



## Implementing LPTS

Local Packet Transport Services (LPTS) maintains tables describing all packet flows destined for the secure domain router (SDR), making sure that packets are delivered to their intended destinations.

For a complete description of the LPTS commands listed in this module, refer to the LPTS Commands module of *IP Addresses and Services Command Reference for Cisco CRS Routers*.

### Feature History for Implementing LPTS

Release	Modification
Release 3.6.0	The LPTS policer configuration feature was introduced.

- [Prerequisites for Implementing LPTS](#) , on page 1
- [Information About Implementing LPTS](#), on page 1
- [Configuring LPTS Policers](#), on page 2
- [Configuration Examples for Implementing LPTS Policers](#), on page 3
- [Additional References](#), on page 8

## Prerequisites for Implementing LPTS

The following prerequisites are required to implement LPTS:

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 Implementing LPTS

To implement LPTS features mentioned in this document you must understand the following concepts:

### LPTS Overview

LPTS uses two components to accomplish this task: the port arbitrator and flow managers. The port arbitrator and flow managers are processes that maintain the tables that describe packet flows for a logical router, known

as the Internal Forwarding Information Base (IFIB). The IFIB is used to route received packets to the correct Route Processor or line card for processing.

LPTS interfaces internally with all applications that receive packets from outside the router. LPTS functions without any need for customer configuration. However, LPTS **show** commands are provided that allow customers to monitor the activity and performance of LPTS flow managers and the port arbitrator.

## LPTS Policers

In Cisco IOS XR, the control packets, which are destined to the Route Processor (RP), are policed using a set of ingress policers in the incoming line cards. These policers are programmed statically during bootup by LPTS components. The policers are applied based on the flow type of the incoming control traffic. The flow type is determined by looking at the packet headers. The policer rates for these static ingress policers are defined in a configuration file, which are programmed on the line card during bootup.

You can change the policer values based on the flow types of these set of ingress policers. You are able to configure the rate per policer per node (locally) and globally using the command-line interface (CLI); therefore, overwriting the static policer values.




---

**Note** If two different ACLs with same ACEs are applied to an LPTS Policer, only the first ACL applied takes effect. When the first ACL is removed, the second ACL does not take effect on the LPTS Policer. If you want the second ACL to take effect on the LPTS Policer, reconfigure it on the LPTS Policer.

---

## Configuring LPTS Policers

This task allows you to configure the LPTS policers.

### SUMMARY STEPS

1. **configure**
2. **lpts pifib hardware police** [location *node-id*]
3. **flow** *flow\_type* {rate *rate*}
4. **commit**
5. **show lpts pifib hardware police** [location {all | *node\_id*}]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure</b>	
Step 2	<b>lpts pifib hardware police</b> [location <i>node-id</i> ]  <b>Example:</b>  RP/0/RP0/CPU0:router(config)# lpts pifib hardware police location 0/2/CPU0 RP/0/RP0/CPU0:router(config-pifib-policer-per-node)#	Configures the ingress policers and enters pifib policer global configuration mode or pifib policer per node configuration mode.  The example shows pifib policer per node configuration mode and global.

	Command or Action	Purpose
	<pre>RP/0/RP0/CPU0:router(config)# lpts pifib hardware   police RP/0/RP0/CPU0:router(config-pifib-policer-global)#</pre>	
<b>Step 3</b>	<p><b>flow</b> <i>flow_type</i> {<b>rate</b> <i>rate</i>}</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router(config-pifib-policer-per-node)#   flow ospf unicast default rate 20000</pre>	<p>Configures the policer for the LPTS flow type. The example shows how to configure the policer for the ospf flow type.</p> <ul style="list-style-type: none"> <li>• Use the <i>flow_type</i> argument to select the applicable flow type. For information about the flow types, see <i>IP Addresses and Services Command Reference for Cisco CRS Routers</i>.</li> <li>• Use the <b>rate</b> keyword to specify the rate in packets per seconds (PPS). The range is from 0 to 4294967295.</li> </ul> <p><b>Note</b> LPTS policy for ntp-default flow type, supports a flow rate of 100 pps on Cisco ASR 9000 Series Router.</p> <p>Starting with Cisco IOS XR Release 6.1.3, LPTS policy for ntp-default flow type, supports a flow rate higher than 100 pps on Cisco ASR 9000 Series Router.</p> <p>Based on the number of NTP client scale requirement, you can increase the flow rate value to allow higher packets per second (PPS). For example,</p> <pre>lpts pifib hardware police location 0/0/CPU0   flow ntp default rate 1000   flow ntp known rate 1000</pre>
<b>Step 4</b>	<b>commit</b>	
<b>Step 5</b>	<p><b>show lpts pifib hardware police</b> [<b>location</b> {<b>all</b>   <i>node_id</i>}]</p> <p><b>Example:</b></p> <pre>RP/0/RP0/CPU0:router# show lpts pifib hardware   police location 0/2/cpu0</pre>	<p>Displays the policer configuration value set.</p> <ul style="list-style-type: none"> <li>• (Optional) Use the <b>location</b> keyword to display pre-Internal Forwarding Information Base (IFIB) information for the designated node. The <i>node-id</i> argument is entered in the <i>rack/slot/module</i> notation.</li> <li>• Use the <b>all</b> keyword to specify all locations.</li> </ul>

## Configuration Examples for Implementing LPTS Policers

This section provides the following configuration example:

## Configuring LPTS Policers: Example

The following example shows how to configure LPTS policers:

```
configure
lpts pifib hardware police
  flow ospf unicast default rate 200
  flow bgp configured rate 200
  flow bgp default rate 100
!
lpts pifib hardware police location 0/2/CPU0
  flow ospf unicast default rate 100
  flow bgp configured rate 300
!
```

The following is the show command and the sample output:

```
show lpts pifib hardware police location 0/2/CPU0
FT - Flow type ID; PPS - Packets per second configured rate
```

FT	Flow type	Rate (PPS)	Accept/Drop
0	unconfigured-default	101	0/0
0			
	unconfigured-default		
101			0/0
1			
	Fragment		
1000		0	
/0			
2			
	OSPF-mc-known		
1500			
32550			
/0			
3			
	OSPF-mc		
-default			
250			0/0
4			
	OSPF-uc-known		
2000			
0			
/0			
5			
	OSPF		
-uc-default			
101			
1			
/0			

```

6
  ISIS-known          250  1500      0/0
7
ISIS
-default
250
  0
  /0
  8
  BGP-known
    2000      17612
  /0
  9
  BGP-default cfg-peer          203
5
  /0
  10 BGP
  -default
500
  4
  /0
  11
  PIM-mcast          1500      0/0
  12 PIM-ucast        1500      0/0
  13 IGMP
    1500
    0/0
  14
  ICMP-local          1046      0/0
  15
  ICMP-app            1000      1046      0/0
  16
  ICMP-control
1000
  0/0
  17 ICMP
  -default
1046      0
  /0
  18
  LDP-TCP-known      1500      9965
  /0
  19
  LDP-TCP-cfg-peer
1500
0/0
20

```

```

LDP-TCP-default
250
  0
  /0
  21 LDP
  -UDP
1000
59759
/0
22 All
-routers
      1500      0/0
23
LMP-TCP-known
      1500      0/0
24
LMP-TCP-cfg-peer
1500
0/0
25
LMP-TCP-default
250
      0/0
26 LMP
-UDP
      1000      0/0
27 RSVP-UDP
      1000      0/0
28 RSVP
1000      0/0
29 IKE
      1000      0/0
30
IPSEC-known
1000
0/0
31 IPSEC
-default
  250
      0/0
32
MSDP-known
      1000      0/0
33
MSDP-cfg-peer
  1000
  0/0
34 MSDP-default
250
      0/0
35 SNMP
1000
0/0
36 NTP

```

```

500
    0/0
37
SSH-known
    1000    0/0
38 SSH
-default
    1000    0/0
39
HTTP-known
    1000    0/0
40 HTTP
-default
1000    0/0
41
SHTTP-known
    1000    0/0
42 SHTTP
-default
    1000    0/0
43
TELNET-known
    500    1000    0/0
44 TELNET
-default

500
    0/0
45
CSS-known

1000
0/0
46 CSS
-default

500
    0/0
47
RSH-known

1000
0/0
48 RSH
-default

500
    0/0
49
UDP-known

2000
    0/0
50
UDP-listen
    1500    0/0
51
UDP-cfg-peer

1500

0
/0
    
```

```

52 UDP
  -default

101
  653
  /0
53
TCP-known
      2000      0/0

54
TCP-listen
      2000      0/0

55
TCP-cfg-peer

2000

0
/0
56 TCP
  -default

101
  6
  /0
57
Mcast-known

2000
0/0
58 Mcast
  -default

101
      0/0
59
Raw-listen
      250      0/0

60 Raw
  -default

250
      0/0
61 ip-sla

1000
      0/0
62 EIGRP
      1500      0/0

63 RIP
      2398      1500      0/0

64
PCEP
      101      0/0

```

## Additional References

The following sections provide references related to implementing LPTS.



**Related Documents**

Related Topic	Document Title
Cisco IOS XR LPTS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<i>Cisco LPTS Commands</i> module in the <i>IP Addresses and Services Command Reference for Cisco CRS Routers</i>

**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: <a href="https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index">https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index</a>

**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.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

