Chapter 28

Denial of Service (DoS) Attack Prevention

Introduction

This chapter describes denial of service (DoS) attacks, how the AlliedWare® operating system defends against DoS attacks, and how to configure defenses against DoS attacks.

About DoS attacks

Denial of service attacks are designed to consume resources so that other users are unable to use the resources and are therefore "denied service". In a computer network environment, the key resources are CPU, memory, and bandwidth.

- By consuming *CPU* resources a DoS attack can prevent a network device from responding to management requests or processing packets, effectively locking up the device.
- By consuming *memory* resources a DoS attack can prevent a network device from processing packets, effectively locking up the device.
- By consuming *bandwidth* resources a DoS attack can reduce the speed and volume of legitimate network traffic.

Protection against DoS attacks is typically configured on edge devices to prevent attacks from entering the aggregation and core layers of the network.

Platform support

The AlliedWare operating system provides protection against DoS attacks on AT-8600 Series switches only.

Most defense mechanisms are implemented in hardware, so you can configure them on all switch ports without affecting switch performance.

Overview of Denial of Service Attacks

This section gives an overview of DoS attacks and how the AlliedWare operating system defends against each type of attack.

The AlliedWare operating system provides protection against the following DoS attacks:

- **IP Options**
- **LAND Attack**
- **Ping of Death Attack**
- **Smurf Attack**
- **SYN Flood Attack**
- **Teardrop Attack**

IP Options

In an IP options attack, the attacker sends packets containing bad IP options to the victim, causing a vulnerable system to freeze or crash as it tries to process the IP options.

Defense mechanism

The defense mechanism monitors the rate, in packets per one second interval, at which IP packets containing IP options are received by a port. An attack is deemed to be in progress when the rate exceeds a pre-defined threshold within a one second time interval. An attack is deemed to be finished when the rate falls below the threshold for a pre-defined time interval.

Response to attacks

When an attack is detected on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS START event trigger is activated, if configured
- the port starts blocking all incoming traffic with IP options

When an attack is finished on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS END event trigger is activated, if configured
- the port stops blocking incoming traffic with IP options

Configuration

You must configure the ports on which the defense is enabled. You can also configure:

- the threshold, in packets per one second interval, at which an attack is deemed to be in progress
- the period of time, in seconds, that must elapse without exceeding the threshold, before an attack is deemed to be finished
- mirroring of all suspect or blocked traffic to a mirror port

The defense mechanism does not examine the IP options field for invalid values, so this defence only identifies a possible attack. It is implemented in the switch ASIC hardware and does not involve the CPU, so you can activate it on as many ports as you want without affecting switch performance.

LAND Attack

In a LAND attack, the attacker sends TCP SYN packets which contain the victim's IP address and an open port as both the source address and destination address. This causes a vulnerable system to go into a loop as it tries to reply to itself.

Defense mechanism

The defense mechanism examines IP packets being received by client and gateway ports.

The device attached to a client port should have an IP address in the local subnet, and be the original source or ultimate destination of IP packets transiting the network. Suspicious packets are incoming packets with a source address that is not in the local subnet.

A gateway port is a port connected directly to a gateway device that is attached to external networks. Apart from a small number of packets from the gateway device itself, all packets arriving at the gateway port should be from other subnets. Suspicious packets are incoming packets with a source IP address that is in the local subnet.

Suspicious packets are blocked and sent to the CPU for checking. An attack is deemed to be in progress when the CPU detects a packet with the same address and port for both the source and destination. An attack is deemed to be finished when no malicious packets have been received for a pre-defined time interval.

Response to attacks

When an attack is detected on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS START event trigger is activated, if configured

When an attack is finished on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS END event trigger is activated, if configured

Regardless of whether or not an attack is in progress, suspicious packets are always blocked because they are invalid.

Configuration

You must configure:

- which ports, if any, are gateway ports
- the ports on which the defense is enabled
- the local subnet address and mask, which is used to determine which IP addresses are local to your network, and which are from other networks

You can also configure:

- the period of time, in seconds, that must elapse without receiving a malicious packet, before an attack is deemed to be finished.
- mirroring of all suspect or blocked traffic to a mirror port

The LAND defense is not CPU intensive, so you can activate it on as many ports as you want without affecting switch performance. We recommend that you enable LAND defense on all client and gateway ports. Do not enable it on ports connected to other devices within your network, such as aggregation devices.

Ping of Death Attack

In a Ping of Death attack, the attacker sends an oversized, fragmented ICMP echo request (ping) packet to the victim. The maximum length of an IP packet, including the header, is 65535 bytes. However, a larger packet can be transmitted if it is fragmented. On a vulnerable system, a buffer overflow can occur when the packet is reassembled, causing the victim to freeze or crash.

Defense mechanism

The defense mechanism sends all fragmented ICMP packets received by a port to the CPU for checking. The CPU checks the size and offset of the last fragment to determine if the packet is oversized. An attack is deemed to be in progress when the first oversized ICMP packet is received. An attack is deemed to be finished when no oversized ICMP packet has been received for a pre-defined time interval.

Response to attacks

When an attack is detected on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS START event trigger is activated, if configured
- the port starts blocking all incoming fragmented ICMP packets

When an attack is finished on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS END event trigger is activated, if configured
- the port stops blocking incoming fragmented ICMP packets

Configuration

You must configure the ports on which the defense is enabled. You can also configure:

- the period of time, in seconds, that must elapse without receiving a malicious packet, before an attack is deemed to be finished
- mirroring of all suspect or blocked fragmented ICMP packets to a mirror port

This defense mechanism requires some involvement by the CPU. This will not impact the forwarding of traffic between switch ports, but it may affect the handling of CPU events, such as the processing of IGMP packets and spanning tree BPDUs. For this reason, we recommend that you limit the use of this defense to ports where an attack is most likely to occur.

Smurf Attack

In a smurf attack, the attacker sends ICMP echo request (ping) packets to an intermediary device. The ICMP packets contain the victim's IP address as the source address and the IP broadcast address of the intermediary device's local network as the destination address. If the intermediary device does not filter ICMP traffic directed to its broadcast address, all the hosts on the intermediary network will receive ICMP echo requests and will reply to the victim's address. This overwhelms the victim with ICMP echo replies and causes severe network congestion.

Defense mechanism

The defense mechanism examines the destination address of all incoming ICMP packets for a broadcast address. An attack is deemed to be in progress when the first ICMP packet is received with a broadcast address as the destination address. An attack is deemed to be finished when no malicious packet has been received for a pre-defined time interval.

Response to attacks

When an attack is detected on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS START event trigger is activated, if configured
- the port starts blocking all incoming ICMP packets that contain a broadcast address as the destination address

When an attack is finished on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS END event trigger is activated, if configured
- the port stops blocking incoming ICMP packets

Configuration

You must configure:

- the ports on which the defense is enabled
- the local subnet address and mask, which is used to determine the IP broadcast address of your network

You can also configure:

- a threshold, in packets per one second interval, at which an attack is deemed to be in progress
- the period of time, in seconds, that must elapse without receiving a malicious packet, or exceeding the threshold if a threshold has been set, before an attack is deemed to be finished
- mirroring of all suspect or blocked ICMP packets to a mirror port

Setting a threshold allows a limited amount of ICMP broadcast traffic through. Many Windows applications use ICMP broadcasts. The default threshold is 0, which means the defense blocks all ICMP broadcast traffic all of the time.

The defense mechanism is implemented in the switch ASIC hardware and does not involve the CPU, so you can activate it on as many ports as you want without affecting switch performance.

SYN Flood Attack

A SYN flood attack exploits the SYN/SYN-ACK/ACK message exchange required to establish a TCP connection. The attacker sends a large number of TCP SYN packets to the victim with source addresses that appear legitimate but which refer to systems that can not or will not respond to SYN-ACK messages. The victim responds with SYN-ACK messages, but does not receive any ACK replies. The TCP connection is never completed and remains half-open. On a vulnerable system, the data structures used to hold pending connections overflow causing the victim to freeze or crash.

Defense mechanism

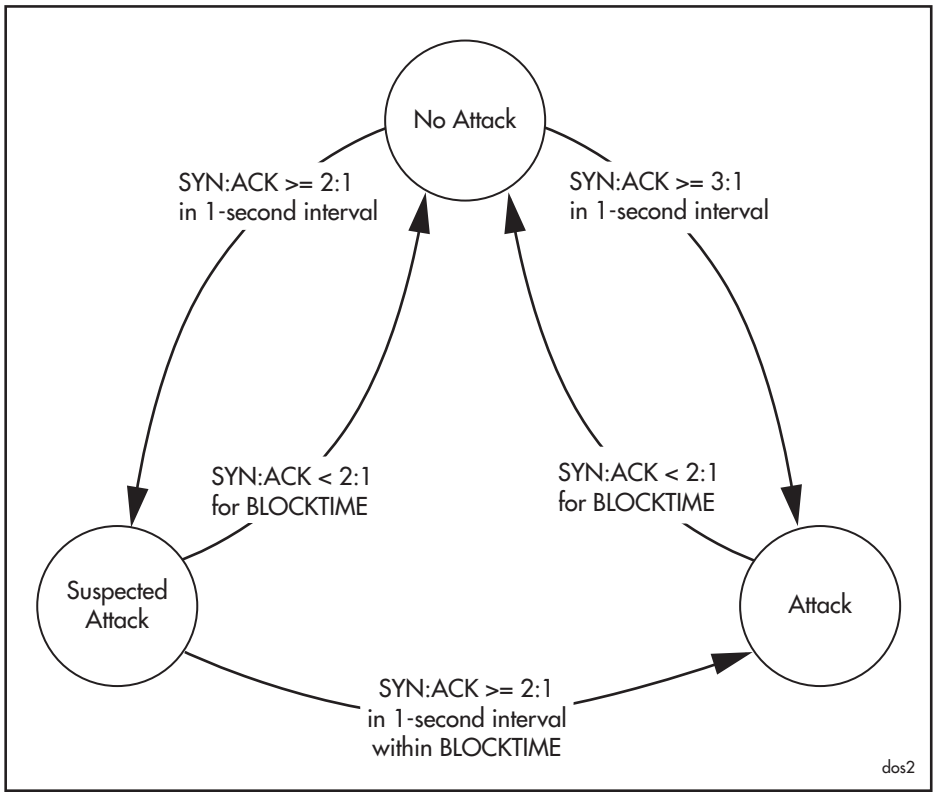
The defense mechanism monitors the number of TCP SYN and ACK messages received by a port.

If you set a threshold, an attack is deemed to be in progress when the number of incoming SYN messages exceeds the number of incoming ACK messages by the threshold within a one second time interval. An attack is deemed to be finished when the difference falls below the threshold for a pre-defined time interval.

If you don't set a threshold, a two step process is used (Figure 28-1). When the rate of incoming SYN messages exceeds 20 packets per one second interval:

- an attack is *suspected* if the ratio of SYN to ACK messages exceeds 2:1 in a one second interval.
- an attack is deemed to be in progress if the ratio of SYN to ACK messages exceeds 3:1 in a one second interval, or if an attack is suspected more than once within a pre-defined time interval
- an attack is deemed to be finished when the ratio of SYN to ACK messages falls below 2:1 in any one second interval for a pre-defined time interval

Figure 28-1: SYN flood attack states



Response to attacks

When an attack is detected on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS START event trigger is activated, if configured
- the port starts blocking all incoming TCP SYN packets
- existing TCP connections are not affected

When an attack is finished on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS END event trigger is activated, if configured
- the port stops blocking incoming TCP SYN packets

Configuration

You must configure the ports on which the defense is enabled. You can also configure:

- the threshold, expressed as the difference between the number of incoming SYN and ACK messages in a one second interval, at which an attack is deemed to be in progress
- the period of time, in seconds, that must elapse without exceeding a SYN:ACK ratio of 2:1, or the threshold if a threshold has been set, before an attack is deemed to be finished
- mirroring of all suspect or blocked traffic to a mirror port

The defense mechanism is implemented in the switch ASIC hardware and does not involve the CPU, so you can activate it on as many ports as you want without affecting switch performance.

Teardrop Attack

In a teardrop attack, the attacker sends a packet to the victim in fragments with overlapping offset values. On a vulnerable system, reassembling the overlapping fragments causes the victim to freeze or crash.

Defense mechanism

The defense mechanism sends all incoming fragmented IP packets to the CPU for checking. The CPU samples the first complete, fragmented IP packet received within a one second time interval. An attack is deemed to be in progress if a fragment is found with an invalid offset value. An attack is deemed to be finished when no malicious packet has been received for a pre-defined time interval.

Because the CPU only examines a sample of the fragmented IP traffic on a port, there is no guarantee that the switch will catch or prevent all occurrences of this attack. The switch will continue to forwarded fragmented traffic until an invalid fragment is detected.

Response to attacks

When an attack is detected on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS START event trigger is activated, if configured
- the port starts blocking all incoming fragmented IP packets

When an attack is finished on a port:

- an SNMP trap is sent to all configured SNMP management stations
- a log message is generated
- a DoS END event trigger is activated, if configured
- the port stops blocking incoming fragmented IP packets

Configuration

You must configure the ports on which the defense is enabled. You can also configure:

- the period of time, in seconds, that must elapse without receiving a malicious packet, before an attack is deemed to be finished
- mirroring of all suspect or blocked fragmented IP packets to a mirror port

This defense is extremely CPU intensive and can affect the handling of CPU events, such as the processing of IGMP packets and spanning tree BPDUs. We recommend that you enable this defense on only one port at a time and where fragments comprise only a small percentage of the total incoming traffic. Also, because the CPU only samples the incoming traffic it will catch some but not necessarily all malicious traffic.

Configuring DoS

This section describes how to configure defenses against DoS attacks. You can configure:

- the same defense on multiple ports
- multiple defenses on the same port
- different settings for different defenses on the same port
- different settings for the same defense on different ports
- mirroring of suspect or blocked traffic to a mirror port for detailed analysis

For information about monitoring and troubleshooting DoS defenses, see "Monitoring and Troubleshooting" on page 28-10.

For an example of a typical configuration setup, see "Configuration Example" on page 28-13.

Enabling and disabling DoS

DoS defense is disabled by default. To enable or disable DoS defense, use the commands:

```
enable dosdefense
```

```
disable dosdefense
```

Clearing a previous configuration

To clear an existing configuration, use the command:

```
purge dosdefense
```

This clears all configuration information, resets all counters to zero, restores all defaults, and disables DoS attack prevention. Use it when you when first configure DoS attack prevention, or when making major changes.

To remove the DoS configuration for some, but not all ports or defenses, use the command:

```
delete dosdefense port={port-list|all}
   DEFense={dos-defense-list|all}
```

Configuring defenses

To configure the threshold, blocking time, and mirroring used by a defense on a port, use the command:

```
set dosdefense port=port-list defense=dos-defense-list
   [blocktime=1..65535] [mirror={on|off}] [threshold=1..1023]
```

Before you enable the LAND or smurf defenses, you must configure the subnet address and mask for each port, using the command:

```
set dosdefense port=port-list defense=dos-defense-list
   ipaddress=ipadd mask=ipadd
```

Before you enable the LAND defense, you must identify any ports that should be treated as gateway ports, using the command:

```
set dosdefense gateway={port-list|none}
```

Enabling and disabling defenses

To enable or disable a defense on a port, use the commands:

```
enable dosdefense port=port-list defense=dos-defense-list
```

```
disable dosdefense port=port-list defense=dos-defense-list
```

Monitoring and Troubleshooting

This section describes how to monitor and troubleshoot defenses against DoS attacks. You can use any of the following techniques:

- **Monitoring** configuration and attack status using the CLI
- **Debugging** attack status and suspect packets using the CLI
- **Mirroring suspect traffic** to a mirror port for detailed analysis
- **Logging** attacks to the Logging Facility
- **SNMP traps**

You can also use **DoS Triggers** for automating responses to attacks — see the next section.

Monitoring

To display general information about DoS defense, including a summary of the defenses enabled on each port, use the command:

```
show dosdefense
```

To display information about the configuration of each DoS defense, use the command:

```
show dosdefense defense={dos-defense-list|all}
```

To display detailed information about the configuration of DoS defenses on a port use the command:

```
show dosdefense port[={port-list|all}]
    [defense=dos-defense-list]
```

To display counters for DoS attacks, use the command:

```
show dosdefense counters
```

You can reset the counters to zero, to make it easier to see changes, using the command:

```
reset dosdefense counters
```

Debugging

You can enable or disable debugging of:

- changes in attack status
- the contents of suspect packets

using the commands:

```
enable dosdefense debug={all|attack|diagnostic|pkt}
    [numpkts={continuous|1..4000000000}]

disable dosdefense debug={all|attack|diagnostic|pkt}
```

Output is sent to the terminal or telnet session from which you entered the command. If you enable packet debugging you should limit the number of packets to debug using the **numpkts** parameter, to prevent large amounts of output making the CLI unresponsive. The default is **continuous**.

For SYN Flood attacks, specifying **pkt** debugging will not produce any output.

Mirroring suspect traffic

You can configure a defense on a port to mirror suspect traffic to a mirror port for detailed analysis, for example using a traffic sniffer.

First, configure a mirror port, using the command:

```
set switch mirror=port
```

Then, configure the defense to mirror suspect traffic to the mirror port, using the command:

```
set dosdefense port=port-list defense=dos-defense-list
   mirror=on
```

When the port is not under attack, suspect traffic examined by the defense mechanism is sent to the mirror port. When an attack is in progress, and the port is blocking traffic, all blocked traffic on the port is mirrored.

You can not configure DoS defenses on a port that has been configured as a mirror port.

Logging

A log message is automatically generated when an attack starts or finishes on a port. Log messages are sent to the Logging facility. To view the log messages, use the command:

```
show log
```

For more information about configuring logging, see Chapter 38, Logging Facility. For example, you can configure the Logging Facility to forward log messages about DoS attacks to an email address.

SNMP traps

A SNMP trap message is automatically generated when an attack starts or finishes on a port. To transmit the trap messages to your NMS, you must enable SNMP and define a trap host, using the commands:

```
enable snmp

create snmp community=name access={read|write} traphost=ipadd
   [manager=prefix[/0..32]]

enable snmp community=name

enable snmp community=name trap
```

For more information about configuring SNMP, see Chapter 32, Simple Network Management Protocol (SNMP).

DoS Triggers

The Trigger Facility automatically runs specific command scripts when particular triggers are activated. When a trigger is activated by an event, parameters specific to the event are passed to the script that is run. For a full description of the Trigger Facility, see Chapter 37, Trigger Facility.

You can configure a trigger that is activated automatically when a DoS attack starts or finishes, using the command:

```
create trigger=trigger-id module=dos event={start|end}
   script=filename [other-trigger-options...]
```

When an attack starts or finishes, the trigger is activated and the script is executed. The script is passed two arguments, the attack type and the port. The script can contain any valid CLI commands. For example, you could use the **mail** command on page 4-22 of Chapter 4, Configuring and Monitoring the System to send an email to a network administrator.

This section describes the following:

- the value you must specify for the **module** parameter (of the **create trigger** command), to identify DoS
- events you can specify in the **event** parameter for DoS
- parameters you can specify as module-specific parameters for DoS
- arguments passed to the script that is activated by the trigger

Module To identify DoS in trigger commands use the parameter **module={dos|143}**.

Event START

Description A DoS attack has started.

Parameters You must specify the **event** and **script** parameters. There are no module-specific parameters for DoS.

Script Arguments The trigger passes the following argument to the script:

Argument	Description
%1	The DoS attack type, listed in uppercase.
%2	The port number.

Event END

Description A DoS attack has finished.

Parameters You must specify the **event** and **script** parameters. There are no module-specific parameters for DoS.

Script Arguments The trigger passes the following argument to the script:

Argument	Description
%1	The DoS attack type, listed in uppercase.
%2	The port number.

Configuration Example

This configuration example shows how to configure defenses against a range of DoS attacks on a edge switch.

In this scenario:

- An AT-8624T/2M 24-port switch is configured as an edge switch, with uplink modules installed in ports 25 and 26.
- Ports 1–22 are attached to client PCs in subnet 192.168.128.0/26.
- Ports 23 and 24 are attached to client PCs in subnet 192.168.192.0/26. The network administrator believes these devices are more likely to be the source of a DoS attack.
- Port 25 connects to an aggregation layer switch.
- Port 26 connects to a gateway router in subnet 192.168.64/26.
- Defenses against IP options, smurf, and SYN flood attacks are enabled on ports 1–24.
- Defenses against LAND attacks are enabled on ports 1–24 and port 26.
- Defense against Ping of Death attacks is enabled on ports 23 and 24.
- Defense against Teardrop attacks is configured but not enabled on ports 23 and 24.
- Log messages are sent to the Logging Facility when an attack starts or finishes.
- An SNMP trap host is defined and enabled to receive SNMP traps when an attack starts or finishes.
- Triggers are created to send an email to the network administrator when an attack starts or finishes.

The configuration is shown is:

- Figure 28-2 on page 28-14—a diagram of the scenario
- Figure 28-3 on page 28-14—the trigger script to execute when a DoS attack starts
- Figure 28-4 on page 28-14—the trigger script to execute when a DoS attack finishes
- Figure 28-5 on page 28-15—the commands to configure the switch

Figure 28-2: Example network for configuring defenses against DoS attacks

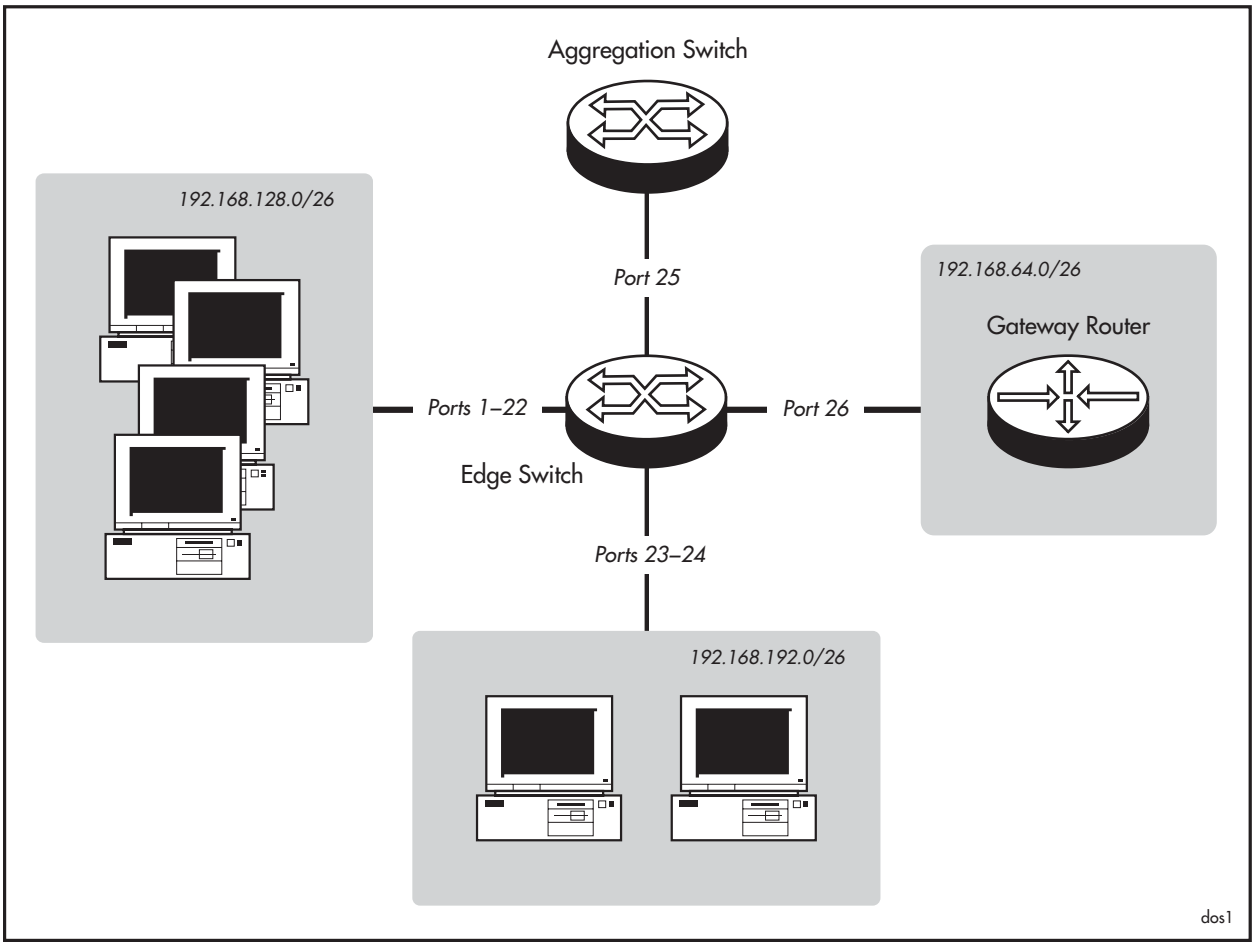


Figure 28-3: Example trigger script to execute when a DoS attack starts

```
#
# atkstart.scp - trigger script executed when a DoS attack starts
#
# %1 - Attack type, uppercase
# %2 - Port under attack
#
mail to=netadmin@mycompany.com mess="%1 attack started on port %2"
  subj="%1 attack started on port %2"
```

Figure 28-4: Example trigger script to execute when a DoS attack finishes

```
#
# atkend.scp - trigger script executed when a DoS attack finishes
#
# %1 - Attack type, uppercase
# %2 - Port under attack
#
mail to=netadmin@mycompany.com mess="%1 attack finished on port %2"
  subj="%1 attack finished on port %2"
```

Figure 28-5: Example script for configuring defenses against DoS attacks

```
# Configure DNS server for MAIL command to look up SMTP server address
add ip dns prim=192.168.1.11

# Enable SNMP
ena sn

# Define a community with a trap host and management statation
cre sn com=private acc=r trap=192.168.1.5 ma=192.168.1.5

# Enable the community and the generation of traps
ena sn com=private
ena sn com=private tr

# Create triggers to respond to DoS attacks
cre trig=1 mod=dos ev=start sc=atkstart.scp
cre trig=2 mod=dos ev=end sc=atkend.scp

# Enable DoS
ena dos

# Clear any previous configuration
purge dos

# Set the gateway port for LAND defense
set dos gate=26

# Set the subnet address and mask required for
# LAND and smurf defenses on ports 1-22
set dos po=1-22 def=land,smur ip=192.168.64.0 mask=255.255.255.192

# Set the subnet address and mask required for
# LAND and smurf defenses on ports 23 and 24
set dos po=23,24 def=land,smur ip=192.168.192.0 mask=255.255.255.192

# Set the subnet address and mask required for
# LAND defense on the gateway port (port 26)
set dos po=26 def=land ip=192.168.64.0 mask=255.255.255.192

# Use default block time, threshold, and mirroring on ports 1-22
# Set lower threshold, longer block time, and mirroring on ports 23, 24
set dos po=22,23 def=ipo thres=30 block=120 mirr=on
set dos po=22,23 def=synf thres=10 block=120 mirr=on
set dos po=22,23 def=smur,ping,tear block=120 mirr=on

# Enable LAND defense on ports 1-24 and 26
ena dos po=1-24,26 def=land

# Enable IP options, smurf, and SYN flood defenses on ports 1 to 24
ena dos po=1-24 def=ipo,smur,synf

# Enable Ping of Death defense on ports 23 and 24
ena dos po=23,24 def=ping

# Check the configuration
sh dos
sh dos def=all
sh dos po=all
sh dos cou
sh sn
sh trig ful
sh ip dns
```

Command Reference

This section describes the commands available on the switch to configure and manage DoS attack prevention.

The shortest valid command is denoted by capital letters in the Syntax section. See "Conventions" on page xxxviii of About this Software Reference in the front of this manual for details of the conventions used to describe command syntax. See Appendix A, Messages for a complete list of error messages and their meanings.

delete dosdefense port

Syntax

```
DELete DOSdefense POrt={port-list}
   DEFense={dos-defense-list}
```

Description

This command deletes the configuration information for a DoS defense from a port. The DoS attack prevention on the switch remains enabled.

Parameter	Description	
POrt	The port to delete the DoS defense from. Port numbers start at 1 and end at *m*, where *m* is the highest numbered port. The *port-list* consists of: a port number a range of ports specified with a hyphen, such as 1-4 a comma-separated list of port numbers and/or ranges Default: no default	
DEFense	The DoS defense to delete from the port. The *dos-defense-list* is a comma-separated list of one or more of the following defenses. Default: no default	
	IPOptions	Defense against IP option attacks.
	LAND	Defense against LAND attacks.
	PINGofdeath	Defense against Ping of Death attacks.
	SMURf	Defense against smurf attacks.
	SYNFlood	Defense against SYN flood attacks.
	TEARdrop	Defense against teardrop attacks.

Examples

To remove protection against IP options and smurf attacks from ports 1 to 24, use the command:

```
del dos po=1-24 def=ipo,smur
```

To remove protection against teardrop attacks from port 5, use the command:

```
del dos po=5 def=tear
```

Related Commands

disable dosdefense
disable dosdefense port
enable dosdefense port
set dosdefense port
show dosdefense
show dosdefense defense
show dosdefense port

disable dosdefense

Syntax

```
DISable DOSdefense
```

Description

This command disables DoS attack prevention. All configuration settings are retained, and are restored when you enable DoS again. DoS attack prevention is disabled by default.

Examples

To disable DoS attack prevention, use the command:

```
dis dos
```

Related Commands

delete dosdefense port
disable dosdefense debug
enable dosdefense
show dosdefense

disable dosdefense debug

Syntax `DISable DOSdefense DEBug={ALL|ATTack|DIAGnostic|PKT}`

Description This command disables debugging of DoS attack prevention.

Parameter	Description	
DEBug	Type of debugging to disable. Default: no default	
	ALL	All debugging options.
	ATTack	Display information about when attacks start and finish.
	DIAGnostic	Display extra diagnostic information.
	PKT	Display a raw hexadecimal dump of the headers of suspect or malicious IP packets, depending on the attack type: For the IP Options defense, all packets with IP options are dumped. For LAND, Ping Of Death, and Teardrop defenses, all packets identified as suspect by the switch hardware are dumped. For the smurf defense, packets identified by the CPU are dumped. For the SYN flood defense, packet debugging is not supported.

Examples To disable all DoS debugging, use the command:

```
dis dos deb=all
```

Related Commands
disable dosdefense
enable dosdefense debug
show dosdefense

disable dosdefense port

Syntax `DISable DOSdefense POrt=`*`port-list`* `DEFense=`*`dos-defense-list`*

Description This command disables protection against different types of DoS attack on individual switch ports.

Parameter	Description	
POrt	The port to disable DoS attack prevention on. Port numbers start at 1 and end at *m*, where *m* is the highest numbered port. The *port-list* consists of: a port number a range of ports specified with a hyphen, such as 1-4 a comma-separated list of port numbers and/or ranges Default: no default	
DEFense	The defense to disable on the port. The *dos-defense-list* is a comma-separated list of one or more of the following defenses. Default: no default	
	IPOptions	Defense against IP option attacks.
	LAND	Defense against LAND attacks.
	PINGofdeath	Defense against Ping of Death attacks.
	SMURf	Defense against smurf attacks.
	SYNFlood	Defense against SYN flood attacks.
	TEARdrop	Defense against teardrop attacks.

Examples To disable protection against IP options and smurf attacks on ports 1 to 24, use the command:

```
dis dos po=1-24 def=ipo,smur
```

To disable protection against teardrop attacks on port 5, use the command:

```
dis dos po=5 def=tear
```

Related Commands

delete dosdefense port
disable dosdefense
disable dosdefense debug
enable dosdefense port
set dosdefense gateway
set dosdefense port
show dosdefense
show dosdefense defense
show dosdefense port

enable dosdefense

Syntax `ENAble DOSdefense`

Description This command enables DoS attack prevention. If DoS attack prevention has previously been enabled and configured, this command will restored the previous configuration. DoS attack prevention is disabled by default.

Examples To enable DoS attack prevention, use the command:

```
ena dos
```

Related Commands **disable dosdefense**
enable dosdefense debug
show dosdefense

enable dosdefense debug

Syntax

```
ENAble DOSdefense DEBug={ALL|ATTack|DIAGnostic|PKT}
   [NUMPKTs={CONTinuous|1..4000000000}]
```

Description

This command enables debugging of DoS attack prevention.

Parameter	Description	
DEBug	Type of debugging to enable. Default: no default	
	ALL	All debugging options.
	ATTack	Display information about when attacks start and finish.
	DIAGnostic	Display extra diagnostic information.
	PKT	Display a raw hexadecimal dump of the headers of suspect or malicious IP packets, depending on the attack type: For the IP Options defense, all packets with IP options are dumped. For LAND, Ping Of Death, and Teardrop defenses, all packets identified as suspect by the switch hardware are dumped. For the smurf defense, packets identified by the CPU are dumped. For the SYN flood defense, packet debugging is not supported.
NUMPKTs	Limits the number of packets displayed by the packet debugging option. Packet debugging may produce large amounts of output in extreme circumstances, preventing you from entering commands and causing the CLI to become unresponsive. We recommend that you use **numpkts** to limit the output whenever you enable packet debugging. Default: **continuous**	
	CONTinuous	No limit. Packet debugging continues until you disable it with the **disable dos debug=pkt** command.
	1..4000000000	Maximum number of packets to be displayed by the packet debugging option. Packet debugging is automatically disabled when this limit is reached.

Examples

To enable all DoS debugging, use the command:

```
ena dos deb=all
```

To enable the debugging of packets and limit the output to 100 packets, use the command:

```
ena dos deb=pkt numpkts=100
```

Related Commands

disable dosdefense debug
enable dosdefense
show dosdefense

enable dosdefense port

Syntax `ENAble DOSdefense POrt=`*`port-list`* `DEFense=`*`dos-defense-list`*

Description This command enables protection against different types of DoS attack on individual switch ports.

You can configure the threshold, blocking time, and mirroring used by each defense on each port using the **set dosdefense port** command on page 28-26.

Parameter	Description	
POrt	The port to enable DoS attack prevention on. Port numbers start at 1 and end at *m*, where *m* is the highest numbered port. You can not enable DoS defenses on a port that has been configured as the mirror port using the **set switch mirror**. The *port-list* consists of: a port number a range of ports specified with a hyphen, such as 1-4 a comma-separated list of port numbers and/or ranges Default: no default	
DEFense	The defense to enable on the port. The *dos-defense-list* is a comma-separated list of one or more of the following defenses. Default: no default	
	IPOptions	Defense against IP option attacks.
	LAND	Defense against LAND attacks. You must identify any gateway ports first, using the **set dosdefense gateway** command on page 28-25. Gateway ports are ports that connect directly to a network gateway device. The LAND defense treats client and gateway ports differently. You must configure the local subnet address and mask first using the **set dosdefense port** command on page 28-26. The subnet address and mask are used to determine which IP addresses are local to your network, and which are from other networks. We recommend enabling LAND defense on all client and gateway ports. Do not enable LAND defense on ports that connect to other devices in your network, such as aggregation devices.
	PINGofdeath	Defense against Ping of Death attacks. This defense mechanism requires some involvement by the CPU. This will not affect the forwarding of traffic between switch ports, but it may affect the handling of CPU events, such as the processing of IGMP packets and spanning tree BPDUs. We recommend that you limit the use of this defense to ports where an attack is most likely to occur.

Parameter	Description	
DEFense (cont.)	SMURf	Defense against smurf attacks. You must configure the local subnet address and mask first using the **set dosdefense port** command on page 28-26. The subnet address and mask are used to determine your network's broadcast address. This defense mechanism does not involve the CPU, so you can activate it on as many ports as you like without affecting switch performance.
	SYNFlood	Defense against SYN flood attacks. This defense mechanism does not involve the CPU, so you can activate it on as many ports as you like without affecting switch performance.
	TEARdrop	Defense against teardrop attacks. The CPU only samples incoming IP traffic on a port, so there is no guarantee that the switch will catch or prevent all occurrences of this attack. This defense is extremely CPU intensive and can affect the handling of CPU events, such as the processing of IGMP packets and spanning tree BPDUs. We recommend that you enable this defense on only one port at a time and where fragments comprise only a small percentage of the total incoming traffic.

Examples

To enable protection against LAND attacks on ports 1 to 24, treating ports 23 and 24 as a gateway ports, and using a local subnet address of 192.168.5.0 and mask of 255.255.255.0, use the commands:

```
set dos gate=23,24
set dos po=1-24 def=land ip=192.168.5.0 mask=255.255.255.0
ena dos po=1-24 def=land
```

To enable protection against IP options and smurf attacks on ports 1 to 24, use the command:

```
ena dos po=1-24 def=ipo,smur
```

To enable protection against teardrop attacks on port 5, use the command:

```
ena dos po=5 def=tear
```

Related Commands

delete dosdefense port
disable dosdefense port
enable dosdefense
enable dosdefense debug
set dosdefense gateway
set dosdefense port
show dosdefense
show dosdefense defense
show dosdefense port

purge dosdefense

Syntax `PURge DOSdefense`

Description This command clears all configuration information for DoS attack prevention, reinitialises all data structures, resets all counters to zero, restores all defenses, and disables DoS attack prevention. It should be used when first configuring DoS attack prevention, or when making major changes.

To remove the configuration for some ports or defenses, use the **delete dosdefense port** command on page 28-16.

Examples To clear the current DoS attack prevention configuration, use the command:

```
pur dos
```

Related Commands
delete dosdefense port
disable dosdefense
enable dosdefense
reset dosdefense counters
show dosdefense

reset dosdefense counters

Syntax `RESET DOSdefense COUnters`

Description This command resets the counters for DoS attack prevention to zero. Use this command when debugging to make it easier to see changes in counter values.

Examples To reset all counters to zero, use the command:

```
reset dos cou
```

Related Commands
disable dosdefense
enable dosdefense
purge dosdefense
show dosdefense

set dosdefense gateway

Syntax `SET DOSdefense GATEway={`*`port-list`*`|NONE}`

Description This command sets the ports that are treated as gateway ports by the LAND defense. You must configure the gateway ports, if any, before enabling defense against LAND attacks.

Parameter	Description	
GATEway	The port to treat as an gateway port. Port numbers start at 1 and end at *m*, where *m* is the highest numbered port. Default: no default	
	port-list	a port number a range of ports specified with a hyphen, such as 1-4 a comma-separated list of port numbers and/or ranges
	NONE	Clears the gateway port. No ports are treated as gateway ports.

Examples To configure ports 23 and 24 as gateway ports for the LAND defense, use the command:

```
set dos gate=23,24
```

To delete the currently configured gateway ports, use the command:

```
set dos gate=none
```

Related Commands

disable dosdefense port
enable dosdefense port
set dosdefense port
show dosdefense
show dosdefense defense
show dosdefense port

set dosdefense port

Syntax

```
SET DOSdefense POrt=port-list DEFense=dos-defense-list
   [BLOCKtime=1..65535] [IPaddress=ipadd] [MASK=ipadd]
   [MIRRor={ON|OFF}] [THREShold=1..1023]
```

Description

This command sets parameters that control the operation of each DoS defense. You can configure different values for different defenses on the same port, or different values for the same defense on different ports.

You must use this command to configure the subnet address and mask before enabling LAND or smurf defense using the **enable dosdefense port** command on page 28-22.

Parameter	Description	
POrt	The port to which these settings apply. Port numbers start at 1 and end at *m*, where *m* is the highest numbered port. You can not configure DoS defenses on a port that has been configured as the mirror port using the **set switch mirror**. The *port-list* consists of: a port number a range of ports specified with a hyphen, such as 1-4 a comma-separated list of port numbers and/or ranges Default: no default	
DEFense	The defense to which these settings apply. The *dos-defense-list* is a comma-separated list of one or more of the following defenses. Default: no default	
	IPOptions	Defense against IP option attacks.
	LAND	Defense against LAND attacks.
	PINGofdeath	Defense against Ping of Death attacks.
	SMURf	Defense against smurf attacks.
	SYNFlood	Defense against SYN flood attacks.
	TEARdrop	Defense against teardrop attacks.
BLOCKtime	The time interval, in seconds, after the last malicious packet is seen before an attack is deemed to be finished. The port will block malicious packets while an attack is in progress. Default: see Table 28-1 on page 28-27	
IPaddress	The subnet address to use for the port. This is required, and only valid, for the LAND and smurf defenses. Default: no default	
MASK	The subnet mask to use for the port. This is required, and only valid, for the LAND and smurf defenses. Default: no default	
MIRRor	Copy suspect traffic to the mirror port for capture and analysis. The mirror port must already be configured using the **set switch mirror** command on page 8-107 of Chapter 8, Switching. Default: **off**	
	ON	Copies suspect traffic to the mirror port.
	OFF	Does not copy suspect traffic to the mirror port.
THREShold	The threshold at which an attack is deemed to be occurring. Default: see Table 28-1 on page 28-27	

Table 28-1: Default thresholds and block times for each DoS defense.

DoS Defence	Default Threshold	Default Block Time
IP Options	60 packets in a one second interval	60 seconds
LAND	n/a	60 seconds
Ping of Death	n/a	60 seconds
Smurf	0 packets per one second interval	60 seconds
SYN Flood	2:1 SYN to ACK ratio above 20 packets per one second interval	60 seconds
Teardrop	n/a	60 seconds

Examples

To set the threshold to 50 packets per one second interval and the blocking time to 2 minutes for the IP options defense on ports 1, 2, 3, 4, and 6, use the command:

```
set dos po=1-4,6 def=ipo thres=50 block=120
```

To configure the LAND defense to use the subnet address 192.168.1.0 and mask 255.255.255.0 on ports 1 to 8, but the subnet address 192.168.5.0 and mask 255.255.255.0 on ports 9 to 16, use the commands:

```
set dos po=1-8 def=land ip=192.168.1.0 mask=255.255.255.0
```

```
set dos po=9-16 def=land ip=192.168.5.0 mask=255.255.255.0
```

Related Commands

delete dosdefense port
disable dosdefense debug
disable dosdefense port
enable dosdefense debug
enable dosdefense port
set dosdefense gateway
show dosdefense
show dosdefense defense
show dosdefense port

show dosdefense

Syntax `SHow DOSdefense`

Description This command displays summary information about DoS attack prevention, and whether or not an attack is under way (Figure 28-6, Table 28-2).

Figure 28-6: Example output from the **show dosdefense** command

```
DoS Configuration
-------------------------------------------------------------
Status ..................... Enabled
Debug enabled .............. Attack, Packet
Debug output limit ........ 100 packets
Gateway port(s) ........... 23,24

DoS Type          State         Ports
-------------------------------------------------------------
-
IP Options        Enabled       5,7
Land              Enabled       1-24
              *** Attack underway on port 17 ***
Ping of Death     Disabled
Smurf             Disabled
SYN Flood         Enabled       2,4,6,8,10,12,14,16,18,20,22
              *** Attack underway on ports 12,14,20 ***
Teardrop          Enabled       24
-------------------------------------------------------------
```

Table 28-2: Parameters in the output of the **show dosdefense** command

Parameter	Meaning
Status	Global state of DoS attack prevention; one of "Enabled" or "Disabled".
Debug enabled	Debug options enabled; either "None" or one or more of "Attack", "Packet" and "Diagnostic".
Debug output limit	Maximum number of packets to be debugged, when packet debugging is enabled, or "None" if there is no limit.
Gateway port(s)	List of ports configured as gateway ports for the LAND defense, or "None" if no gateway ports are configured.
DoS Type	Type of DoS attack.
State	State of defense against the DoS attack type; one of: "Enabled" - the defense is configured, and DoS attack prevention is enabled on the switch "Disabled" - the defense is not configured "Set" - the defense is configured, but DoS attack prevention is disabled on the switch.
Ports	List of ports, if any, on which the defense is enabled.

Examples To display summary information about DoS attack prevention, use the command:

```
sh dos
```

Related Commands

disable dosdefense
disable dosdefense debug
disable dosdefense port
enable dosdefense
enable dosdefense debug
enable dosdefense port
set dosdefense gateway
show dosdefense counters
show dosdefense defense
show dosdefense port

show dosdefense counters

Syntax `SHow DOSdefense COUnters`

Description This command displays counters for DoS attack prevention (Figure 28-7, Table 28-3). The display lists only ports for which at least one DoS defense is currently enabled.

Figure 28-7: Example output from the **show dosdefense counters** command

```
DoS Attack Counters (*=under attack)

Counters last reset 3 days 14:28:11 (311291 seconds) ago

Port    IPOptions   Land    PingOfDeath   Smurf    SYN Flood  Teardrop
-------------------------------------------------------------------------
2           -          0          -          -          -          -
3           -          0          0          -          -          -
16          -          2          -          -          -          -
17*         5*         3          -          -          -          -
18          -          0          -          -          -          -
-------------------------------------------------------------------------
```

Table 28-3: Parameters the output of the **show dosdefense counters** command

Parameter	Meaning
Port	The port number, followed by an asterisk ("*") if an attack is in progress on the port.
IPOptions Land PingOfDeath Smurf SYN Flood Teardrop	For each DoS attack type, either: a hyphen, if defense against the DoS attack type is not enabled on the port, or the number of one second time intervals during which an attack has been detected on the port (if defense against the DoS attack type is enabled on the port) followed by an asterisk ("*") if an attack is in progress on the port

Examples To display DoS counters, use the command:

```
sh dos cou
```

Related Commands

disable dosdefense
disable dosdefense port
enable dosdefense
enable dosdefense port
show dosdefense
show dosdefense defense
show dosdefense port

show dosdefense defense

Syntax `SHow DOSdefense DEFense={`*`dos-defense-list`*`|ALL}`

Description This command displays detailed information about the configuration of DoS defenses (Figure 28-7, Table 28-3 on page 28-30).

Parameter	Description	
DEFense	The defense to display information for. The *dos-defense-list* is a comma-separated list of one or more of the following defenses. Default: no default	
	ALL	All defenses.
	IPOptions	Defense against IP option attacks.
	LAND	Defense against LAND attacks.
	PINGofdeath	Defense against Ping of Death attacks.
	SMURf	Defense against smurf attacks.
	SYNFlood	Defense against SYN flood attacks.
	TEARdrop	Defense against teardrop attacks.

Figure 28-8: Example output from the **show dosdefense defense** command

```
DoS Configuration
-------------------------------------------------------
IP Options:
  State ................ Enabled
  Mirrored Ports ....... None
  Ports ................ 1,5-10,14
  Attack Status ........ *** UNDER ATTACK: ports 7,10

Land:
  State ................ Enabled
  Mirrored Ports ....... None
  Ports ................ 1,5-10,14
  Gateway Ports ........ 14
  Attack Status ........ None

Smurf:
  State ................ Enabled
  Mirrored Ports ....... 5,7
  Ports ................ 1,5-10,14
  Attack Status ........ None

SYN Flood:
  State ................ Enabled
  Mirrored Ports ....... None
  Ports ................ 1,5-10,14
  Attack Status ........ *** SUSPECTED ATTACK: port 8

Teardrop:
  State ................ Enabled
  Mirrored Ports ....... 1
  Ports ................ 1,5-10,14
  Attack Status ........ None
-------------------------------------------------------
```

Table 28-4: Parameters in the output of the **show dosdefense defense** command

Parameter	Meaning
State	State of defense against the DoS attack type; one of: "Enabled" - the defense is configured, and DoS attack prevention is enabled on the switch "Disabled" - the defense is not configured "Set" - the defense is configured, but DoS attack prevention is disabled on the switch.
Mirrored Ports	List of ports for which suspect traffic is copied to the mirror port, or "None" if no ports are being mirrored.
Ports	List of ports on which the defense is enabled or "None" if the defense is not enabled.
Gateway port(s)	List of ports configured as gateway ports for the LAND defense, or "None" if no gateway ports are configured. Displayed only for LAND defense.
Attack Status	Whether or not an attack is in progress; one of "None", "*** SUSPECTED ATTACK", or "*** UNDER ATTACK". If an attack is in progress, the ports under attack are listed.

Examples

To display detailed information about the LAND defense, use the command:

```
show dos def=land
```

To display detailed information about the smurf and SYN flood defenses, use the command:

```
show dos def=smur,synf
```

To display detailed information about all defenses, use the command:

```
show dos def=all
```

Related Commands

disable dosdefense
disable dosdefense port
enable dosdefense
enable dosdefense port
set dosdefense port
set dosdefense gateway
show dosdefense
show dosdefense counters
show dosdefense port

show dosdefense port

Syntax

```
SHow DOSdefense POrt[={port-list|ALL}]
   [DEFense=dos-defense-list]
```

Description

This command displays detailed information about the configuration of DoS attack prevention on switch ports.

Parameter	Description	
POrt	The port to display information about. Port numbers start at 1 and end at *m*, where *m* is the highest numbered port. Default: no default	
	(no value)	Display summary information for every port that has at least one defense enabled (Figure 28-9, Table 28-5 on page 28-34).
	port-list	Display detailed information for each port in *port-list* (Figure 28-10 on page 28-35, Table 28-6 on page 28-36). The *port-list* consists of: a port number a range of ports specified with a hyphen, such as 1-4 a comma-separated list of port numbers and/or ranges
	ALL	Display detailed information for every port (Figure 28-10 on page 28-35, Table 28-6 on page 28-36).
DEFense	Only display information about defenses in *dos-defense-list*. The *dos-defense-list* is a comma-separated list of one or more of the following defenses. Default: no default	
	IPOptions	Defense against IP option attacks.
	LAND	Defense against LAND attacks.
	PINGofdeath	Defense against Ping of Death attacks.
	SMURf	Defense against smurf attacks.
	SYNFlood	Defense against SYN flood attacks.
	TEARdrop	Defense against teardrop attacks.

Figure 28-9: Example summary output from the **show dosdefense port** command

```
DoS Port Configuration

Port   Defenses Enabled (*=under attack)
-------------------------------------------------------------------------------
2      Land
3      Land
4      Land
11     IP Options, Smurf, Ping Of Death
14*    IP Options, Smurf*, SYN Flood*
16     Smurf, Land, Teardrop
-------------------------------------------------------------------------------
```

Table 28-5: Parameters in the summary output of the **show dosdefense port** command

Parameter	Meaning
Port	Port number.
Defenses Enabled	List of defenses enabled on the port; one or more of "IP Options", "Land", "Ping Of Death", "Smurf", "SYN Flood", or "Teardrop".

Figure 28-10: Example detailed output from the **show dosdefense port** command

```
DoS Port Configuration

Port 1:
------------------------------------------------------------
IP Options:
  State ................ Enabled
  Attack Status ........ *** UNDER ATTACK
  Mirrored ............. No
  Threshold ............ 20 packets per second
  Block Time ........... 60 seconds

Land:
  State ................ Enabled
  Attack Status ........ None
  Mirrored ............. No
  Subnet IP ............ 149.11.11.1
  Subnet Mask .......... 0.0.0.63
  Block Time ........... 60 seconds

Ping of Death:
  State ................ Enabled
  Attack Status ........ None
  Mirrored ............. No
  Threshold ............ 0 packets per second
  Block Time ........... 60 seconds

Smurf:
  State ................ Enabled
  Attack Status ........ None
  Mirrored ............. No
  Subnet IP ............ 149.11.11.1
  Subnet Mask .......... 0.0.0.63
  Threshold ............ 0 packets per second
  Block Time ........... 60 seconds

SYN Flood:
  State ................ Enabled
  Attack Status ........ *** SUSPECTED ATTACK
  Mirrored ............. No
  Threshold ............ 60 packets per second
  Block Time ........... 60 seconds

Teardrop:
  State ................ Enabled
  Attack Status ........ None
  Mirrored ............. No
  Block Time ........... 60 seconds
------------------------------------------------------------
```

Table 28-6: Parameters in the detailed output of the **show dosdefense port** command

Parameter	Meaning
State	State of the defense on the port; one of: "Enabled" - the defense is configured, and DoS attack prevention is enabled on the switch "Disabled" - the defense is not configured "Set" - the defense is configured, but DoS attack prevention is disabled on the switch.
Attack Status	Whether or not an attack is in progress on the port; one of "None", "*** SUSPECTED ATTACK", or "*** UNDER ATTACK".
Mirrored	Whether suspect traffic is being mirrored to the mirror port; either "Yes" or "No".
Subnet IP	The local subnet IP address. Displayed only for LAND and smurf defenses.
Subnet Mask	The local subnet mask. Displayed only for LAND and smurf defenses.
Threshold	The threshold at which an attack is deemed to be in progress. This varies with each DoS defense.
Block Time	The time interval, in seconds, after the last malicious packet is seen before an attack is deemed to be finished. The port will block malicious packets while an attack is in progress.

Examples

To display summary DoS port information, use the command:

```
sh dos po
```

To display detailed information about the DoS configuration on port 1, use the command:

```
sh dos po=1
```

To display detailed information about the configuration of the LAND defense on port 1, use the command:

```
show dos po=1 def=land
```

Related Commands

disable dosdefense
disable dosdefense port
enable dosdefense
enable dosdefense port
set dosdefense gateway
set dosdefense port
show dosdefense
show dosdefense counters
show dosdefense defense