Configuring Storm Control

Information About Storm Control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic broadcast and multicast suppression (or storm control) feature prevents LAN ports from being disrupted by a broadcast, multicast and unicast traffic storm on physical interfaces.

A broadcast 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.

Broadcast and Multicast Suppression monitors incoming traffic levels over a 1-second traffic storm control interval and, during the interval compares the traffic level with the traffic storm control level configured. The traffic storm control threshold level is a percentage of the total available bandwidth of the port. Each port has different storm control levels for broadcast, multicast, and unicast type of traffic.

Storm control uses rising and falling thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets.

- The rising threshold is the traffic limit after which, that particular traffic is blocked.
- The falling threshold is the traffic limit below which, that particular starts forwarding again, if it was already blocked.

Note If a particular type of ingress traffic (unicast, broadcast and multicast) is more than the rising threshold configured on it, the interface goes to blocked state for that particular traffic.

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. Storm control is applicable for physical interfaces and is used to restrict the unicast, broadcast and multicast ingress traffic on the Layer2 interfaces.

Storm control for unicast is a combination of known unicast and unknown unicast traffic. When storm control for unicast is configured, and it exceeds the configured value, the storm will hit each type of traffic through

the hardware policer. The following example describes how the unicast traffic is filtered, when the configured storm is 10%:

- Incoming traffic is unknown unicast 8% + known unicast 7%. Total of 15% storm is not filtered in hardware by the hardware policer.
- Incoming traffic is unknown unicast 11% + known unicast 7%. Total of 18% storm will hit unknown unicast traffic type, and the hardware policer will filter unknown traffic that exceeds 11%.
- Incoming traffic is unknown unicast 11% + known unicast 11%. Total of 22% storm will hit unknown unicast traffic and known unicast traffic, and the hardware policer will filter both unknown and unknown unicast traffic.

Configuring Storm Control

You can set the percentage of total available bandwidth that the controlled traffic can use.

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`	Enter global configuration mode.
Step 3	**interface** *interface-id* **Example:** `Router(config)# interface gigabitethernet 0/1/1`	Enters interface configuration mode.
Step 4	**storm-control** {**broadcast** | **multicast** | **unicast** | **unknown-unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]} **Example:**	Configure broadcast, multicast, unicast or unknown-unicast control. By default, storm control is disabled. • For *level*, specify the rate limit for broadcast, multicast, or unicast traffic as a percentage of the bandwidth. The port suppresses traffic when the rising threshold is reached. For optional *level_low*, specify the low level of the rate limit, as a percentage of the bandwidth. When action SNMP trap is enabled, and the traffic rate exceeds the level then drops below the *level_low*, the port will send out an SNMP trap.

	Command or Action	Purpose
		Note The optional *level-low* will take affect only when storm control SNMP trap is enabled. The minimum acceptable level is 0.01, which means 0.01% of the bandwidth. If level 0 is configured, it will be converted to 0.01 internally. • For bps *bps*, specify the rising threshold level for broadcast, multicast, or unicast traffic in bits per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. (Optional) For *bps-low*, specify the falling threshold level in bits per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is 0.0 to 10000000000.0. • For pps *pps*, specify the rising threshold level for broadcast, multicast, or unicast traffic in packets per second (up to one decimal place). The port blocks traffic when the rising threshold is reached. The range is 0.0 to 10000000000.0. (Optional) For *pps-low* , specifies the falling threshold level in packets per second (up to one decimal place). It can be less than or equal to the rising threshold level. The port forwards traffic when traffic drops below this level. The range is **0.0 to** 10000000000.0. **Note** Do not configure both **storm-control unicast** and **storm-control unknown-unicast** commands on an interface. For BPS and PPS settings, you can use metric suffixes such as k, m, and, g for large number thresholds.

	Command or Action	Purpose
Step 5	**storm-control action** {**shutdown** | **trap**} **Example:** `Router(config-if)# storm-control action trap`	If none of shutdown or SNMP trap is configured, by default the traffic will be suppressed when traffic exceeds the threshold specified by *level*. If *shutdown* is configured, the interface will enter err-disable when traffic exceeds the threshold specified by *level*. If *trap* is configured, the interface will send SNMP trap when traffic exceeds the threshold specified by level. And when traffic drops below the *level_low*, another SNMP trap will be sent out.
Step 6	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.
Step 7	**show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast** | **unknown-unicast**]	Verify the storm control rate limit set on the interface for the specified traffic type.
Step 8	**exit** **Example:** `Router(config)# exit`	Returns the router to global configuration mode.