



Packet Trace

First Published: August 03, 2016

The Packet-Trace feature provides a detailed understanding of how data packets are processed by the Cisco IOS XE platform, and thus helps customers to diagnose issues and troubleshoot them more efficiently. This module provides information about how to use the Packet-Trace feature.

- [Information About Packet Trace, page 1](#)
- [Usage Guidelines for Configuring Packet Trace, page 2](#)
- [Configuring Packet Trace, page 3](#)
- [Displaying Packet-Trace Information, page 5](#)
- [Removing Packet-Trace Data, page 5](#)
- [Configuration Examples for Packet Trace, page 5](#)
- [Additional References, page 8](#)
- [Feature Information for Packet Trace, page 9](#)

Information About Packet Trace

The Packet-Trace feature provides three levels of inspection for packets: accounting, summary, and path data. Each level provides a detailed view of packet processing at the cost of some packet processing capability. However, Packet Trace limits inspection to packets that match the debug platform condition statements, and is a viable option even under heavy-traffic situations in customer environments.

The following table explains the three levels of inspection provided by packet trace.

Table 1: Packet-Trace Level

Packet-Trace Level	Description
Accounting	Packet-Trace accounting provides a count of packets that enter and leave the network processor. Packet-Trace accounting is a lightweight performance activity, and runs continuously until it is disabled.

Packet-Trace Level	Description
Summary	<p>At the summary level of packet trace, data is collected for a finite number of packets. Packet-Trace summary tracks the input and output interfaces, the final packet state, and punt, drop, or inject packets, if any. Collecting summary data adds to additional performance compared to normal packet processing, and can help to isolate a troublesome interface.</p>
Path data	<p>The packet-trace path data level provides the greatest level of detail in packet trace. Data is collected for a finite number of packets. Packet-Trace path data captures data, including a conditional debugging ID that is useful to correlate with feature debugs, a timestamp, and also feature-specific path-trace data.</p> <p>Path data also has two optional capabilities: packet copy and Feature Invocation Array (FIA) trace. The packet-copy option enables you to copy input and output packets at various layers of the packet (layer 2, layer 3 or layer 4). The FIA- trace option tracks every feature entry invoked during packet processing and helps you to know what is happening during packet processing.</p> <p>Note Collecting path data consumes more packet-processing resources, and the optional capabilities incrementally affect packet performance. Therefore, path-data level should be used in limited capacity or in situations where packet performance change is acceptable.</p>

Usage Guidelines for Configuring Packet Trace

Consider the following best practices while configuring the Packet-Trace feature:

- Use of ingress conditions when using the Packet-Trace feature is recommended for a more comprehensive view of packets.
- Packet-trace configuration requires data-plane memory. On systems where data-plane memory is constrained, carefully consider how you will select the packet-trace values. A close approximation of the amount of memory consumed by packet trace is provided by the following equation:

$$\text{memory required} = (\text{statistics overhead}) + \text{number of packets} * (\text{summary size} + \text{data size} + \text{packet copy size}).$$

When the Packet-Trace feature is enabled, a small, fixed amount of memory is allocated for statistics. Similarly, when per-packet data is captured, a small, fixed amount of memory is required for each packet for summary data. However, as shown by the equation, you can significantly influence the amount of memory consumed by the number of packets you select to trace, and whether you collect path data and copies of packets.

Configuring Packet Trace

Perform the following steps to configure the Packet-Trace feature.



Note

The amount of memory consumed by the Packet-Trace feature is affected by the packet-trace configuration. You should carefully select the size of per-packet path data and copy buffers and the number of packets to be traced in order to avoid interrupting normal services. You can check the current data-plane DRAM memory consumption by using the **show platform hardware qfp active infrastructure exmem statistics** command.

SUMMARY STEPS

1. **enable**
2. **debug platform packet-trace packet** *pkt-num* [**fia-trace** | **summary-only**] [**circular**] [**data-size** *data-size*]
3. **debug platform packet-trace punt**
4. **debug platform condition** [**ipv4** | **ipv6**] [**interface** *interface*][**access-list** *access-list-name* | *ipv4-address / subnet-mask* | *ipv6-address / subnet-mask*] [**ingress**| **egress**]
5. **debug platform condition start**
6. **debug platform condition stop**
7. **show platform packet-trace** {**configuration** | **statistics** | **summary** | **packet** {**all** | *pkt-num*}}
8. **clear platform condition all**
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables the privileged EXEC mode. Enter your password if prompted.
Step 2	debug platform packet-trace packet <i>pkt-num</i> [fia-trace summary-only] [circular] [data-size <i>data-size</i>] Example: Router# debug platform packet-trace packets 2048 summary-only	Collects summary data for a specified number of packets. Captures feature path data by the default, and optionally performs FIA trace. <i>pkt-num</i> —Specifies the maximum number of packets maintained at a given time. fia-trace —Provides detailed level of data capture, including summary data, feature-specific data. Also displays each feature entry visited during packet processing. summary-only —Enables the capture of summary data with minimal details. circular —Saves the data of the most recently traced packets.

	Command or Action	Purpose
		<i>data-size</i> —Specifies the size of data buffers for storing feature and FIA trace data for each packet in bytes. When very heavy packet processing is performed on packets, users can increase the size of the data buffers if necessary. The default value is 2048.
Step 3	debug platform packet-trace punt Example: Router# debug platform packet-trace punt	Enables tracing of punted packets from Layer2 to Layer3.
Step 4	debug platform condition [ipv4 ipv6] [interface interface][access-list access-list -name ipv4-address / subnet-mask ipv6-address / subnet-mask] [ingress egress] Example: Router# debug platform condition interface g0/0/0 ingress	Specifies the matching criteria for tracing packets. Provides the ability to filter by protocol, IP address and subnet mask, access control list (ACL), interface, and direction.
Step 5	debug platform condition start Example: Router# debug platform condition start	Enables the specified matching criteria and starts packet tracing.
Step 6	debug platform condition stop Example: Router# debug platform condition start	Deactivates the condition and stops packet tracing.
Step 7	show platform packet-trace {configuration statistics summary packet {all pkt-num}} Example: Router# show platform packet-trace 14	Displays packet-trace data according to the specified option. See {start cross reference} Table 21-1 {end cross reference} for detailed information about the show command options.
Step 8	clear platform condition all Example: Router(config)# clear platform condition all	Removes the configurations provided by the debug platform condition and debug platform packet-trace commands.
Step 9	exit Example: Router# exit	Exits the privileged EXEC mode.

Displaying Packet-Trace Information

Use these **show** commands to display packet-trace information.

Table 2: show Commands

Command	Description
show platform packet-trace configuration	Displays packet trace configuration, including any defaults.
show platform packet-trace statistics	Displays accounting data for all the traced packets.
show platform packet-trace summary	Displays summary data for the number of packets specified.
show platform packet-trace {all <i>pkt-num</i>} [decode]	Displays the path data for all the packets or the packet specified. The decode option attempts to decode the binary packet into a more human- readable form.

Removing Packet-Trace Data

Use these commands to clear packet-trace data.

Table 3: clear Commands

Command	Description
clear platform packet-trace statistics	Clears the collected packet-trace data and statistics.
clear platform packet-trace configuration	Clears the packet-trace configuration and the statistics.

Configuration Examples for Packet Trace

This section provides the following configuration examples:

Example: Configuring Packet Trace

This example describes how to configure packet trace and display the results. In this example, incoming packets to Gigabit Ethernet interface 0/0/2 are traced, and FIA-trace data is captured for the first 128 packets.

Also, the input packets are copied. The **show platform packet-trace packet 10** command displays the summary data and each feature entry visited during packet processing for packet 10.

```

Router>
enable
Router# debug platform packet-trace packet 128 fia-trace
Router# debug platform packet-trace punt
Router# debug platform condition interface g0/0/2 ingress
Router# debug platform condition start
Router#! ping to UUT
Router# debug platform condition stop
Router# show platform packet-trace packet 10
Packet: 10          CBUG ID: 52
Summary
  Input       : GigabitEthernet0/0/0
  Output      : internal0/0/rp:1
  State       : PUNT 55 (For-us control)
  Timestamp
    Start     : 597718358383 ns (06/06/2016 09:00:13.643341 UTC)
    Stop      : 597718409650 ns (06/06/2016 09:00:13.643392 UTC)
Path Trace
Feature: IPV4
  Input       : GigabitEthernet0/0/0
  Output      : <unknown>
  Source      : 10.64.68.2
  Destination : 224.0.0.102
  Protocol    : 17 (UDP)
  SrcPort     : 1985
  DstPort     : 1985
Feature: FIA_TRACE
  Input       : GigabitEthernet0/0/0
  Output      : <unknown>
  Entry       : 0x8a0177bc - DEBUG_COND_INPUT_PKT
  Lapsed time : 426 ns
Feature: FIA_TRACE
--More--
  Input       : GigabitEthernet0/0/0
  Output      : <unknown>
  Entry       : 0x8a017788 - IPV4_INPUT_DST_LOOKUP_CONSUME
  Lapsed time : 386 ns
Feature: FIA_TRACE
  Input       : GigabitEthernet0/0/0
  Output      : <unknown>
  Entry       : 0x8a01778c - IPV4_INPUT_FOR_US_MARTIAN
  Lapsed time : 13653 ns
Feature: FIA_TRACE
  Input       : GigabitEthernet0/0/0
  Output      : internal0/0/rp:1
  Entry       : 0x8a017730 - IPV4_INPUT_LOOKUP_PROCESS_EXT
  Lapsed time : 2360 ns
Feature: FIA_TRACE
  Input       : GigabitEthernet0/0/0
  Output      : internal0/0/rp:1
  Entry       : 0x8a017be0 - IPV4_INPUT_IPOPTIONS_PROCESS_EXT
  Lapsed time : 66 ns
Feature: FIA_TRACE
  Input       : GigabitEthernet0/0/0
  Output      : internal0/0/rp:1
  Entry       : 0x8a017bfc - IPV4_INPUT_GOTO_OUTPUT_FEATURE_EXT
  Lapsed time : 680 ns
--More--
Feature: FIA_TRACE
  Input       : GigabitEthernet0/0/0
  Output      : internal0/0/rp:1
  Entry       : 0x8a017d60 - IPV4_INTERNAL_ARL_SANITY_EXT
  Lapsed time : 320 ns
Feature: FIA_TRACE
  Input       : GigabitEthernet0/0/0
  Output      : internal0/0/rp:1
  Entry       : 0x8a017a40 - IPV4_VFR_REFRAG_EXT
  Lapsed time : 106 ns
Feature: FIA_TRACE
  Input       : GigabitEthernet0/0/0

```

```

Output      : internal0/0/rp:1
Entry       : 0x8a017d2c - IPV4_OUTPUT_DROP_POLICY_EXT
Lapsed time : 1173 ns
Feature: FIA_TRACE
Input       : GigabitEthernet0/0/0
Output      : internal0/0/rp:1
Entry       : 0x8a017940 - INTERNAL_TRANSMIT_PKT_EXT
Lapsed time : 20173 ns
IOSd Path Flow: Packet: 10      CBUG ID: 52
Feature: INFRA
  Pkt Direction: IN
  Packet Rcvd From CPP
Feature: IP
  Pkt Direction: IN
  Packet Enqueued in IP layer
  Source        : 10.64.68.2
  Destination   : 224.0.0.102
  Interface     : GigabitEthernet0/0/0
Feature: UDP
  Pkt Direction: IN
  src           : 10.64.68.2(1985)
  dst           : 224.0.0.102(1985)
  length        : 14
Router# clear platform condition all
Router# exit

```

Example: Using Packet Trace

This example provides a scenario in which packet trace is used to troubleshoot packet drops for a NAT configuration on a Cisco ASR 1006 Router. This example shows how you can effectively utilize the level of detail provided by the Packet-Trace feature to gather information about an issue, isolate the issue, and then find a solution.

In this scenario, you can detect that there are issues, but are not sure where to start troubleshooting. You should, therefore, consider accessing the Packet-Trace summary for a number of incoming packets.

```

Router# debug platform condition ingress
Router# debug platform packet-trace packet 2048 summary-only
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Pkt  Input          Output          State  Reason
0    Gi0/0/2.3060     Gi0/0/2.3060   DROP   402 (NoStatsUpdate)
1    internal0/0/rp:0 internal0/0/rp:0 PUNT   21 (RP<->QFP keepalive)
2    internal0/0/recycle:0 Gi0/0/2.3060  FWD

```

The output shows that packets are dropped due to NAT configuration on Gigabit Ethernet interface 0/0/0, which enables you to understand that an issue is occurring on a specific interface. Using this information, you can limit which packets to trace, reduce the number of packets for data capture, and increase the level of inspection.

```

Router# debug platform packet-trace packet 256
Router# debug platform packet-trace punt
Router# debug platform condition interface Gi0/0/0
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Router# show platform packet-trace 15
Packet: 15      CBUG ID: 238
Summary
Input          : GigabitEthernet0/0/0
Output         : internal0/0/rp:1
State          : PUNT 55 (For-us control)
Timestamp
Start          : 1166288346725 ns (06/06/2016 09:09:42.202734 UTC)
Stop           : 1166288383210 ns (06/06/2016 09:09:42.202770 UTC)

```

```

Path Trace
Feature: IPV4
  Input      : GigabitEthernet0/0/0
  Output     : <unknown>
  Source     : 10.64.68.3
  Destination : 224.0.0.102
  Protocol   : 17 (UDP)
  SrcPort    : 1985
  DstPort    : 1985
IOSd Path Flow: Packet: 15   CBUG ID: 238
Feature: INFRA
  Pkt Direction: IN
  Packet Rcvd From CPP
Feature: IP
  Pkt Direction: IN
  Source        : 10.64.68.122
  Destination   : 10.64.68.255
Feature: IP
  Pkt Direction: IN
  Packet Enqueued in IP layer
  Source        : 10.64.68.122
  Destination   : 10.64.68.255
  Interface     : GigabitEthernet0/0/0
Feature: UDP
  Pkt Direction: IN
  src           : 10.64.68.122 (1053)
  dst           : 10.64.68.255 (1947)
  length        : 48

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	<i>Cisco IOS Master Commands List, All Releases</i>

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at this URL: {start hypertext}http://www.cisco.com/go/mibs{end hypertext}

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	{start hypertext}; http://www.cisco.com/cisco/web/support/index.html {end hypertext}

Feature Information for Packet Trace

{start cross reference} Table 21-4 {end cross reference} lists the features in this module and provides links to specific configuration information.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to {start hypertext} <http://www.cisco.com/go/cfn> {end hypertext}. An account on Cisco.com is not required.

**Note**

{start cross reference} Table 21-4 {end cross reference} lists only the software releases that support a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 4: Feature Information for Packet Trace

Feature Name	Releases	Feature Information
Packet Trace	Cisco IOS XE 3.10S	<p>The Packet Trace feature provides information about how data packets are processed by the Cisco IOS XE software.</p> <p>In Cisco IOS XE Release 3.10S, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were introduced or modified:</p> <ul style="list-style-type: none"> • debug platform packet-trace packet <i>pkt-num</i> [fia-trace summary-only] [data-size <i>data-size</i>] [circular] • debug platform packet-trace copy packet {input output both} [size <i>num-bytes</i>] [L2 L3 L4] • show platform packet-trace {configuration statistics summary packet {all <i>pkt-num</i>}}
	Cisco IOS XE 3.11S	<p>In Cisco IOS XE Release 3.11S, this feature was enhanced to include the following features:</p> <ul style="list-style-type: none"> • Matched versus traced statistics. • Trace stop timestamp in addition to trace start timestamp. <p>The following commands were introduced or modified:</p> <ul style="list-style-type: none"> • debug platform packet-trace drop [code <i>drop-num</i>] • show platform packet-trace packet {all <i>pkt-num</i>} [decode]

Feature Name	Releases	Feature Information
	Cisco IOS XE Denali 16.3.1	<p>In Cisco IOS XE Denali 16.3.1, this feature was enhanced to include Layer3 packet tracing along with IOSd.</p> <p>The following commands were introduced or modified: debug platform packet-trace punt.</p>

