

Traffic Storm Control

This chapter contains the following sections:

- About Traffic Storm Control, on page 1
- Storm Control Guidelines and Limitations, on page 1
- Configuring a Traffic Storm Control Policy Using the GUI, on page 4
- Configuring a Traffic Storm Control Policy Using the NX-OS Style CLI, on page 5
- Configuring a Storm Control SNMP Trap, on page 7

About Traffic Storm Control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. You can use traffic storm control policies to prevent disruptions on Layer 2 ports by broadcast, unknown multicast, or unknown unicast traffic storms on physical interfaces.

By default, storm control is not enabled in the ACI fabric. ACI bridge domain (BD) Layer 2 unknown unicast flooding is enabled by default within the BD but can be disabled by an administrator. In that case, a storm control policy only applies to broadcast and unknown multicast traffic. If Layer 2 unknown unicast flooding is enabled in a BD, then a storm control policy applies to Layer 2 unknown unicast flooding in addition to broadcast and unknown multicast traffic.

Traffic storm control (also called traffic suppression) allows you to monitor the levels of incoming broadcast, multicast, and unknown unicast traffic over a one second interval. During this interval, the traffic level, which is expressed either as percentage of the total available bandwidth of the port or as the maximum packets per second allowed on the given port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends. An administrator can configure a monitoring policy to raise a fault when a storm control threshold is exceeded.

Storm Control Guidelines and Limitations

Configure traffic storm control levels according to the following guidelines and limitations:

- Typically, a fabric administrator configures storm control in fabric access policies on the following interfaces:
  - A regular trunk interface.

  - A direct port channel on a single leaf switch.
  - A virtual port channel (a port channel on two leaf switches).

- Beginning with release 4.2(1), support is now available for triggering SNMP traps from Cisco Application Centric Infrastructure (ACI) when storm control thresholds are met, with the following restrictions:
  - There are two actions associated with storm control: drop and shutdown. With the shutdown action, interface traps will be raised, but the storm control traps to indicate that the storm is active or clear is not determined by the shutdown action. Storm control traps with the shutdown action on the policy should therefore be ignored.
  - If the ports flap with the storm control policy on, clear and active traps are seen together when the stats are collected. Clear and active traps are typically not seen together, but this is expected behavior in this case.
- For port channels and virtual port channels, the storm control values (packets per second or percentage) apply to all individual members of the port channel.



Note For switch hardware, beginning with Cisco Application Policy Infrastructure Controller (APIC) release 1.3(1) and switch release 11.3(1), for port channel configurations, the traffic suppression on the aggregated port may be up to two times the configured value. The new hardware ports are internally subdivided into these two groups: slice-0 and slice-1. To check the slicing map, use the `vsh_lc` command `show platform internal hal l2 port gpd` and look for `slice 0` or `slice 1` under the `Sl` column. If port channel members fall on both slice-0 and slice-1, allowed storm control traffic may become twice the configured value because the formula is calculated based on each slice.

- When configuring by percentage of available bandwidth, a value of 100 means no traffic storm control and a value of 0.01 suppresses all traffic.
- Due to hardware limitations and the method by which packets of different sizes are counted, the level percentage is an approximation. Depending on the sizes of the frames that make up the incoming traffic, the actual enforced level might differ from the configured level by several percentage points. Packets-per-second (PPS) values are converted to percentage based on 256 bytes.
- Maximum burst is the maximum accumulation of rate that is allowed when no traffic passes. When traffic starts, all the traffic up to the accumulated rate is allowed in the first interval. In subsequent intervals, traffic is allowed only up to the configured rate. The maximum supported is 65535 KB. If the configured rate exceeds this value, it is capped at this value for both PPS and percentage.
- The maximum burst that can be accumulated is 512 MB.
- On an egress leaf switch in optimized multicast flooding (OMF) mode, traffic storm control will not be applied.
- On an egress leaf switch in non-OMF mode, traffic storm control will be applied.
- Storm control does not police spanning tree protocol (STP) and OSPF traffic.
- On a leaf switch for FEX, traffic storm control is not available on host-facing interfaces.

- Traffic storm control unicast/multicast differentiation is not supported on Cisco Nexus C93128TX, C9396PX, C9396TX, C93120TX, C9332PQ, C9372PX, C9372TX, C9372PX-E, or C9372TX-E switches.
- SNMP traps for traffic storm control are not supported on Cisco Nexus C93128TX, C9396PX, C9396TX, C93120TX, C9332PQ, C9372PX, C9372TX, C9372PX-E, C9372TX-E switches.
- Traffic storm control traps is not supported on Cisco Nexus C93128TX, C9396PX, C9396TX, C93120TX, C9332PQ, C9372PX, C9372TX, C9372PX-E, or C9372TX-E switches.
- Storm Control Action is supported only on physical Ethernet interfaces and port channel interfaces.

  Beginning with release 4.1(1), Storm Control **Shutdown** option is supported. When the **shutdown** action is selected for an interface with the default Soak Instance Count, the packets exceeding the threshold are dropped for 3 seconds and the port is shutdown on the 3rd second. The default action is **Drop**. When **Shutdown** action is selected, the user has the option to specify the soaking interval. The default soaking interval is 3 seconds. The configurable range is from 3 to 10 seconds.
- If the data plane policing (DPP) policer that is configured for the interface has a value that is lower than storm policer's value, the DPP policer will take the precedence. The lower value that is configured between the DPP policer and storm policer is honored on the configured interface.
- Beginning with release 4.2(6), the storm policer is enforced for all forwarded control traffic in the leaf switch for the DHCP, ARP, ND, HSRP, PIM, IGMP, and EIGRP protocols regardless of whether the bridge domain is configured for **Flood in BD** or **Flood in Encapsulation**. This behavior change applies only to EX and later leaf switches.
  - With EX switches, you can configure both the supervisor policer and storm policer for one of the protocols. In this case, if a server sends traffic at a rate higher than the configured supervisor policer rate (Control Plane Policing, CoPP), then the storm policer will allow more traffic than what is configured as the storm policer rate. If the incoming traffic rate is equal to or less than supervisor policer rate, then the storm policer will correctly allow the configured storm traffic rate. This behavior is applicable irrespective of the configured supervisor policer and storm policer rates.
  - One side effect of the storm policer now being enforced for all forwarded control traffic in the leaf switch for the specified protocols is that control traffic that gets forwarded in the leaf switch will now get subjected to storm policer drops. In previous releases, no such storm policer drops occur for the protocols that are affected by this behavior change.
- Traffic storm control cannot police multicast traffic in a bridge domain or VRF instance that has PIM enabled.
- When the storm control policer is applied on a port channel interface, the allowed rate may be more than the configured rate. If the member links of the port channel span across multiple slices, then the allowed traffic rate will be equal to the configured rate multiplied by the number of slices across which the member links span.

  The port-to-slice mapping depends on the switch model.

  As an example, assume that there is a port channel that has member links port1, port2, and port3 with a storm policer rate of 10Mbps.
  - If port1, port2, and port3 belong to slice1, then traffic is policed to 10Mbps.
  - If port1 and port2 belong to slice1 and port3 belongs to slice2, then traffic is policed to 20Mbps.
  - If port1 belongs to slice1, port2 belongs to slice2, and port3 belongs to slice3, then traffic is policed to 30Mbps.

Configuring a Traffic Storm Control Policy Using the GUI

Procedure

Step 1 In the menu bar, click **Fabric**.

Step 2 In the submenu bar, click **Access Policies**.

Step 3 In the **Navigation** pane, expand **Policies**.

Step 4 Expand **Interface**.

Step 5 Right-click **Storm Control** and choose **Create Storm Control Interface Policy**.

Step 6 In the **Create Storm Control Interface Policy** dialog box, enter a name for the policy in the **Name** field.

Step 7 In the **Configure Storm Control** field, click the radio button for either **All Types** or **Unicast, Broadcast, Multicast**.

Note
Selecting the **Unicast, Broadcast, Multicast** radio button allows you to configure Storm Control on each traffic type separately.

Step 8 In the **Specify Policy In** field, click the radio button for either **Percentage** or **Packets Per Second**.

Step 9 If you chose **Percentage**, perform the following steps:

a) In the **Rate** field, enter a traffic rate percentage.

Enter a number between 0 and 100 that specifies a percentage of the total available bandwidth of the port. When the ingress traffic is either equal to or greater than this level during a one second interval, traffic storm control drops traffic for the remainder of the interval. A value of 100 means no traffic storm control. A value of 0 suppresses all traffic.

b) In the **Max Burst Rate** field, enter a burst traffic rate percentage.

Enter a number between 0 and 100 that specifies a percentage of the total available bandwidth of the port. When the ingress traffic is equal to or greater than, traffic storm control begins to drop traffic.

Note
The **Max Burst Rate** should be greater than or equal to the value of **Rate**.

Step 10 If you chose **Packets Per Second**, perform the following steps:

a) In the **Rate** field, enter a traffic rate in packets per second.

During this interval, the traffic level, expressed as packets flowing per second through the port, is compared with the traffic storm control level that you configured. When the ingress traffic is equal to or greater than the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

b) In the **Max Burst Rate** field, enter a burst traffic rate in packets per second.

During this interval, the traffic level, expressed as packets flowing per second through the port, is compared with the burst traffic storm control level that you configured. When the ingress traffic is equal to or greater than the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

Step 11 The policy action can be altered from the default by selecting shutdown in the **Storm Control Action** and adjusting the default in **Storm Control Soak Count** fields.

Note
When the **shutdown** action is selected for an interface with the default Soak Instance Count, the packets exceeding the threshold are dropped for 3 seconds and the port is shutdown on the 3rd second.

Step 12 Click **Submit**.

Step 13 Apply the storm control interface policy to an interface port.

a) In the menu bar, click **Fabric**.
b) In the submenu bar, click **Access Policies**.
c) In the **Navigation** pane, expand **Interfaces**.
d) Expand **Leaf Interfaces**.
e) Expand **Policy Groups**.
f) Select **Leaf Policy Groups**.

Note
If your APIC version is earlier than 2.x, you select **Policy Groups**.

g) Select the leaf access port policy group, the PC interface policy group, the vPC interface policy group, or the PC/vPC override policy group to which you want to apply the storm control policy.
h) In the **Work** pane, click the drop down for **Storm Control Interface Policy** and select the created **Traffic Storm Control Policy**.
i) Click **Submit**.

Configuring a Traffic Storm Control Policy Using the NX-OS Style CLI

SUMMARY STEPS

1. Enter the following commands to create a PPS policy:
2. Enter the following commands to create a percent policy:
3. Configure storm control on physical ports, port channels, or virtual port channels:
4. To alter the policy action:
5. Configure the soak-instance count which is applicable for port **Shutdown** action only.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	Enter the following commands to create a PPS policy: **Example:**	

	Command or Action	Purpose
	`(config)# template policy-group pg1` `(config-pol-grp-if)# storm-control pps 10000 burst-rate 10000`	

Step 2	Enter the following commands to create a percent policy:
	Example:
	`(config)# template policy-group pg2`
	`(config-pol-grp-if)# storm-control level 50 burst-rate 60`	

Step 3	Configure storm control on physical ports, port channels, or virtual port channels:
	Example:
	`[no] storm-control [unicast|multicast|broadcast] level <percentage> [burst-rate <percentage>]`
	`[no] storm-control [unicast|multicast|broadcast] pps <packet-per-second> [burst-rate <packet-per-second>]`
	
	`sd-tb2-ifc1# configure terminal`
	
	`sd-tb2-ifc1(config)# leaf 102`
	
	`sd-tb2-ifc1(config-leaf)# interface ethernet 1/19`
	
	`sd-tb2-ifc1(config-leaf-if)# storm-control unicast level 35 burst-rate 45`
	`sd-tb2-ifc1(config-leaf-if)# storm-control broadcast level 36 burst-rate 36`
	`sd-tb2-ifc1(config-leaf-if)# storm-control broadcast level 37 burst-rate 38`
	`sd-tb2-ifc1(config-leaf-if)#`
	
	`sd-tb2-ifc1# configure terminal`
	
	`sd-tb2-ifc1(config)# leaf 102`
	
	`sd-tb2-ifc1(config-leaf)# interface ethernet 1/19`
	
	`sd-tb2-ifc1(config-leaf-if)# storm-control broadcast pps 5000 burst-rate 6000`
	`sd-tb2-ifc1(config-leaf-if)# storm-control unicast pps 7000 burst-rate 7000`
	`sd-tb2-ifc1(config-leaf-if)# storm-control unicast pps 8000 burst-rate 10000`
	`sd-tb2-ifc1(config-leaf-if)#`	

Step 4	To alter the policy action:
	Example:
	`apic1(config-leaf-if)# storm-control action ?`
	`drop drop`
	`shutdown shutdown`	

Step 5	Configure the soak-instance count which is applicable for port **Shutdown** action only. **Example:**	

	Command or Action	Purpose
	apic-ifc1(config-leaf)# int eth 1/27 apic-ifc1(config-leaf-if)# storm-control soak-instance-count ? <3-10> Storm Control SI-Count Instances	

Configuring a Storm Control SNMP Trap

This section describes how to configure a storm control SNMP trap on leaf switches.

You can configure a storm control on SNMP trap using a trap name on the MIB definition. An event on MIB for an interface and when the storm is detected and cleared, a trap is filtered on the same leaf to configure the storm. You can configure the storm in two ways:

- Granular configuration—Sets the type of traffic such as, unicast, multicast and broadcast.
- Non-granular configuration—Sets all types of traffic.

For details on restrictions for triggering the SNMP traps from Cisco ACI when storm control thresholds are met, see Storm Control Guidelines and Limitations, on page 1. For details on Cisco Nexus switches that are not supported on traffic storm control traps, see the guidelines for Storm Control.

Storm Trap

The storm trap will be triggered whenever there is an event and the storm is active or cleared.

```
cpscEventRev1 NOTIFICATION-TYPE
        OBJECTS    { cpscStatus }
        STATUS      current
        DESCRIPTION
```

The implementation sends this notification when a storm event occurs on an interface with respect to a particular traffic type.

The storm status is updated in the fields: `bcDropIncreased`, `uucDropIncreased`, `mcDropIncreased`, and `dropIncreased` for broadcast, unicast, multicast and non-granular traffic types respectively of `dbgIfStorm` MO. The granular and non-granular configurations use flags to set the storm. When a strom is active the flag is set to 1 and when the storm is cleared the flag is set to 2. The following flags generate the events required for the SNMP trap trigger.

```
cat /mit/sys/phys-\[eth--1\]/dbgIfStorm/summary

# Interface Storm Drop Couters
bcDropBytes   :0
bcDropIncreased   :2
childAction    :
dn         :sys/phys-[eth/1]/dbgIfStorm
dropBytes      :0
dropIncreased  :2
mcDropBytes    :0
mcDropIncreased :2
modTs           :never
monPoIDn        :uni/infra/moninfra-default
m               :dbgIfStorm
status          :
uucDropBytes    :0
uucDropIncreased :2
```