Security Configuration Guide: Storm Control, Cisco IOS XE Everest 3.18SP (Cisco NCS 4200 Series)

First Published: 2016-07-29

Configuring 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.

Prerequisites for Storm Control

- Port-level storm control should be configured on EVC interfaces.
- Storm control threshold value should be configured as CIR (bps, kbps, %).
- Applicable only to broadcast, multicast and unicast packets.

Restrictions for Storm Control

- Storm control is only enabled for ports with EVC configurations.
- Storm control is specific to the Layer2 physical interfaces and port-channels; It is *not* supported on the Layer 3 interfaces or BDI.
- Storm control is supported only for unknown unicast, broadcast, and unknown multicast ingress traffic; It is *not* supported for egress traffic.
- Port-level storm control is supported on the router. EFP-level storm control is *not* supported.
- Strom control on local connect and cross-connect is *not* supported.

Restrictions for RSP3 Module

In addition to the above, the following are applicable on the RSP3 module:

- Storm control on port channel is supported starting Cisco IOS XE Fuji 16.9.3 Release.
- The BPS threshold level is 146kbps.
- The PPS threshold level is 285pps.
- Storm control interface statistics is *not* supported.

- Storm detection does *not* work with jumbo frames.
- Storm control detection is accurate with 5% deviation of configured rate.
- Broadcast storm control is detected even when there is no EFP configured or no matching EFP under interface, and the behavior is due to hardware limitation.

Restrictions for Configuring Storm Control on the RSP3 Module

- Maximum upper threshold value is upto the link capacity, and minimum lower thresholds values are 146Kbps and 285PPS.
- Storm detection is accurate with +/- 5% deviation of the configured value, due to policer resolutions.
- A slight delay may occur while detecting and un-detecting storms, when the thresholds are configured in PPS mode. This is a hardware behavior.
- A delay is observed while detecting a storm in an EFP scaled setup.
- A delay (around 1 minute) is observed while detecting a storm after a soft OIR of the interface module with member-links is performed. This issue is observed after a shutdown that is followed by a no shutdown action is issued on the port-channel.
- TRAP messages may not be displayed on the console, as the console or logging buffers are subjected to interval-based message limiting. This feature suppresses the messages at the same time interval.
- Storm control does not detect the IEEE MAC group (01:80:C2:00:00:0x) in a multicast LACP configuration.
- Storm control does not detect DHCP broadcast packets with DHCP-specific-client or server ports that have high trap strength.
- Only shutdown and traffic type filtered traps are supported.
- Storm control commands do not support the following keywords:

  action-state

  action-status

  current-rate

  falling-threshold

  filter-state

  rising-threshold

  trap-state

  trap-status

  trap-sent

Information on Storm Control

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. The feature is disabled by default on the Cisco ASR 903 router.

Storm Control on Port Channel on the RSP3 Module

Storm control prevents traffic on a LAN from disruptions by a broadcast, multicast, or unicast storm on a port.

Starting with Cisco IOS XE Gibraltar 16.11.1, the RSP3 module supports storm control over port-channel configuration. Storm control over port-channel is applicable on port-channel interfaces, and is used for restricting the unicast, broadcast, and multicast ingress traffic.

Note Storm control is disabled by default on the router.

Configuring Storm Control

Before you begin

Procedure

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 **interface** *interface-id*

Example:

```
Router# interface gigabitethernet 0/0/0
```

Specifies an interface type and enters interface configuration mode.

Step 4 **storm-control broadcast** | **multicast** | **unicast** { **level** { *rising_threshold falling_threshold* | **bps** *rising_threshold falling_threshold* | **pps** *rising_threshold falling_threshold* } }

Example:

```
Router# storm-control broadcast level 1 .50
```

Specifies the global broadcast, multicast, or unicast storm control suppression level as a percentage of total bandwidth.

- **broadcast**—Configure broadcast storm control.
- **multicast**—Configure multicast storm control.
- **unicast**—Configure unknown unicast storm control.
- **level**—Specifies the threshold levels for broadcast, multicast, or unicast traffic.
- *rising_threshold*—Upper threshold level.
- *falling_threshold*—Lower threshold level.
- **bps**—Specifies the suppression level in bits per second.
- **pps**—Specifies the suppression level in packets per second.

Step 5 **storm-control action** {**shutdown** | **trap**}

Example:

```
Router# storm control action trap
```

Specifies the action to take when a storm occurs on a port

- **shutdown**—Disables the port during a storm. The **shutdown** action sets the port to shut state during a storm. The port remains in shutdown state until recovered by giving a **no shutdown** command when the storm goes below the configured lower threshold .
- **trap**—Sends an SNMP trap. The **trap** action generates an SNMP trap when a storm is detected . The default is to restrict the particular ingress traffic and not to send out traps.

Step 6 exit

Example:

```
Router# exit
```

Exits interface configuration mode and returns the router to global configuration mode.

Configuration Example

```
interface GigabitEthernet0/0/1
 no ip address
 negotiation auto
 storm-control broadcast level bps 50k 40k
 storm-control multicast level pps 100 90
 storm-control unicast level 1.00 0.50
service instance 1 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1
!
```

Configuring Storm Control on the Port Channel on the RSP3 Module

```
interface Port-channel1
 mtu 9216
 no ip address
 load-interval 30
 carrier-delay msec 0
 no negotiation auto
 storm-control broadcast level bps 200m 100m
 storm-control multicast level pps 7000 2000
 storm-control unicast level 20 10
 storm-control action trap
 storm-control action shutdown
service instance 2 ethernet
  encapsulation dot1q 2
  rewrite ingress tag pop 1 symmetric
  bridge-domain 2
!
service instance 4000 ethernet
  encapsulation untagged
  l2protocol peer stp lacp
  bridge-domain 4000
 !
!
```

Verifying Storm Control

- Use the **show storm-control** command to verify the Broadcast and Multicast Suppression feature configuration.

  ```
  Router# show storm-control Gi0/15/1

  Interface   Type    Filter State    Upper        Lower        Current
  ---------  ------  -------------  -----------  -----------  ----------
  Gi0/0/0     Bcast    Forwarding     0 pps         0 pps       0 pps
  Gi0/0/0     Ucast    Forwarding     80.00%        20.00%      0.00%
  Gi0/0/1     Bcast    Blocking       50k bps       40k bps     0 bps
  ```

```
Gi0/0/1     Mcast    Blocking       100 pps       90 pps      0 pps
Gi0/0/1     Ucast    Blocking       1.00%         0.50%       0.00%
```

- Use the **show storm-control GigabitEthernet** command to verify the Broadcast and Multicast Suppression feature configuration at the interface.

```
Router # show storm control GigabitEthernet 0/0/1

Interface   Type    Filter State   Upper        Lower        Current
---------  ------   -------------  -----------  -----------  ----------
Gi0/0/1    Bcast    Blocking        50k bps      40k bps     0 bps
Gi0/0/1    Mcast    Blocking        100 pps      90 pps      0 pps
Gi0/0/1    Ucast    Blocking        1.00%         0.50%      0.00%
```

- Use the **show run interface** command to verify the action trap configured on the port.

```
Router# show run interface GigabitEthernet 0/4/2

Building configuration...
Current configuration : 300 bytes
!
interface GigabitEthernet0/4/2
 no ip address
 negotiation auto
storm-control broadcast level 9.00 7.00
 storm-control action trap
 service instance trunk 1 ethernet
  encapsulation dot1q 1-200
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
 !
end
```

- The following example shows the **action trap** being sent when a storm is hit.

```
Router# show storm-control G 0/4/2
Interface   Type   Filter State   Upper        Lower        Current
---------  ------   -------------  -----------  -----------  ----------
Gi0/4/2    Bcast    Blocking         9.00%        7.00%       11.00%
May 29 14:46:28.008 IST: %STORM_CONTROL-3-TRAP: A packet storm was detected on Gi0/4/2.

Sending SNMP trap
```

- The following example shows the **action shutdown** configured.

```
Router# show run interface Gi0/4/2

Building configuration...
Current configuration : 300 bytes
!
interface GigabitEthernet0/4/2
 no ip address
 negotiation auto
storm-control broadcast level 9.00 7.00
 storm-control action shutdown
 service instance trunk 1 ethernet
  encapsulation dot1q 1-200
  rewrite ingress tag pop 1 symmetric
  bridge-domain from-encapsulation
 !
end
```

Verifying Storm Control on Port Channel on the RSP3 Module

Use the show storm-control command to verify the storm control on the router.

```
Router# show storm-control

Key: U - Unicast, B - Broadcast, M - Multicast
Interface  Filter State   Upper        Lower        Current     Action     Type
---------  -------------  -----------  -----------  ----------  ---------  ----
Po1        Link Down        200m bps     100m bps       0 bps  Trap       B
Po1        Link Down        200m bps     100m bps       0 bps  Trap       M
Po1        Link Down        200m bps     100m bps       0 bps  Trap       U
Po2        Blocking           2g bps     500m bps       0 bps  None       B
Po2        Blocking           2g bps     500m bps       0 bps  None       M
Po2        Blocking           2g bps     500m bps       0 bps  None       U
Po48       Link Down        250m bps     100m bps       0 bps  Trap       B
Po48       Link Down        250m bps     100m bps       0 bps  Trap       M
Po48       Link Down        250m bps     100m bps       0 bps  Trap       U

Router# show storm-control

Key: U - Unicast, B - Broadcast, M - Multicast
Interface  Filter State   Upper        Lower        Current     Action     Type
---------  -------------  -----------  -----------  ----------  ---------  ----
Po1        Forwarding       200m bps     100m bps       0 bps  Trap       B
Po1        Forwarding       200m bps     100m bps       0 bps  Trap       M
Po1        Forwarding       200m bps     100m bps       0 bps  Trap       U
Po2        Blocking           2g bps     500m bps       0 bps  None       B
Po2        Blocking           2g bps     500m bps       0 bps  None       M
Po2        Blocking           2g bps     500m bps       0 bps  None       U
Po48       Forwarding       250m bps     100m bps       0 bps  Trap       B
Po48       Forwarding       250m bps     100m bps       0 bps  Trap       M
Po48       Forwarding       250m bps     100m bps       0 bps  Trap       U
```