Configuring Proxy Mobile IPv6 Local Mobility Anchor

Local Mobility Anchor (LMA) acts as the home agent for a mobile node (MN) in a Proxy Mobile IPv6 domain, which is the network where the mobility management of an MN is handled using the Proxy Mobile IPv6 (PMIPv6) protocol. LMA is the topological anchor point for the MN's home network prefix(es) and is the entity that manages the MN's binding state. This module explains how to configure LMA on Cisco ASR 9000 Series Aggregation Services Routers.

Note For a complete description of the PMIPv6 LMA configuration commands listed in this module, refer to the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference* publication.

Feature History for Configuring Proxy Mobile IPv6 Local Mobility Anchor on the Cisco ASR 9000 Series Router

Release	Modification
Release 5.2.2	This feature was introduced.
Release 5.3.1	Smart Licensing feature was added.

Information About Proxy Mobile IPv6 Support for LMA Functionality

Proxy Mobile IPv6 Overview

Proxy Mobile IPv6 (PMIPv6) provides network-based IP Mobility management to a mobile node (MN), without requiring the participation of the MN in any IP mobility-related signaling. The mobility entities in the network track the movements of the MN, initiate the mobility signaling, and set up the required routing state.

The major functional entities of PMIPv6 are Mobile Access Gateways (MAGs), Local Mobility Anchors (LMAs), and MNs.

Mobile Access Gateway

A Mobile Access Gateway (MAG) performs mobility-related signaling on behalf of the mobile nodes (MN) attached to its access links. MAG is the access router for the MN; that is, the MAG is the first-hop router in the localized mobility management infrastructure.

A MAG performs the following functions:

- Obtains an IP address from a Local Mobility Anchor (LMA) and assigns it to an MN
- Tunnels traffic from an MN to LMA

Local Mobility Anchor

Local Mobility Anchor (LMA) is the home agent for a mobile node (MN) in a Proxy Mobile IPv6 (PMIPv6) domain. It is the topological anchor point for MN home network prefixes and manages the binding state of an MN. An LMA has the functional capabilities of a home agent as defined in the Mobile IPv6 base specification (RFC 3775 and RFC 5213) along with the capabilities required for supporting the PMIPv6 protocol.

The LMA retains and shares the IP address of an MN when the MN roams across MAGs.

Smart Licensing for PMIPv6 LMA

Smart Licensing method of licensing is available for PMIPv6 LMA on the Cisco ASR 9000 Series Aggregation Services Routers. The licensing mode is soft-enforced mode. The licensing string available is A9K-SESSION-128K with maximum supported scale of 128K LMA bindings.

For more information about Smart Licensing, see *Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide*.

Mobile Node

A mobile node (MN) is an IP host whose mobility is managed by the network. An MN can be an IPv4-only node, an IPv6-only node, or a dual-stack node, which is a node with IPv4 and IPv6 protocol stacks. An MN is not required to participate in any IP mobility-related signaling for achieving mobility for an IP address or a prefix that is obtained in the Proxy Mobile IPv6 (PMIPv6) domain.

How to Configure Proxy Mobile IPv6 LMA

This section contains the following tasks:

Configuring a Proxy Mobile IPv6 LMA Domain

This task enables you to configure Proxy Mobile IPv6 LMA domain:

SUMMARY STEPS

1. **configure**
2. **ipv6 mobile pmipv6-domain** *domain-name*
3. **auth-option spi** *hex-value* **key ascii** *string*
4. **nai** *[user]@realm*
5. **network** *network-identifier*
6. **service { ipv4 | ipv6 | dual }**
7. (Optional) **customer** *customer-name*
8. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv6 mobile pmipv6-domain** *domain-name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 mobile pmipv6-domain cisco.com`	Configures a PMIPv6 domain and enters PMIPv6 domain configuration mode.
Step 3	**auth-option spi** *hex-value* **key ascii** *string* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-domain)# auth-option spi 67 key ascii key1`	Configures the authentication option to all MAGs in the domain that includes an SPI value specified in hexadecimal format and a shared secret key which is specified as an ASCII string.
Step 4	**nai** *[user]@realm* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-domain)# nai example@cisco.com`	Configures a network access identifier (NAI) of the mobile node (MN) within the PMIPv6 domain and enters PMIPv6 domain MN configuration mode. The NAI must be of form *username@realm* or just *@realm*

	Command or Action	Purpose
Step 5	**network** *network-identifier* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-domain-nai)# network network2`	Corresponds to a network configured under LMA comprising of an IPv4 and IPv6 address/prefix pool. The Mobile Node (MN) is assigned HoA or HNP from this network. Associates a network with the LMA under which an IPv4 or IPv6 pool can be enabled.
Step 6	**service { ipv4 | ipv6 | dual }** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-domain-nai)# service dual`	Configures the service provided to the MN within the PMIPv6 domain.
Step 7	(Optional) **customer** *customer-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-domain-nai)# customer CUST1`	(Optional) Configures the name of the customer to which this NAI belongs. The customer is configured during LMA Mobile Local Loop service configuration as described in Configuring VRF Aware LMA, on page 13.
Step 8	**commit**	

Example: Configuring a Proxy Mobile IPv6 LMA Domain

This example shows sample configuration of PMIPv6 LMA domain:

```
ipv6 mobile pmipv6-domain cisco.com
 !
 auth-option spi 67 key ascii key1
 nai example@cisco
  network network2
 !
 nai example@ctc
  network network3
  service dual
  customer CUST1
 !
!
```

Configuring Proxy Mobile IPv6 LMA with Peer MAG

This task lists detailed configuration steps for configuring Proxy Mobile IPv6 LMA with dynamic MAG learning:

SUMMARY STEPS

1. **configure**
2. **ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name*
3. **address { ipv4 | ipv6 }** *address*
4. **hnp maximum** *number*
5. **bce maximum** *number*

6. **bce lifetime** *seconds*
7. **bce delete-wait-time** *milliseconds*
8. **replay-protection timestamp window** *seconds*
9. **default profile** *profile-name*
10. **bri delay { min | max }** *milliseconds*
11. **bri retries** *count*
12. **aaa accounting [interim** *interim-interval* **]**
13. **mag** *mag-identifier domain-name*
14. Execute one of these:
    - **ipv4 address** *address*
    - **ipv6 address** *address*
15. **auth-option spi** *hex-value* **key ascii** *value*
16. **encap {gre-ipv4 | gre-ipv6 }**
17. **tunnel interface** *interface-type node-id*
18. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 mobile pmipv6-lma lma1 domain cisco.com`	Enables the LMA service on the router, configures the PMIP domain for the LMA, and enters LMA configuration mode.
Step 3	**address { ipv4 | ipv6 }** *address* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# address ipv6 2001:DB8::1`	Configures an IPv4 or IPv6 address for the LMA.
Step 4	**hnp maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# hnp maximum 2`	Configures the maximum number of home network prefixes (HNP) that a mobile node can posses.
Step 5	**bce maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce maximum 2500`	Configures the maximum number of binding cache entries (BCEs) or bindings that the LMA can support.

	Command or Action	Purpose
Step 6	**bce lifetime** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce lifetime 2500`	Configures the permitted lifetime of a binding in seconds. The granted lifetime is minimum of this configured value and the value received from the MAG in the PBU packet.
Step 7	**bce delete-wait-time** *milliseconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce delete-wait-time 100`	Configures the time in milliseconds that LMA must wait before it deletes a BCE of a MN, upon receiving a PBU message from a MAG with a lifetime value of 0.
Step 8	**replay-protection timestamp window** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# replay-protection timestamp window 18`	Configures the time window between the LMA's running clock and the timestamp value received in the PBU from the MAG that the LMA can tolerate for the binding request to be accepted. If the calculated window is larger than this configured value, then the PBU is rejected with status code 156.
Step 9	**default profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# default profile profile1`	Enables the default profile for the MN.

Step 10	**bri delay { min | max }** *milliseconds*
	Example:
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay min 500`
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay max 2500`
		Configures the minimum and maximum time in milliseconds for which an LMA should wait before transmitting the Binding Revocation Indication (BRI) message to a MAG.

Step 11	**bri retries** *count* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri retries 5`	Configures the maximum number of times an LMA should retransmit a BRI message until a Binding Revocation Acknowledgment (BRA) is received from the MAG.
Step 12	**aaa accounting [interim** *interim-interval* **]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# aaa accounting interim 2`	Enables LMA accounting. If **interim** *interim-interval* option is specified, Interim-Update records are sent to the RADIUS security server at the configured *interim-interval* specified in minutes. Otherwise, only Start and Stop records are sent to the RADIUS security server.

	Command or Action	Purpose
		There are two types of accounting sessions, one for Mobile Nodes and one for tunnels. Interim-Update records are enabled only for tunnel accounting and not for Mobile Node accounting.
Step 13	**mag** *mag-identifier domain-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# mag mag1 dn1`	Configures the MAG for the LMA and enters LMA-MAG configuration mode.

Step 14	Execute one of these:
	• **ipv4 address** *address*
	• **ipv6 address** *address*
	Example:
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma-mag)# ipv4 address 192.168.0.4`
	`or`
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma-mag)# ipv6 address 2004:DC5::2`
		Configures an IPv4 address for the LMA in case the transport between the MAG and the LMA is IPv4.
		Configures an IPv6 address for the LMA in case the transport between the MAG and the LMA is IPv6.

Step 15	**auth-option spi** *hex-value* **key ascii** *value* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mag)# auth-option spi 87E key ascii key2`	Configures authentication for the LMA within the MAG.
Step 16	**encap {gre-ipv4 | gre-ipv6 }** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mag)# encap gre-ipv6`	Configures a tunnel encapsulation mode type between the MAG and the LMA.
Step 17	**tunnel interface** *interface-type node-id* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mag)# tunnel interface tunnel-ip 097`	Configures a static GRE tunnel to peering MAG. This step is required since GRE tunnel cannot be created dynamically.
Step 18	**commit**	

Example: Configuring Proxy Mobile IPv6 LMA with Peer MAG

This example shows sample configuration of Proxy Mobile IPv6 LMA with Peer MAG:

```
ipv6 mobile pmipv6-lma lma1 domain cisco.com
 address ipv6 2001:DB8::1
 hnp maximum 2
 bce maximum 2500
```

```
 bce lifetime 2500
 bce delete-wait-time 100
 replay-protection timestamp window 18
 default profile profile1
 aaa accounting interim 2
 !
 mag mag1 dn1
  ipv4 address 192.168.0.4
  auth-option spi 87E key ascii key2
  encap gre-ipv6
  tunnel interface tunnel-ip 097
 !
!
```

Configuring Proxy Mobile IPv6 LMA with Dynamic MAG Learning

This task lists detailed configuration steps for configuring Proxy Mobile IPv6 LMA with dynamic MAG learning:

SUMMARY STEPS

1. **configure**
2. **ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name*
3. **address { ipv4 | ipv6 }** *address*
4. **hnp maximum** *number*
5. **heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value*
6. **bce maximum** *number*
7. **bce lifetime** *seconds*
8. **bce delete-wait-time** *milliseconds*
9. **replay-protection timestamp window** *seconds*
10. **default profile** *profile-name*
11. **bri delay { min | max }** *milliseconds*
12. **bri retries** *count*
13. **dynamic mag learning**
14. **aaa accounting [interim** *interim-interval* **]**
15. **network** *network-name*
16. **pool { mobile-node | mobile-network } { ipv4 | ipv6 } start-address** *address* **pool-prefix** *prefix* **[network-prefix** *prefix***]**
17. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 mobile`	Enables the LMA service on the router, configures the PMIPv6 domain for the LMA, and enters LMA configuration mode.

	Command or Action	Purpose
	`pmipv6-lma lma1 domain cisco.com`	
Step 3	**address { ipv4 | ipv6 }** *address* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# address ipv6 2001:DB8::1`	Configures an IPv4 or IPv6 address for the LMA.
Step 4	**hnp maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# hnp maximum 2`	Configures the maximum number of home network prefixes (HNP) that a mobile node can posses.
Step 5	**heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# heartbeat interval 100 retries 5 timeout 10`	Configures global LMA heartbeat options. *interval-value* specifies the interval between two heartbeat messages in seconds. *retries-value* specifies the number of retries (in the absence of reply from the peer) before the path to the peer is declared as down. *timeout-value* specifies the timeout value to wait for a response from the peer after which the request is declared as timed out.
Step 6	**bce maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce maximum 2500`	Configures the maximum number of binding cache entries (BCEs) or bindings that the LMA can support.
Step 7	**bce lifetime** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce lifetime 2500`	Configures the permitted lifetime of a binding in seconds. The granted lifetime is minimum of this configured value and the value received from the MAG in the PBU packet.
Step 8	**bce delete-wait-time** *milliseconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce delete-wait-time 100`	Configures the time in milliseconds that LMA must wait before it deletes a BCE of a MN, upon receiving a PBU message from a MAG with a lifetime value of 0.
Step 9	**replay-protection timestamp window** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)#`	Configures the time window between the LMA's running clock and the timestamp value received in the PBU from the MAG that the LMA can tolerate for the binding request to be accepted. If the calculated window is larger than this

	Command or Action	Purpose
	`replay-protection timestamp window 18`	configured value, then the PBU is rejected with status code 156.
Step 10	**default profile** *profile-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# default profile profile1`	Enables the default profile for the MN.

Step 11	**bri delay { min | max }** *milliseconds*
	Example:
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay min 500`
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay max 2500`
		Configures the minimum and maximum time in milliseconds for which an LMA should wait before transmitting the Binding Revocation Indication (BRI) message to a MAG.

Step 12	**bri retries** *count* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri retries 5`	Configures the maximum number of times an LMA should retransmit a BRI message until a Binding Revocation Acknowledgment (BRA) is received from the MAG.
Step 13	**dynamic mag learning** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# dynamic mag learning`	Enables an LMA to accept Proxy Mobile IPv6 (PMIPv6) signaling messages from any Mobile Access Gateway (MAG) that is not locally configured.
Step 14	**aaa accounting [interim** *interim-interval* **]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# aaa accounting interim 2`	Enables LMA accounting. If **interim** *interim-interval* option is specified, Interim-Update records are sent to the RADIUS security server at the configured *interim-interval* specified in minutes. Otherwise, only Start and Stop records are sent to the RADIUS security server. There are two types of accounting sessions, one for Mobile Nodes and one for tunnels. Interim-Update records are enabled only for tunnel accounting and not for Mobile Node accounting.
Step 15	**network** *network-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# network network1`	Configures the network that comprises of one or more pools from which the LMA assigns IP addresses to the Mobile Nodes.

	Command or Action	Purpose
Step 16	**pool { mobile-node | mobile-network } { ipv4 | ipv6 } start-address** *address* **pool-prefix** *prefix* **[network-prefix** *prefix***]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-network)# pool mobile-node ipv4 start-address 192.168.0.2 pool-prefix 8`	Configures the IPv4 or IPv6 address pool from which LMA assigns IP addresses to the mobile nodes.
Step 17	**commit**	

Example: Configuring Proxy Mobile IPv6 LMA with Dynamic MAG Learning

This example shows sample configuration of Proxy Mobile IPv6 LMA with dynamic MAG learning:

```
ipv6 mobile pmipv6-lma lma1 domain cisco.com
 address ipv6 2001:DB8::1
 hnp maximum 2
 heartbeat interval 100 retries 5 timeout 10
 bce maximum 2500
 bce lifetime 2500
 bce delete-wait-time 100
 replay-protection timestamp window 18
 default profile profile1
 dynamic mag learning
 aaa accounting interim 2
 network network1
  pool mobile-node ipv4 start-address 192.168.0.2 pool-prefix 8
  pool mobile-node ipv6 start-address 2002:10::1 pool-prefix 62
 !
!
```

VRF Aware LMA

This section contains the following topics:

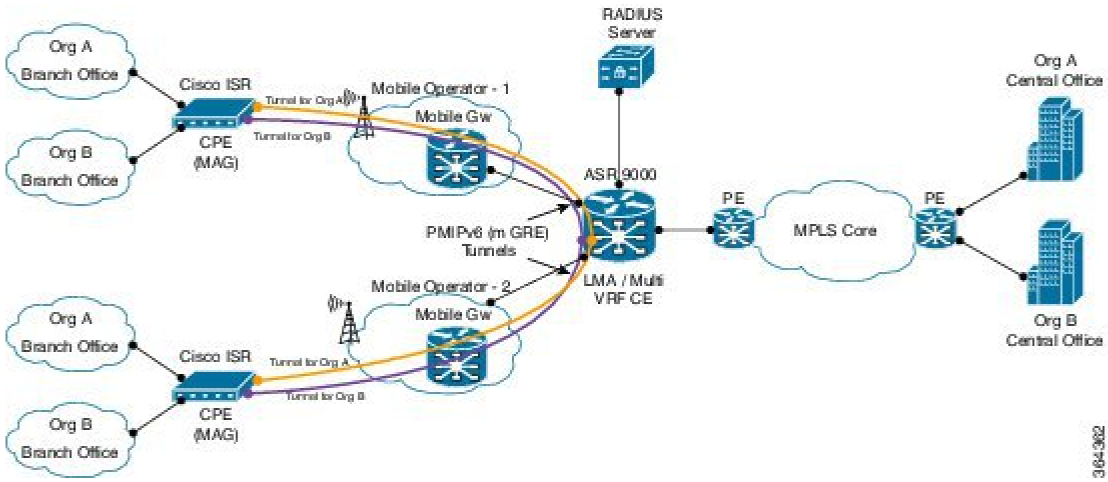
VRF Aware LMA Solution

Local Mobility Anchor (LMA) supports VRF awareness on Cisco ASR 9000 Series Aggregation Services Routers. This feature includes the following capabilities:

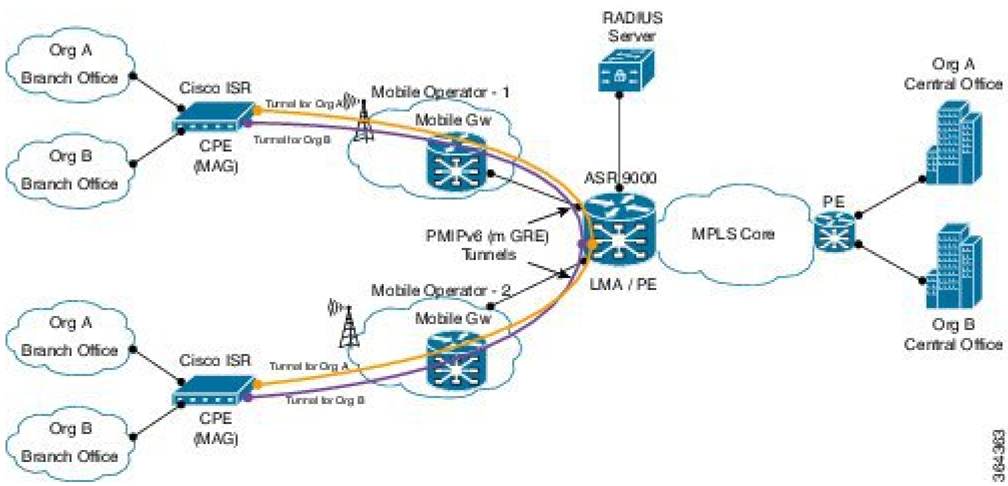
- Awareness of multiple customers belonging to different VRFs
- Peer with multiple mobile operators for transport towards the Customer Premises Equipment (CPE)/Mobile Access Gateway (MAG) devices in separate peering or transport VRFs
- AAA accounting for Mobile Nodes and tunnels

Topology

The following figure is a sample topology of Mobile Local Loop service hosted on Multiprotocol Label Switching (MPLS) multi-VRF Customer Edge (CE) routers:



The following figure is a sample topology of Mobile Local Loop service hosted on MPLS Provider Edge (PE) routers:



In these diagrams:

- Mobile Local Loop (MLL) service allows enterprises Org A and Org B to securely link their remote small branch offices over mobile networks of Mobile Operator 1 and 2 without the need for dedicated leased lines or IP Security (IPSec) VPN cloud. The topologies are examples of MLL service deployment. The service uses Proxy Mobile IPv6 (PMIPv6) based overlay transport.
- At the branch office, CPE/MAG devices such as Cisco ISR series routers are equipped with Cisco HWIC (High-Speed WAN Interface Card) 3G/4G service modules. These devices are used for IP connectivity and setting up overlay transport for service access.
- MLL service provider hosts the LMA function of PMIPv6 and the MLL service on Cisco ASR 9000 series routers which could either be MPLS Provider Edge (PE) routers or MPLS Multi-VRF Customer Edge (CE) routers. LMA can peer with multiple mobile operators (such as Mobile Operators 1 and 2) to enable service access to CPE/MAG devices that can have connectivity to the mobile operators.

- If accounting is enabled, LMA sends accounting records to AAA server with service usage counters.

Configuring VRF Aware LMA

Perform the following steps to configure VRF aware Proxy Mobile IPv6 LMA:

SUMMARY STEPS

1. **configure**
2. **ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name*
3. **hnp maximum** *number*
4. **heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value*
5. **bce maximum** *number*
6. **bce lifetime** *seconds*
7. **bce delete-wait-time** *milliseconds*
8. **replay-protection timestamp window** *seconds*
9. **bri delay { min | max }** *milliseconds*
10. **bri retries** *count*
11. **dynamic mag learning**
12. **aaa accounting [interim** *interim-interval* **]**
13. **dscp control-plane** *dscp-value* **[force]**
14. **mobility-service mobile-local-loop**
15. **customer** *customer-name* **vrf** *vrf-name*
16. **auth-option spi** *hex-value* **key ascii** *value*
17. **heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value*
18. **bce lifetime** *seconds*
19. **network** { **unauthorized | authorized** *network-name* }
20. **pool { mobile-node | mobile-network } { ipv4 | ipv6 } start-address** *address* **pool-prefix** *prefix* **[network-prefix** *prefix***]**
21. **transport** [**vrf** *vrf-name*]
22. **address { ipv4 | ipv6 }** *address*
23. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**ipv6 mobile pmipv6-lma** *lma-identifier* **domain** *domain-name* **Example:** `RP/0/RSP0/CPU0:router(config)# ipv6 mobile pmipv6-lma lma1 domain cisco.com`	Enables the LMA service on the router, configures the PMIPv6 domain for the LMA, and enters LMA configuration mode.

	Command or Action	Purpose
Step 3	**hnp maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# hnp maximum 2`	Configures the maximum number of home network prefixes (HNP) that a mobile node can posses.
Step 4	**heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# heartbeat interval 100 retries 5 timeout 10`	Configures global LMA heartbeat options. *interval-value* specifies the interval between two heartbeat messages in seconds. *retries-value* specifies the number of retries (in the absence of reply from the peer) before the path to the peer is declared as down. *timeout-value* specifies the timeout value to wait for a response from the peer after which the request is declared as timed out.
Step 5	**bce maximum** *number* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce maximum 2500`	Configures the maximum number of binding cache entries (BCEs) or bindings that the LMA can support.
Step 6	**bce lifetime** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce lifetime 2500`	Configures the permitted lifetime of a binding in seconds. The granted lifetime is minimum of this configured value and the value received from the MAG in the PBU packet.
Step 7	**bce delete-wait-time** *milliseconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bce delete-wait-time 100`	Configures the time in milliseconds that LMA must wait before it deletes a BCE of a MN, upon receiving a PBU message from a MAG with a lifetime value of 0.
Step 8	**replay-protection timestamp window** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# replay-protection timestamp window 18`	Configures the time window between the LMA's running clock and the timestamp value received in the PBU from the MAG that the LMA can tolerate for the binding request to be accepted. If the calculated window is larger than this configured value, then the PBU is rejected with status code 156.

Step 9	**bri delay { min | max }** *milliseconds*
	Example:
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay min 500`
	`RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri delay max 2500`
		Configures the minimum and maximum time in milliseconds for which an LMA should wait before transmitting the Binding Revocation Indication (BRI) message to a MAG.

	Command or Action	Purpose
Step 10	**bri retries** *count* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# bri retries 5`	Configures the maximum number of times an LMA should retransmit a BRI message until a Binding Revocation Acknowledgment (BRA) is received from the MAG.
Step 11	**dynamic mag learning** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# dynamic mag learning`	Enables an LMA to accept Proxy Mobile IPv6 (PMIPv6) signaling messages from any Mobile Access Gateway (MAG) that is not locally configured.
Step 12	**aaa accounting [interim** *interim-interval* **]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# aaa accounting interim 2`	Enables LMA accounting. If the **interim** *interim-interval* option is specified, Interim-Update records are sent to the RADIUS security server at the configured *interim-interval* specified in minutes. Otherwise, only Start and Stop records are sent to the RADIUS security server. There are two types of accounting sessions, one for Mobile Nodes and one for tunnels. Interim-Update records are enabled only for tunnel accounting and not for Mobile Node accounting. For information about AAA/RADIUS configuration for accounting, see the *Authentication, Authorization, and Accounting Commands* chapter in Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference.
Step 13	**dscp control-plane** *dscp-value* **[force]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# dscp control-plane 45`	Configures the value of Differentiated Services Code Point (DSCP) in the outgoing PMIPv6 control plane messages. The outgoing packets include locally generated packets such as Proxy Binding Revocation Indications (PBRIs), Proxy Binding Revocation Acknowledgments (PBRAs), Heartbeat Requests, and packets sent in response to packets received from MAG such as Proxy Binding Acknowledgments (PBAs), PBRIs, PBRAs, and Heartbeat Responses. If *dscp-value* is not specified, then the DSCP received in a request is used in the outgoing response packet. DSCP is not set in the other outgoing packets. If *dscp-value* is specified without the **force** option: • The configured DSCP value is set in locally generated packets. • If the received packet does not have DSCP marking, the configured value is set in the outgoing packet.

	Command or Action	Purpose
		• If the received packet has DSCP marking that matches the configured value, then the DSCP received is set in the outgoing response packet. • If the received packet has DSCP marking that does not match the configured value, then the DSCP received is used in the outgoing response packet. If *dscp-value* is specified with the **force** option, then the configured DSCP value is set in all outgoing packets.
Step 14	**mobility-service mobile-local-loop** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma)# mobility-service mobile-local-loop`	Configures Mobile Loop Local (MLL) service on the LMA and enters the service configuration mode.
Step 15	**customer** *customer-name* **vrf** *vrf-name* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll)# customer CUST1 vrf VRF1`	Configures the name and the VRF of a customer. The command enters the customer configuration mode where other parameters of the customer are configured. Use the **no** form of this command to remove an existing customer. There can be many customers, however no two customers can be configured with the same VRF.
Step 16	**auth-option spi** *hex-value* **key ascii** *value* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust)# auth-option spi 87E key ascii KEY1`	Configures customer-specific authentication for the LMA within the MLL. The authentication option includes an SPI value specified in hexadecimal format and a shared secret key which is specified as an ASCII string. This configuration overrides the global **auth-option** configuration in the PMIPv6 LMA Domain.
Step 17	**heartbeat interval** *interval-value* **retries** *retries-value* **timeout** *timeout-value* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust)# heartbeat interval 30 retries 10 timeout 10`	Configures customer-specific heartbeat options. *interval-value* specifies the interval between two heartbeat messages in seconds. *retries-value* specifies the number of retries (in the absence of reply from the peer) before the path to the peer is declared as down. *timeout-value* specifies the timeout value to wait for a response from the peer after which the request is declared as timed out. This configuration overrides the global LMA heartbeat configuration.
Step 18	**bce lifetime** *seconds* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust)# bce lifetime 1500`	Configures customer-specific permitted lifetime of binding cache entries (BCEs) in seconds. This configuration overrides the global LMA BCE configuration.
Step 19	**network** { **unauthorized** | **authorized** *network-name* }	Configures customer-specific network.

	Command or Action	Purpose
	Example: `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust)# network authorized NETW1`	Use the **unauthorized** keyword to configure an unauthorized network. In this case, no network pools are configured for address assignment. The address/prefix of the Logical Mobile Node (LMN) on the MAG and the network prefixes on the Mobile Network interfaces are accepted as received in the Proxy Binding Update (PBU). Use the **authorized** keyword to configure a named network. In this case, the address/prefix of the LMN and Mobile Network prefixes are validated against the configured network pool. The uniqueness of the named network is ensured. Use the **no** form of this command to remove an existing network.
Step 20	**pool { mobile-node | mobile-network } { ipv4 | ipv6 } start-address** *address* **pool-prefix** *prefix* **[network-prefix** *prefix***]** **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust-network)# pool mobile-node ipv4 start-address 192.168.0.2 pool-prefix 8`	Perform this step only if you have configured a named network in the previous step using the **network authorized** command. Configures the IPv4 or IPv6 address pool(s) from which LMA assigns IP addresses to the mobile nodes. The pool is characterized by whether it is for Mobile Nodes or Mobile Networks for the customer, whether it is for IPv4 or IPv6 address family, the start address of the pool, the pool prefix and the network prefix of the pool.
Step 21	**transport** [**vrf** *vrf-name*] **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust)# transport vrf TVRF1`	Configures customer's transport options. They include peering or transport VRF and the LMA IPv4 and/or IPv6 addresses. The addresses are configured in the transport configuration mode using the **address** command. A customer can have multiple transports and can have the same addresses in all transports. However, each customer must have a unique IPv4 and/or a unique IPv6 address. **Note** If the transport is in global VRF, then VRF and *vrf-name* can be omitted in this command.
Step 22	**address { ipv4 | ipv6 }** *address* **Example:** `RP/0/RSP0/CPU0:router(config-pmipv6-lma-mll-cust-tpt)# address ipv6 2001:DB8::1`	Configures customer-specific LMA IPv4 and/or IPv6 addresses. There can only be two instances of addresses, one for IPv4 and one for IPv6.
Step 23	**commit**	

Example: Configuring VRF Aware LMA in a MLL

This example shows sample configuration of VRF aware LMA in a MLL:

```
/* Domain Configuration */

ipv6 mobile pmipv6-domain D1
 lma LMA
 !
 nai @CUST1
  lma LMA
  network CUST1
  service dual
  customer CUST1
 !
 nai @CUST2
  lma LMA
  network CUST2
  service dual
  customer CUST2
 !
!


/* AAA/RADIUS configuration for accounting */

radius-server host 10.10.10.2 auth-port 1645 acct-port 1646
 key 7 094F471A1A0A
!
aaa accounting mobile default group radius


/* LMA Configuration */

ipv6 mobile pmipv6-lma LMA domain D1
 aaa accounting interim 2
 bce maximum 128000
 dscp control-plane 45
 dynamic mag learning
 mobility-service mobile-local-loop
  customer CUST1 vrf VRF1
   bce lifetime 300
   network unauthorized
   heartbeat interval 30 retries 10 timeout 10
   auth-option spi 100 key ascii xyz123
   transport vrf CUSTSP
    address ipv4 15.15.15.2
    address ipv6 2002:15::2
   !
  !
  customer CUST2 vrf VRF2
   network authorized CUST2
   pool mobile-node ipv4 start-address 10.10.10.1 pool-prefix 24
   pool mobile-node ipv6 start-address 2002:10:10:1::1 pool-prefix 48
   pool mobile-network ipv4 start-address 20.20.20.1 pool-prefix 24 network-prefix 28
   pool mobile-network ipv6 start-address 2002:20:0:1::1 pool-prefix 40 network-prefix 64
   !
   transport vrf CUSTSP
    address ipv4 16.16.16.2
    address ipv6 2002:16::2
   !
  !
 !
!
```

Additional References

The following sections provide references related to PMIPv6 LMA

Related Documents

Related Topic	Document Title
PMIPv6 LMA commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Proxy Mobile IPv6 Local Mobility Anchor Commands IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*

Standards and RFCs

Standard/RFC	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

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

Technical Assistance

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

Prerequisites for Configuring NSR, TCP, UDP, Transports

The following prerequisites are required to implement NSR, TCP, UDP, Transports:

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Information About Configuring NSR, TCP, UDP Transports

To configure NSR, TCP, and UDP transports, you must understand the following concepts:

NSR Overview

Nonstop Routing (NSR) is provided for Open Shortest Path First (OSPF) and Label Distribution Protocol (LDP) protocols for the following events:

- Route Processor (RP) failover
- Process restart for either OSPF, LDP, or TCP
- In-service software upgrades (ISSU)

In the case of the RP failover, NSR is achieved by for both TCP and the applications (OSPF or LDP).

NSR is a method to achieve High Availability (HA) of the routing protocols. TCP connections and the routing protocol sessions are migrated from the active RP to standby RP after the RP failover without letting the peers know about the failover. Currently, the sessions terminate and the protocols running on the standby RP reestablish the sessions after the standby RP goes active. Graceful Restart (GR) extensions are used in place of NSR to prevent traffic loss during an RP failover but GR has several drawbacks.

You can use the **nsr process-failures switchover** command to let the RP failover be used as a recovery action when the active TCP or active LDP restarts. When standby TCP or LDP restarts, only the NSR capability is lost till the standby instances come up and the sessions are resynchronized but the sessions do not go down. In the case of the process failure of an active OSPF, a fault-management policy is used. For more information, refer to *Implementing OSPF on Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

TCP Overview

TCP is a connection-oriented protocol that specifies the format of data and acknowledgments that two computer systems exchange to transfer data. TCP also specifies the procedures the computers use to ensure that the data arrives correctly. TCP allows multiple applications on a system to communicate concurrently, because it handles all demultiplexing of the incoming traffic among the application programs.

Any IP protocol other than TCP or UDP is known as a RAW protocol.

For most sites, the default settings for the TCP, UDP, and RAW transports need not be changed.

UDP Overview

The User Datagram Protocol (UDP) is a connectionless transport-layer protocol that belongs to the IP family. UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and TFTP.

Any IP protocol other than TCP, UDP, is known as a RAW protocol.

For most sites, the default settings for the TCP, UDP, and RAW transports need not be changed.

During external port scanning on ports 19 and 20, the UDP packets dropped by Nmap tool without sending an ICMP response, cause uncertainty in identifying the true state of the ports. The port states can be open, closed, or filtered.

Due to no response from the target system, the port states might misclassify as open instead of a closed or filtered state, and can lead to a false-positive situation.

Table 1: UDP port availability for Applications

Platform	Start of Range	End of Range	Availability
Cisco IOS XR 64-bit Operating System	15000	57344	Available
Cisco IOS XR 64-bit Operating System	57345	65535	Reserved
Cisco IOS XR 32-bit Operating System	15000	65535	Available

How to Configure Failover as a Recovery Action for NSR

This section contains the following procedure:

Configuring Failover as a Recovery Action for NSR

This task allows you to configure failover as a recovery action to process failures of active instances.

When the active TCP or the NSR client of the active TCP terminates or restarts, the TCP sessions go down. To continue to provide NSR, failover is configured as a recovery action. If failover is configured, a switchover is initiated if the active TCP or an active application (for example, LDP, OSPF, and so forth) restarts or terminates.

For information on how to configure MPLS Label Distribution Protocol (LDP) for NSR, refer to the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*.

For information on how to configure NSR on a per-process level for each OSPF process, refer to the *Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

Note Before performing this procedure, enable RP isolation using the **isolation enable** command for improved troubleshooting. Without enabling RP isolation, the failing process will not generate the logs required to find the root cause of the failure.

SUMMARY STEPS

1. **configure**
2. nsr process-failures switchover
3. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	nsr process-failures switchover **Example:** `RP/0/RSP0/CPU0:router(config)# nsr process-failures switchover`	Configures failover as a recovery action for active instances to switch over to a standby route processor (RP) to maintain nonstop routing (NSR.
Step 3	**commit**	

XIPC Tail Drop Detection and Correction for TCP

Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Extended IPC (XIPC) Tail drop is one of the more commonly used congestion avoidance mechanisms. Tail drop treats all traffic equally and does not differentiate between classes of service. Queues fill during periods of congestion. When the output queue is full and tail drop is in effect, packets are dropped until the congestion is eliminated and the queue is no longer full.

This feature introduces XIPC as a new policer, and culprit session falls into this bucket and is policed heavily. This feature improves the serviceability of the XIPC queues owned by TCP. To perform this, the TCP monitors and identifies the sessions that are receiving more data. TCP revisits the statistics at regular intervals, and based on the data, it decides whether the sessions need to be policed or added to default policer rate. Therefore, other sessions are given a fair chance to use the XIPC queue, and high-data sessions are throttled down at hardware.

To detect the culprit session, TCP internal queue size is considered along with rate-limit. If the overall queue size reaches the threshold value and per session rate-limit value is exceeded then the culprit sessions in that queue are detected.

After applying the dynamic policer, culprit sessions may flap. As per the TCP dumpfiles and logs, this is an expected behavior. If a culprit BGP session has aggressive timers (KA 3 sec and Hold timer 9 sec), even then the sessions may flap and we may not verify the LPTS packet drops using the **show lpts** commands.

TCP Configurations to Enable XIPC Tail Drop

The following configuration enables XIPC tail drop on TCP:

```
RP/0/0/CPU0:Router (config)# tcp num-thread Ingress-threads-TCP max-threads
RP/0/0/CPU0:Router (config)# pak-rate tcp stats-start [rate-limit packet rate | max-pkt-size
 max-pkt-size-value max-pak-rate max-pak-rate-value]
```

Verification

The following example displays the statistics of TCP packet rate.

```
RP/0/RSP0/CPU0:Router# show tcp pak-rate stats

       PR -  Number of packets in 30 sec (display, if more than Rate-limit)
       MPR - Maximum size packets in 30 sec (display, if more than Maximum packet rate)

         Time          Foreign Address    Local Address     VRF          PR        MPR
------------------------------------------------------------------------------------------

 Nov 19 15:56:08.464   6.6.13.7:179      6.6.13.6:23898    0x60000000  18767      1502
 Nov 19 15:56:08.464   6.6.1.7:46922     6.6.1.6:179       0x60000000  107802     8932
```

Note

- These are the culprit session information and applied LPTS dynamic policer on these sessions.
- Using default BGP timers (60 sec KA and 180 sec hold timer expiry) and show commands, we can observe the number of packets received in the last 30 sec.
- After applying policer, if the number of packets received are less than the configured packet rate, after 85 sec, above details will be removed from the show command.

The following example verifies the sessions statistics at XIPC policer-index level and per-session level.

```
RP/0/RSP0/CPU0:Router# show lpts pifib hardware police location 0/3/cPU0 | i XIPC
                                  Accept Drop
XIPC  97  Local  1000  9600   3912960      368661   01234567
```

```
RP/0/RSP0/CPU0:Router# show lpts pifib hardware police location 0/3/cPU0 | i XIPC
                                   Accept Drop
  XIPC  97  Local  1000  9600      0          0       01234567
```

Note Statistics are cleared when last session under this policer index is removed.

The following example verifies the sessions statistics at XIPC policer and also provides the entries present in the hardware.

```
 RP/0/RSP0/CPU0:Router# show lpts pifib hardware entry statistics location 0/3/cpu0 | i
6.6.1.7,
                                                  Accept/Drop
1754   IPV4 default     TCP    any       LU(30)     4021290/456698  any, 179 6.6.1.7,
46922
2584   IPV4 default     TCP    any       LU(30)       0/0           any, 179 6.6.1.7,
any
```

Additional References

The following sections provide references related to configuring NSR, TCP, and UDP transports.

Related Documents

Related Topic	Document Title
the Cisco ASR 9000 Series Router Transport Stack commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Transport Stack Commands in the IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
the Cisco ASR 9000 Series Router MPLS LDP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*MPLS Label Distribution Protocol Commands in the MPLS Command Reference for Cisco ASR 9000 Series Routers*
the Cisco ASR 9000 Series Router OSPF commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*OSPF Commands in the Routing Command Reference for Cisco ASR 9000 Series Routers*
MPLS Label Distribution Protocol feature information	*Implementing MPLS Label Distribution Protocol in the MPLS Configuration Guide for Cisco ASR 9000 Series Routers*
OSPF feature information	*Implementing OSPF in the Routing Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport