Traffic Storm Control

This chapter contains the following sections:

- About Traffic Storm Control, on page 1
- Storm Control Guidelines, on page 1
- Configuring a Traffic Storm Control Policy Using the GUI, on page 2
- Configuring a Traffic Storm Control Policy Using the NX-OS Style CLI, on page 4
- Configuring a Traffic Storm Control Policy Using the REST API, on page 5

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

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).

• 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. Do not configure storm control on interfaces that are members of a port channel.

**Note**

On switch hardware starting with the APIC 1.3(x) and switch 11.3(x) release, 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.

• 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.

### Configuring a Traffic Storm Control Policy Using the GUI

**Procedure**

1. **Step 1**
   In the menu bar, click **Fabric**.
2. **Step 2**
   In the submenu bar, click **External 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 Click Submit.

Step 12 Apply the storm control interface policy to an interface port.

a) In the menu bar, click Fabric.

b) In the submenu bar, click External 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**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | Enter the following commands to create a PPS policy:  
  **Example:**  
  (config)# template policy-group pg1  
  (config-pol-grp-if)# storm-control pps  
  10000 burst-rate 10000 | Purpose |
| 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 | Purpose |
| 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 | Purpose |
### Configuring a Traffic Storm Control Policy Using the REST API

To configure a traffic storm control policy, create a `stormctrl:IfPol` object with the desired properties.

To create a policy named `MyStormPolicy`, send this HTTP POST message:

```
POST https://192.0.20.123/api/mo/uni/infra/stormctrlifp-MyStormPolicy.json
```

In the body of the POST message, include the following JSON payload structure to specify the policy by percentage of available bandwidth:

```json
{"stormctrlIfPol":
  {"attributes":
   {"dn":"uni/infra/stormctrlifp-MyStormPolicy",
    "name":"MyStormPolicy",
    "rate":"75",
    "burstRate":"85",
    "rn":"stormctrlifp-MyStormPolicy",
    "status":"created"
   },
   "children":[]
  }
}
```

In the body of the POST message, include the following JSON payload structure to specify the policy by packets per second:

```json
{"stormctrlIfPol":
  {"attributes":
   {"dn":"uni/infra/stormctrlifp-MyStormPolicy",
    "name":"MyStormPolicy",
    "ratePps":"12000",
    "burstPps":"15000",
    "rn":"stormctrlifp-MyStormPolicy",
    "status":"created"
   },
   "children":[]
  }
}
```
Apply the traffic storm control interface policy to an interface port.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<infraInfra status='created,modified'>
  <infraHPathS name='__ui_l101_eth1--3' status='created,modified'>
    <infraRsPathToAccBaseGrp tDn='uni/infra/funcprof/accportgrp-__ui_l101_eth1--3' status='created,modified'>
    </infraRsPathToAccBaseGrp>
    <infraRsHPathAtt tDn='topology/pod-1/paths-101/pathep-[eth1/3]' status='created,modified'>
    </infraRsHPathAtt>
  </infraHPathS>
  <infraFuncP status='created,modified'>
    <infraAccPortGrp name='__ui_l101_eth1--3' status='created,modified'>
      <infraRsStormctrlIfPol status='created,modified' tnStormctrlIfPolName='__ui_l101_eth1--3'>
      </infraRsStormctrlIfPol>
    </infraAccPortGrp>
  </infraFuncP>
  <stormctrlIfPol status='created,modified' uucRate='11' uucBurstPs='0xffffffff' isUcMcBcStormPktCfgValid='1' name='__ui_l101_eth1--3' uucRatePs='0xffffffff' uucBurstRate='22'>
  </stormctrlIfPol>
</infraInfra>
```