



Configuration Guide

DoS Protection

This configuration guide provides an overview of the denial of service (DoS) protection feature available in some ADTRAN Operating System (AOS) switch products. This guide is an overview of the information provided by the DoS protection feature, as well as how to configure the feature using the Web-based graphical user interface (GUI) and the AOS command line interface (CLI).

This guide consists of the following sections:

- *Introduction to DoS Protection* on page 2
- *Hardware and Software Requirements and Limitations* on page 2
- *Configuring DoS Protection Using the GUI* on page 2
- *Configuring DoS Protection Using the CLI* on page 8
- *Troubleshooting* on page 9
- *Command Summary Tables* on page 10

Introduction to DoS Protection

DoS attacks are malicious attacks intended to prevent network resources from being available for use by legitimate network traffic. DoS attacks, in a general sense, consume resources. Often this is done by bombarding the target with communication requests. This puts a strain on hardware resources and prevents normal network function.

The AOS DoS protection feature has been designed to use built-in hardware security registers to protect against many common DoS attacks.

The DoS protection feature provides protection similar to that achieved by configuring hardware access control lists (ACLs) in AOS. The primary advantage of the DoS protection feature is that it uses registers built into the chipset. Using the chipset registers allows the DoS protection feature to be enabled without negatively impacting the hardware resources of the switch.

DoS threats are broken down into five categories according to error statistics. Each threat is assigned a threat ID for ease of configuration through the CLI. A categorized list of these threats and their corresponding IDs can be found using the **show dos-id** command in the CLI.

This guide contains a detailed list of available CLI commands related to the DoS protection feature, as well as screenshots from the GUI that provide an outline of the displayed information and configuration of the feature.

Hardware and Software Requirements and Limitations

The DoS protection feature was implemented in AOS version 17.7 and is available on AOS products as outlined in the ADTRAN knowledge base article number 2272, *Product Feature Matrix*. This matrix is available online at <http://kb.adtran.com>.

The DoS protection feature is disabled by default.

The DoS protection feature does not protect against every possible type of DoS attack that can occur.

Configuring DoS Protection Using the GUI

To configure DoS protection using the GUI, follow these steps:

1. Open a new Web page in your Internet browser.
2. Type your AOS product's IP address in the Internet browser's address field in the following form:
http://<ip address>. For example:
http://65.162.109.200

3. At the prompt, enter your user name and password and select **OK**.



*The default user name is **admin** and the default password is **password**.*

4. Navigate to **Data > Switch > DOS Protection**.



5. Select the **Configuration** tab to display the Configuration pane. This pane is the default view, and displays all DoS threat protections that can be enabled using the DoS protection feature. The threats are organized into five threat categories: **DOS L4 Header Error**, **DOS L3 Header Error**, **DOS ICMP Error**, **DOS Fragment Error**, and **Miscellaneous**.

Denial of Service (DOS) Protection

Configuration | Summary by Type | Summary by Port

Check the DOS (Denial of Service) attack(s) from the list below for the switch to drop if encountered. Click on the description for more information on the attack.

DOS L4 Header Error

- [TCP packets with control flags set and seq # equal to 0](#)
- [TCP packets with SYN and FIN bits set](#)
- [TCP packets with FIN,URG, PSH bits set with ACK bit & seq # equal to 0](#)
- [TCP packets with source port equal to destination port](#)
- [UDP packets with source port equal to destination port](#)
- [TCP SYN packets with source port 0-1023 for the first fragment](#)
- [TCP fragments with TCP header smaller than](#) Bytes (0-255)

DOS L3 Header Error

- [Packets with source IP equal to destination IP \(Land Attack\)](#)

DOS ICMP Error

- [ICMP fragments](#)
- [ICMPv4 ping packets with payload greater than](#) Kilo-Bytes (0-16)
- [ICMPv6 ping packets with payload greater than](#) Kilo-Bytes (0-16)

DOS Fragment Error

- [TCP fragments with offset value set to 1](#)

Miscellaneous

- [Packets with source MAC equal to destination MAC](#)

- To enable protection for a threat, select the blank check box next to the desired threat name. Once all threats have been checked, select the **Apply** button to save the new settings. To return the check boxes to their original status, select the **Reset** button (before selecting **Apply**).



*Selecting a threat type in the **Configuration** pane opens a new browser window that contains a detailed description of that particular threat.*

- Select the **Summary by Type** tab to display the DoS attack statistics. Selecting this tab displays the number of DoS attacks, broken down by the five threat categories. The **Summary by Type** tab is only a representation of threat data, no configuration options or additional data are available from this tab. The threat counters can be reset by selecting the **Clear Statistics** button located on the **Port Statistics** pane.

The screenshot shows a web interface titled "Denial of Service (DOS) Protection". At the top, there are three tabs: "Configuration", "Summary by Type", and "Summary by Port". The "Summary by Type" tab is currently selected. Below the tabs is a table with four rows of data:

Threat Category	Count
DOS L4 Header Errors	964
DOS L3 Header Errors	0
DOS ICMP Errors	0
DOS Fragment Errors	0

8. Select the **Summary by Port** tab. Selecting this tab opens a pane containing a list of all ports on the unit. Next to each port is the total number of DoS attacks since the last time the port statistics were cleared.

The screenshot shows the 'Denial of Service (DOS) Protection' configuration page. The 'Summary by Port' tab is selected. A message above the table reads: 'To view more details on what the DOS errors are, click on the desired port.' The table below lists 29 ports, each with a 'Total DOS Errors' column. The first port, 'q1ga-swx 0/1', has 965 errors, while all other ports have 0 errors.

Name	Total DOS Errors
q1ga-swx 0/1	965
q1ga-swx 0/2	0
q1ga-swx 0/3	0
q1ga-swx 0/4	0
q1ga-swx 0/5	0
q1ga-swx 0/6	0
q1ga-swx 0/7	0
q1ga-swx 0/8	0
q1ga-swx 0/9	0
q1ga-swx 0/10	0
q1ga-swx 0/11	0
q1ga-swx 0/12	0
q1ga-swx 0/13	0
q1ga-swx 0/14	0
q1ga-swx 0/15	0
q1ga-swx 0/16	0
q1ga-swx 0/17	0
q1ga-swx 0/18	0
q1ga-swx 0/19	0
q1ga-swx 0/20	0
q1ga-swx 0/21	0
q1ga-swx 0/22	0
q1ga-swx 0/23	0
q1ga-swx 0/24	0
q1ga-swx 0/25	0
q1ga-swx 0/26	0
q1ga-swx 0/27	0
q1ga-swx 0/28	0

9. Select an individual port to open the **Port Statistics** pane for that particular port. DoS protection statistics are located at the bottom of the **Port Statistics** pane, as indicated by the red outline. DoS protection statistics can be cleared, along with other port statistics, by selecting **Clear Statistics** located at the bottom of the pane. To open the **Port Statistics** pane without going through the **Summary by Port** pane, navigate to **Data > Ports** using the sidebar, and select the desired port.

Port Statistics for giga-swxx 0/1

Admin Status	Up
Line Status	Up
Power Over Ethernet Status	Off
Jumbo Frames	
Total Jumbo Frames	0
Input Stats	
5 Minute Input Rate	10064 bits/sec 12 packets/sec
Packets Received (Bytes)	11296 (1659345) bytes
Unicast Packets	4614
Multicast Packets	1700
Broadcast Packets	4982
Input Errors	0
Runts	0
Giants	0
Symbol Errors	0
Discards	2853
Unknown Protocols	0
No Buffers	0
Overruns	0
Internal Receive Errors	0
CRC Errors	0
Alignment Errors	0
Output Stats	
5 Minute Output Rate	8456 bits/sec 3 packets/sec
Packets Transmitted (Bytes)	2369 (630093) bytes
Unicast Packets	2237
Multicast Packets	45
Broadcast Packets	87
Output Errors	0
Deferred Transmission	0
Discards	0
Single Collisions	0
Multiple Collisions	0
Late Collisions	0
Excessive Collisions	0
Underruns	0
Carrier Sense Errors	0
Internal Transmit Errors	0
Resets	0
Throttles	0
L3 Stats	
Packets Received	2142
Packets Forwarded	0
Header Errors	0
Discards	0
Denial of Service (DOS) Stats	
L4 Header Errors	1105
L3 Header Errors	0
ICMP Errors	0
Fragment Errors	0

Refresh in 1 seconds...

Configuring DoS Protection Using the CLI

The following section outlines the procedure for configuring the DoS protection feature using the CLI.

Accessing the DoS Protection Feature in the CLI

The CLI can be accessed by several different methods. A VT100 terminal, a terminal emulation program on a PC, or Telnet can all be used. In order to access any AOS unit, you must know the login information. The IP address of the unit is also required if accessing the unit using Telnet. For more information on connecting to your AOS unit, refer to the quick start guide shipped with your unit. The quick start guide can also be found on the *AOS Documentation* CD shipped with your unit or online at <http://kb.adtran.com>.

All DoS protection commands are entered from the Enable or Global Configuration modes. A password is required to enter the Enable mode.

Show Commands

DoS protection information can be displayed in the CLI using **show** commands. All **show** commands are entered from the Enable mode. To display a categorized list of DoS threats along with their corresponding threat IDs, use the **show dos-id** command. The **show interface** command also includes a section displaying DoS protection statistics for any enabled threat IDs.

Show Command Example

The following example displays a list of DoS threats along with their corresponding threat IDs:

```
>enable
Password:
#show dos-id
DOS L4 Header Error
    TCP pkts w/ control flags and seq# equal to 0           [1]
    TCP pkts w/ SYN and FIN bits set                       [2]
    TCP pkts w/ FIN, URG, PSH bits set with ACK bit & seq# equal to 0 [3]
    TCP pkts w/ source port equal to destination port      [4]
    UDP pkts w/ source port equal to destination port      [5]
    TCP SYN pkts w/ source port 0-1023 for the first fragment [6]

DOS L3 Header Error
    Source IP equal to Destination IP                       [20]

DOS ICMP Error
    Fragmented ICMP pkts                                   [40]
    ICMPV4 ping pkts w/payload greater than specified      [41]
    ICMPV6 ping pkts w/payload greater than specified      [42]

DOS Fragment Error
    TCP fragments w/ offset value set to 1                 [60]
    First TCP fragments w/ TCP header smaller than specified [61]

Source MAC equal Destination MAC                           [100]
```


Configuration Commands

Configuration commands allow the user to enable or disable the DoS protection feature. DoS protection may be enabled or disabled globally, or by specific threat IDs. Warning thresholds may be set for certain DoS attacks as well.

A complete listing of configuration commands can be found in the table *Configuration Commands* on page 10.

Configuration Command Example

The following example enables DoS protection against all available threats except for the Source MAC equal Destination MAC threat (Threat ID 100).

```
>enable
Password:
#config
(config)#dos-protection except 100
(config)#
```

Troubleshooting

No debug commands are currently associated with the DoS protection feature. DoS protection is a hardware-based feature.

To clear attack data collected by the DoS Protection feature, issue the **clear counters** command from the Enable mode.

Command Summary Tables

Configuration Commands

Prompt	Command	Description
(config)#	[no] dos-protection <all except <id(s)> <id(s)>>	Enables or disables DoS protection on all threats or only indicated threats. The all keyword enables protection against all threats. The except keyword enables protection against all threats except the specified threat ID(s). The no form of this command disables all DoS protection.
(config)#	[no] dos-protection max-icmpv4-payload <bytes>	Sets the maximum Internet Control Message Protocol (ICMP) payload size for IPv4 packets. The range is 0 to 16 kB with a default of 512 bytes. A warning will be given if ICMPv4 protection has not been enabled. The no form of this command returns the maximum ICMP payload size for IPv4 packets to the default.
(config)#	[no] dos-protection max-icmpv6-payload <bytes>	Sets the maximum ICMP payload size for IPv6 packets. The range is 0 to 16 kB with a default of 512 bytes. A warning will be given if ICMPv6 protection has not been enabled. The no form of this command returns the maximum ICMP payload size for IPv6 packets to the default.
(config)#	[no] dos-protection min-tcp-header <bytes>	Sets the minimum Transmission Control Protocol (TCP) header size. The range is 0 to 255 bytes with a default of 20 bytes. A warning will be given if TCP protection has not been enabled.

Show Command

Prompt	Command	Description
#	show dos-id	Provides a categorized list of DoS threats and their corresponding threat IDs.