Storm Control

This feature module describes the Storm Control feature that helps to monitor the incoming broadcast, multicast, and unknown unicast packets and prevent them from flooding the LAN ports.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Prerequisites for Storm Control

- Cisco IOS Release 15.3(3)S or a later release that supports the Storm Control feature must be installed previously on the Cisco ASR 901 Series Aggregation Services Router.

Restrictions for Storm Control

- The storm-control command is not recommended on an interface that is part of a port channel.

- Storm-control counters are not supported on port channel as the counters are based on physical ports.

- Discarded counters are not displayed for port channel. You should check the port channel member-ports for discarded counters.

- The current rate field is not supported for show commands in hardware based storm control.

- Supports only drop counters. Total broadcast received in storm control is not supported.

Information About Storm Control

A traffic storm occurs when huge amount of broadcast, multicast, or unknown unicast packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation or in the network configuration can also cause a storm. The mechanism to prevent and control such events is known as storm control or broadcast suppression.

The Storm Control feature prevents switchports on a LAN from being disrupted by a broadcast, multicast, or unknown unicast storm on one of the interfaces. This feature monitors incoming traffic statistics over a time period and compares the measurement with a predefined suppression level threshold. The threshold represents the percentage of the total available bandwidth of the port. If the threshold of a traffic type is reached, the system takes the appropriate storm control action until the incoming traffic falls below the threshold level.

Storm control also acts as a policer, and it drops only the storms that breaches the configured storm level.

This feature supports the following:

- Ethernet port: per port configuration for broadcast, multicast, and unknown unicast traffic.

- 10 GigabitEthernet interfaces.

- SNMP trap and SYSLOG messages: indicating storm control detection.

- Individual dropped packet counters: for broadcast, multicast, and unknown unicast flows.

- Error disable recovery feature with storm control shutdown action.

Configuring Storm Control

To configure Storm Control feature, complete the following steps:

Note   This feature is disabled by default.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	**Purpose**
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface gigabitethernet 0/1	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**storm-control {action {shutdown | trap}| {broadcast | multicast | unicast} {level {level | bps bps-level| pps pps-level}}** **Example:** Router(config-if)# storm-control broadcast level 70	Configures broadcast, multicast, or unknown unicast storm control. • **action**—Specifies the action to take when a storm occurs on a port. • **shutdown**—Disables the port during a storm. • **trap**—Sends an SNMP trap. • **broadcast**—Configures broadcast storm control. • **multicast**—Configures multicast storm control. • **unicast**—Configures unknown unicast storm control. • **level**—Specifies the rising threshold level for broadcast, multicast, or unicast traffic as a percentage of the bandwidth. • *level*—Threshold level. The valid range is from 1 to 100 percent. There can also be a fractional part in the level ranging from 0 to 99, which is expressed in percentage. So a level of 49.99 on a GigabitEthernet interface means that once the number of broadcast (or configured type) packets on the interface exceeds 499.90Mbps, all the exceeding packets are dropped. • **bps**—Specifies the suppression level in bits per second. • *bps-level*—Threshold level. • **pps**—Specifies the suppression level in packets per second. • *pps-level*—Threshold level.
Step 5	**end** **Example:** Router(config-if)# end	Exits the interface configuration mode and enters the privileged EXEC mode.

What to do next

Note To disable Storm Control feature, use the no storm-control command.

Verifying Storm Control

To verify the Storm Control feature configuration, use the show command described in the following example.

```
Router# show storm-control broadcast
Interface    Type     Filter State   Level        Current
---------   ------   -------------  -----------  ----------
Gi0/1        Bcast    Forwarding     200 pps      0 pps
Gi0/1        Mcast    Forwarding     300 pps      0 pps
! The "current" field is not supported for storm control.
```

To verify the dropped counters, use the show command described in the following example.

```
Router# show interface gigabitethernet 0/1 counters storm-control
Port   UcastSupp UcastSuppDiscards McastSupp McastSuppDiscards BcastSupp BcastSuppDiscards
        %/ps                        %/ps                        %/ps
Gi0/1  100.00%   0                  20000p    1065163           100.00%   0
```

Configuring Error Disable Recovery

The Cisco ASR 901 router supports error disable recovery for traffic storm control. When a storm is detected, the interfaces configured with the shutdown action of the storm control command are brought down. By default, the error recovery is disabled. You can configure automatic recovery by enabling the error disable recovery at the global configuration level and by setting a time-interval for error recovery.

To configure error disable recovery, complete the following steps:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**errdisable recovery cause storm-control** **Example:**	Configure recovery mechanism and recovery from a specific cause.

	Command or Action	Purpose
	`Router(config)# errdisable recovery cause storm-control`	
Step 4	**errdisable recovery interval** *seconds* **Example:** `Router(config)# errdisable recovery interval 30`	Configures the period to recover from a specified error-disable cause. • *seconds*—Specifies the time to recover from a specified error-disable cause.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and enters the privileged EXEC mode.

Monitoring Error Disable Recovery

To display the information about the error-disable recovery timer, use the show command described in the following example.

```
Router# show errdisable recovery

ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Disabled
lsgroup              Enabled
l2ptguard            Disabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
mac-limit            Disabled
unicast-flood        Disabled
storm-control        Enabled
arp-inspection       Disabled
loopback             Disabled
link-monitor-fail    Disabled
oam-remote-failur    Disabled
oam-remote-failur    Disabled
oam-remote-failur    Disabled
dot1ad-incomp-ety    Disabled
dot1ad-incomp-tun    Disabled
mlacp-minlink        Disabled
Timer interval: 30 seconds
Interfaces that will be enabled at the next timeout:
Interface       Errdisable reason     Time left(sec)
----------      --------------------    --------------
   Gi0/3           storm-control              4
```

Configuration Example for Storm Control

The following is a sample configuration of Storm Control feature on the Cisco ASR 901 router.

```
!
interface GigabitEthernet0/1
no ip address
negotiation auto
storm-control broadcast level pps 200
storm-control multicast level pps 300
storm-control action trap
end
!
```

Troubleshooting Tips for Storm Control

Use the following debug command to enable the debug feature to help in troubleshooting the storm control feature.

```
Router# debug platform hardware ether SC
```

Additional References

The following sections provide references related to Storm Control feature.

Related Documents

Related Topic	Document Title
Cisco IOS Commands	Cisco IOS Master Commands List, All Releases
Cisco ASR 901 Router Commands	Cisco ASR 901 Series Aggregation Services Router Command Reference

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 the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Storm Control

Table 1: Feature Information for Storm Control, on page 7 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 http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Note   Table 1: Feature Information for Storm Control, on page 7 lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 1: Feature Information for Storm Control

Feature Name	Releases	Feature Information
Storm Control	15.3(3)S	This feature was introduced on the Cisco ASR 901 routers. The following section provides information about this feature: