

Table of Contents

<u>Understanding Selective Packet Discard (SPD)</u>	1
<u>Document ID: 29920</u>	1
<u>Introduction</u>	1
<u>Before You Begin</u>	1
<u>Conventions</u>	1
<u>Prerequisites</u>	1
<u>Components Used</u>	1
<u>Overview</u>	2
<u>The SPD Process</u>	2
<u>SPD State Check</u>	2
<u>Input Queue Check</u>	3
<u>Miscellaneous</u>	5
<u>Related Information</u>	6

Understanding Selective Packet Discard (SPD)

Document ID: 29920

Introduction

Before You Begin

Conventions

Prerequisites

Components Used

Overview

The SPD Process

SPD State Check

Input Queue Check

Miscellaneous

Related Information

Introduction

This document explains the Selective Packet Discard (SPD) mechanism, and how it can be monitored and tuned.

Note: This document does not explain how to troubleshoot an increasing number of input drops in the **show interfaces** output on a Cisco 12000 Series Internet Router. For this, see Troubleshooting Input Drops on the Cisco 12000 Series Internet Router.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

The information in this document is based on the software and hardware versions below:

- Cisco 7200 Series Router
- Cisco 7500 Series Router
- Cisco 12000 Series Internet Router
- All versions of Cisco IOS® software

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Overview

Selective Packet Discard (SPD) is a mechanism to manage the process level input queues on the Route Processor (RP). The goal of SPD is to provide priority to routing protocol packets and other important traffic control Layer 2 keepalives during periods of process level queue congestion.

Historically, on platforms such as the Cisco 7x00 and non-Cisco Express Forwarding (CEF) 7500 systems, significant numbers of transit packets were forwarded by the Route Processor in order to populate the fast switching cache. Consequently, SPD was required in this case to prioritize the routing protocol packets over the transit packets which share the same queue.

Currently, on the Cisco 12000 Series Internet Router and on the 7500 running CEF, only traffic destined to the router itself is sent to process level. In this case, SPD is used to prioritize routing protocol packets when management traffic such as Simple Network Management Protocol (SNMP) is present or when a Denial of Service (DoS) attack sending traffic to the RP is occurring.

The SPD Process

On the Cisco 12000 Series, when a line card determines that an incoming packet needs to be punted to the RP for processing, the packet travels across the switch fabric as Cisco Cells and is eventually received by the Cisco Cell Segmentation and Reassembly (CSAR) Field Programmable Gate Array (FPGA).

Its purpose is to handle the traffic between the switch fabric and the RP CPU, and this is where the SPD checks are performed. This applies to IP packets, Connectionless Network Service (CLNS) packets, Layer 2 keepalives, and similar packets punted to the RP. SPD makes two checks and can potentially drop a packet in one of these two states:

- SPD state check
- Input queue check

SPD State Check

The IP process queue on the RP is divided into two parts: a general packet queue and a priority queue. Packets put in the general packet queue are subject to the SPD state check, and those that are put in the priority queue are not. Packets that qualify for the priority packet queue are high priority packets such as those of IP precedence 6 or 7 and should never be dropped. The non-qualifiers, however, can be dropped here depending on the length of the general packet queue depending on the SPD state. The general packet queue can be in three states and, as such, the low priority packets may be serviced differently:

- NORMAL: queue size \leq min
- RANDOM DROP: min \leq queue size \leq max
- FULL DROP: max \leq queue size

In the NORMAL state, we never drop well-formed and malformed packets.

In the RANDOM DROP state, we randomly drop well-formed packets. If aggressive mode is configured, we drop all malformed packets; otherwise, we treat them as well-formed packets.

In FULL DROP state, we drop all well-formed and malformed packets. These minimum (default 73) and maximum (default 74) values are derived from the smallest hold-queue on the chassis, but can be overridden with the global commands **ip spd queue min-threshold** and **ip spd queue max-threshold**.

Aggressive Mode

SPD can be configured for two different modes: normal (default) and aggressive. The only difference between the two is how the router accounts for invalid IP packets (invalid checksum, incorrect version, incorrect header length, incorrect packet length). Malformed IP packets are dropped by SPD when we are in aggressive mode and in the Random drop state. Aggressive mode can be configured using the **ip spd mode aggressive** command.

Note: Aggressive mode is not implemented on the Cisco 12000 Series Internet Router since malformed IP packets are dropped directly by the ingress line card, and these packets are not punted to the Gigabit Route Processor (GRP). As a result, aggressive mode is not needed on this particular platform.

Input Queue Check

The input queue is maintained per hardware interface, shared amongst all subinterfaces. Without SPD, all packets are dropped if the input queue is full when the packet is received. The default input queue size is 75 and is configurable per interface using the **hold-queue [size] in** interface configuration command. The number of packets in the input queue can be seen in the "input queue" field in the **show interfaces** command.

```
router#show interfaces pos 3/0
POS3/0 is up, line protocol is up
Hardware is Packet over SONET
Internet address is 137.40.55.2/24
MTU 4470 bytes, BW 2488000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation PPP, crc 32, loopback not set
Keepalive not set
Scramble disabled
LCP Open
Open: IPCP, CDPCP, OSICP, TAGCP
Last input 00:00:01, output 00:00:00, output hang never
Last clearing of "show interface" counters 2w3d
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
30 second input rate 9000 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
  456292 packets input, 917329913 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
      0 parity
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
112046977 packets output, 32078928095 bytes, 0 underruns
0 output errors, 0 applique, 3 interface resets
0 output buffer failures, 0 output buffers swapped out
1 carrier transitions
```

Note: Decreasing the input queue size on one interface can cause a huge number of input drops on all the other interfaces. Be sure to have a minimum input hold queue size of at least 75.

SPD Headroom

Even with SPD, the behavior of normal IP packets is not changed; however, routing protocol packets are given higher priority because SPD recognizes routing protocol packets by the IP precedence field. Hence, if the IP precedence is set to 6, then the packet is given priority.

SPD prioritizes these packets by allowing the software to enqueue them into the process level input queue above the normal input queue limit. The number of packets allowed in excess of the normal limit is called the spd headroom, the default being 100, which means that a high precedence packet is not dropped if the size of

the input hold queue is lower than 175 (input queue default size + spd headroom size).

As from Cisco IOS Software Release 12.0(22)S, the spd headroom default is 1000 for the Cisco 12000 Series Internet Router to accommodate larger SP networks. This is due to the fact that Border Gateway Protocol (BGP) peering is used with an ever-growing number of neighbors to advertise an ever-growing number of routes over ever-faster interfaces. A single clearing of BGP can often result in thousands of input queue drops on a single interface, which can severely hamper convergence times.

SPD headroom is configurable using the **spd headroom** command. Its current level can be seen in the output of the **show spd** or **show ip spd** command.

```
Router#show spd
Headroom: 1000, Extended Headroom: 10

Router#show ip spd
Current mode: normal
Queue min/max thresholds: 73/74, Headroom: 1000, Extended Headroom: 10
IP normal queue: 0, priority queue: 0.
SPD special drop mode: none
```

Note: The size of the IP normal queue can also be monitored by the **show ip spd** command.

Extended SPD Headroom

Non-IP packets, such as Connectionless Network Service Intermediate System-to-Intermediate System (CLNS ISIS) packets, Point-to-Point Protocol (PPP) packets, and High-Level Data Link Control (HDLC) keepalives were, until recently, treated as normal priority as a result of being Layer 2 instead of Layer 3. In addition, Interior Gateway Protocols (IGPs) operating at Layer 3 or higher were given priority over normal IP packets, but given the same priority as BGP packets. So, during BGP convergence or during times of very high BGP activity, IGP hellos and keepalives were often dropped, causing IGP adjacencies to go down.

Since IGP and link stability are more tenuous and more crucial than BGP stability, such packets are now given the highest priority and are given extended SPD headroom with a default of 10 packets. This means that these packets are not dropped if the size of the input hold queue is lower than 185 (input queue default size + spd headroom size + spd extended headroom).

Extended SPD headroom is configurable using the **spd extended [size]** command, and its current level can be seen from the output of the **show spd** or **show ip spd** command.

```
Router#show ip spd
Current mode: normal
Queue min/max thresholds: 73/74, Headroom: 100, Extended Headroom: 10
IP normal queue: 0, priority queue: 0.
SPD special drop mode: none
```

Note: On the Cisco 12000 Series Internet Router, HDLC and PPP keepalives, along with CLNS ISIS routing protocol packets are treated as high priority and might be enqueued in the extended SPD headroom since Cisco IOS Software Release 12.0(12)S1. Since Cisco IOS Software Release 12.0(18)S, all IGP packets might be enqueued in the extended SPD headroom as well.

Diagram of Input Queue

The default values, prior to Cisco IOS Software Release 12.0(22)S, are:

- Input queue size = 75

- SPD headroom size = 100
- Extended headroom size = 10

The default values, after Cisco IOS Software Release 12.0(22)S, are:

- Input queue size = 75
- SPD headroom size = 1000
- Extended headroom size = 10

In the first case, this gives:

Input queue (hold queue)	SPD headroom	Extended headroom
0	75	175
185		

Normal IP, BGP, ISIS, OSPF, HDLC	BGP, ISIS, OSPF, HDLC	ISIS, OSPF, HDLC
0	75	175
		185

- IP packets with normal precedence are allowed to enqueue up to the default queue limit (75)
- High priority IP packets are allowed to enqueue up to the default queue limit + spd_headroom (175 or 1075 based on the Cisco IOS software release)
- CLNS, IGP and LC keepalive packets are allowed to enqueue up to the default queue limit + spd_headroom + spd_ext_headroom (185 or 1085 based on the Cisco IOS software release).

Miscellaneous

Here are some additional tips/information about SPD:

- By default, SPD is "on". It can be enabled/disabled using the **spd enable** global command.
- Initially, SPD was only available on Packet Over Sonet (PoS) interfaces.
- Prior to Cisco IOS Software Release 12.0(21)S, SPD did not function on Gigabit Ethernet line cards (Engine 1 and Engine 2) and Fast Ethernet line cards that are installed in a Cisco 12000 Series Internet router. The input hold queue had to be increased to store the excess packets.
- On the Cisco 7200/7500 Series router, the SPD flushes (drops) counter can be seen in the output of the **show interfaces** command since Cisco IOS Software Releases 12.1(1), 12.1(1)T, and 12.0(9)ST for non FIFO (First In First Out) queueing and since 12.2(7), 12.2(7)T, and 12.1(7)E for FIFO queueing. On other releases and on the Cisco 12000 Series Internet Router, this counter is only seen by typing the **show interface switching** command. For instance, the **show interface pos 0/1 switching** command can be used to see SPD flushes, aggressive drops, and priority.

Here is an example:

```
7500_Router#show interfaces
FastEthernet0/0/0 is up, line protocol is up
Hardware is cyBus FastEthernet Interface, address is 0090.9282.7000 (bia 0090)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set
```

```
Keepalive set (10 sec)

Full-duplex, 100Mb/s, 100BaseTX/FX

ARP type: ARPA, ARP Timeout 04:00:00

Last input 00:00:01, output 00:00:01, output hang never

Last clearing of "show interface" counters never

Queueing strategy: fifo

Output queue 0/40, 0 drops; input queue 0/75, 0 drops, 0 flushes

30 second input rate 4000 bits/sec, 9 packets/sec

30 second output rate 0 bits/sec, 0 packets/sec

2628397 packets input, 546327119 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

0 watchdog, 0 multicast

0 input packets with dribble condition detected

264792 packets output, 225434458 bytes, 0 underruns

0 output errors, 0 collisions, 20 interface resets

0 babbles, 0 late collision, 0 deferred

22 lost carrier, 0 no carrier

0 output buffer failures, 0 output buffers swapped out
```

Related Information

- [Troubleshooting Input Drops on the Cisco 12000 Series Internet Router](#)
- [Troubleshooting High CPU Caused by the BGP Scanner or BGP Router Process](#)
- [Technical Support – Cisco Systems](#)

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jun 27, 2005

Document ID: 29920
