ICMP port-unreachable message (since hosts typically do not support LISP). When received, the new xTR considers the dynamic-EID to be spoofed, will not register it to the mapping database system, will remove dynamic-EID state from its cache, and will issue a syslog message.

- If the host representing the dynamic-EID has in fact moved and is no londer be located at the the currently-registered locator, no TCP reset packet or ICMP port-unreachable message will be received by the new xTR (after approximately six (6) seconds), the dynamic-EID is considered valid and will be registered to the mapping database system.

Note Due to the nature of the dynamic-EID verification process operations, **secure-handoff** is not suitable for use when LISP VM-mobility is used with OTV for extending subnets. It is only suitable for verifying dynamic-EID roaming across subnets.

Note This verification process enabled by the optional **secure-handoff** command is intended to be generic and applicable to all types of devices that may roam. Various server virtualization hypervisor environments may provide their own VM roaming spoof detection capabilities.

Examples

The following example enables dynamic-EID **secure-handoff** under the LISP dynamic-EID policy named **Roamer-1**.

```
Router(config)# lisp dynamic-eid Roamer-1
Router(config-lisp-dynamic-eid)# secure-handoff
```

Related Commands

Command	Description
lisp dynamic-eid	Configures a LISP dynamic-EID roaming policy.
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
lisp mobility	Configure an interface on an ITR to participate in LISP VM-mobility.

LISP DDT Configuration Commands

lisp ddt

To configure a router to perform LISP Delegated Database Tree (DDT) functionality, use the **lisp ddt** command in global configuration mode. To remove LISP DDT functionality, us the **no** form of this command.

> **[no] lisp ddt**

Syntax Description

This command has no arguments or keywords.

Defaults

The router does not provide LISP DDT services.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

Use this command to enable a router to function in a LISP DDT node. This command is configured on DDT-enabled Map-Resolvers, Map-Servers, and DDT-only devices.

LISP Delegated Database Tree (DDT) is a hierarchical, distributed database delegating authority to provide mappings from LISP EIDs to RLOCs. LISP DDT functions in the same role as LISP ALT. However, DDT is superior in that it provides inherent support for LISP virtualization (instance-IDs), as well as support for other EID address families besides IPv4 and IPv6.

This command only enables DDT support. Additional DDT commands are required to configure the specific LISP DDT role(s) supported by this DDT node within the DDT hierarchical database. A DDT node may be configured as "authoritative" for one or more EID-prefixes, along with the set of RLOCs for other DDT nodes to which more-specific EID-prefixes are delegate.

> **Note** LISP DDT services must be enabled via the **lisp ddt** command before any other DDT functions can be configured.

Examples

The following example configures LISP DDT functionality on the router.

```
Router(config)# lisp ddt
```

Related Commands

Command	Description
lisp ddt authoritative-prefix	Configure an extended EID prefix (instance-ID and EID-Prefix) for which a LISP DDT node is authoritative.

lisp ddt delegate	Configure a LISP DDT node to delegate to another LISP DDT node the authority for the specified extended EID prefix (instance-ID and EID-Prefix).
lisp ddt map-server-peer	Configure the IPv4 or IPv6 locator locator address and extended EID prefix (instance-ID and EID-Prefix) for a peer Map-Server operating in a delegation hierarchy.
lisp ddt root	Configure an IPv4 or IPv6 locator for a DDT root node within the delegation hierarchy on a DDT-enabled Map-Resolver.

lisp ddt authoritative-prefix

To configure a LISP DDT node to be authoratative for the specified EID-prefix, use the **lisp ddt authoritative-prefix** command in global configuration mode. To remove a specific EID-prefix from being represented as authoritative on this device, us the **no** form of this command.

[no] lisp ddt authoritative-prefix [instance-id *iid*] **eid-prefix** *eid-prefix*

Syntax Description

instance-id *iid*	(Optional) Configure the instance-id associated with the specified EID-prefix, or a range of instance-IDs.
eid-prefix *eid-prefix*	Configures the IPv4 or IPv6 EID prefix for which this LISP DDT node is authoratative.

Defaults

By default, a LISP DDT node is not configured to be authoritative for any EID-prefixes.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

Use this command to configure an EID-prefix and optional instance-ID, or instance-ID range for which the LISP DDT-node or DDT-enabled Map-Server will be authoritative.

This enables their ability to send a negative Map-Referral message in response to a DDT-based Map-Request for an EID that matches the EID-prefix specified in this **lisp ddt authoritative-prefix** command but does not match an EID-prefix specified in any **lisp ddt delegate** commands, or in the case of a DDT-enabled Map-Server, does not match any configured LISP site EID-prefix.

When a DDT node receives a DDT Map-Request, it does the following:

1. The requested EID is checked for a match against any EID-prefixes specified in any configured **lisp ddt authoritative-prefix** commands.

    -   If there is no match, the DDT node sends a negative Map-Referral message back to the requesting Map-Resolver, indicating that it is not authoritative for the EID. The Map-Resolver caches this information and drops the Map-Request.
    -   If there is a match, the DDT node processing continues below.

LISP-109

2. The requested EID is checked for a match against any EID-prefixes specified in any **lisp ddt delegate** commands. If the DDT node is also a Map-Server, the EID is checked against EID-prefixes specified in **lisp site** commands as well.

    -   If there is no match, the DDT node sends a negative Map-Referral message covering the coarsest negative prefix within the configured EID-prefix range for which the DDT-node is authoritative. This indicates that the requested EID is within a delegation-hole and is (currently) not a LISP destination.

    -   If there is a match and the DDT node but is not also a Map-Server, the DDT node sends a Map-Referral message with the matched more-specific EID-prefix and the set of RLOCs for the delegated (child) DDT nodes. When the configured **lisp ddt delegate** command also includes the optional **map-server** keyword, the returned Map-Referral message also indicates for the receiving Map-Resolver that the next Map-Request will be to a DDT-enabled Map-Server. If the DDT node is a Map-Server, the Map-Server replies with the most appropriate response to the EID in the Map-Request. (See the lisp **ddt map-server-peer** command for details).

When the **lisp ddt authoritative-prefix** command is configured to specify authority for a specific LISP instance-ID, or for a range of instance-IDs, the optional **instance-id** keyword is included with the command. The value associated with the **instance-id** keyword will be specified as follows, depending upon the instance-ID scope being configured:

-   For a single instance-ID for a specific EID-prefix, *iid* is specified as an integer between 1 and 16777215 in the form:

    lisp ddt authoritative-prefix instance-id *iid* **eid-prefix** *eid-prefix*

-   For a range of instance-IDs, *iid* can either be specified in "x-y" format, where y must be greater than x and the range must be in a power-of 2 block (where x is a power-of-2 and y is a power-of-2 minus 1) with a range representable by a 24 bit "instance-id/mask," or in IPv4 prefix format. An EID-prefix cannot be included when an instance-ID range is specified. The command is entered in either of these forms:

    lisp ddt authoritative-prefix instance-id *X-Y*

    lisp ddt authoritative-prefix instance-id *A.B.C.D/LEN*

-   For the entire EID address space, for all address-families, and for all instance-IDs, the ***** character can be included. In this case, an EID-prefix is not included and the command is entered in the form:

    lisp ddt authoritative-prefix *

Note The ulitimate root DDT node can be configured using the command **lisp ddt authoritative-prefix *** to indicate that it is authoritative for all EID-prefixes, for all address-families, and for all instance-IDs.

Note When a child LISP DDT node is configured with the **lisp ddt authoritative-prefix** command for an EID-prefix (and/or instance-ID) space, the parent LISP DDT node must also be configured with a **lisp ddt delegate** command with matching EID-prefix (and/or instance-ID) space.

Examples

The following example configures the LISP DDT node to be authoritative for the IPv4 EID-prefix **172.16.0.0/16** and the IPv6 EID-prefix **2001:db8:eeee::/48**. Note that in this case, the optional instance-id keyword and value are not specified and hence, the EID-prefixes are only associated with the default instance-ID (0).

```
Router(config)# lisp ddt authoritative-prefix eid-prefix 172.16.0.0/16
Router(config)# lisp ddt authoritative-prefix eid-prefix 2001:db8:eeee::/48
Router(config)# sh lisp ddt
---<skip>---
Configured authoritative EID-prefixes:
    [0] 172.16.0.0/16
    [0] 2001:db8:eeee::/48
Router(config)#
```

In the following example, the LISP DDT node is configured to be authoritative for the IPv4 EID-prefix **172.16.0.0/16** within the instance-ID **1234**.

```
Router(config)# lisp ddt authoritative-prefix instance-id 1234 eid-prefix 172.16.0.0/16
Router(config)# sh lisp ddt
---<skip>---
Configured authoritative EID-prefixes:
    [1234] 172.16.0.0/16
Router(config)#
```

In the following example, the LISP DDT node is configured to be authoritative for all EID-prefixes within the instance-ID range of **16 to 31**. (Note that this is equivalent to using the prefix format of 0.0.0.16/28).

```
Router(config)# lisp ddt authoritative-prefix instance-id 16-31
Router(config)# sh lisp ddt
---<skip>---
Configured authoritative EID-prefixes:
    [16-31 (0.0.0.16/28)] *
Router(config)#
```

In the following example, a root LISP DDT node is configured to be authoritative for all EID-prefixes, for all address-families, and for all instance-IDs.

```
Router(config)# lisp ddt authoritative-prefix *
Router(config)# sh lisp ddt
---<skip>---
Configured authoritative EID-prefixes:
    [*] *
Router(config)#
```

Related Commands

Command	Description
lisp ddt	Configure a router to enable LISP DDT functionality.
lisp ddt delegate	Configure a LISP DDT node to delegate to another LISP DDT node the authority for the specified extended EID prefix (instance-ID and EID-Prefix).
lisp ddt map-server-peer	Configure the IPv4 or IPv6 locator locator address and extended EID prefix (instance-ID and EID-Prefix) for a peer Map-Server operating in a delegation hierarchy.
lisp ddt root	Configure an IPv4 or IPv6 locator for a DDT root node within the delegation hierarchy on a DDT-enabled Map-Resolver.

lisp ddt delegate

To configure the RLOC address of another LISP DDT node within the delegation hierarchy for which a specified EID-prefix is being delegated, use the **lisp ddt delegate** command in global configuration mode. To remove this delegation for the specific EID-prefix, us the **no** form of this command.

> **[no] lisp ddt delegate** *child-locator* **[instance-id** *iid*] **eid-prefix** *eid-prefix* **[map-server]**

Syntax Description

child-locator	Configure the IPv4 or IPv6 locator address of the delegation DDT node or Map-Server
instance-id *iid*	(Optional) Configure the instance-id associated with the specified EID-prefix, or a range of instance-IDs.
eid-prefix *eid-prefix*	Configures the IPv4 or IPv6 EID prefix for which this LISP DDT node is delegating authority.
map-server	(Optional) Indicates that the delegated (child) DDT node being referenced is a Map-Server for the configured IPv4 or IPv6 EID prefix.

Defaults

By default, a LISP DDT node is not configured to delegate the authority for any EID-prefixes.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

Use this command to configure on a parent DDT node the IPv4 or IPv6 locator address and EID-prefix and optional instance-id that is delegated to a child DDT node within the delegation hierarchy. This enables the DDT node to send a Map-Referral message in response to a DDT-based Map-Request for an EID that matches the EID-prefix specified in this **lisp ddt delegate** command.

✎

Note For correct hierarchical delegation, the EID prefix specified in the parent's **lisp ddt delegate** command must match the EID prefix in the child DDT node's **lisp ddt authoritative-prefix** command

When a DDT node receives a DDT Map-Request, it does the following:

1. The requested EID is checked for a match against any EID-prefixes specified in any configured **lisp ddt authoritative-prefix** commands.

   - If there is no match, the DDT node sends a negative Map-Referral message back to the requesting Map-Resolver, indicating that it is not authoritative for the EID. The Map-Resolver caches this information and drops the Map-Request.

   - If there is a match, the DDT node processing continues below.

2. The requested EID is checked for a match against any EID-prefixes specified in any **lisp ddt delegate** commands. If the DDT node is also a Map-Server, the EID is checked against EID-prefixes specified in **lisp site** commands as well.

   - If there is no match, the DDT node sends a negative Map-Referral message covering the coarsest negative prefix within the configured EID-prefix range for which the DDT-node is authoritative. This indicates that the requested EID is within a delegation-hole and is (currently) not a LISP destination.

   - If there is a match and the DDT node but is not also a Map-Server, the DDT node sends a Map-Referral message with the matched more-specific EID-prefix and the set of RLOCs for the delegated (child) DDT nodes. When the configured **lisp ddt delegate** command also includes the optional **map-server** keyword, the returned Map-Referral message also indicates for the receiving Map-Resolver that the next Map-Request will be to a DDT-enabled Map-Server. If the DDT node is a Map-Server, the Map-Server replies with the most appropriate response to the EID in the Map-Request. (See the lisp **ddt map-server-peer** command for details).

When the **lisp ddt delegate** command is configured to delegate a specific LISP instance-ID, or for a range of instance-IDs, the optional **instance-id** keyword is included with the command. The value associated with the keyword will be specified as follows, depending upon the instance-ID scope being configured:

   - For a single instance-ID for a specific EID-prefix, *iid* is specified as an integer between 1 and 16777215 in the form:

       lisp ddt delegate *child-locator* **instance-id** *iid* **eid-prefix** *eid-prefix*

   - For a range of instance-IDs, *iid* can either be specified in "x-y" format, where y must be greater than x and the range must be in a power-of 2 block (where x is a power-of-2 and y is a power-of-2 minus 1)

LISP-112

with a range representable by a 24 bit "instance-id/mask," or in IPv4 prefix format. An EID-prefix cannot be included when an instance-ID range is specified. The command is entered in either of these forms:

> **lisp ddt delegate** *child-locator* **instance-id** *X-Y*
>
> **lisp ddt delegate** *child-locator* **instance-id** *A.B.C.D/LEN*

✎

Note When a LISP DDT node is configured with a **lisp ddt delegate** command for the an EID-prefix (and/or instance-ID) space, the child LISP DDT node must be configured with the **lisp ddt authoritative-prefix** command with matching EID-prefix (and/or instance-ID) space.

Examples

The following example configures a LISP DDT node to delegate authority for the IPv4 EID-prefix **172.16.0.0/16** and the IPv6 EID-prefix **2001:db8:eeee::/48** to the DDT node with child locator 10.1.1.1. Note that in this case, the optional instance-id keyword and value are not specified and hence, the EID-prefixes are only associated with the default instance-ID (0).

```
Router(config)# lisp ddt delegate 10.1.1.1 eid-prefix 172.16.0.0/16
Router(config)# lisp ddt delegate 10.1.1.1 eid-prefix 2001:db8:eeee::/48
Router(config)# sh lisp ddt
---<skip>---
Configured DDT delegated nodes/map-servers:
    [0] 172.16.0.0/16 -> 10.1.1.1, p/w: 0/0
    [0] 2001:db8:eeee::/48 -> 10.1.1.1, p/w: 0/0
Router(config)#
```

In the following example, a LISP DDT node is configured to delegate authority for the IPv4 EID-prefix **172.16.0.0/16** to the DDT node with child locator 10.1.1.1, and where the child is specified as a Map-Server.

```
Router(config)# lisp ddt delegate 10.1.1.1 eid-prefix 172.16.0.0/16 map-server
Router(config)# sh lisp ddt
---<skip>---
Configured DDT delegated nodes/map-servers:
    [0] 172.16.0.0/16 -> 10.1.1.1, p/w: 0/0, map-server-child
 Router(config)#
```

In the following example, the LISP DDT node is configured to be authoritative for all EID-prefixes within the instance-ID range of **0 to 15** to the DDT node with child locator 10.1.1.1. (Note that this is equivalent to using the prefix format of 0.0.0.0/28).

```
Router(config)# lisp ddt delegate 10.1.1.1 instance-id 0-15
Router(config)# sh lisp ddt
---<skip>---
Configured DDT delegated nodes/map-servers:
    [0-15 (0.0.0.0/28)] * -> 10.1.1.1, p/w: 0/0
Router(config)#
```

Related Commands

Command	Description
lisp ddt	Configure a router to enable LISP DDT functionality.
lisp ddt authoritative-prefix	Configure an extended EID prefix (instance-ID and EID-Prefix) for which a LISP DDT node is authoritative.
lisp ddt map-server-peer	Configure the IPv4 or IPv6 locator locator address and extended EID prefix (instance-ID and EID-Prefix) for a peer Map-Server operating in a delegation hierarchy.
lisp ddt root	Configure an IPv4 or IPv6 locator for a DDT root node within the delegation hierarchy on a DDT-enabled Map-Resolver.

lisp ddt map-server-peer

To configure on a DDT-enabled Map-Server the locator and EID-prefix (and/or instance-ID) for a Map-Server peer within the LISP DDT delegation hierarchy, use the use the **lisp ddt map-server-peer** command in global configuration mode. To remove the Map-Server as a peer, us the **no** form of this command.

[no] lisp ddt map-server-peer *map-server-locator* **[instance-id** *iid***] eid-prefix** *eid-prefix*

Syntax Description

map-server-locator	Configure the IPv4 or IPv6 locator address of this Map-Server, or of a peer Map-Server that is also authoritative for the same EID-prefix (and/or instance-ID).
instance-id *iid*	(Optional) Configure the instance-id associated with the specified EID-prefix, or a range of instance-IDs.
eid-prefix *eid-prefix*	Configures the IPv4 or IPv6 EID prefix for which this Map-Server, or a peer Map-Server is authoritative.

Defaults

By default, no Map-Server peers are configured.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

Use this command to configure the IPv4 or IPv6 locator address of peer Map-Servers that are all configured to be authoritative and acting as Map-Servers for the same EID-prefix (and/or instance-ID) within the LISP DDT delegation hierarchy. This enables the Map-Server to provide the appropriate response when the EID in a DDT-based Map-Request matches the EID-prefix specified in this **lisp ddt map-server-peer** command.

A Map-Server is generally configured with one or more **lisp site** configurations that include EID prefixes (and possibly instance-IDs) for which one or more LISP Sites and ETRs may be registering. In addition, there may be more than one Map-Server to which a LISP Site and its ETRs may be configured to register (for example, in a redundant Map-Servers are deployment). When multiple Map-Servers are deployed within a LISP DDT delegation hierarchy and they are all configured to be authoritative for the same EID-prefix (and/or instance-ID) space they are then considered peers. Map-Server peers also have upstream LISP DDT node(s) delegating the same EID-prefix (and/or instance-ID) space to them. In this case, the following considerations are important:

- Each Map-Server must be identically configured with **lisp ddt map-server-peer** commands specifying each Map-Server locator, <u>including their own</u>, for each EID-prefix (and/or instance-ID) represented by the Map-Server and its peers.

- Each Map-Server must be identically configured with **lisp ddt authoritative-prefix** commands with an EID-prefix (and/or instance-ID) matching the one used within the **lisp ddt map-server-peer** commands.

- The EID-prefix configured in **lisp ddt map-server-peer** and **lisp ddt authoritative-prefix** commands must cover the EID-prefix(es) contained in the **lisp site** configurations. If there are multiple **lisp site** configurations and the EID-prefix(es) can be summarized by a coarse aggregate, the EID-prefix configured in **lisp ddt map-server-peer** and **lisp ddt authoritative-prefix** commands may use this aggregate instead of the individual EID-prefixes from each **lisp site** configuration.

- For a given authoritative-prefix, each Map-Server must have identical **lisp site** configurations, regardless of whether the LISP Site is configured to register to all/any one Map-Server or not. This is because when the upstream LISP DDT node configures the **lisp ddt delegate** command and includes the **map-server** keyword, the Map-Referral message it returns to the querying Map-Resolver includes the set of RLOCs for all Map-Servers (referral target DDT nodes) to which the EID-prefix has been delegated. Thus, any Map-Server in the peer group can receive subsequent DDT Map-Requests from the map-resolver.

- Depending on the EID-prefix(es) configured in **lisp ddt map-server-peer** and **lisp ddt authoritative-prefix** commands and the state of LISP Site registrations, the following responses may be generated by this Map-Server.

  a. When the EID in an DDT Map-Request **matches** an EID-prefix for a LISP site that is **currently registered** to THIS Map-Server, the Map-Server forwards the ECM-based Map-Request to the ETR at that LISP site (or sends a Map-Reply if it is providing proxy Map-Reply services). This ETR will send a Map-Reply back to the requesting ITR. The Map-Server also returns a Map-Referral back to the Map-Resolver indicating that it successfully processed the Map-Request and forwarded it to the registering ETR.

  b. When the EID in an DDT Map-Request **matches** an EID-prefix for a LISP site that is configured but **not currently registered** to THIS Map-Server, the Map-Server returns a Map-Referral message back to the Map-Resolver. The Map-Resolver caches the fact that the LISP site is configured but not currently registered to THIS Map-Server, and proceeds to query the other peer Map-Servers for the EID-prefix. If one of those Map-Servers has the LISP site registered, it will respond as in (a) above. If none of the peer Map-Servers has the LISP site registered, the Map-Resolver will send a Negative-Map-Reply (TTL 1 minute) back to the requesting ITR.

  c. When the EID in an DDT Map-Request **does not match** any EID-prefix for configured LISP sites but is within the EID-prefix (and/or instance-ID) configured in **lisp ddt map-server-peer** and **lisp ddt authoritative-prefix** commands, this means that the EID-prefix (or Instance-ID) configured in **lisp ddt map-server-peer** and **lisp ddt authoritative-prefix** commands is a coarse-aggregate and a LISP Site has not been configured to cover some portion of it. In this case, the Map-Server returns a negative Map-Referral back to the Map-Resolver indicating that the EID does not match any EID-prefix (and/or instance-ID) delegated to the Map-Server. This negative Map-Referral contains the "least-specific" EID-prefix that covers the delegation hole, allowing the Map-Resolver then to create and send a Negative-Map-Reply (TTL 15 minutes) back to the requesting ITR.

    ✎

    Note Because all Map-Server peers must be identically configured, a DDT map-resolver receiving a negative Map-Referral from a DDT map-server can accept it without further need for checking of the other Map-Server peers for a configured or registered LISP Site.

When the **lisp ddt map-server-peer** command is configured for a specific LISP instance-ID, or for a range of instance-IDs, the optional **instance-id** keyword is included with the command. The value associated with the keyword will be specified as follows, depending upon the instance-ID scope being configured:

- For a single instance-ID for a specific EID-prefix, *iid* is specified as an integer between 1 and 16777215 in the form:

  lisp ddt map-server-peer *map-server-locator* **instance-id** *iid* **eid-prefix** *eid-prefix*

- For a range of instance-IDs, *iid* can either be specified in "x-y" format, where y must be greater than x and the range must be in a power-of 2 block (where x is a power-of-2 and y is a power-of-2 minus 1) with a range representable by a 24 bit "instance-id/mask," or in IPv4 prefix format. An EID-prefix cannot be included when an instance-ID range is specified. The command is entered in either of these forms:

  lisp ddt map-server-peer *map-server-locator* **instance-id** *X-Y*

  lisp ddt map-server-peer *map-server-locator* **instance-id** *A.B.C.D/LEN*

Examples

The following example configures a LISP DDT Map-Server as authoritative for the IPv4 EID-prefix **172.16.0.0/16** and the IPv6 EID-prefix **2001:db8:eeee::/48** for its own locator 10.1.1.1, as well as one other Map-Server peer (for the same EID-prefix space) with map-server-locator 10.2.1.1. Note that in this case, the optional instance-id

LISP-115

keyword and value are not specified and hence, the EID-prefixes are only associated with the default instance-ID (0).

```
Router(config)# lisp ddt map-server-peer 10.1.1.1 eid-prefix 172.16.0.0/16
Router(config)# lisp ddt map-server-peer 10.2.1.1 eid-prefix 172.16.0.0/16
Router(config)# lisp ddt authoritative-prefix eid-prefix 172.16.0.0/16
Router(config)# lisp ddt map-server-peer 10.1.1.1 eid-prefix 2001:db8:eeee::/48
Router(config)# lisp ddt map-server-peer 10.2.1.1 eid-prefix 2001:db8:eeee::/48
Router(config)# lisp ddt authoritative-prefix eid-prefix 2001:db8:eeee::/48
Router(config)# show lisp ddt
---<skip>---
  Configured DDT delegated nodes/map-servers:
    [0] 172.16.0.0/16 -> 10.1.1.1, p/w: 0/0, map-server-peer
    [0] 172.16.0.0/16 -> 10.2.1.1, p/w: 0/0, map-server-peer
    [0] 2001:db8:eeee::/48 -> 10.1.1.1, p/w: 0/0, map-server-peer
    [0] 2001:db8:eeee::/48 -> 10.2.1.1, p/w: 0/0, map-server-peer
  Configured authoritative EID-prefixes:
    [0] 172.16.0.0/16
    [0] 2001:db8:eeee::/48
Router(config)#
```

In the following example, a LISP DDT Map-Server is configured as authoritative for all EID-prefixes within the instance-ID range of **0 to 15.** Its own locator is 10.1.1.1; one other Map-Server peer with locator 10.2.1.1 is configured for the same Instance-ID space. (Note that this is equivalent to using the prefix format of 0.0.0.0/28).

```
Router(config)# lisp ddt map-server-peer 10.1.1.1 instance-id 0-15
Router(config)# lisp ddt map-server-peer 10.2.1.1 instance-id 0-15
Router(config)# lisp ddt authoritative-prefix instance-id 0-15
Router(config)# show lisp ddt
---<skip>---
  Configured DDT delegated nodes/map-servers:
    [0-15 (0.0.0.0/28)] * -> 10.1.1.1, p/w: 0/0, map-server-peer
    [0-15 (0.0.0.0/28)] * -> 10.2.1.1, p/w: 0/0, map-server-peer
  Configured authoritative EID-prefixes:
    [0-15 (0.0.0.0/28)] *
Router(config)#
```

Commands

Command	Description
lisp ddt	Configure a router to enable LISP DDT functionality.
lisp ddt authoritative-prefix	Configure an extended EID prefix (instance-ID and EID-Prefix) for which a LISP DDT node is authoritative.
lisp ddt delegate	Configure a LISP DDT node to delegate to another LISP DDT node the authority for the specified extended EID prefix (instance-ID and EID-Prefix).
lisp ddt root	Configure an IPv4 or IPv6 locator for a DDT root node within the delegation hierarchy on a DDT-enabled Map-Resolver.

lisp ddt root

To configure an IPv4 or IPv6 locator for a DDT root node within the delegation hierarchy on a DDT-enabled Map-Resolver, use the **lisp ddt root** command in global configuration mode. To remove this root DDT node reference, us the **no** form of this command.

> **[no] lisp ddt root** *root-locator*

Syntax Description

root-locator	Configure an IPv4 or IPv6 locator address of the DDT root node.

Defaults

By default, a Map-Resolver running DDT is not configured to point to a DDT root node.

Command Modes

Global configuration

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

Use this command to configure a Map-Resolver running DDT to point to a DDT root node within the delegation hierarchy.

✎

Note Up to eight (8) DDT root node references (summed across all address-families) may be configured on a Map-Resolver. When multiple DDT root nodes are configured, the Map-Resolver uses load-balancing mechnisms to send DDT-based Map-Requests to these DDT root nodes.

Unlike a standalone Map Resolver or one that uses the ALT mapping system, a DDT Map Resolver uses an iterative process of following referrals to find the correct ETR to answer a Map-Request. This requires a DDT Map Resolver to maintain additional state, including a Map-Referral cache and a lookup-queue of Map-Requests that are going through the iterative referral process.

When a DDT-enabled Map-Resolver receives an ECM-based Map-Request from an ITR, A Map-Resolver running DDT begins the iterative process by sending a DDT-based Map-Request to a DDT root node referenced by in the **lisp ddt root** command. The DDT root node is configured with the appropriate **lisp ddt authoritative-prefix** and **lisp ddt delegate** commands to satisfy the request, or refer the Map-Resolver to the next (set of) DDT node(s) and ultimately, DDT Map-Server(s) within the DDT hierarchy that can provide the most appropriate response for the EID in the Map-Request. (See the **lisp ddt authoritative-prefix** command, **lisp ddt delegate** command, and **lisp ddt map-server-peer** command for details on response behavior.)

Examples

The following example configures a LISP DDT Map-Resolver to refer to three LISP DDT root node locators: 10.1.1.1, 10.2.1.1, and 2001:db8:1::1111.

```
Router(config)# lisp ddt root 10.1.1.1
Router(config)# lisp ddt root 10.2.1.1
Router(config)# lisp ddt root 2001:db8:1::1111
Router(config)# show lisp ddt
LISP-DDT Configuration in VRF "default"
  Configured DDT roots: 10.1.1.1  10.2.1.1  2001:db8:1::1111
---<skip>---
Router(config)#
```

Related Commands

Command	Description
lisp ddt	Configure a router to enable LISP DDT functionality.
lisp ddt authoritative-prefix	Configure an extended EID prefix (instance-ID and EID-Prefix) for which a LISP DDT node is authoritative.
lisp ddt delegate	Configure a LISP DDT node to delegate to another LISP DDT node the

LISP-117

	authority for the specified extended EID prefix (instance-ID and EID-Prefix).
lisp ddt map-server-peer	Configure the IPv4 or IPv6 locator locator address and extended EID prefix (instance-ID and EID-Prefix) for a peer Map-Server operating in a delegation hierarchy.

Other LISP Configuration Commands

redistribute lisp

To configure BGP running on a LISP Map-Server to redistribute and advertise EID-prefixes from registered LISP sites, use the **redistribute lisp route-map** command in BGP configuration mode. To remove the configuration, use the **no** form of this command.

> **[no] redistribute lisp route-map** *route-map*

Syntax Description

route-map *route-map*	Configure a route-map to filter BGP advertisments from LISP into BGP.

Defaults

By default, no EID-prefixes are redistributed into BGP.

Command Modes

BGP configuration mode.

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When a Map-Server registers LISP sites, the EID-prefixes from these registered LISP sites are typically advertised via BGP into the VRF used by the LISP-ALT. This can be accomplished using the **redistribute lisp route-map** command in BGP configuration mode.

Only after an ETR has successfully registered through the Map-Registration process, will the EID-prefixes from that LISP site be advertised in the URIB or U6RIB by the LISP process. BGP will then redistribute the EID-prefixes, according to the **route-map** rules, into the LISP-ALT.

Note The use of the **route-tag** under the eid-prefix command is recommended to simplifying processes of redistributing EID-prefixes into BGP.

Note The Map-Server must be connected to the LISP-ALT. Refer to {**ip|ipv6**} **lisp alt-vrf** for more information.

Examples

The following example redistributes registered LISP site EID-prefixes, according to the rules of the route-map Valid-LISP.

```
Router(config)# router bgp 65001
Router(config-router)# vrf lisp
Router(config-router-vrf)# address-family ipv4 unicast
Router(config-router-vrf)# redistribute lisp route-map Valid-LISP
Router(config-router-vrf)# address-family ipv6 unicast
Router(config-router-vrf)# redistribute lisp route-map Valid-LISP
```

Related Commands

Command	Description
eid-prefix	Configure the EID-prefixes that are allowed in a Map-Register message sent by an ETR
ip lisp alt-vrf	Configure which VRF supporting the IPv4 address-family LISP should use when sending Map Requests for an IPv4 EID-to-RLOC mapping directly over the ALT.
ipv6 lisp alt-vrf	Configure which VRF supporting the IPv6 address-family LISP should use when sending Map Requests for an IPv6 EID-to-RLOC mapping directly over the ALT.

LISP Show Commands

show ip lisp

To display the IPv4 LISP configuration status, use the **show ip lisp** command in privileged EXEC mode.

> **show ip lisp** [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Display statistics for the specified VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was modified.

Usage Guidelines

This command is used to display the IPv4 LISP configuration status for the local device. When the optional **vrf** *vrf-name* is used, the IPv4 LISP configuration status related to the specified VRF context only is displayed.

Examples

The following sample output from the **show ip lisp** command displays information about the current IPv4 LISP configuration status. The output varies, depending on the LISP features configured.

```
Router# show ip lisp
LISP IP Configuration Information for VRF "default" (iid 0)
  LISP Geo Coordinates:        (37-11-40-N, 121-49-1-W)
  Ingress Tunnel Router (ITR): enabled
  Egress Tunnel Router (ETR):  enabled
  Proxy-ITR Router (PTR):      disabled
  Proxy-ETR Router (PETR):     disabled
  Map Resolver (MR):           disabled
  Map Server (MS):             disabled
  LISP control-plane security: enabled (weak-mode)
  Locator VRF:                 default
  Last-resort source locator:  172.22.156.23
  LISP-NAT Interworking:       disabled
  Use locators from BGP RIB:   disabled
  ITR send Map-Request:        enabled
  ITR send Data-Probe:         disabled
  LISP ALT-VRF:                not configured
  LISP-DDT:                    disabled
  ITR Map-Resolver:            172.22.156.35
  ETR Map-Server(s):           172.22.156.35, 172.22.132.89
  Last Map-Register sent to MS: 00:00:45
  ETR glean mapping:           disabled, verify disabled
  ETR accept mapping data:     disabled, verify disabled
  ETR map-cache TTL:           24 hours
```

```
     Shortest EID-prefix allowed:     /16
     Use Proxy-ETRs:                  172.16.2.1
     Locator Reachability Algorithms:
       Echo-nonce algorithm:          disabled
       TCP-counts algorithm:          disabled
       RLOC-probe algorithm:          enabled
     Static mappings configured:      0
     Map-cache limit:                 10000
     Map-cache size:                  3
     ETR Database, global LSBs: 0x00000001:
       EID-prefix: 192.168.12.0/24, LSBs: 0x00000001
         Locator: 172.22.156.23, priority: 1, weight: 100
                  Uptime: 09:27:15, state: up, local
Router#
```

The following sample output from the **show ip lisp** command displays information about the current IPv4 LISP configuration status when on the `ip lisp etr map-server` command has been configured, and the Map-Resolver locator is taken to be the same as the configured Map-Server locator.

```
Router# show ip lisp
LISP IP Configuration Information for VRF "default" (iid 0)
---<skip>---
  LISP ALT-VRF:                    not configured
  ETR Map-Server(s):               10.1.1.1, also Map-Resolver(s)
```

Table 1 describes the significant fields shown in the display.

Table 1 show ip lisp Field Descriptors

Field	Description
Ingress Tunnel Router (ITR)	This field indicates whether the router is configured as an ITR (see **ip lisp itr**)
Egress Tunnel Router (ETR)	This field indicates whether the router is configured as an ETR. (see **ip lisp etr**)
Proxy-ITR	This field indicates whether the router is configured as a PITR. (see **ip lisp proxy-itr**)
Proxy-ETR	This field indicates whether the router is configured as a PETR. (see **ip lisp proxy-etr**)
Map-Resolver (MR)	This field indicates whether the router is configured as a MR. (see **ip lisp map-resolver**)
Map-Server (MS)	This field indicates whether the router is configured as a MS. (see **ip lisp map-server**)
LISP control-plane security	This field indicates whether LISP-SEC functionality is enabled and its mode. (see **lisp security**)
Locator VRF	This field indicates the VRF in which to resolver locators. (see **ip lisp locator-vrf**)
Last-resort source locator	Last-resort source locator for LISP messages.
LISP-NAT Interworking	This field indicates whether the router is configured for LISP NAT (see **ip lisp translate**)
Use locators from BGP RIB	This field indicates whether LISP is configured to use iBGP routes as EID-prefixes and their BGP RIB next-hop addresses as locators (see **ip lisp use-bgp-locators**)
ITR send Map-Request	This field indicates whether sending Map-Requests is enabled. (see **ip lisp itr map-resolver**)
ITR send Data-Probe	This field indicates whether **ip lisp itr send-data-probe** is enabled
LISP ALT-VRF	This field indicates whether a LISP-ALT VRF configured and identifies the VRF name. (see **ip lisp alt-vrf**)
LISP-DDT	This field indicates whether LISP-DDT has been enabled or not. (see **lisp ddt**)
ITR Map-Resolver	Identifies the configured ITR Map-Resolver. (see **ip lisp itr map-resolver**).
ETR Map-Server(s)	Identifies the configured ETR Map-Server(s). (see **ip lisp etr map-server**).
Last Map-Register sent to MS	This field indicates when this device last sent a Map-Registration message to the configured Map-Server(s).

ETR glean mapping	Indicates whether the ETR is configured to glean mapping data contained in a encapsulated packet (see **ip lisp etr glean-mapping**)
ETR accept mapping data	Indicates whether the ETR is configured to cache the mapping data contained in a Map-Request (see **ip lisp etr accept-map-request-mapping**)
ETR map-cache TTL	Identifies the current ETR map-cache TTL (see **ip lisp etr map-cache-ttl**)
Shortest EID-prefix allowed	This field indicates the EID-prefix length accepted in a Map-Reply. (see **ip lisp shortest-eid-prefix-length**)
Use Proxy-ETRs	When configured, indicates whether the router uses a PETR and lists the PETR locator.
Locator Reachability Algorithms	Indicates the status of the available locator reachability algorithms (Echo-nonce, TCP-counts, RLOC-probing) (see **lisp loc-reach-algorithm**)
Static mappings configured	Indicates the number of static cache-map entries are configured (see **ip lisp map-cache**)
Map-cache limit	Indicates the current map-cache limit and identifies any configured reserve-list. (see **ip lisp map-cache-limit**).
Map-cache size	Indicates the current number of entries in the map-cache.
ETR Database	Lists global LSBs, configured EID-prefixes and Locators.

Related Commands

Command	Description
lisp ddt	Configure a router to enable LISP DDT functionality.
ip lisp etr	Configures the router to act as an IPv4 LISP Egress Tunnel Router (ETR)
ip lisp etr accept-map-request-mapping	Configure an ETR to cache IPv4 mapping data contained in a Map-Request message
ip lisp etr glean-mapping	Configure an ETR to glean inner header (EID) source address to outer header (RLOC) source address mappings from encapsulated data packets to its EID-to-RLOC cache IPv4 mapping data.
ip lisp etr map-cache-ttl	Configures the TTL value inserted into a LISP Map-Reply message sent by an ETR in response to a Map-Request for an IPv4 EID-to-RLOC mapping.
ip lisp etr map-server	Configured the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv4 EID prefixes.
ip lisp itr	Configure the router to act as an IPv4 LISP Ingress Tunnel Router (ITR)
ip lisp itr map-resolver	Configured the IPv4 or IPv6 locator address of the LISP Map-Resolver to which the ITR sends IPv4 Map-Request messages
ip lisp itr send-data-probes	Configure an ITR or PITR to sending a Data Probe rather than a Map-Request message for IPv4 EID-to-RLOC mapping resolution.
ip lisp locator-vrf	Configures LISP to resolve IPv4 locators in the specified VRF.
ip lisp map-cache	Configures a static IPv4 EID-prefix to locator map-cache entry.
ip lisp map-cache-limit	Configure the maximum number of IPv4 LISP map-cache entries allowed to be stored by the router.
ip lisp source- locator	To configure a source locator to be used for an IPv4 LISP encapsulated packets
ip lisp proxy-etr	Configures the router to act as an IPv4 LISP Proxy Egress Tunnel Router (PETR)
ip lisp proxy-itr	Configures the router to act as an IPv4 LISP Proxy Ingress Tunnel Router (PITR)
ip lisp use-bgp-locators	Configures LISP to use iBGP routes as EID-prefixes and their BGP RIB next-hop addresses as locators.
ip lisp use-petr	Configures an ITR or PITR to use the PETR for traffic destined to non-LISP IPv4 destinations.

show ip lisp data-cache

To display the LISP IPv4 EID-to-RLOC data-cache mapping on an ITR, use the **show ip lisp data-cache** command in privileged EXEC mode.

show ip lisp data-cache [*destination-EID*][**vrf** *vrf-name*]

Syntax Description

destination-EID	(Optional) Displays mappings for the specified destination EID.
vrf *vrf-name*	(Optional) Display per-VRF information.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command is used on LISP ITR devices to display the LISP IPv4 EID-to-RLOC data-cache mappings. Data-cache mappings are built when a Map-Request is sent and are maintained until a valid (matching nonce) Map-Reply is received. The data-cache entry is then moved to the map-cache.

Examples

The following sample output from the **show ip lisp data-cache** command.

```
Router# show ip lisp data-cache
LISP IP Mapping Data Cache for Context "default", 0 entries, hwm: 4
Complete entries removed after 15-second period: 0
Incomplete entries removed after 1-minute period: 0
Router#
```

Related Commands

Command	Description
ip lisp map-cache	Display the current dynamic and static IPv4 EID-to-RLOC map-cache entries.

---

show ip lisp database

To display LISP ETR configured local IPv4 EID-prefixes and associated locator sets, use the **show ip lisp database** command in privileged EXEC mode.

show ip lisp database [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Display information for the specified VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command is used on LISP ETR devices to display the configured local IPv4 EID-prefixes and associated locator set(s).

Examples

The following sample output from the **show ip lisp database** command displays the configured IPv4 EID-prefix block(s) and associated locator set(s). As illustrated, the output of this command shows the configured IPv4 EID-to-RLOC database mappings.

```
Router# show run
...<skip>...
!
ip lisp database-mapping 192.168.12.0/24 172.22.156.23 priority 1 weight 100
!

Router# show ip lisp database
LISP ETR IP Mapping Database for VRF "default" (iid 0), global LSBs: 0x00000001

EID-prefix: 192.168.12.0/24, instance-id: 0, LSBs: 0x00000001
  Locator: 172.22.156.23, priority: 1, weight: 100
          Uptime: 10:36:59, state: up, local
Router#
```

The following sample output from the **show ip lisp database** command displays the configured IPv4 EID-prefix block(s) and associated locator set(s) using the configured VRF context **customer1**. As illustrated, the output of this command shows the configured IPv4 EID-to-RLOC database mappings.

```
Router# show run
...<skip>...
!
ip lisp database-mapping 10.10.10.0/24 172.16.1.1 priority 1 weight 100
!

Router# show ip lisp database vrf customer1
LISP ETR IP Mapping Database for VRF "customer1" (iid 0), global LSBs: 0x00000000

EID-prefix: 10.10.10.0/24, instance-id: 0, LSBs: 0x00000001
  Locator: 172.16.1.1, priority: 1, weight: 1
          Uptime: 00:00:10, state: up, local
Router#
```

Related Commands

Command	Description
ip lisp database-mapping	Configure an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy.

show ip lisp locator-hash

To display source and destination locators that are used for a given IPv4 source and destination EID pair, use the **show ip lisp locator-hash** command in privileged EXEC mode.

show ip lisp locator-hash {*source-EID dest-EID*} | *dest-EID-prefix*} [**vrf** *vrf-name*]

Syntax Description

source-EID	IPv4 source EID
dest-EID	IPv4 destination EID
dest-EID-prefix	IPv4 destination EID-prefix
vrf *vrf-name*	(Optional) Specifies the vrf within which to resolve EIDs

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command is used to display the source and destination locators that are used for a given IPv4 source and destination EID pair as the result of the locator hashing process. The source locator is chosen based on the source EID from the EID-prefix database configured via the **ip lisp etr database-mapping** command. The destination locator is selected by finding the destination EID in the EID-to-RLOC map-cache.

When the *dest-EID-prefix* form of the command is used, the locator hash array is display, indicating which locator will be used for each of 25 different flow hash buckets.

When the **vrf** *vrf-name* form of the command is used, IPv4 EIDs are resolved within the specified VRF in order to display the locator-hash.

Examples

The following sample output from the **show ip lisp locator-hash** command displays the locators used between the IPv4 source-dest EID pairs 153.16.12.1 and 153.16.11.1.

```
Router# show ip lisp database
LISP ETR IP Mapping Database for VRF "default", global LSBs: 0x00000001

EID-prefix: 153.16.12.0/24, LSBs: 0x00000001
  Locator: 128.223.156.23, priority: 1, weight: 100
          Uptime: 04:14:41, state: up, local

Router# show ip lisp map-cache
---<skip>---
153.16.11.0/24, uptime: 04:12:35, expires: 19:47:24, via map-reply, auth
  Locator        Uptime     State       Priority/  Data        Control
                                        Weight     in/out      in/out
  67.169.7.150  04:12:35   up          1/100      1968/1967   3/2

Router# show ip lisp locator-hash 153.16.12.1 153.16.11.1
```

```
EIDs 153.16.12.1 -> 153.16.11.1 yields:
  RLOCs 128.223.156.23 -> 67.169.7.150
  Address hash: 0x07 (7), hash bucket: 7, RLOC index: 0
Router#
```

The following sample output from the **show ip lisp locator-hash** command displays the full locator hash bucket for the IPv4 destination EID-prefix 153.16.11.0/24.

```
Router# show ip lisp locator-hash 153.16.11.0/24
RLOC Hash Indexes for EID-prefix 153.16.11.0/24:
    [00000-00000-00000-00000-00000]
Router#
```

Related Commands

Command	Description
ip lisp database-mapping	Configure an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy.

---

show ip lisp map-cache

To display the current dynamic and static IPv4 EID-to-RLOC map-cache entries, use the **show ip lisp map-cache** command in privileged EXEC mode.

show ip lisp map-cache [*destination-EID | destination-EID-prefix/prefix-length* | **vrf** *vrf-name*][**detail**]

Syntax Description

destination-EID	(Optional) Destination EID for which to display mapping information.
destination-EID-prefix/prefix-length	(Optional) Destination EID-prefix to display mapping for.
vrf *vrf-name*	(Optional) Display detailed EID-to-RLOC cache mapping information for the referenced VRF.
detail	(Optional) Display verbose mapping information.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command is used to display the current dynamic and static IPv4 EID-to-RLOC map-cache entries. When no IPv4 EID or IPv4 EID-prefix is specified, summary information is listed for all current dynamic and static IPv4 EID-to-RLOC map-cache entries. When an IPv4 EID or IPv4 EID-prefix is included, information is listed for the longest-match lookup in the cache. When the **vrf** option is used, summary information related to the referenced *vrf-name* is listed.

Examples

The following sample output from the **show ip lisp map-cache** command (without the use of an IPv4 EID or IPv4 EID-prefix) displays a summary list of current dynamic and static IPv4 EID-to-RLOC map-cache entries. The display shows IPv4 EID-prefix and associated information.

```
Router# show ip lisp map-cache
LISP IP Mapping Cache for VRF "default", 4 entries

153.16.1.0/24, uptime: 04:41:40, expires: 19:18:19, via map-reply, auth
  Locator          Uptime    State        Priority/ Data        Control
                                          Weight    in/out      in/out
  129.250.1.255    04:41:40  up           254/0     0/0         0/0
  129.250.26.242   04:41:40  up           1/100     1139/1138   1/0
---<skip>---
Router#
```

The following sample output from the **show ip lisp map-cache** command with a specific IPv4 EID-prefix displays detailed information associated with that IPv4 EID prefix entry.

```
Router# show ip lisp map-cache 153.16.11.0/24
LISP IP Mapping Cache for VRF "default", 4 entries

153.16.11.0/24, uptime: 04:43:21, expires: 19:16:38, via map-reply, auth
  State: complete, last modified: 04:43:21, map-source: 67.169.7.150
  Locator          Uptime    State        Priority/ Data        Control
                                          Weight    in/out      in/out
  67.169.7.150   04:43:21  up           1/100     2214/2213   3/2
    Last up/down state change:     04:43:21, state change count: 0
    Last data packet in/out:       00:00:14/00:00:14
    Last control packet in/out:    00:45:23/00:45:23
    Last priority/weight change:   never/never
Router#
```

Related Commands

Command	Description
show ip lisp	Display the IPv4 LISP configuration status for the local device.

---

show ip lisp statistics

To display LISP IPv4 address-family packet count statistics, use the **show ip lisp statistics** command in privileged EXEC mode.

   show ip lisp statistics [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Display statistics for the specified VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command is used to display IPv4 LISP statistics related to packet encapsulations, de-encapsulations, map-requests, map-replies, map-registers, and other LISP-related packets.

Examples

The following sample output from the **show ip lisp statistics** command displays the current LISP IPv4 address family statistics. The output varies, depending on the LISP features configured and the state of various LISP components.

```
Router# show ip lisp statistics
LISP Statistics for VRF "default" - last cleared: never
Data Forwarding:
  IPv4-in-IPv4 encap/decap packets:    4687/33220
  IPv4-in-IPv6 encap/decap packets:    0/3555
  Translated packets in/out:           0/0
  Map-cache lookup succeeded/failed:   5908/78
  LISP-ALT lookup succeeded/failed:    0/0
  Loc-reach-bit changes local/remote:  0/0
Control Packets:
  Data-Probes in/out:                  0/0
  Map-Requests in/out:                 654/90
    Encapsulated Map-Requests in/out:  0/90
    RLOC-probe Map-Requests in/out:    607/0
    SMR-based Map-Requests in/out:     0/0
  Map-Replies in/out:                  73/654
    Security header included in/out:   0/0
    Authoritative in/out:              4/654
    Non-authoritative in/out:          69/0
    Negative Map-Replies in/out:       69/0
    RLOC-probe Map-Replies in/out:     0/607
  Map-Registers in/out:                0/294
    Authentication failures:           0
  Map-Notifies in/out:                 0/0
    Authentication failures:           0
  Map-Notify-Acks in/out:              0/0
Errors:
  Encapsulations failed:               78
  Map-Request format errors:           0
  Map-Reply format errors:             0
  Map-Reply spoof alerts:              0
  Map-Reply signature failed:          0
Cache Related:
  Cache entries created/timed-out:     40/36
  Number of EID-prefixes in map-cache: 4
  Number of negative map-cache entries: 1
  Number of translation cache entries: 0
  Total number of RLOCs in map-cache:  6
  Number of best-priority RLOCs:       5
  Average RLOCs per EID-prefix:        1
Router#
```

Related Commands

Command	Description
show ip lisp	Display the IPv4 LISP configuration status for the local device.

show ip lisp translate-cache

To display the LISP IPv4 address translation cache and statistics associated with each entry, use the **show ip lisp translation-cache** command in privileged EXEC mode.

> **show ip lisp translation-cache** [*non-routable-EID*]

Syntax Description

non-routable-EID	(Optional) IPv4 address of inside non-routable EID.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command is used to display the LISP IPv4 address translation cache and statistics associated with each entry. This command is only applicable when the **ip lisp translate** command is used to configure LISP translation.

When the *non-routable-EID* form of the command is used, only the statistics associated with that single translation are displayed.

Examples

The following sample output from the **show ip lisp translate-cache** command displays the current LISP IPv4 translation statistics. The output varies depending on the configuration of the **ip lisp translate** command and traffic.

```
Router# show ip lisp translate-cache
LISP EID Translation Cache for VRF "default" - 1 entries
Inside: 10.1.1.1 outside: 172.16.1.1, ingress/egress count: 0/0
  Last ingress packet: never, last egress packet: never
Router#
```

Related Commands

Command	Description
show ip lisp	Display the IPv4 LISP configuration status for the local device.

show ipv6 lisp

To display the LISP IPv6 configuration status, use the **show ipv6 lisp** command in privileged EXEC mode.

show ipv6 lisp [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Display statistics for the specified VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command is used to display the IPv6 LISP configuration status for the local device. When the optional vrf vrf-name is used, the IPv6 LISP configuration status related to the specified VRF context only is displayed.

Examples

The following sample output from the **show ipv6 lisp** command displays information about the current IPv6 LISP configuration status. The output varies, depending on the LISP features configured.

```
Router# show ipv6 lisp
LISP IPv6 Configuration Information for VRF "default" (iid 0)
  Ingress Tunnel Router (ITR):     enabled
  Egress Tunnel Router (ETR):      enabled
  Proxy-ITR Router (PTR):          disabled
  Proxy-ETR Router (PETR):         disabled
  Map Resolver (MR):               disabled
  Map Server (MS):                 disabled
  LISP control-plane security:     enabled (weak-mode)
  Locator VRF:                     default
  Last-resort source locator:      2001:db8:d01:9c::80df:9c17
  LISP-NAT Interworking:           disabled
  Use locators from BGP RIB:       disabled
  ITR send Map-Request:            enabled
  ITR send Data-Probe:             disabled
  LISP-ALT vrf:                    not configured
  ITR Map-Resolver:                172.22.156.35
  ETR Map-Server(s):               172.22.156.35, 172.22.132.89
  Last Map-Register sent to MS:    00:00:20
  ETR glean mapping:               disabled, verify disabled
  ETR accept mapping data:         disabled, verify disabled
  ETR map-cache TTL:               24 hours
  Send IP Map-Reply:               enabled
```

```
   Shortest EID-prefix allowed:    /48
   Use Proxy-ETRs:                 172.16.2.1
Locator Reachability Algorithms:
   Echo-nonce algorithm:          disabled
   TCP-counts algorithm:          disabled
   RLOC-probe algorithm:          disabled
 Static mappings configured:      0
 Map-cache limit:                 1000
 Map-cache size:                  3
 ETR Database, global LSBs: 0x00000001:
   EID-prefix: 2001:db8:1203::/48, LSBs: 0x00000001
     Locator: 172.22.156.23, priority: 1, weight: 100
             Uptime: 09:27:51, state: up, local
Router#
```

The following sample output from the **show ipv6 lisp** command displays information about the current IPv6 LISP configuration status when on the `ipv6 lisp etr map-server` command has been configured, and the Map-Resolver locator is taken to be the same as the configured Map-Server locator.

```
Router# show ipv6 lisp
LISP IP Configuration Information for VRF "default" (iid 0)
---<skip>---
  LISP ALT-VRF:                    not configured
  ETR Map-Server(s):               2001:db8:bb::2, also Map-Resolver(s)
```

Table 2 describes the significant fields shown in the display.

Table 2 show ipv6 lisp Field Descriptors

Field	Description
Ingress Tunnel Router (ITR)	This field indicates whether the router is configured as an ITR (see **ipv6 lisp itr**)
Egress Tunnel Router (ETR)	This field indicates whether the router is configured as an ETR. (see **ipv6 lisp etr**)
Proxy-ITR	This field indicates whether the router is configured as a PITR. (see **ipv6 lisp proxy-itr**)
Proxy-ETR	This field indicates whether the router is configured as a PETR. (see **ipv6 lisp proxy-etr**)
Map-Resolver (MR)	This field indicates whether the router is configured as a MR. (see **ipv6 lisp map-resolver**)
Map-Server (MS)	This field indicates whether the router is configured as a MS. (see **ipv6 lisp map-server**)
LISP control-plane security	This field indicates whether LISP-SEC functionality is enabled and its mode. (see **lisp security**)
Locator VRF	This field indicates the VRF in which to resolver locators. (see **ipv6 lisp locator-vrf**)
Last-resort source locator	Last-resort source locator for LISP messages.
LISP-NAT Interworking	This field indicates whether the router is configured for LISP NAT (see **ipv6 lisp translate**)
Use locators from BGP RIB	This field indicates whether LISP is configured to use iBGP routes as EID-prefixes and their BGP RIB next-hop addresses as locators (see **ipv6 lisp use-bgp-locators**)
ITR send Map-Request	This field indicates whether sending Map-Requests is enabled. (see **ipv6 lisp itr map-resolver**)
ITR send Data-Probe	This field indicates whether **ipv6 lisp itr send-data-probe** is enabled
LISP-ALT vrf	This field indicates whether a LISP-ALT VRF configured and identifies the VRF name. (see **ipv6 lisp alt-vrf**)
ITR Map-Resolver	Identifies the configured ITR Map-Resolver. (see **ipv6 lisp itr map-resolver**).
ETR Map-Server(s)	Identifies the configured ETR Map-Server(s). (see **ipv6 lisp etr map-server**).
Last Map-Register sent to MS	This field indicates when this device last sent a Map-Registration message

LISP-132

	to the configured Map-Server(s).
ETR glean mapping	Indicates whether the ETR is configured to glean mapping data contained in a encapsulated packet (see **ipv6 lisp etr glean-mapping**)
ETR accept mapping data	Indicates whether the ETR is configured to cache the mapping data contained in a Map-Request (see **ipv6 lisp etr accept-map-request-mapping**)
ETR map-cache TTL	Identifies the current ETR map-cache TTL (see **ipv6 lisp etr map-cache-ttl**)
Shortest EID-prefix allowed	This field indicates the EID-prefix length accepted in a Map-Reply. (see **ipv6 lisp shortest-eid-prefix-length**)
Use Proxy-ETRs	When configured, indicates whether the router uses a PETR and lists the PETR locator.
Locator Reachability Algorithms	Indicates the status of the available locator reachability algorithms (Echo-nonce, TCP-counts, RLOC-probing) (see **lisp loc-reach-algorithm**)
Static mappings configured	Indicates the number of static cache-map entries are configured (see **ipv6 lisp map-cache**)
Map-cache limit	Indicates the current map-cache limit and identifies any configured reserve-list. (see **ipv6 lisp map-cache-limit**).
Map-cache size	Indicates the current number of entries in the map-cache.
ETR Database	Lists global LSBs, configured EID-prefixes and Locators.

Related Commands

Command	Description
ipv6 lisp etr	Configures the router to act as an IPv6 LISP Egress Tunnel Router (ETR)
ipv6 lisp etr accept-map-request-mapping	Configure an ETR to cache IPv6 mapping data contained in a Map-Request message
Ipv6 lisp etr glean-mapping	Configure an ETR to glean inner header (EID) source address to outer header (RLOC) source address mappings from encapsulated data packets to its EID-to-RLOC cache IPv6 mapping data.
ipv6 lisp etr map-cache-ttl	Configures the TTL value inserted into a LISP Map-Reply message sent by an ETR in response to a Map-Request for an IPv6 EID-to-RLOC mapping.
ipv6 lisp etr map-server	Configured the IPv4 or IPv6 locator address of the LISP Map-Server to which an ETR should register for its IPv6 EID prefixes.
ipv6 lisp itr	Configure the router to act as an IPv6 LISP Ingress Tunnel Router (ITR)
ipv6 lisp itr map-resolver	Configured the IPv4 or IPv6 locator address of the LISP Map-Resolver to which the ITR sends IPv6 Map-Request messages
ipv6 lisp itr send-data-probes	Configure an ITR or PITR to sending a Data Probe rather than a Map-Request message for Ipv6 EID-to-RLOC mapping resolution.
Ipv6 lisp locator-vrf	Configures LISP to resolve IPv6 locators in the specified VRF.
ipv6 lisp map-cache	Configures a static IPv6 EID-prefix to locator map-cache entry.
ipv6 lisp map-cache-limit	Configure the maximum number of IPv6 LISP map-cache entries allowed to be stored by the router.
ipv6 lisp source- locator	To configure a source locator to be used for an IPv6 LISP encapsulated packets
ipv6 lisp proxy-etr	Configures the router to act as an IPv6 LISP Proxy Egress Tunnel Router (PETR)
ipv6 lisp proxy-itr	Configures the router to act as an IPv6 LISP Proxy Ingress Tunnel Router (PITR)
ip lisp use-bgp-locators	Configures LISP to use iBGP routes as EID-prefixes and their BGP RIB next-hop addresses as locators.
ipv6 lisp use-petr	Configures an ITR or PITR to use the PETR for traffic destined to non-LISP IPv6 destinations.

show ipv6 lisp data-cache

To display the LISP IPv6 EID-to-RLOC data-cache mapping on an ITR, use the **show ipv6 lisp data-cache** command in privileged EXEC mode.

>   **show ipv6 lisp data-cache** [*destination-EID*][**vrf** *vrf-name*]

Syntax Description

destination-EID	(Optional) Displays mappings for the specified destination EID.
vrf *vrf-name*	(Optional) Display per-VRF information.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command is used on LISP ITR devices to display the LISP IPv6 EID-to-RLOC data-cache mappings. Data-cache mappings are built when a Map-Request is sent and are maintained until a valid (matching nonce) Map-Reply is received. The data-cache entry is then moved to the map-cache.

Examples

The following sample output from the **show ipv6 lisp data-cache** command.

```
Router# show ipv6 lisp data-cache
LISP IPv6 Mapping Data Cache for Context "default", 0 entries, hwm: 1
Complete entries removed after 15-second period: 0
Incomplete entries removed after 1-minute period: 1
Router#
```

Related Commands

Command	Description
ipv6 lisp map-cache	Display the current dynamic and static IPv6 EID-to-RLOC map-cache entries.

---

show ipv6 lisp database

To display LISP ETR configured local IPv6 EID-prefixes and associated locator sets, use the **show ipv6 lisp database** command in privileged EXEC mode.

LISP-134

show ipv6 lisp database [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Display information for the specified VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command is used on LISP ETR devices to display the configured local IPv6 EID-prefixes and associated locator set(s).

Examples

The following sample output from the **show ipv6 lisp database** command displays the configured IPv6 EID-prefix block(s) and associated locator set(s). As illustrated, the output of this command shows the configured IPv6 EID-to-RLOC database mappings.

```
Router# show run
...<skip>...
!
ipv6 lisp database-mapping 2001:DB8:1209::/48 172.22.156.222 priority 1 weight 100
!

Router# show ipv6 lisp database
LISP ETR IPv6 Mapping Database for VRF "default" (iid 0), global LSBs: 0x0000000f

EID-prefix: 2001:db8:1209::/48, instance-id: 0, LSBs: 0x0000000f
  172.22.156.222, priority: 1, weight: 100, state: up, local
Router#
```

Related Commands

Command	Description
ipv6 lisp database-mapping	Configure an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy.

show ipv6 lisp locator-hash

To display source and destination locators that are used for a given IPv6 source and destination EID pair, use the **show ipv6 lisp locator-has** command in privileged EXEC mode.

>   **show ipv6 lisp locator-hash** {*source-EID dest-EID*} | *dest-EID-prefix*} [**vrf** *vrf-name*]

Syntax Description

source-EID	IPv6 source EID
dest-EID	IPv6 destination EID
dest-EID-prefix	IPv6 destination EID-prefix
vrf *vrf-name*	(Optional) Specifies the vrf within which to resolve EIDs

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command is used to display the source and destination locators that are used for a given IPv6 source and destination EID pair as the result of the locator hashing process. The source locator is chosen based on the source EID from the EID-prefix database configured via the **ipv6 lisp etr database-mapping** command. The destination locator is selected by finding the destination EID in the EID-to-RLOC map-cache.

When the *dest-EID-prefix* form of the command is used, the locator hash array is display, indicating which locator will be used for each of 25 different flow hash buckets.

When the **vrf** *vrf-name* form of the command is used, IPv6 EIDs are resolved within the specified VRF in order to display the locator-hash.

Examples

The following sample output from the **show ipv6 lisp database** command and **show ipv6 lisp map-cache** command is displayed for reference, and then output from the **show ipv6 lisp locator-hash** command is displayed for the locators used between the IPv6 source-dest EID pairs 2610:d0:1203::1 and 2610:d0:210f::1.

```
Router# show ipv6 lisp database
LISP ETR IPv6 Mapping Database for VRF "default", global LSBs: 0x00000001

EID-prefix: 2610:d0:1203::/48, LSBs: 0x00000001
  Locator: 128.223.156.23, priority: 1, weight: 100
          Uptime: 04:25:06, state: up, local
Router# show ipv6 lisp map-cache
---<skip>---
2610:d0:210f::/48, uptime: 04:18:39, expires: 19:41:20, via map-reply, auth
```

LISP-136

```
     Locator          Uptime      State      Priority/  Data     Control
                                              Weight     in/out   in/out
     85.184.2.10       04:18:39    up         0/100      0/0      0/0
     2001:6e0:4:2::2   04:18:39    up         0/100      0/0      0/0

Router# show ipv6 lisp locator-hash 2610:d0:1203::1 2610:d0:210f::1
EIDs 2610:d0:1203::1 -> 2610:d0:210f::1 yields:
  RLOCs 128.223.156.23 -> 85.184.2.10
  Address hash: 0x00 (0), hash bucket: 0, RLOC index: 0
Router#
```

The following sample output from the **show ip lisp locator-hash** command displays the full locator hash bucket for the IPv6 destination EID-prefix 2610:d0:210f::/48.

```
Router# show ipv6 lisp locator-hash 2610:d0:210f::/48
RLOC Hash Indexes for EID-prefix 2610:d0:210f::/48:
    [00000-00000-00000-00000-00000]
Router#
```

Related Commands

Command	Description
ipv6 lisp database-mapping	Configure an IPv6 EID-to-RLOC mapping relationship and associated traffic policy.

---

show ipv6 lisp map-cache

To display the current dynamic and static IPv6 EID-to-RLOC map-cache entries, use the **show ipv6 lisp map-cache** command in privileged EXEC mode.

> **show ipv6 lisp map-cache** [*destination-EID* | *destination-EID-prefix/prefix-length* | **vrf** *vrf-name*][**detail**]

Syntax Description

destination-EID	(Optional) Destination EID for which to display mapping information.
destination-EID-prefix/prefix-length	(Optional) Destination EID-prefix to display mapping for.
vrf *vrf-name*	(Optional) Display detailed EID-to-RLOC cache mapping information for the referenced VRF.
detail	(Optional) Display verbose mapping information.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command is used to display the current dynamic and static IPv6 EID-to-RLOC map-cache entries. When no IPv6 EID or IPv6 EID-prefix is specified, summary information is listed for all current dynamic and static IPv6 EID-to-RLOC map-cache entries. When an IPv4 EID or IPv4 EID-prefix is included, information is listed for the longest-match lookup in the cache. When the **vrf** option is used, summary information related to the referenced *vrf-name* is listed.

Examples

The following sample output from the **show ipv6 lisp map-cache** command (without the use of an IPv6 EID or IPv6 EID-prefix) displays a summary list of current dynamic and static IPv6 EID-to-RLOC map-cache entries. The display shows IPv6 EID-prefix and associated information.

```
Router# show ipv6 lisp map-cache
LISP IPv6 Mapping Cache for VRF "default", 1 entries

2610:d0:210f::/48, uptime: 04:48:44, expires: 19:11:15, via map-reply, auth
  Locator          Uptime     State       Priority/  Data      Control
                                          Weight     in/out    in/out
  85.184.2.10      04:48:44   up          0/100      0/0       0/0
  2001:6e0:4:2::2  04:48:44   up          0/100      0/0       0/0
---<skip>---
Router#
```

The following sample output from the **show ipv6 lisp map-cache** command with a specific IPv6 EID-prefix displays detailed information associated with that IPv6 EID prefix entry.

```
Router# show ipv6 lisp map-cache 2610:d0:210f::/48
LISP IPv6 Mapping Cache for VRF "default", 1 entries

2610:d0:210f::/48, uptime: 04:50:43, expires: 19:09:16, via map-reply, auth
  State: complete, last modified: 04:50:43, map-source: 85.184.2.10
  Locator          Uptime     State       Priority/  Data      Control
                                          Weight     in/out    in/out
  85.184.2.10      04:50:43   up          0/100      0/0       0/0
    Last up/down state change:    04:50:43, state change count: 0
    Last data packet in/out:      never/never
    Last control packet in/out:   never/never
    Last priority/weight change:  never/never
  2001:6e0:4:2::2  04:50:43   up          0/100      0/0       0/0
    Last up/down state change:    04:50:43, state change count: 0
    Last data packet in/out:      never/never
    Last control packet in/out:   never/never
    Last priority/weight change:  never/never
Router#
```

Related Commands

Command	Description
show ipv6 lisp	Display the IPv6 LISP configuration status for the local device.

show ipv6 lisp statistics

To display LISP IPv6 address-family statistics, use the **show ipv6 lisp statistics** command in privileged EXEC mode.

> **show ipv6 lisp statistics** [**vrf** *vrf-name*]

LISP-138

Syntax Description

vrf *vrf-name*	(Optional) Display statistics for the specified VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command is used to display IPv6 LISP statistics related to packet encapsulations, de-encapsulations, map-requests, map-replies, map-registers, and other LISP-related packets.

Examples

The following sample output from the **show ipv6 lisp statistics** command displays the current LISP IPv6 address family statistics. The output varies, depending on the LISP features configured and the state of various LISP components.

```
Router# show ipv6 lisp statistics
LISP Statistics for VRF "default" - last cleared: never
Data Forwarding:
  IPv6-in-IPv4 encap/decap packets:    1239/0
  IPv6-in-IPv6 encap/decap packets:    0/0
  Translated packets in/out:           0/0
  Map-cache lookup succeeded/failed:   2461/1260
  LISP-ALT lookup succeeded/failed:    0/0
  Loc-reach-bit changes local/remote:  0/0
Control Packets:
  Data-Probes in/out:                  0/0
  Map-Requests in/out:                 1219/1280
    Encapsulated Map-Requests in/out:  0/1280
    RLOC-probe Map-Requests in/out:    0/0
    SMR-based Map-Requests in/out:     0/0
  Map-Replies in/out:                  1243/1217
    Security header included in/out:   0/0
    Authoritative in/out:              1243/1219
    Non-authoritative in/out:          0/0
    Negative Map-Replies in/out:       0/0
    RLOC-probe Map-Replies in/out:     0/0
  Map-Registers in/out:                0/614
    Authentication failures:           0
  Map-Notifies in/out:                 0/0
    Authentication failures:           0
  Map-Notify-Acks in/out:              0/0
Errors:
  Encapsulations failed:               1260
  Map-Request format errors:           0
  Map-Reply format errors:             0
  Map-Reply spoof alerts:              0
```

LISP-139

```
  Map-Reply signature failed:        0
Cache Related:
  Cache entries created/timed-out:   32/27
  Number of EID-prefixes in map-cache: 5
  Number of negative map-cache entries: 4
  Number of translation cache entries: 0
  Total number of RLOCs in map-cache: 6
  Number of best-priority RLOCs:     6
  Average RLOCs per EID-prefix:      1
Router#
```

Related Commands

Command	Description
show ipv6 lisp	Display the IPv6 LISP configuration status for the local device.

---

show ipv6 lisp translate-cache

To display the LISP IPv6 address translation cache and statistics associated with each entry, use the **show ipv6 lisp translation-cache** command in privileged EXEC mode.

> **show ipv6 lisp translation-cache** [*non-routable-EID*]

Syntax Description

non-routable-EID	(Optional) IPv6 address of inside non-routable EID.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command is used to display the LISP IPv6 address translation cache and statistics associated with each entry. This command is only applicable when the **ipv6 lisp translate** command is used to configure LISP translation.

When the *non-routable-EID* form of the command is used, only the statistics associated with that single translation are displayed.

Examples

The following sample output of the **show ipv6 lisp translate-cache** command displays current IPv6 translation statistics. The output varies depending on the configuration of the **ipv6 lisp translate** command and traffic.

LISP-140

```
Router# show ipv6 lisp translate-cache
LISP EID Translation Cache for VRF "default" - 1 entries
Inside: 2001:db8:aa::1 outside: 2001:db8:bb::1, ingress/egress count: 0/0
  Last ingress packet: never, last egress packet: never
Router#
```

Related Commands

Command	Description
show ipv6 lisp	Display the IPv6 LISP configuration status for the local device.

---

show lisp ddt

To display the configured DDT root(s) and/or DDT delegation nodes on a router enabled for LISP DDT, use the **show lisp ddt** command in privileged EXEC mode.

> **show lisp ddt**

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

Use this command to display the configured DDT root(s) and/or DDT delegation nodes on a router enabled for LISP DDT node.

Examples

The following example shows the output of **show lisp ddt** command for a LISP DDT node configured as a Map-Resolver refering to three LISP DDT root nodes with locators: 10.1.1.1, 10.2.1.1, and 10.3.1.1, and configured as a Map-Server for the EID-prefixes 172.16.0.0/16 and 2001:db8:eeee::/48 in the default (0) instance-ID for its own locator (10.1.10.10) and a peer Map-Server locator (10.2.10.10).

```
Router# show lisp ddt
LISP-DDT Configuration in VRF "default"
  DDT IP Map-Resolver configured
  DDT IPv6 Map-Resolver configured
  DDT IP Map-Server configured
  DDT IPv6 Map-Server configured
  Configured DDT roots: 10.1.1.1  10.2.1.1  10.3.1.1
  Configured DDT delegated nodes/map-servers:
    [0] 172.16.0.0/16 -> 10.1.10.10, p/w: 0/0, map-server-peer
    [0] 172.16.0.0/16 -> 10.2.10.10, p/w: 0/0, map-server-peer
    [0] 2001:db8:eeee::/48 -> 10.1.10.10, p/w: 0/0, map-server-peer
```

LISP-141

```
    [0] 2001:db8:eeee::/48 -> 10.2.10.10, p/w: 0/0, map-server-peer

  Configured authoritative EID-prefixes:
    [0] 172.16.0.0/16
    [0] 2001:db8:eeee::/48
Router#
```

Related Commands

Command	Description
show lisp ddt queue	Display the DDT lookup queue stored on a DDT-enabled Map-Resolver.
show lisp ddt referral-cache	Display the DDT referral cache stored on a DDT-enabled Map-Resolver.

---

show lisp ddt referral

To display the DDT referral cache stored on a DDT-enabled Map-Resolver, use the **show lisp ddt referral-cache** command in privileged EXEC mode.

> **show lisp ddt referral-cache** [[**instance-id** *iid*] *eid*] [**vrf** *vrf-name*]

Syntax Description

instance-ID *iid*	(Optional) Display the DDT referral cache related to this single instance-ID.
eid	(Optional) Display the DDT referral cache related to this single EID.
vrf *vrf-name*	(Optional) Display the DDT referral cache related to this VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

Use this command to display the referral cache on a DDT Map-Resolver.

A DDT Map Resolver uses an iterative process of following referrals to find the correct ETR to answer a Map-Request; this requires a DDT Map Resolver to maintain additional state: a Map-Referral cache and a lookup queue of Map-Requests that are going through the iterative referral process. The **show lisp ddt referral-cache** command displays the contents of the Map-Referral cache.

When **show lisp ddt referral-cache** is specified using the optional *eid* entry, the display is limited to any referral cache entries that are less specific than *eid*.

When **show lisp ddt referral-cache** is specified using the optional **instance-id** *iid* entry, the display is limited to all referral cache entries within **instance-id** *iid*. When **show lisp ddt referral-cache** is specified using the optional **instance-id** *iid eid* entry, the display is limited to only referral cache entries that are less specific than *eid* only within **instance-id** *iid*.

When **show lisp ddt referral-cache** is specified using the optional **vrf** *vrf-name* entry, the display is limited to the referral cache entries related to **vrf** *vrf-name*.

LISP-142

Examples

The following example shows the output of **show lisp ddt referral-cache** command for a LISP DDT node configured as a Map-Resolver refering to three LISP DDT root nodes with locators: 10.1.1.1, 10.2.1.1, and 10.3.1.1, and configured as a Map-Server for the EID-prefixes 172.16.0.0/16 and 2001:db8:eeee::/48 in the default (0) instance-ID for its own locator (10.1.10.10) and a peer Map-Server locator (10.2.10.10). (Assume the Map-Resolver has been operating for sufficient time to populate its referral cache.)

```
Router# show lisp ddt referral-cache
LISP-DDT Referral Cache in VRF "default", 14 entries

[*] *, uptime: 1d19h, roots:
  -> 10.1.1.1, requests-sent: 1935, no-responses: 0
  -> 10.2.1.1, requests-sent: 1556, no-responses: 1
  -> 10.3.1.1, requests-sent: 1502, no-responses: 0

[0] 0.0.0.0/2, uptime: 00:03:59, expires: 00:11:00, ttl: 15
  Source: root 10.1.1.1, delegation-hole
---<skip>---
[0] 172.16.1.0/24, uptime: 18:21:28, expires: 05:38:31, ttl: 1440
  Source: map-server 10.10.2.1, ms-ack, referrals:
  -> 10.1.1.1, requests-sent: 0, no-responses: 0
  -> 10.2.1.1, requests-sent: 1, no-responses: 0
  -> 10.3.1.1, requests-sent: 0, no-responses: 0

[0] 172.16.2.0/24, uptime: 18:21:28, expires: 05:38:31, ttl: 1440
  Source: map-server 10.10.2.1, ms-ack, referrals:
  -> 10.1.1.1, requests-sent: 1, no-responses: 0
  -> 10.2.1.1, requests-sent: 0, no-responses: 0
  -> 10.3.1.1, requests-sent: 0, no-responses: 0
---<skip>---
 [0] 0::/3, uptime: 00:10:57, expires: 00:04:02, ttl: 15
  Source: root 10.1.1.1, delegation-hole
---<skip>---
 [0] 2001:db8:eeee:1001::/48, uptime: 00:00:59, expires: 0.172576, ttl: 1
  Source: map-server 10.10.2.1, ms-not-registered, referrals:
  -> 10.1.1.1, requests-sent: 0, no-responses: 0, dont-use
  -> 10.2.1.1, requests-sent: 1, no-responses: 0, dont-use
  -> 10.3.1.1, requests-sent: 1, no-responses: 0, dont-use
---<skip>---
[0] 2001:db8:eeee:2001::/48, uptime: 18:12:17, expires: 05:47:42, ttl: 1440
  Source: map-server 10.10.2.1, ms-ack, referrals:
  -> 10.1.1.1, requests-sent: 1, no-responses: 0
  -> 10.2.1.1, requests-sent: 1, no-responses: 0
  -> 10.3.1.1, requests-sent: 0, no-responses: 0
---<skip>---
Router#
```

Related Commands

Command	Description
show lisp ddt	Display the the configured DDT root(s) and/or DDT delegation nodes.
show lisp ddt queue	Display the DDT lookup queue stored on a DDT-enabled Map-Resolver.

---

show lisp ddt queue

To display the DDT lookup queue stored on a DDT-enabled Map-Resolver, use the **show lisp ddt queue** command in privileged EXEC mode.

> **show lisp ddt queue** [[**instance-id** *iid*] *eid*] [**vrf** *vrf-name*]

Syntax Description

instance-ID *iid*	(Optional) Display the DDT lookup queue related to this single instance-ID.
eid	(Optional) Display the DDT lookup queue related to this single EID.

LISP-143

| vrf *vrf-name* | (Optional) Display the DDT lookup queue related to this VRF. |

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

Use this command to display the lookup queue on a DDT Map-Resolver.

A DDT Map Resolver uses an iterative process of following referrals to find the correct ETR to answer a Map-Request; this requires a DDT Map Resolver to maintain additional state: a Map-Referral cache and a lookup queue of Map-Requests that are going through the iterative referral process. The **show lisp ddt queue** command displays the contents of the lookup queue of Map-Requests.

When **show lisp ddt queue** is specified using the optional *eid* entry, the display is limited to any lookup queue entries that are less specific than *eid*.

When **show lisp ddt queue** is specified using the optional **instance-id** *iid eid* entry, the display is limited to any lookup queue entries that are less specific than *eid* only within **instance-id** *iid*.

When **show lisp ddt queue** is specified using the optional **vrf** *vrf-name* entry, the display is limited to the lookup queue entries related to **vrf** *vrf-name*.

Examples

The following example shows the output of **show lisp ddt queue** command for a LISP DDT node configured as a Map-Resolver. Note that queue entries will likely only be found when the Map-Resolver is under some load, as referrals should be handled efficiently.

```
Router# show lisp ddt queue
LISP-DDT Map-Request Queue in VRF "default", 1 entries in queue, hwm: 1909

[0] 172.16.3.1 <- 10.50.50.5, PITR: 10.2.2.2
  Nonce: 0x457834cb-0x4ebdb342
  Last sent: 0.126847, send-count: 0
  Awaiting reply from: 10.2.1.1
Router#
```

Related Commands

Command	Description
show lisp ddt	Display the the configured DDT root(s) and/or DDT delegation nodes.
show lisp ddt referral-cache	Display the DDT referral cache stored on a DDT-enabled Map-Resolver.

show lisp dynamic-eid

To display the LISP dynamic-EIDs configured and discovered on this device, use the **show lisp dyanmic-eid** command in privileged EXEC mode.

LISP-144

show lisp dyanmic-eid [summary] [*dynamic-eid-name*] [**vrf** *vrf-name*] [**detail**]

Syntax Description

summary	(Optional) Display one-line summary of discovered dynamic-EIDs
dynamic-eid-name	(Optional) Display LISP dynamic-EID information for a single dynamic-EID.
vrf *vrf-name*	(Optional) Display dynamic-EID information for the specified VRF.
detail	(Optional) Increase the detail of all displayed LISP dynamic-EIDs.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13) (August update)	This command was introduced.
Cisco NX-OS Release 5.0(3.lisp)	This command was modified.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command is used on LISP VM routers to display information related to LISP dynamic-EIDs configured and discovered on this device. The displayed output indicates, among other things, the number of roaming dynamic-EIDs configured, including associated database-mapping information, and the number of roaming dynamic-EIDs.

When the summary keyword is used, a one-line listing is presented per discovered dynamic-EID. When the *dynamic-eid-name* entry is listed, then information related to that single entry is displayed. When the **vrf** option is used, information related to LISP dynamic-EIDs within the referenced *vrf-name* is displayed. When the **detail** keyword is added, a list of discovered roaming EIDs is displayed.

Examples

The following sample output from the **show lisp dyanmic-eid** command displays summary information related to all configured and discovered LISP LISP dynamic-EIDs.

```
xTR# show lisp dynamic-eid
LISP Dynamic EID Information for VRF "default"
Dynamic-EID name: Roamer-1
  Database-mapping EID-prefix: 153.16.19.2/32, registering more-specifics
    Locator: 173.8.188.25, priority: 1, weight: 50, local
    Locator: 173.8.188.26, priority: 1, weight: 50, local
  Map-Server(s): 204.69.200.7
  Number of roaming dynamic-EIDs discovered: 0
xTR#
```

The following sample output from the **show lisp dyanmic-eid** command displays detailed information related to the specific dynamic-EID named **bc4**.

```
XTR# show lisp dynamic-eid bc4 detail
LISP Dynamic EID Information for VRF "default"
Dynamic-EID name: bc4
  Database-mapping EID-prefix: 30.1.110.104/32, LSBs: 0x00000001
    Locator: 90.1.93.1, priority: 1, weight: 10, local
  Registering more-specific dynamic-EIDs
  Map-Server(s): 90.32.32.32
```

LISP-145

```
   Number of roaming dynamic-EIDs discovered: 1
   Last dynamic-EID discovered: 30.1.110.104, 00:08:06 ago
   Roaming dynamic-EIDs:
     30.1.110.104, Ethernet2/5, uptime: 00:08:06, last activity: 0.998355
 XTR#
```

The following sample output from the **show lisp dyanmic-eid summary** command displays summary information related to discovered dynamic-EIDs. In this case, only the dynamic-EID named **bc4** is discovered and listed.

```
 XTR# show lisp dynamic-eid summary
 LISP Dynamic EID Summary for VRF "default"
 Dyn-EID Name   Dynamic-EID      Interface     Uptime    Last Packet  SMR-mode
 bc4            172.16.110.104   Ethernet10/18 22:05:35  0.370583     no
 XTR#
```

Related Commands

Command	Description
show ip lisp	Display the IPv4 LISP configuration status for the local device.
lisp dynamic-eid	Configure a LISP dynamic-EID policy
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
lisp mobility	Configure an interface on an ITR to participate in LISP VM-mobility (dynamic-EID roaming)

show lisp negative-prefix

To compute and display the negative prefix hole in the LISP ALT for an IPv4 EID address, use the **show lisp negative-prefix** command in privileged EXEC mode.

> **show lisp negative-prefix {**IPv4-*EID-address* **|** *IPv6-EID-address***}**

Syntax Description

IPv4-EID-address	IPv4 EID address to use when computing the negative-prefix hole in EID space.
IPv6-EID-address	IPv6 EID address to use when computing the negative-prefix hole in EID space.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.2(0.266.lisp-58)	This command was added.

Usage Guidelines

This command is used to compute and display the prefix within the ALT that covers the IPv4 or IPv6 EID address queried. If the ALT contains a LISP EID prefix covering the address queried, it is displayed. If the ALT does not contain a LISP EID prefix covering the address queried, it displays the longest negative-prefix covering the address queried.

Examples

The following partial sample output from the **show ip route vrf lisp** command displays some of the entries in the example LISP ALT. Output from the **show alt negative-prefix** command is then shown to illustrate its use in locating holes in the ALT prefixes.

```
Map-Server# show ip route vrf lisp
---<skip>---
172.16.1.0/24, ubest/mbest: 1/0
    *via Null0, [10/0], 2w6d, lisp, alt-eid, tag 666
172.16.3.0/24, ubest/mbest: 1/0
    *via 10.0.254.101, [200/0], 1w5d, bgp-32768.10, internal, tag 2147483658
172.16.4.0/24, ubest/mbest: 1/0
    *via 10.0.254.101, [200/0], 1w5d, bgp-32768.10, internal, tag 2147483658
172.16.5.0/24, ubest/mbest: 1/0
    *via 10.0.254.101, [200/0], 1w5d, bgp-32768.10, internal, tag 2147483658
172.16.8.0/24, ubest/mbest: 1/0
    *via 10.0.254.12, [200/0], 1w6d, bgp-32768.10, internal, tag 2147483658
---<skip>---
Map-Server# show lisp negative-prefix 172.16.1.1
Compute negative prefix for EID 172.16.1.1:
  ALT summary route found, negative-prefix 172.16.1.1/32
  Site cache entry found, EID-prefix: 172.16.1.0/24, registered
  Action: forward Map-Request to site ETR
Map-Server# show lisp negative-prefix 172.16.6.1
Compute negative prefix for EID 172.16.6.1:
  ALT summary route found, negative-prefix 172.16.6.0/23
  Site cache entry not found, negative-prefix: 172.16.6.0/24
  Action: build negative Map-Reply with site-based negative-prefix 172.16.6.0/24
Map-Server#
```

Related Commands

There are no related commands.

---

show lisp proxy-itr

To display a list of Proxy-ITRs (PITRs) that have been discovered through Map-Requests having been received for them, use the **show lisp proxy-itr** command in privileged EXEC mode.

   show lisp proxy-itr [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) VRF within which to clear locator address of the PITR

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(3.lisp-80)	This command was introduced.

Usage Guidelines

Due to the unidirectional nature of data flows for Proxy-ITRs (PITRs), an xTR will never have a map-cache entry that contains locators for PITRs. However, when an xTR receives a Map-Request from a PITR for an EID-to-RLOC mapping resolution, the locator address of the PITR is saved (separately from the map-cache) by an xTR for later in the event that there is a need to send Solicit-Map-Requests (SMRs) to other LISP devices, including PITRs. The number of locators currently cached is eight (8).

This command displays the list of PITRs that have been discovered through Map-Requests having been received for them. When the **vrf** *vrf-name* form is used, all PITR locators associated with this VRF are displayed.

Examples

The following displays sample output for the **show lisp proxy-itr** command.

```
Router# show lisp proxy-itr
Discovered Proxy-ITRs (PITRs) in VRF "default"
  10.20.10.60
Router#
```

Related Commands

There are no related commands.

---

show lisp site

On a LISP Map-Server, to display configured LISP sites, use the **show lisp site** command in privileged EXEC mode.

> **show lisp site** [*EID* | *EID-prefix*] [**instance-id** *iid*]] | [*site-name*] [**vrf** *vrf-name*] [**detai**l]

Syntax Description

EID	(Optional) Display LISP site information matching this destination EID.
EID-prefix	(Optional) Display LISP site information matching this destination EID-prefix.
instance-id *iis*	(Optional) Display LISP site information matching this instance-id.
site-name	(Optional) Display LISP site information matching this site-name.
vrf *vrf-name*	(Optional) Display LISP site information for the referenced VRF.
detail	(Optional) Increase the detail of all displayed LISP site information when no other parameters are used.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin
network-operator
vdc-operator

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

This command is used on a LISP Map-Server to display information related to configured LISP sites. The displayed output indicates, among other things, whether a site is actively registered.

By design, three levels of detail can be displayed using various forms of the **show lisp site** command:

show lisp site	When this base form of the command is used, summary information related to all configured LISP sites is displayed.
show lisp site *site-name*	When the *site-name* form is used, the displayed information contains all EID-prefixes configured for the named LISP site.
show lisp site *site-name* detail	When the **detail** keyword is added, all available details for the specific command form are presented.

In addition to the above details, additional parameters may be added to further tune the displayed output.

- When the *IPv4-dest-EID* form is used, a longest-match is done to return the site with the best matching EID-prefix and the displayed information applies specifically to that LISP site.
- When the *IPv4-dest-EID-prefix* form is used, exact-match is done to return the site configured with the EID-prefix and the displayed information applies specifically to that LISP site.
- When the **instance-id** iid form is used, information is displayed for the registered LISP site covering the EID/EID-prefix and that instance-id.
- When the **vrf** *vrf-name* form is used, information is displayed only for LISP sites that contain the referenced VRF.

Examples

The following sample output from the **show lisp site** command displays summary information related to all configured LISP sites.

```
Map-Server# show lisp site
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address

Site Name      Last       Actively   Who last        EID-prefix
               Registered Registered Registered
cisco-it-xtr   00:00:47   yes        172.16.81.170   2001:db8:110c::/48
               00:00:18   yes        172.17.81.170   192.168.5.0/24
dmm-xtr-1      00:00:56   yes        172.30.156.134  2001:db8:1200::/48
               00:00:56   yes        172.31.65.94    192.168.10.0/24
dmm-xtr-2      00:00:48   yes        172.30.156.23   2001:db8:1203::/48
               never      no         --              192.168.12.0/24
Map-Server#
```

The following sample output from the **show lisp site** command displays detailed information related specifically to the LISP site **a1-xtr-1**.

```
Map-Server# show lisp site a1-xtr-1
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address

Site name:   "a1-xtr-1"
Description: Contact – customer1 email
Allowed configured locators: any
Allowed EID-prefixes:
  Configured EID-prefix: 2001:db8:1200::/48, instance-id: 0
    More-specifics registered: 0 MSMR# sh lisp site instance-id 101
LISP Site Instance-ID Registration Information for VRF "default"
Site Name      Actively   Instance  EID-prefix
               Registered ID
Left           yes        101       192.168.1.0/24
Left           yes        101       2001:db8:a:a::/64
Right          yes        101       192.168.2.0/24
Right          yes        101       2001:db8:a:b::/64
```

LISP-149

```
      Currently registered: yes
      First registered:     07:54:01
      Last registered:      00:00:10
      Who last registered:      172.30.156.134
      Routing table tag:        0x00000000
      Proxy Replying:           no
      Wants Map-Notifications:  no
      Registering as a LISP-MN: no
      Registered TTL:           1440 minutes
      Registered locators:
        172.30.156.134 (up), priority: 1, weight: 50
        172.31.65.94   (up), priority: 1, weight: 50
      Registration errors:
        Authentication failures: 0
        Allowed locators mismatch: 0
    Configured EID-prefix: 192.168.10.0/24, instance-id: 0
      More-specifics registered: 0
      Currently registered:     yes
      First registered:         2w0d
      Last registered:          00:00:36
      Who last registered: 172.30.156.134
      Routing table tag:        0x00000000
      Proxy Replying:           no
      Wants Map-Notifications:  no
      Registering as a LISP-MN: no
      Registered TTL:           1440 minutes
      Registered locators:
        172.30.156.134 (up), priority: 1, weight: 50
        172.31.65.94   (up), priority: 1, weight: 50
      Registration errors:
        Authentication failures: 0
        Allowed locators mismatch: 0
  Map-Server#
```

Related Commands

Command	Description
show ip lisp	Display the IPv4 LISP configuration status for the local device.

LISP Debug Commands

debug-filter ip lisp

To configure the EID VRF for which all following LISP debug commands apply, use the **debug-filter ip lisp** command in privileged EXEC mode. To disable debug filtering, use the **no** form of this command.

> **debug-filter ip lisp** {[**locator-vrf** *vrf-name*] | [**vrf** *vrf-name*]}
>
> **no debug-filter ip lisp** [[**locator-vrf** *vrf-name*] | [**vrf** *vrf-name*]]

Syntax Description

locator-vrf *vrf-name*	Debug information for the specified locator VRF .
vrf *vrf-name*	Debug information for the specified EID VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

The **debug-filter ip lisp** command defines either the locator or the EID VRF for which all following LISP debug commands apply. Without this command, LISP debug commands apply to the default VRF.

Use of this command may be useful to help troubleshoot interactions between various VRF contexts used by LISP. For example, when the systems *default* VRF is used for locators and the EID VRF is used by LISP-ALT, when an IPv4 Map-Request from an ITR arrives at the Map-Resolver configured to use the LISP-ALT, the Map-Resolver receives the Map-Request in the *default* VRF. After decapsulating the Map-Request from its ECM header, the Map-Resolver forwards the Map-Request to the next-hop found in the VRF dedicated to the LISP-ALT. Since the LISP-ALT uses the VRF referred to in the **ip lisp alt-vrf** *vrf-name* command, the **debug-filter ip lisp vrf** command must also refer to this same *vrf-name*.

✎
Note This command is also required when LISP is configured in more than one VRF in order to debug activities related specifically to EIDs in that VRF.

When an xTR is configured to use a locator VRF that is different from the default VRF or from the EID VRF, the **debug-filter ip lisp locator-vrf** command defines the locator VRF for which all following LISP debug commands apply. Without this command, LISP debug commands apply to the default VRF.

✎
Note The command **undebug all** does not remove debug-filter entries. They must be removed using the **no** form of the specific **debug-filter** entry.

Examples

In the following example, debug filtering is applied to the EID VRF named *lisp*, the VRF context specified to be used by the LISP ALT in this case.

```
Router# debug-filter ip lisp vrf lisp
```

In the following example, suppose LISP is configured to use the EID VRF named **red** and the locator VRF **default**. In order to see Map-Register activity for VRF **red** when it is configured to use the locator-VRF **default**, use the following commands:

LISP Config (partial):

```
Router(config)# vrf context red
Router(config-vrf)# ip lisp locator-vrf default
```

Then, use the following LISP debug commands:

```
Router# debug-filter ip lisp vrf red
Router# debug-filter ip lisp locator-vrf default
Router# debug lisp mapping register
```

Related Commands

Command	Description
ip lisp alt-vrf	Configure which VRF supporting the IPv4 address-family LISP should use when sending Map Requests for an IPv4 EID-to-RLOC mapping directly over the ALT.
ip lisp locator-vrf	Configure the VRF context to be used by local locators on this device.

---

debug ip lisp mapping

To display logs for Map-Request, Map-Reply, and other LISP IPv4 mapping activities, use the **debug ip lisp mapping** command in privileged EXEC mode. To disable this debugging, use the **no** form of the command.

> **debug ip lisp mapping** {**control** | **data**} [*EID-prefix*]
>
> **no debug ip lisp mapping** {**control** | **data**} [*EID-prefix*]

Syntax Description

control	Messages from the NX-OS LISP process are displayed.
data	Messages from the NX-OS Netstack process are displayed.
EID-prefix	(Optional) Filter debug output displays for this IPv4 EID-prefix.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The **debug ip lisp mapping** command displays logs for Map-Request, Map-Reply, and other LISP IPv4 mapping activities. When the **control** keyword is used, all mapping debug messages related to the NX-OS LISP process are displayed. When the **data** keyword is used, mapping debug messages related to the NX-OS LISP process are displayed. When the optional *EID-prefix* is configured, logs related to that EID-prefix are displayed.

Examples

In the following example, IPv4 data mapping debugging is enabled for the control process.

```
Router# debug ip lisp mapping control
2010 Mar 11 19:00:41.890493 lisp: Map-cache entry EID-prefix 192.0.0.0/3 has timed out
2010 Mar 11 19:00:41.890529 lisp: Delete mapping for EID: 192.0.0.0/3, removing all locators
2010 Mar 11 19:01:28.224770 lisp: Mapping record for EID 153.16.12.0/24, ttl: 1440, locator
count: 1, a-bit: 0
2010 Mar 11 19:01:28.224805 lisp:   Locator: 128.223.156.23, upriority/uweight: 1/100,
mpriority/mweight: 255/0, state: up
2010 Mar 11 19:01:28.224953 lisp: Encapsulate LISP IP Map-Request from 128.223.156.23 to
configured map-resolver 128.223.156.35
2010 Mar 11 19:01:28.225597 lisp: Add mapping, EID: 64.0.0.0/2, state: forward-native, ttl:
15 mins, locator: 0.0.0.0, loc-state: up, up/uw/mp/mw: 0/0/0/0, source: 128.223.156.35,
protocol-source: map-reply, a: 0
2010 Mar 11 19:03:12.300924 lisp: Mapping record for EID 153.16.12.0/24, ttl: 1440, locator
count: 1, a-bit: 0
2010 Mar 11 19:03:12.301811 lisp: Recalculation of RLOC hash indexes for 192.0.0.0/3:
2010 Mar 11 19:03:12.301836 lisp:   Current indexes: [*****-*****-*****-*****-*****]
2010 Mar 11 19:03:12.301881 lisp:   New indexes: [00000-00000-00000-00000-00000]
Router# no debug ip lisp mapping control
```

Related Commands

Command	Description
debug ip lisp packet	Display IPv4 LISP encapsulation/de-encapsulation debug messages

---

debug ip lisp packet

To display logs for IPv4 packets that are encapsulated by the ITR or de-encapsulated by the ETR, use the **debug ip lisp packet** command in privileged EXEC mode. To disable this debugging output, use the **no** form of this command.

> **debug ip lisp packet** [**all** | **decap** | **encap**] [*EID-prefix*] [**detail**] [**translate**]
>
> **no debug ip lisp packet** [**all** | **decap** | **encap**] [*EID-prefix*] [**detail**] [**translate**]

Syntax Description

all	(Optional) Display messages for LISP decap and encap processes (ETR and ITR).
decap	(Optional) Display messages for LISP decap process (ETR).
encap	(Optional) Display messages for LISP encap process (ITR).
EID-prefix	(Optional) Filter debug output displays for this IPv4 EID-prefix.
detail	(Optional) Display more detailed messages.
translate	(Optional) Display messages for LISP decap and/or encap that use address translation.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The **debug ip lisp packet** command displays logs for IPv4 packets that are encapsulated by the ITR or de-encapsulated by the ETR. When the **decap** keyword is used, logs for IPv4 packets that are de-encapsulated by the ETR are displayed. When the **encap** keyword is used, logs for IPv4 packets that are encapsulated by the ITR are displayed. When the **all** keyword is used, logs for both packets processes are displayed. When *EID-prefix* is configured, only the logs related to that EID-prefix are displayed. When the **detail** keyword is used, more detailed logs are displayed. When the **translate** keyword is used, logs for packets that also LISP address translation are displayed. LISP addresses translation is configured using the **ip lisp translate** command.

✎

Note When **debug ip lisp packet** is used and an IPv4 packet (EID) is encapsulated in an IPv6 header(RLOC) because the locator chosen was an IPv6 locator, the destination site will only show debug output for the decapsulation log message when **debug ipv6 lisp packet** is enabled.

Examples

In the following example, IPv4 data encapsulation/decapsulation debugging is enabled.

```
Router# debug ip lisp packet 153.16.12.0/24
2010 Mar 11 22:28:55.365180 netstack: liblisp [3757] LISP decapsulate packet, outer:
149.20.48.60 -> 128.223.156.23, inner: 85.184.2.202 -> 153.16.12.1, nonce(on): 0x00db0b3c,
lsb(off): 0x00000000
2010 Mar 11 22:28:57.022462 netstack: liblisp [3757] LISP decapsulate packet, outer:
149.20.48.60 -> 128.223.156.23, inner: 95.24.213.135 -> 153.16.12.61, nonce(on): 0x00037dbb,
lsb(off): 0x00000000
2010 Mar 11 22:28:57.029734 netstack: liblisp [3757] LISP decapsulate packet, outer:
149.20.48.60 -> 128.223.156.23, inner: 85.184.2.202 -> 153.16.12.1, nonce(on): 0x0071da45,
lsb(off): 0x00000000
2010 Mar 11 22:28:57.173398 netstack: liblisp [3757] LISP decapsulate packet, outer:
149.20.48.60 -> 128.223.156.23, inner: 188.36.50.127 -> 153.16.12.102, nonce(on): 0x0008fa9f,
lsb(off): 0x00000000
Router# no debug ip lisp packet 153.16.12.0/24
```

Related Commands

Command	Description
debug ip lisp packet	Display IPv4 LISP encapsulation/de-encapsulation debug messages
debug ipv6 lisp packet	Display IPv6 LISP encapsulation/de-encapsulation debug messages
ip lisp translate	Configure IPv4 LISP translation mapping.

debug ip lisp traceroute

On an ITR, to display logs related to caching operations for traceroute headers and modifying to ICMP Time Exceeded messages, use the **debug ip lisp packet** command in privileged EXEC mode. To disable this debugging output, use the **no** form of this command.

debug ip lisp traceroute
no debug ip lisp traceroute

LISP-154

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

Special support for IPv4 traceroute is provided for sources in a LISP site to a destination site. In order for a user to see the path from an ITR to the ETR across the core, special mechanisms must keep track of traceroute headers and returned ICMP Time Exceeded messages returned to the ITR.

Different support is required for traceroute in IPv4 than for IPv6. In IPv6, the entire invoking packet is included in an ICMPv6 Time Exceeded message and an ITR can forward the ICMPv6 message back to the traceroute source in a stateless manner. In IPv4, however, only the invoking IP header and 8 bytes of IP payload are included in the ICMP Time Exceeded message which only covers the outer encapsulated header that the ITR prepended and the UDP header for the LISP encapsulation. Therefore, an IPv4 ITR must cache traceroute headers and modify ICMP Time Exceeded messages returned to the ITR for forwarding back to the traceroute source. The **debug ip lisp traceroute** command displays messages related to these caching operations for traceroute headers and modifying to ICMP Time Exceeded messages.

Examples

In the following example, a host with the LISP IPv4 source address 153.16.10.19 initiated a traceroute to the LISP IPv4 destination address 153.16.11.1. (Truncated output shown.)

```
Router# debug ip lisp traceroute
2010 Mar 11 23:55:09.948642 netstack: liblisp [3762] Found traceroute packet, UDP ports:
56591/33435, seq_num: 1
2010 Mar 11 23:55:09.948720 netstack: liblisp [3762] Caching traceroute header with UDP port
key: 0xffad, index: 13, IP ident: 33599, for 153.16.10.19 -> 153.16.11.1, ttl: 1
2010 Mar 11 23:55:09.948947 netstack: liblisp [3762] Found traceroute packet, UDP ports:
52086/33436, seq_num: 2
2010 Mar 11 23:55:09.948994 netstack: liblisp [3762] Caching traceroute header with UDP port
key: 0xffae, index: 14, IP ident: 33855, for 153.16.10.19 -> 153.16.11.1, ttl: 2
2010 Mar 11 23:55:09.949215 netstack: liblisp [3762] Found traceroute packet, UDP ports:
41872/33437, seq_num: 3
2010 Mar 11 23:55:09.949262 netstack: liblisp [3762] Caching traceroute header with UDP port
key: 0xffaf, index: 15, IP ident: 34111, for 153.16.10.19 -> 153.16.11.1, ttl: 3
2010 Mar 11 23:55:09.949482 netstack: liblisp [3762] Found traceroute packet, UDP ports:
51262/33438, seq_num: 4
2010 Mar 11 23:55:09.949529 netstack: liblisp [3762] Caching traceroute header with UDP port
key: 0xffb0, index: 0, IP ident: 34367, for 153.16.10.19 -> 153.16.11.1, ttl: 4
---<skip>---
Router#
```

Related Commands

Command	Description
debug ip lisp packet	Display IPv4 LISP encapsulation/de-encapsulation debug messages

debug-filter ipv6 lisp

To configure the EID VRF for which all following LISP debug commands apply, use the **debug-filter ipv6 lisp** command in privileged EXEC mode. To disable debug filtering, use the **no** form of this command.

> **debug-filter ipv6 lisp** {[**locator-vrf** *vrf-name*] | [**vrf** *vrf-name*]}
> **no debug-filter ipv6 lisp** [[**locator-vrf** *vrf-name*] | [**vrf** *vrf-name*]]

Syntax Description

locator-vrf *vrf-name*	Debug information for the specified locator VRF.
vrf *vrf-name*	Debug information for the specified EID VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

The **debug-filter ipv6 lisp** command defines either the locator or the EID VRF for which all following LISP debug commands apply. Without this command, LISP debug commands apply to the default VRF.

Use of this command may be useful to help troubleshoot interactions between between various VRF contexts used by LISP. For example, when the systems *default* VRF is used for locators and the EID VRF is used by LISP-ALT, whenan IPv4 Map-Request from an ITR arrives at the Map-Resolver configured to use the LISP-ALT, the Map-Resolver receives the Map-Request in the *default* VRF. After decapsulating the Map-Request from its ECM header, the Map-Resolver forwards the Map-Request to the next-hop found in the VRF dedicated to the LISP-ALT. Since the LISP-ALT uses the VRF referred to in the **ipv6 lisp alt-vrf** *vrf-name* command, the **debug-filter ipv6 lisp vrf** command must also refer to this same *vrf-name*.

✎
Note This command is also required when LISP is configured in more than one VRF in order to debug activities related specifically to EIDs in that VRF.

When an xTR is configured to use a locator VRF that is different from the default VRF or from the EID VRF, the **debug-filter ipv6 lisp locator-vrf** command defines the locator VRF for which all following LISP debug commands apply. Without this command, LISP debug commands apply to the default VRF.

✎
Note The command **undebug all** does not remove debug-filter entries. They must be removed using the **no** form of the specific **debug-filter** entry.

Examples

In the following example, debug filtering is applied to the EID VRF named *lisp*, which is the VRF context specified to be used by the LISP ALT in this case.

```
Router# debug-filter ipv6 lisp vrf lisp
```

LISP-156

In the following example, suppose LISP is configured to use the EID VRF named **red** and the locator VRF **default**. In order to see Map-Register activity for VRF **red** when it is configured to use the locator-VRF **default**, use the following commands:

LISP Config (partial):

```
Router(config)# vrf context red
Router(config-vrf)# ipv6 lisp locator-vrf default
```

Then, use the following LISP debug commands:

```
Router# debug-filter ipv6 lisp vrf red
Router# debug-filter ipv6 lisp locator-vrf default
Router# debug lisp mapping register
```

Related Commands

Command	Description
Ipv6 lisp alt-vrf	Configure which VRF supporting the IPv6 address-family LISP should use when sending Map Requests for an IPv6 EID-to-RLOC mapping directly over the ALT.
ipv6 lisp locator-vrf	Configure the VRF context to be used by local locators on this device.

debug ipv6 lisp mapping

To display logs for Map-Request, Map-Reply, and other LISP IPv6 mapping activities, use the **debug ipv6 lisp mapping** command in privileged EXEC mode. To disable this output, use the **no** form of this command.

debug ipv6 lisp mapping {**control** | **data**} [*EID-prefix*]

no debug ipv6 lisp mapping {**control** | **data**} [*EID-prefix*]

Syntax Description

control	Messages from the NX-OS LISP process are displayed.
data	Messages from the NX-OS Netstack process are displayed.
EID-prefix	(Optional) Filter debug output displays for this IPv6 EID-prefix.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The **debug ip lisp mapping** command displays logs for Map-Request, Map-Reply, and other LISP IPv4 mapping activities. When the **control** keyword is used, all mapping debug messages related to the NX-OS LISP process are displayed. When the **data** keyword is used, all mapping debug messages related to the NX-OS LISP process are displayed. When *EID-prefix* is configured, only the mlogs related to that EID-prefix are displayed.

LISP-157

Examples

In the following example, IPv4 data mapping debugging is enabled for the control process.

```
Router# debug ipv6 lisp mapping control
2010 Mar 12 00:13:13.974876 lisp: Build LISP Map-Request for 2001:6e0:4:200::2/128, nonce:
0x0821f4a5-0x352c2008, ITR RLOC: 128.223.156.134
2010 Mar 12 00:13:13.975049 lisp: Mapping record for EID 2610:d0:1200::/48, ttl: 1440,
locator count: 2, a-bit: 0
2010 Mar 12 00:13:13.975084 lisp:   Locator: 128.223.156.134, upriority/uweight: 1/100,
mpriority/mweight: 255/0, state: up
2010 Mar 12 00:13:13.975120 lisp:   Locator: 2001:468:d01:9c::80df:9c86, upriority/uweight:
2/100, mpriority/mweight: 255/0, state: up
2010 Mar 12 00:13:13.975279 lisp: Encapsulate LISP IPv6 Map-Request from 128.223.156.134 to
configured map-resolver 128.223.156.35
2010 Mar 12 00:13:13.975962 lisp: Add mapping, EID: 2000::/6, state: forward-native, ttl: 15
mins, locator: 0.0.0.0, loc-state: up, up/uw/mp/mw: 0/0/0/0, source: 128.223.156.35,
protocol-source: map-reply, a: 0
2010 Mar 12 00:13:13.976003 lisp: Recalculation of RLOC hash indexes for 2000::/6:
2010 Mar 12 00:13:13.976029 lisp:   Current indexes: [*****-*****-*****-*****-*****]
2010 Mar 12 00:13:13.976075 lisp:   New indexes: [00000-00000-00000-00000-00000]
Router# no debug ipv6 lisp mapping control
```

Related Commands

Command	Description
debug ip lisp packet	Display IPv4 LISP encapsulation/de-encapsulation debug messages

---

debug ipv6 lisp packet

To display logs for IPv6 packets that are encapsulated by the ITR or de-encapsulated by the ETR, use the **debug ipv6 lisp packet** command in privileged EXEC mode. To disable this debugging output, use the **no** form of this command.

> **debug ipv6 lisp packet** [**all** | **decap** | **encap**] [*EID-prefix*] [**detail**] [**translate**]
>
> **no debug ipv6 lisp packet** [**all** | **decap** | **encap**] [*EID-prefix*] [**detail**] [**translate**]

Syntax Description

all	(Optional) Display messages for LISP decap and encap processes (ETR and ITR).
decap	(Optional) Display messages for LISP decap process (ETR).
encap	(Optional) Display messages for LISP encap process (ITR).
EID-prefix	(Optional) Filter debug output displays for this IPv6 EID-prefix.
detail	(Optional) Display more detailed messages.
translate	(Optional) Display messages for LISP decap and/or encap that use address translation.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The **debug ip lisp packet** command displays logs for IPv6 packets that are encapsulated by the ITR or de-encapsulated by the ETR. When the **decap** keyword is used, logs for IPv6 packets that are de-encapsulated by the ETR are displayed. When the **encap** keyword is used, logs for IPv6 packets that are encapsulated by the ITR are displayed. When the **all** keyword is used, logs for both packets processes are displayed. When *EID-prefix* is configured, only the logs related to that EID-prefix are displayed. When the **detail** keyword is used, more detailed logs are displayed. When the **translate** keyword is used, logs for packets that also LISP address translation are displayed. LISP addresses translation is configured using the **ip lisp translate** command.

> ✎
>
> **Note** When **debug ipv6 lisp packet** is used and an IPv6 packet (EID) is encapsulated in an IPv4 header(RLOC) because the locator chosen was an IPv4 locator, the destination site will only show debug output for the decapsulation log message when **debug ip lisp packet** is enabled. (The source site will show the encapsulation using **debug ipv6 lisp packet** however).

Examples

In the following example, IPv6 data encapsulation/decapsulation debugging is enabled.

```
Router# debug ipv6 lisp packet
2010 Mar 12 00:17:28.256710 netstack: liblisp [3762] LISP encapsulate packet, outer:
128.223.156.134 -> 85.184.2.10, inner: 2610:d0:1200::153:16:10:254 -> 2610:d0:210f:100::100,
nonce(on): 0x005cbf9e, lsb(on): 0x00000003
2010 Mar 12 00:17:29.609767 netstack: liblisp [3762] LISP encapsulate packet, outer:
128.223.156.134 -> 85.184.2.10, inner: 2610:d0:1200::153:16:10:254 -> 2610:d0:210f:100::100,
nonce(on): 0x006b176e, lsb(on): 0x00000003
2010 Mar 12 00:17:30.958423 netstack: liblisp [3762] LISP encapsulate packet, outer:
128.223.156.134 -> 85.184.2.10, inner: 2610:d0:1200::153:16:10:254 -> 2610:d0:210f:100::100,
nonce(on): 0x00331e89, lsb(on): 0x00000003
2010 Mar 12 00:17:31.653782 netstack: liblisp [3762] LISP encapsulate packet, outer:
2001:468:d01:9c::80df:9c86 -> 2001:470:1f05:a6:21b:21ff:fe1c:79f1, inner:
2610:d0:1200::153:16:10:6 -> 2610:d0:1202:1:5054:ff:fe21:6920, nonce(on): 0x000ac1b
Router# no debug ip lisp packet 153.16.12.0/24
```

Related Commands

Command	Description
debug ip lisp packet	Display IPv4 LISP encapsulation/de-encapsulation debug messages
debug ipv6 lisp packet	Display IPv6 LISP encapsulation/de-encapsulation debug messages
lpv6 lisp translate	Configure IPv6 LISP translation mapping.

---

debug lisp ddt

To display logs for all activities related to sending, receiving, and timing-out LISP DDT messages, use the **debug lisp ddt** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

> **debug lisp ddt**
>
> **no debug lisp ddt**

Syntax Description

This command has no arguments or keywords.

LISP-159

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

LISP DDT uses an iterative process of following referrals to find the correct ETR to answer a Map-Request. The **debug lisp ddt** command enables the display of activities related to sending, receiving, and timing-out LISP DDT messages.

Examples

No example is provided.

Related Commands

Command	Description
show lisp ddt	Display the the configured DDT root(s) and/or DDT delegation nodes.
show lisp ddt queue	Display the DDT lookup queue stored on a DDT-enabled Map-Resolver.
show lisp ddt referral-cache	Display the DDT referral cache stored on a DDT-enabled Map-Resolver.
clear lisp ddt referral-cache	Clear the DDT referral cache stored on a DDT-enabled Map-Resolver.

---

debug lisp loc-reach-algorithm

To display logs for activities related to the LISP locator-reachability algorithm rloc-probing, use the **debug lisp loc-reach-algorithm** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

> **debug lisp loc-reach-algorithm** [**receive-probe** | **send-probe**]
> **no debug lisp loc-reach-algorithm** [**receive-probe** | **send-probe**]

Syntax Description

receive-probe	Messages related to the responder-side of the rloc-probe are displayed.
send-probe	Messages related to the sender-side of the rloc-probe are displayed.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification

| Cisco NX-OS Release 5.0(1.13) | This command was introduced. |

Usage Guidelines

Three different locator reachability algorithms are available in LISP, including **tcp-count**, **echo-nonce**, and **rloc-probing**. These algorithms are configured using the **lisp loc-reach-algorithm** command. When the loc-reach algorithm rloc-probing is configured, debug output related to the sent and received probes can be display.

Use the **debug lisp loc-reach-algorithm** command to display logs for activities related to the LISP locator-reachability algorithm rloc-probing. When the **receive-probe** keyword is used, only the debug messages associated with the responder-side of RLOC-probing are displayed. When the **send-probe** keyword is used, only the debug messages associated with the sender-side of RLOC-probing are displayed. When neither keyword is used, debug messages associated with both sides of RLOC-probing are displayed.

Examples

In the following example, loc-reach debugging is enabled.

```
Router# debug lisp loc-reach-algorithm
2010 Mar 12 00:42:30.826419 netstack: liblisp [3762] Received RLOC-probe from locator
85.184.2.10 -> 207.98.65.94 with nonce 0x0cbbc1e4-0x7201a9b3
2010 Mar 12 00:42:30.826563 netstack: liblisp [3762] Send RLOC-probe reply to locator
128.223.156.134 -> 85.184.2.10 with nonce 0x0cbbc1e4-0x7201a9b3
2010 Mar 12 00:42:30.827352 netstack: liblisp [3762] Received RLOC-probe from locator
85.184.2.10 -> 128.223.156.134 with nonce 0xc7e3b56c-0x7d462a15
2010 Mar 12 00:42:30.827471 netstack: liblisp [3762] Send RLOC-probe reply to locator
128.223.156.134 -> 85.184.2.10 with nonce 0xc7e3b56c-0x7d462a15
Router#
Router# no debug lisp loc-reach-algorithm
```

Related Commands

Command	Description
lisp loc-reach-algorithm	Configure a LISP locator reachability algorithm

---

debug lisp mapping register

To display logs for activities related to sending, receiving, and timing-out site-based Map-Register messages, use the **debug lisp mapping register** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

> **debug lisp mapping register**
> **no debug lisp mapping register**

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When an ETR registers with a Map-Server, it sends a Map-Register message. A Map-Server receives Map-Register messages from all of its configured LISP sites. The **debug lisp mapping register** command enables the display of activities related to sending, receiving, and timing-out site-based Map-Register messages, NAT-traversal activity, and sending and receiving Map-Notify messages.

Examples

In the following example, mapping register debugging is enabled on a LISP ETR.

```
Router# debug lisp mapping register
2010 Mar 12 00:54:11.415927 lisp: Build IPv4 Map-Register
2010 Mar 12 00:54:11.415974 lisp: Mapping record for EID 153.16.10.0/24, ttl: 0, locator
count: 3, a-bit: 1
2010 Mar 12 00:54:11.416008 lisp:   Locator: 128.223.156.134, upriority/uweight: 1/50,
mpriority/mweight: 255/0, state: up
2010 Mar 12 00:54:11.416039 lisp:   Locator: 207.98.65.94, upriority/uweight: 1/50,
mpriority/mweight: 255/0, state: up
2010 Mar 12 00:54:11.416077 lisp:   Locator: 2001:468:d01:9c::80df:9c86, upriority/uweight:
2/100, mpriority/mweight: 255/0, state: up
2010 Mar 12 00:54:11.416125 lisp: Send IPv4 Map-Register to Map-Server 128.223.156.35
2010 Mar 12 00:54:11.416701 lisp: Build IPv6 Map-Register
2010 Mar 12 00:54:11.416737 lisp: Mapping record for EID 2610:d0:1200::/48, ttl: 0, locator
count: 2, a-bit: 1
2010 Mar 12 00:54:11.416774 lisp:   Locator: 128.223.156.134, upriority/uweight: 1/100,
mpriority/mweight: 255/0, state: up
2010 Mar 12 00:54:11.416812 lisp:   Locator: 2001:468:d01:9c::80df:9c86, upriority/uweight:
2/100, mpriority/mweight: 255/0, state: up
2010 Mar 12 00:54:11.416855 lisp: Send IPv6 Map-Register to Map-Server 128.223.156.35
Router# no debug lisp mapping register
```

Related Commands

Command	Description
ip lisp etr	Configure the router to act as an IPv4 LISP Egress Tunnel Router (ETR)
ipv6 lisp etr	Configure the router to act as an IPv6 LISP Egress Tunnel Router (ETR)
ip lisp map-server	Configure a device to function as an IPv4 LISP Map-Server.
Ipv6 lisp map-server	Configure a device to function as an IPv6 LISP Map-Server.

debug lisp mapping stats

To display logs for activities related to collecting statistics for mapping active EID flows into the aggregated LISP map-cache, use the **debug lisp mapping stats** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

> **debug lisp mapping stats**
> **no debug lisp mapping stats**

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

LISP devices run a process that maps active EID flows into the aggregated LISP map-cache. Statistics related to this process can be displayed using the **debug lisp mapping stats** command. This may be useful in troubleshooting mapping system issues.

Examples

In the following example, mapping statistics debugging is enabled on a LISP ITR.

```
Router# debug lisp mapping stats
2010 Mar 12 01:05:12.615683 lisp: Adding stats for EID 81.57.6.59 to map-cache entry
64.0.0.0/2
2010 Mar 12 01:05:12.615714 lisp:   IPC locator stats for 149.20.48.60, data in/out: 1/0,
control in/out:  0/0
2010 Mar 12 01:05:12.615746 lisp: Adding stats for EID 74.125.154.129 to map-cache entry
64.0.0.0/2
2010 Mar 12 01:05:12.615776 lisp:   IPC locator stats for 149.20.48.60, data in/out: 4/0,
control in/out:  0/0
2010 Mar 12 01:05:12.615808 lisp: Adding stats for EID 153.16.1.146 to map-cache entry
153.16.1.0/24
2010 Mar 12 01:05:12.615839 lisp:   IPC locator stats for 129.250.26.242, data in/out: 13/13,
control in/out:  0/0
2010 Mar 12 01:05:12.615867 lisp:   Map-cache locator stats data in/out: 32990/32976, control
in/out: 568/567
2010 Mar 12 01:05:12.615901 lisp: Adding stats for EID 94.198.233.234 to map-cache entry
64.0.0.0/2
Router# no debug lisp mapping stats
```

Related Commands

Command	Description
show ip lisp map-cache	Displays the LISP IPv4 EID-to-RLOC data-cache mapping on an ITR.
show ipv6 lisp map-cache	Displays the LISP IPv6 EID-to-RLOC data-cache mapping on an ITR.

---

debug lisp smr

To display logs for Solicit Map-Request (SMR) activities, use the **debug lisp smr** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

> **debug lisp smr** [*EID-prefix* | *EID-prefix6*]
> **no debug lisp smr** [*EID-prefix* | *EID-prefix6*]

Syntax Description

EID-prefix	(Optional) IPv4 EID-prefix range.
EID-prefix6	(Optional) IPv6 EID-prefix range.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was introduced.

Usage Guidelines

Whenever an ETR recognizes that changes have occurred for one of its EID-to-RLOC mappings, for example when a locator address changes or its status changes (up to down), or a priority or weight changes, then the local map-cache entry on an ITR that has changed this data requires updating in order to contain the latest information. When an ETR recognizes that a change has occurred, it initiates a Solicit Map-Request (SMR) exchange. The **debug lisp smr** command display logs for these activities. This may be useful to help troubleshoot various LISP map-cache issues. An optional IPv4 or IPv6 EID-prefix range can be supplied to limit outputs to the specified prefix.

Examples

No example is available for this command.

Related Commands

Command	Description
ip lisp database-mapping	Configures an IPv4 EID-to-RLOC mapping relationship and its associated traffic policy.
Ipv6 lisp database-mapping	Configures an IPv6 EID-to-RLOC mapping relationship and its associated traffic policy.

---

debug lisp ufdm

To display logs for activities between the LISP process and the Nexus 7000 UFDM process, use the **debug lisp ufdm** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

> **debug lisp ufdm** [**detail**]
> **no debug lisp ufdm** [**detail**]

Syntax Description

detail	(Optional) Display more detailed messages.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

When hardware-forwarding is enabled on the Nexus 7000 (by default), there is an interaction between the LISP process and the UFDM process that programs the Earl8 hardware with LISP map-cache and database entries. The **debug lisp ufdm** command display logs for these activities between the LISP process and the UFDM process. This may be useful to help troubleshoot various LISP issues on the Nexus 7000. When the **detail** keyword is used, per-entry level debugging is displayed.

Examples

No example is available for this command.

Related Commands

Command	Description
lisp beta	Enable LISP functionality on the Nexus 7000 router.
ip lisp hardware-forwarding	Display debug messages related to activities between the LISP process and the UFDM process and which program the EARL8.
ipv6 lisp hardware-forwarding	Display debug messages related to activities between the LISP process and the UFDM process and which program the EARL8.

LISP Clear Commands

clear ip lisp data-cache

To clear the LISP IPv4 data-cache, use the **clear ip lisp data-cache** command in privilege EXEC mode.

clear ip lisp data-cache [*EID*] [**vrf** *vrf-name*]

Syntax Description

EID	(Optional) IPv4 EID to clear from LISP map-cache
vrf *vrf-name*	(Optional) VRF within which to clear the data-cache.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The **clear ip lisp data-cache** command removes all IPv4 EID-to-RLOC mapping in the forwarding data-cache. Data-cache entries are present in two cases only. First, when **ip lisp itr send-data-probe** is configured, after a data-probe is sent, this data-probed is stored in the data-cache until a Map-Reply is returned. Second, when the **ip lisp etr glean-mapping** functionality is configured, gleaned EID-to-RLOC mapping data is stored in the data-cache until it is verified. When the optional **vrf** keyword is used, the data-cache is cleared for the specified VRF. When the *EID* option is used, only the EID-to-RLOC mapping for that entry is cleared.

Examples

The following example clears the IPv4 LISP data-cache.

```
Router# clear ip lisp data-cache
```

Related Commands

Command	Description
show ip lisp data-cache	Displays the LISP IPv4 EID-to-RLOC data-cache mapping on an ITR.

---

clear ip lisp map-cache

To clear the LISP IPv4 map-cache, use the **clear ip lisp map-cache** command in privilege EXEC mode.

clear ip lisp map-cache [*EID-prefix*] [**vrf** *vrf-name*]

Syntax Description

EID-prefix	(Optional) IPv4 EID-prefix to clear from LISP map-cache
vrf *vrf-name*	(Optional) VRF within which to clear the map-cache.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The **clear ip lisp map-cache** command removes all IPv4 dynamic EID-to-RLOC map-cache entries in the map-cache. When the optional *EID-prefix* is specified, only the EID-to-RLOC mapping for that entry is cleared. Otherwise, the entire data-cache is cleared. When the optional **vrf** keyword is specified, the data-cache is cleared for the specified VRF.

Examples

The following example clears the entire IPv4 LISP map-cache.

```
Router# clear ip lisp map-cache
Router# show ip lisp map-cache
LISP IP Mapping Cache for VRF "default", 0 entries
```

The following example shows all LISP map-cache entries, and then clears the LISP map-cache for the IPv4 EID-prefix 153.16.1.0/24.

```
Router# show ip lisp map-cache
LISP IP Mapping Cache for VRF "default", 2 entries

153.16.1.0/24, uptime: 00:00:06, expires: 23:59:53, via map-reply, auth
  Locator          Uptime    State         Priority/  Data     Control
                                           Weight     in/out   in/out
  129.250.1.255   00:00:06  up            254/0      0/0      0/0
  129.250.26.242  00:00:06  up            1/100      0/0      0/0

153.16.12.0/24, uptime: 00:00:04, expires: 23:59:55, via map-reply, self
  Locator          Uptime    State         Priority/  Data     Control
                                           Weight     in/out   in/out
  128.223.156.23  00:00:04  up            1/100      0/0      0/0
Router# clear ip lisp map-cache 153.16.1.0/24
Router# show ip lisp map-cache
LISP IP Mapping Cache for VRF "default", 1 entries

153.16.12.0/24, uptime: 00:00:46, expires: 23:59:13, via map-reply, self
  Locator          Uptime    State         Priority/  Data     Control
                                           Weight     in/out   in/out
  128.223.156.23  00:00:46  up            1/100      0/0      2/1
Router#
```

Related Commands

Command	Description
show ip lisp map-cache	Display current dynamic and static IPv4 EID-to-RLOC map-cache entries.

clear ip lisp statistics

To clear the LISP ITR and ETR IPv4 address-family packet count statistics, use the **clear ip lisp statistics** command in privilege EXEC mode.

> **clear ip lisp statistics** [vrf *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) VRF within which to clear the LISP statistics.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.0(3.lisp)	This command was modified.

Usage Guidelines

The **clear ip lisp statistics** command clears all of the LISP ITR and ETR IPv4 address-family packet count statistics. IPv4 address family packet count statistics are maintained for all LISP control plane packets. These packet counters are displayed using the **show ip lisp statistics** command.

Examples

The following example shows all IPv4 LISP control plane statistics (packet counters), and then clears these statistics.

```
Router# show ip lisp statistics
LISP Statistics for VRF "default" - last cleared: 00:42:59
Data Forwarding:
  IPv4-in-IPv4 encap/decap packets:    681/4040
  IPv4-in-IPv6 encap/decap packets:    0/516
  Translated packets in/out:           0/0
  Map-cache lookup succeeded/failed:   853/16
---<skip>---
Router# clear ip lisp statistics
Router# show ip lisp statistics
LISP Statistics for VRF "default" - last cleared: 00:00:02
Data Forwarding:
  IPv4-in-IPv4 encap/decap packets:    0/0
  IPv4-in-IPv6 encap/decap packets:    0/0
  Translated packets in/out:           0/0
  Map-cache lookup succeeded/failed:   0/0
---<skip>---
Router#
```

Related Commands

Command	Description
show ip lisp statistics	Display LISP IPv4 address-family statistics.

---

clear ipv6 lisp data-cache

To clear the LISP IPv6 data-cache, use the **clear ipv6 lisp data-cache** command in privilege EXEC mode.

> **clear ipv6 lisp data-cache** [*EID*] [**vrf** *vrf-name*]

Syntax Description

EID	(Optional) IPv6 EID to clear from LISP map-cache
vrf *vrf-name*	(Optional) VRF within which to clear the data-cache.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The **clear ipv6 lisp data-cache** command removes all IPv6 EID-to-RLOC mapping in the forwarding data-cache. Data-cache entries are present in two cases only. First, when **ipv6 lisp itr send-data-probe** is configured, after a data-probe is sent, this data-probed is stored in the data-cache until a Map-Reply is returned. Second, when **ipv6 lisp etr glean-mapping** functionality is configured, gleaned EID-to-RLOC mapping data is stored in the data-cache until it is verified. When the optional **vrf** keyword is used, the data-cache is cleared for the specified VRF. When the *EID* option is used, only the EID-to-RLOC mapping for that entry is cleared.

Examples

The following example clears the IPv6 LISP data-cache.

```
Router# clear ipv6 lisp data-cache
```

Related Commands

Command	Description
show ipv6 lisp data-cache	Displays the LISP IPv6 EID-to-RLOC data-cache mapping on an ITR.

---

clear ipv6 lisp map-cache

To clear the LISP IPv6 map-cache, use the **clear ipv6 lisp map-cache** command in privilege EXEC mode.

> **clear ipv6 lisp map-cache** [*EID-prefix*] [**vrf** *vrf-name*]

Syntax Description

EID-prefix	(Optional) IPv6 EID-prefix to clear from LISP map-cache
vrf *vrf-name*	(Optional) VRF within which to clear the map-cache.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The **clear ipv6 lisp map-cache** command removes all IPv6 dynamic EID-to-RLOC map-cache entries in the map-cache. When the optional *EID-prefix* is specified, only the EID-to-RLOC mapping for that entry is cleared. Otherwise, the entire data-cache is cleared. When the optional **vrf** keyword is specified, the data-cache is cleared for the specified VRF.

Examples

The following example clears the entire IPv6 LISP map-cache.

```
Router# clear ipv6 lisp map-cache
Router# show ipv6 lisp map-cache
LISP IPv6 Mapping Cache for VRF "default", 0 entries
Router#
```

The following example shows all LISP map-cache entries, and then clears the LISP map-cache for the IPv6 EID-prefix 2610:d0:210f::/48.

```
Router# show ipv6 lisp map-cache
LISP IPv6 Mapping Cache for VRF "default", 1 entries

2610:d0:210f::/48, uptime: 00:00:58, expires: 23:59:01, via map-reply, auth
  Locator          Uptime    State          Priority/ Data      Control
                                            Weight    in/out    in/out
  85.184.2.10      00:00:58  up             0/100     0/0       0/0
  2001:6e0:4:2::2  00:00:58  up             0/100     0/0       0/0

Router# clear ipv6 lisp map-cache 2610:d0:210f::/48
Router# show ipv6 lisp map-cache
LISP IPv6 Mapping Cache for VRF "default", 0 entries
Router#
```

Related Commands

Command	Description
show ipv6 lisp map-cache	Display current dynamic and static IPv4 EID-to-RLOC map-cache entries.

---

clear lisp ddt

To clear the DDT referral cache stored on a DDT-enabled Map-Resolver, use the **clear lisp ddt referral-cache** command in privileged EXEC mode.

   clear lisp ddt referral-cache [[**instance-id** *iid*] *eid*] [**vrf** *vrf-name*]

Syntax Description

instance-ID *iid*	(Optional) Display the DDT referral cache related to this single instance-ID.
eid	(Optional) Display the DDT referral cache related to this single EID.
vrf *vrf-name*	(Optional) Display the DDT referral cache related to this VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

Use this command to clear the referral cache on a DDT Map-Resolver.

A DDT Map Resolver uses an iterative process of following referrals to find the correct ETR to answer a Map-Request; this requires a DDT Map Resolver to maintain additional state: a Map-Referral cache and a lookup queue of Map-Requests that are going through the iterative referral process. The **clear lisp ddt referral-cache** command clears the contents of the Map-Referral cache.

When **clear lisp ddt referral-cache** is specified using the optional *eid* entry, the single referral cache entry *eid* is removed.

When **clear lisp ddt referral-cache** is specified using the optional **instance-id** *iid* entry, all referral cache entries related to that **instance-id** *iid* are removed. When **clear lisp ddt referral-cache** is specified using the optional **instance-id** *iid eid* entry, the single referral cache entry *eid* within **instance-id** *iid* is removed.

When **clear lisp ddt referral-cache** is specified using the optional **vrf** *vrf-name* entry, all referral cache entries related to **vrf** *vrf-name* are removed.

Examples

The following example clears the lisp ddt referral cache using the **clear lisp ddt referral-cache** command, and then displays the output of **show lisp ddt referral-cache** command.

```
Router# clear lisp ddt referral-cache
Router# show lisp ddt referral-cache
LISP-DDT Referral Cache in VRF "default", 0 entries

Router#
```

Related Commands

Command	Description
show lisp ddt	Display the the configured DDT root(s) and/or DDT delegation nodes.
show lisp ddt queue	Display the DDT lookup queue stored on a DDT-enabled Map-Resolver.
show lisp ddt referral-cache	Display the DDT referral cache stored on a DDT-enabled Map-Resolver.

---

clear ipv6 lisp statistics

To clear the LISP ITR and ETR IPv6 address-family packet count statistics, use the **clear ipv6 lisp statistics** command in privilege EXEC mode.

clear ipv6 lisp statistics [vrf *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) VRF within which to clear the LISP statistics.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.0(3.lisp)	This command was modified.

Usage Guidelines

The **clear ipv6 lisp statistics** command clears all of the LISP ITR and ETR IPv6 address-family packet count statistics. IPv6 address family packet count statistics are maintained for all LISP control plane packets. These packet counters are displayed using the **show ipv6 lisp statistics** command.

Examples

The following example shows all IPv4 LISP control plane statistics (packet counters), and then clears these statistics.

```
Router# show ipv6 lisp statistics
LISP Statistics for VRF "default" - last cleared: never
Data Forwarding:
  IPv6-in-IPv4 encap/decap packets:     2477/0
  IPv6-in-IPv6 encap/decap packets:     0/0
  Translated packets in/out:            0/0
  Map-cache lookup succeeded/failed:    4922/2532
---<skip>---

Router# clear ipv6 lisp statistics
Router# show ipv6 lisp statistics
LISP Statistics for VRF "default" - last cleared: 00:00:06
Data Forwarding:
  IPv6-in-IPv4 encap/decap packets:     0/0
  IPv6-in-IPv6 encap/decap packets:     0/0
  Translated packets in/out:            0/0
  Map-cache lookup succeeded/failed:    0/0
---<skip>---
Router#
```

Related Commands

Command	Description
show ipv6 lisp statistics	Display LISP IPv6 address-family statistics.

clear lisp dynamic-eid

To clear the cache for a dynamic-EID, use the **clear lisp dynamic-eid** command in privilege EXEC mode.

clear lisp dynamic-eid *dynamic-eid-addr* [vrf *vrf-name*]

Syntax Description

dynamic-eid-addr	IPv4 address of LISP dynamic-EID entry to clear.
vrf *vrf-name*	(Optional) VRF within which to clear the dynamic-EID LISP cache (state).

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)(August update)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.
Cisco NX-OS Release 5.2(1.lisp-r5-20)	This command was modified.

Usage Guidelines

The **clear lisp dynamic-eid** command clears the cache is cleared for the IPv4 dynamic-EID *dynamic-eid-addr*. When the **vrf** *vrf-name* form is used, the scope of the clear command is limted to the specified VRF. When no *dynamic-eid-addr* is provided, the entire IPv4 dynamic-EID cache is cleared.

Examples

The following example clears the dynamically learned dynamic-EIDs associated with the LISP dynamic-EID policy called **bc4**.

```
XTR# show lisp dynamic-eid bc4 detail
LISP Dynamic EID Information for VRF "default"
Dynamic-EID name: bc4
  Database-mapping EID-prefix: 30.1.110.104/32, LSBs: 0x00000001
    Locator: 90.1.93.1, priority: 1, weight: 10, local
  Registering more-specific dynamic-EIDs
  Map-Server(s): 90.32.32.32
  Number of roaming dynamic-EIDs discovered: 1
  Last dynamic-EID discovered: 30.1.110.104, 00:08:06 ago
  Roaming dynamic-EIDs:
    30.1.110.104, Ethernet2/5, uptime: 00:08:06, last activity: 0.998355
xTR# clear lisp dynamic-eid 30.1.110.104
XTR# show lisp dynamic-eid bc4 detail
LISP Dynamic EID Information for VRF "default"
Dynamic-EID name: bc4
  Database-mapping EID-prefix: 30.1.110.104/32, LSBs: 0x00000001
    Locator: 90.1.93.1, priority: 1, weight: 10, local
  Registering more-specific dynamic-EIDs
  Map-Server(s): 90.32.32.32
  Number of roaming dynamic-EIDs discovered: 0
XTR#
```

Related Commands

Command	Description
show lisp site	Display LISP site information. Applicable only for the Map-Server.
lisp dynamic-eid	Configure a LISP dynamic-EID policy
lisp site	Configure a LISP site and enter site configuration mode on a Map-Server
lisp mobility	Configure an interface on an ITR to support LISP VM-mobility (dynamic-EID roaming)

clear lisp proxy-itr

To clear the list of Proxy-ITR (PITR) locators that have been discovered through Map-Requests, use the **clear lisp proxy-itr** command in privilege EXEC mode.

> **clear lisp proxy-itr** [*locator*] [**vrf** *vrf-name*]

Syntax Description

locator	(Optional) IPv4 or IPv6 locator address of the PITR to clear
vrf *vrf-name*	(Optional) VRF within which to clear locator address of the PITR

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(3.lisp-80)	This command was introduced.

Usage Guidelines

When an xTR receives a Map-Request from a PITR for an EID-to-RLOC mapping resolution, the locator address of the PITR is saved (separately from the map-cache) by an xTR for later in the event that there is a need to send Solicit-Map-Requests (SMRs) to other LISP devices, including PITRs. The number of locators currently cached is eight (8).

The **clear lisp proxy-itr** command removes all of the Proxy-ITR (PITR) locators that have been discovered through Map-Requests. When the *locator* form is used, only this PITR locator entry is removed. When the **vrf** *vrf-name* form is used, all PITR locators associated with this VRF are removed.

Examples

The following example clears all discovered PITR locators. The output from the command **show lisp proxy-itr** is used to validate the effect of the clear command.

```
Router# show lisp proxy-itr
Discovered Proxy-ITRs (PITRs) in VRF "default"
  10.20.10.60

Router# clear lisp proxy-itr
Router# show lisp proxy-itr
Discovered Proxy-ITRs (PITRs) in VRF "default"

Router#
```

Related Commands

Command	Description
show lisp proxy-tir	Display a list of PITRs discovered through Map-Requests

clear lisp site

To clear the registration data for the specified LISP site, use the **clear lisp site** command in privilege EXEC mode.

> **clear lisp site** *site-name* [**instance-id** *iid*] [**vrf** *vrf-name*]

Syntax Description

site-name	LISP site to clear registration data for.
instance-id *iid*	Configure the instance-id for this xTR (value between 1 and 16777215).
vrf *vrf-name*	(Optional) Display statistics for the specified VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

The **clear lisp site** *site-name* command clears the entire registration dataset for the specified LISP site. When the **instance-id** *iid* optional entry is added, only the registration dataset for the specified LISP site relevant to the specified instance-id is cleared. When the **vrf** *vrf-name* optional entry is added, only the registration dataset for the specified LISP site relevant to the specified VRF context is cleared.

✎

Note The **clear lisp site** command can only be used on a LISP Map-Server.

Examples

The following example clears the LISP registration data for the LISP site called Customer-1.

```
Router# show lisp site Customer-1
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address

Site name:   "Customer-1"
Description: none configured
Allowed configured locators: any
Allowed EID-prefixes:
  EID-prefix: 2610:d0:1200::/48
    Currently registered: yes
    First registered:     22:48:01
    Last registered:      00:00:48
---<skip>---
Router# clear lisp site Customer-1
Router# show lisp site Customer-1
LISP Site Registration Information for VRF "default"
* = truncated IPv6 address

Site name:   "Customer-1"
```

```
  Description: none configured
  Allowed configured locators: any
  Allowed EID-prefixes:
    EID-prefix: 2610:d0:1200::/48
      Currently registered: no
      First registered:     never
      Last registered:      never
---<skip>---
Router#
```

Related Commands

Command	Description
show lisp site	Display LISP site information. Applicable only for the Map-Server.

Other LISP Related Commands

lig

To initiate a LISP Internet Groper (**lig**) operation for a destination EID or to test the routers' local EID prefix(es), use the **lig** command in privileged EXEC mode.

> **lig** {*hostname* | *destination-EID*} [**count** *count*][**source** *source-EID*][**to** *map-resolver*][**vrf** *vrf-name*]

> **lig** {**self** | **self6** | **version**} [**count** *count*][**source** *source-EID*][**to** *map-resolver*][**vrf** *vrf-name*]

Syntax Description

hostname	Destination hostname
destination-EID	Destination IPv4 or IPv6 Endpoint Identifier (EID) to **lig** for.
self	Test to see if the local IPv4 EID-prefix is registered in the mapping database.
self6	Test to see if the local IPv6 EID-prefix is registered in the mapping database.
version	Displays the version of lig that the system is supporting.
source *source-EID*	(Optional) Send the Map-Request using this IPv4 or IPv6 source EID.
to *map-resolver*	(Optional) Send the Map-Request(s) to this map-resolver locator instead of the configured Map-Resolver
count *count*	(Optional) Send this number of Map-Requests (value between 1 and 5).
vrf *vrf-name*	(Optional) Display statistics for the specified VRF.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.
Cisco NX-OS Release 5.2(0.266.lisp-52)	This command was modified.

Usage Guidelines

This command initiates a LISP Internet Groper (**lig**) query for the indicated destination hostname or EID, or the routers local EID-prefix. The **lig** function is analogous to the DNS-related **dig** function. Use this command as a simple means of testing whether a destination EID exists in the LISP mapping database system, or as a convenient way to see if your site is registered with the mapping database system. When the optional **vrf** *vrf-name* is used, the **lig** function is conducted within the specified VRF context.

When a **lig** query is initiated with a hostname or destination EID, the router sends a Map-Request to the configured Map-Resolver for the indicated destination hostname or EID. When a Map-Reply is returned, its contents are displayed to the user and entered in the LISP map-cache.

When a **lig self** query is initiated, the routers local EID-prefix is substituted in place of the destination EID when the router sends a Map-Request to the configured Map-Resolver.

The following operational attributes apply to **lig**:

- By default, at a minimum one Map-Request is sent to the Map-Resolver but up to three Map-Requests may be sent to the Map-Resolver. Once a Map-Reply is returned for a Map-Request, no further Map-Requests are sent. When the **count** option is applied, the specified number of Map-Requests is sent.

LISP-177

- By default, the source of the Map-Request will be the first configured EID-prefix for the site (with the host-bit set to zero). For example, if the local EID-prefix is 153.16.21.0/24, the source EID will be 153.16.21.0 for the Map-Request. When the **source** option is applied, a specific source EID may be used. However, the source-EID must be one of the EID addresses assigned to the LISP router.
- When **lig** is used with the **self** option, the destination IPv4 EID will also be the first configured EID-prefix for the site (with the host-bit set to zero). For example, if the local IPv4 EID-prefix is 153.16.21.0/24, the destination EID will be 153.16.21.0 for the Map-Request. The **self6** option performs similarly, but for IPv6 addresses.
- By default when **lig** is invoked, the Map-Request is sent to the configured Map-Resolver. However, the **to** option can be specified to cause the Map-Request to be forwarded to a specified Map-Resolver instead. Send a Map-Request to a different Map-Resolver can be useful for testing that your EID-prefix has been properly injected into the ALT infrastructure. In this case, the **lig** Map-Request is processed by the specified Map-Resolver and propagated through each ALT router hop to the Map-Server you have registered to. The Map-Server returns the Map-Request to your site. Your site then generates a Map-Reply to the source of the Map-Request – which could be itself, or a different xTR within your LISP site.

Examples

The following example uses the **lig self** and **lig self6** commands to test that the local EID-prefixes have registered with the Map-Server.

```
Router# lig self
Send loopback map-request to 128.223.156.35 for 153.16.12.0 ...
Received map-reply from 128.223.156.23 with rtt 0.002770 secs

Map-cache entry for EID 153.16.12.0:
153.16.12.0/24, uptime: 00:00:02, expires: 23:59:57, via map-reply, self
  Locator          Uptime    State       Priority/  Data      Control
                                          Weight     in/out    in/out
  128.223.156.23  00:00:02  up          1/100      0/0       0/0

Router# lig self6
Send loopback map-request to 128.223.156.35 for 2610:d0:1203:: ...
Received map-reply from 128.223.156.23 with rtt 0.001148 secs

Map-cache entry for EID 2610:d0:1203:::
2610:d0:1203::/48, uptime: 00:00:02, expires: 23:59:57, via map-reply, self
  Locator          Uptime    State       Priority/  Data      Control
                                          Weight     in/out    in/out
  128.223.156.23  00:00:02  up          1/100      0/0       0/0

Router#
```

The following example shows all LISP map-cache entries, and then uses **lig** to test for the remote IPv6 EID-prefix 2610:d0:210f::/48.

```
Router# show ipv6 lisp map-cache
LISP IPv6 Mapping Cache for VRF "default", 0 entries

Router# lig 2610:d0:210f::1
end map-request to 128.223.156.35 for 2610:d0:210f::1 ...
Received map-reply from 85.184.2.10 with rtt 0.204710 secs

Map-cache entry for EID 2610:d0:210f::1:
2610:d0:210f::/48, uptime: 00:00:01, expires: 23:59:58, via map-reply, auth
  Locator          Uptime    State       Priority/  Data      Control
                                          Weight     in/out    in/out
  85.184.2.10      00:00:01  up          0/100      0/0       0/0
  2001:6e0:4:2::2  00:00:01  up          0/100      0/0       0/0

Router# show ipv6 lisp map-cache
LISP IPv6 Mapping Cache for VRF "default", 1 entries

2610:d0:210f::/48, uptime: 00:01:25, expires: 23:58:34, via map-reply, auth
  Locator          Uptime    State       Priority/  Data      Control
                                          Weight     in/out    in/out
```

LISP-178

```
    85.184.2.10       00:01:25   up            0/100      0/0        0/0
    2001:6e0:4:2::2  00:01:25   up            0/100      0/0        0/0

Router#
```

The following example displays the version of **lig** being used by the system.

```
Router# lig version
http://tools.ietf.org/html/draft-ietf-lisp-09
http://tools.ietf.org/html/draft-farinacci-lisp-lig-01
```

Related Commands

Command	Description
show ip lisp map-cache	Display the current dynamic and static IPv4 EID-to-RLOC map-cache entries.
show ipv6 lisp map-cache	Display the current dynamic and static IPv6 EID-to-RLOC map-cache entries.

ping[6]

To diagnose basic network connectivity and test reachability and/or liveness of a destination EID or RLOC address, use the **ping** or **ping6** command in privileged EXEC mode.

> **ping** {*hostname|destination-addr*} [**count** *count*] [**df-bit**] [**packet-size** *size*] [**source** *source-addr*] [**vrf** *vrf-name*]
>
> **ping6** {*hostname|destination-addr*} [**count** *count*] [**packet-size** *size*] [**source** *source-addr*] [**vrf** *vrf-name*]

Syntax Description

hostname	Hostname of the system to ping.
destination-addr	IPv4 (**ping**) or IPv6 (**ping6**) Address of the system to ping.
count *count*	(Optional) Specifies the number of times the ping should be sent (default 5).
df-bit	(Optional) Enables the "do not fragment" bit in the IP header (IPv4 only)
packet-size *size*	(Optional) Size, in bytes, of the ping datagram (default 100).
source *source-addr*	(Optional) IPv4 (**ping**) or IPv6 (**ping6**) Address used by this system to ping.
vrf *vrf-name*	(Optional) The name of the VPN (VRF context) within which to ping.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The **ping** command sends an ICMP Echo Request (ICMP Type 8, Code 0) packet to the specified IPv4 address then waits for a corresponding ICMP Echo Reply (ICMP Type 0, Code 0) packet reply. The **ping6** command is used for IPv6, and sends an ICMP Echo Request (ICMP Type 128, Code 0) packet to the specified IPv6 address then waits for a corresponding ICMP Echo Reply (ICMP Type 129, Code 0) packet reply.

LISP-179

Note The descriptions provided here represent a subset of all possible **ping** or **ping6** options and uses; in particular, those relevant to LISP. Other **ping** or **ping6** command options and uses beyond those described are covered in the general-use description of the **ping** or **ping6** command found at: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/nx-os/fundamentals/command/reference/fnd_commands.html.

Note The descriptions provided below show **ping** details and examples. The use of **ping6** is identical and thus not shown.

LISP has separate control plane and data plane functions. The diagnostic tool **ping** can be used to test reachability and liveness of various the LISP data plane and control plane functions.

- If a Map-Cache entry exists for a specified destination EID, **ping** can be used to test the LISP data plane by using the **source** keyword to specify a source address that is an EID. Note that the LISP site for the destination EID must also have an existing Map-Cache entry in order for **ping** to succeed.
- If a Map-Cache entry does not exist for a specified destination EID, **ping** can be used to test the LISP control plane by first causing the router to generate a Map-Request for destination EID. Note that the **source** keyword must be used to specify a source address that is an EID, and the LISP site for the destination EID must also have an existing Map-Cache entry or use the LISP control plane to obtain one in order for **ping** to succeed.
- To test control plane RLOC namespace reachability and liveness of LISP devices, use **ping** with destination and use the **source** keyword to specify a source RLOC addresses.
- When a Proxy Ingress Tunnel Router (PITR) is involved, **ping** can be used to test used to test its functionality by using a non-LISP address for the destination and using the **source** keyword to specify a source address that is an EID.

Consider the following operational modes when using the **ping** command with LISP.

- Entering the **ping** command without any keywords or argument values causes an interactive system dialog to prompt the user for the additional syntax appropriate to the protocol specified.
- To test a connection in the context of a specific VPN connection, use the **ping vrf** command. If the **vrf** *vrf-name* keyword and argument are not displayed, it is because only the default VRF is being used (a VRF has not been configured).
- The optional data, **df-bit** (IPv4-only), **count**, and **packet-size** keywords can be used to customize **ping** effectiveness in diagnosing particular issues. You can use as many of these keywords as you need, and you can use them in any order after the hostname or system-address arguments. For example, **df-bit** (IPv4-only) and **packet-size** can be used together to test effective path MTU, while **count** can be used to check counters.

Caution To maximize the effectiveness and minimize ambiguity, the **source** keyword should always be used with **ping** to ensure that the correct namespace (EID or RLOC) is used within ping packets.

Examples

In the following example, a LISP map cache entry already exists in both sites and the ping command is used to verify the LISP data plane connectivity between source EID 192.168.1.255 and destination EID 192.168.2.1 with a repeat count of 100.

```
Router# ping 192.168.2.1 source 192.168.1.255 count 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.255
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/7/28 ms
Router#
```

LISP-180

In the following example, LISP map cache entries do not exists on either sites and the ping command is used to test the LISP control plane for source EID 192.168.1.255 and destination EID 192.168.2.1 and a **count** of 10. Note that the first two ping packets fail. Once the map-cache is populated, the remaining ping packets succeed.

```
Router# ping 192.168.2.1 source 192.168.1.255 count 10
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.255
..!!!!!!!!
Success rate is 80 percent (8/10), round-trip min/avg/max = 2/6/11 ms
Router#
```

Related Commands

Command	Description
lig	Initiate a LISP Internet Groper (**lig**) operation to test the LISP control plane.
traceroute[6]	Discover the path packets take when traveling to their destination..

---

rig

To initiate a LISP **rig** (Referral Internet Groper) operation to query the LISP-DDT hierarchy for a destination EID, use the **rig** command in privileged EXEC mode.

   rig [**instance-id** *iid*] {*eid-hostname* | *eid*} **to** {*ddt-nodename* | *ddt-node-locator*}

Syntax Description

instance-id *iid*	(Optional) Specify the instance-ID for the IPv4 or IPv6 EID to perform **rig** operation on.
eid-hostname	DNS hostname for the EID to perform **rig** operation on.
eid	IPv4 or IPv6 EID to perform **rig** operation on.
ddt-nodename	DNS hostname for the DDT node locator to which the **rig** map-referral is to be sent.
ddt-node-locator	IPv4 or IPv6 for the DDT node locator to which the **rig** map-referral is to be sent.

Command Modes

Privileged EXEC

Supported User Roles

network-admin
vdc-admin

Command History

Release	Modification
Cisco NX-OS Release 5.2(1.lisp-r7-39)	This command was introduced.

Usage Guidelines

This command initiates a LISP Referral Internet Groper (**rig**) operation to query the LISP-DDT hierarchy for the indicated destination hostname or EID.

The **rig** function initiates an ECM-based Map-Request for the specified EID or extended EID (instance-id *iid eid*) and sends it to the specified DDT node. The DDT-node receiving the query return an appropriate Map-Referral message (based on its knowledge of the queried EID) and this information is displayed.

✎

Note When the **rig** command is entered and referrals are returned, these referrals do not create or modify state in the referral cache.

LISP-181

Examples

The following example uses the **rig** command to query the LISP DDT hierarcy for the EID 172.16.17.17.

```
Router# rig 172.16.17.17 to 10.1.1.1
rig LISP-DDT hierarchy for EID [0] 172.16.17.17
Send Map-Request to DDT-node 10.1.1.1 ... replied, rtt: 0.007072 secs
  EID-prefix [0] 172.16.17.16/28, ttl: 1, action: ms-not-registered, referrals:
    10.1.1.1, priority/weight: 0/0
    10.2.1.1, priority/weight: 0/0
    10.3.1.1, priority/weight: 0/0

Router#
```

Related Commands

Command	Description
show lisp ddt	Display the the configured DDT root(s) and/or DDT delegation nodes.
show lisp ddt queue	Display the DDT lookup queue stored on a DDT-enabled Map-Resolver.
show lisp ddt referral-cache	Display the DDT referral cache stored on a DDT-enabled Map-Resolver.

traceroute[6]

To discover the path that packets take when traveling to a destination EID or RLOC address, use the **traceroute** or **traceroute6** command in privileged EXEC mode.

> **traceroute** {*hostname* | *destination-addr*} [**source** *source-addr*] [**vrf** *vrf-name*]

> **traceroute6** {*hostname* | *destination-addr*} [**source** *source-addr*] [**vrf** *vrf-name*]

Syntax Description

hostname	Hostname of the system to ping.
destination-addr	IPv4 (**traceroute**) or IPv6 (**traceroute6**) Address of the system to traceroute to.
source *source-addr*	(Optional) IPv4 (**traceroute**) or IPv6 (**traceroute6**) Address used the **traceroute** or **traceroute6** source address
vrf *vrf-name*	(Optional) The name of the VPN (VRF context) within which to traceroute.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco NX-OS Release 5.0(1.13)	This command was introduced.

Usage Guidelines

The **traceroute** and **traceroute6** commands work by taking advantage of the error messages generated by routers when a datagram exceeds its hop limit value. The **traceroute** command starts by sending UDP probe datagrams with a hop limit (TTL) of 1. Including a hop limit of 1 with a probe datagram causes the neighboring routers to discard the probe datagram and send back an ICMP Time Exceeded (ICMP Type 11, Code 0) error message. The traceroute command sends several probes with increasing hop limits and displays the round-trip time for each. The **traceroute** command terminates when the destination responds with an ICMP Destination unreachable, Port Unreachable (Type 3, Code 3) message, when the hop limit is exceeded, or when the user interrupts the trace with the escape sequence. By default, to invoke the escape sequence, type Ctrl-^ X—by simultaneously pressing and releasing the Ctrl, Shift, and 6 keys, and then pressing the X key.

LISP-182

The traceroute command sends out one probe at a time. Each outgoing packet might result in one or more ICMP error message replies. A time-exceeded error message indicates that an intermediate router has seen and discarded the probe. A destination unreachable error message indicates that the destination node has received and discarded the probe because the hop limit of the packet reached a value of 0. If the timer goes off before a response comes in, the traceroute command prints an asterisk (*).

> **Note** The descriptions provided here represent a subset of all possible **traceroute** options and uses; in particular, those relevant to LISP. Other **traceroute** command options and uses beyond those described are covered in the general-use description of the **traceroute** command found at: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_2/nx-os/fundamentals/command/reference/fnd_commands.html.

LISP has separate control plane and data plane functions. The diagnostic tool **traceroute** can be used to test reachability and liveness of various the LISP data plane and control plane functions.

- If a Map-Cache entry exists for a specified destination EID, **traceroute** can be used to test the LISP data plane by using the **source** keyword to specify a source address that is an EID. Note that the LISP site for the destination EID must also have an existing Map-Cache entry in order for **traceroute** to succeed. Since the ICMP Time Exceeded will happen in the underlying network and their destination address will be and EID address of the sending router, Proxy Ingress Tunnel Router (PITR) functionality is required in order to get the ICMP Time Exceeded messages back to the sending router.
- If a Map-Cache entry does not exist for a specified destination EID, **traceroute** can be used to test the LISP control plane by first causing the router to generate a Map-Request for destination EID. Note that the **source** keyword must be used to specify a source address that is an EID, and the LISP site for the destination EID must also have an existing Map-Cache entry or use the LISP control plane to obtain one in order for **traceroute** to succeed.
- To test control plane RLOC namespace reachability and liveness of LISP devices, use **traceroute** with destination and use the **source** keyword to specify a source RLOC addresses.
- When a Proxy Ingress Tunnel Router (PITR) is involved, **ping** can be used to test used to test its functionality by using a non-LISP address for the destination and using the **source** keyword to specify a source address that is an EID.

Consider the following operational modes when using the **traceroute** command with LISP.

- Entering the **traceroute** command without any keywords or argument values causes an interactive system dialog to prompt the user for the additional syntax appropriate to the protocol specified.
- To test a connection in the context of a specific VPN connection, use the **traceroute vrf** command. If the **vrf** *vrf-name* keyword and argument are not displayed, it is because only the default VRF is being used (a VRF has not been configured).

> **Caution** In order to maximize the effectiveness of **traceroute** and minimize ambiguity in results, the **source** keyword should always be used with **traceroute** to ensure that the correct namespace (EID or RLOC) is used within traceroute packets.

> **Note** The descriptions provided below show **traceroute** details and examples. The use of **traceroute6** is identical and thus not shown.

Examples

In the following example, a LISP map cache entry already exists in both sites and the **ping** command is used to verify the LISP data plane connectivity between source EID 192.168.1.255 and destination EID 192.168.2.1. Then, **traceroute** is used to identify the path packets take to the destination EID.

```
Router# ping 192.168.2.1 source 192.168.1.255
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 192.168.1.255
```

LISP-183

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/16 ms
Router# traceroute 192.168.2.1 source 192.168.1.255
Type escape sequence to abort.
Tracing the route to 192.168.2.1
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.0.1 1 msec 1 msec 5 msec
  2 10.0.0.6 13 msec 1 msec 2 msec
  3 172.16.2.1 2 msec *  10 msec
Router#
```

In the following example, the **ping** command is used to verify the connectivity to a destination RLOC, and then **traceroute** is used to identify the path packets take to the destination RLOC.

```
Router# ping 10.0.0.6 source 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.6, timeout is 2 seconds:
Packet sent with a source address of 10.0.0.2
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/17 ms
Router#
 Router# traceroute 10.0.0.6 source 10.0.0.2 port 4342
Type escape sequence to abort.
Tracing the route to 10.0.0.6
VRF info: (vrf in name/id, vrf out name/id)
  1 10.0.0.1 1 msec 0 msec 1 msec
  2 10.0.0.6 6 msec *  11 msec
Router#
```

Related Commands

Command	Description
lig	Initiate a LISP Internet Groper (**lig**) operation to test the LISP control plane.
ping[6]	Diagnose basic network connectivity and test reachability and/or liveness of a destination EID or RLOC.