Implementing EPFT

The Excessive Punt Flow Trap (EPFT) feature attempts to identify and mitigate control packet traffic from remote devices that send more than their allocated share of control packet traffic. A remote device can be a device on a VLAN interface or a device identified by its source MAC address. When remote devices send control packet traffic to the router, the control packets are punted and policed by a local packet transport service (LPTS) queue to protect the router's CPU. If one device sends an excessive rate of control packet traffic, the policer queue fills up, causing many packets to be dropped. If the rate from one "bad actor" device greatly exceeds that of other devices, most of the other devices do not get any of their control packets through to the router. The Excessive Punt Flow Trap feature addresses this situation.

For a complete description of the EPFT commands listed in this module, refer to the EPFT Commands module of *Cisco IOS XR IP Addresses and Services Configuration Guide for the Cisco CRS Router*.

Feature History for Implementing EPFT

Release	Modification
Release 5.3.2	EPFT feature support on Cisco CRS-3 Modular Services Line Card was introduced.
Release 5.3.1	The EPFT configuration feature was introduced.

Information About EPFT

The Excessive Punt Flow Trap feature monitors control packet traffic arriving from physical interfaces, sub-interfaces, bundle interfaces, and bundle sub-interfaces. If the source that floods the punt queue with packets is a device with an interface handle, then all punts from that bad actor interface are penalty policed.

The EPFT feature supports policing the bad actors for Address Resolution Protocol (ARP). ARP has a static punt rate and a penalty rate. For example, the sum total of all ARP punts from remote devices is policed at 1000 packets per second (pps) to the router's CPU. If one remote device sends an excessive rate of ARP traffic and is trapped, then ARP traffic from that bad actor is policed at 10 pps. The remaining (non-bad) remote devices continue to use the static 1000 pps queue for ARP. The excessive rate required to cause an interface

to get trapped has nothing to do with the static punt rate (for example, 1000 pps for ARP). The excessive rate is a rate that is significantly higher than the current average rate of other control packets being punted. The excessive rate is not a fixed rate, and is dependent on the current overall punt packet activity.

Once a bad actor is trapped, it is penalty policed on its punted protocol (ARP), irrespective of the protocol that caused it to be identified as a bad actor. A penalty rate of 10 pps is sufficient to allow the other protocols to function normally. When an interface is trapped, it is placed in a "penalty box" for a period of time (a default of 15 minutes). At the end of the penalty timeout, it is removed from penalty policing (or dropping). If there is still an excessive rate of control packet traffic coming from the remote device, then the interface is trapped again.

For more information about enabling the Excessive Punt Flow Trap feature, see Enabling Excessive Punt Flow Trap Processing, on page 2.

Note Even when the Excessive Punt Flow Trap feature is not enabled, the "bad actors" can affect services for only other devices; they cannot bring down the router.

Prerequisites for Implementing EPFT

The following prerequisites are required to implement EPFT:

- The EPFT feature is supported on Cisco CRS-3 Modular Services Line Card and Cisco CRS-X Line Card.
- 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.

Restrictions for Implementing EPFT

These restrictions apply to implementing EPFT feature:

- This feature is non-deterministic. In some cases, the EPFT feature can give a false positive, i.e. it could trap an interface that is sending legitimate punt traffic.
- The EPFT feature traps flows based on the relative rate of different flows; thus, the behavior depends on the ambient punt rates. A flow that is significantly higher than other flows could be trapped as a bad actor. Thus the feature is less sensitive when there are many flows, and more sensitive when there are fewer flows present.
- Sometimes control packet traffic can occur in bursts. EPFT has safeguards against triggering on short bursts, but longer bursts could trigger a false positive trap.

Enabling Excessive Punt Flow Trap Processing

Perform this task to enable the Excessive Punt Flow Trap (EPFT) feature. The task also enables you to set the penalty policing rate and penalty timeout for a protocol and exclude EPFT processing on a specific interface.

SUMMARY STEPS

1. **configure**
2. **lpts punt excessive-flow-trap non-subscriber-interfaces**
3. **lpts punt excessive-flow-trap penalty-rate** *protocol penalty_policer_rate*
4. **lpts punt excessive-flow-trap penalty-timeout** *protocol time*
5. **lpts punt excessive-flow-trap exclude interface** *interface-name*
6. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	
Step 2	**lpts punt excessive-flow-trap non-subscriber-interfaces** **Example:** `RP/0/RP0/CPU0:router(config)# lpts punt excessive-flow-trap non-subscriber-interfaces`	Enables the Excessive Punt Flow Trap feature on non-subscriber interfaces.
Step 3	**lpts punt excessive-flow-trap penalty-rate** *protocol penalty_policer_rate* **Example:** `RP/0/RP0/CPU0:router(config)# lpts punt excessive-flow-trap penalty-rate arp 10`	Sets the penalty policing rate for a protocol. The penalty policer rate is in packets-per-second (pps) and ranges from 2 to 100. **Note** The penalty policing rate for a protocol consumes a policer rate profile.
Step 4	**lpts punt excessive-flow-trap penalty-timeout** *protocol time* **Example:** `RP/0/RP0/CPU0:router(config)# lpts punt excessive-flow-trap penalty-timeout arp 10`	Sets the penalty timeout value, which is a period of time that the interface trapped is placed in the penalty box, for a protocol. The penalty timeout value is in minutes and ranges from 1 to 1000. The default penalty timeout value is 15 minutes.
Step 5	**lpts punt excessive-flow-trap exclude interface** *interface-name* **Example:** `RP/0/RP0/CPU0:router(config)# lpts punt excessive-flow-trap exclude interface GigabitEthernet0/6/0/6.111`	Excludes EPFT processing on a specific interface.
Step 6	**commit**	

Enabling Excessive Punt Flow Trap Processing: Example

This is an example for enabling the Excessive Punt Flow Trap for non-subscriber interfaces, using the default penalty rate (10 pps) and setting the ARP penalty timeout to 2 minutes.

```
configure
lpts punt excessive-flow-trap non-subscriber-interfaces
lpts punt excessive-flow-trap penalty-rate arp 10
```

```
lpts punt excessive-flow-trap penalty-timeout arp 2
lpts punt excessive-flow-trap exclude interface GigabitEthernet0/6/0/6.111
end
!!
```

Use any of the following **show** commands in EXEC mode to display information about bad actors, penalty status, and other details about the Excessive Punt Flow Trap feature:

- **show lpts punt excessive-flow-trap** [*protocol*]
- **show lpts punt excessive-flow-trap interface** *interface-name* [*protocol*]
- **show running lpts punt excessive-flow-trap**
- **show lpts punt excessive-flow-trap information**

Additional References

The following sections provide references related to implementing Network Stack IPv4 and IPv6.

Related Documents

Related Topic	Document Title
Address resolution configuration tasks	*Configuring ARP* module in this publication.
Mapping host names to IP addresses	*Host Services and Applications Commands* module in the *IP Addresses and Services Command Reference for Cisco CRS Routers*
Network stack IPv4 and IPv6 commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Network Stack IPv4 and IPv6 Commands* section in the *IP Addresses and Services Command Reference for Cisco CRS 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 using Cisco IOS XR software, 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