Implementing Storm Control

This module describes how to configure traffic storm control for Virtual Private LAN Services (VPLS) bridge domains.

Storm Control for VPLS Bridge Domains

Table 1: Feature History Table

Feature Name	Release Information	Feature Description
Storm Control for VPLS Bridge Domains	Release 7.6.3	A traffic storm occurs when packets from broadcast, multicast, or unicast traffic flood Virtual Private LAN Services (VPLS) bridge, creating excessive traffic and degrading network performance. Storm control prevents LAN ports being disrupted by the traffic storm. This feature detects the VPLS bridge disruption and drops the traffic when the number of packets reaches configured threshold levels. You can configure storm control for different types of traffic on a bridge domain under a VPLS bridge. This feature introduces the following command: • **storm-control**

Storm control provides Layer 2 port security under a Virtual Private LAN Services (VPLS) bridge by preventing excess traffic from disrupting the bridge.

A traffic storm occurs when packets flood a VPLS bridge, creating excessive traffic and degrading network performance. Storm control prevents VPLS bridge disruption by suppressing traffic when the number of packets reaches configured threshold levels. You can configure separate threshold levels for different types of traffic on a bridge domain under a VPLS bridge.

Storm control monitors incoming traffic levels on a port or a subinterface, and drops traffic when the number of packets reaches the configured threshold level during any 1-second interval. The 1-second interval is set in the hardware and is not configurable. The number of packets allowed to pass during this interval is configurable, per subinterface, per port, per traffic type. During this interval, the traffic level is compared with

the configured storm control level. When the incoming traffic reaches the storm control level configured on the bridge port, storm control drops traffic until the end of storm control interval. At the beginning of a new interval, traffic of the specified type is allowed to pass on the port. The thresholds are configured using a packets per second (pps) and kilobit per second (kbps) rate.

Supported Traffic Types for Storm Control

On each VPLS bridge port, you can configure up to three storm control thresholds—one for each of the supported traffic types. If you do not configure a threshold for a traffic type, then storm control is not enabled on that port or interface for that traffic type.

The supported traffic types are:

- Broadcast traffic—Packets with a packet destination MAC address equal to FFFF.FFFF.FFFF.
- Multicast traffic—Packets with a packet destination MAC address not equal to the broadcast address, but with the multicast bit set to 1. The multicast bit is bit 0 of the most significant byte of the MAC address.
- Unknown unicast traffic—Packets with a packet destination MAC address not yet learned.

Restrictions for Storm Control

- If you apply storm control to one bridge port, you cannot use storm control on another bridge port or sub-interface under the same main port. If you do so, the system displays an error message, and you'll need to manually disable the configuration on the second bridge port or sub-interface.
- Bridge Protocol Data Unit (BPDU) packets are not filtered through storm control.
- Storm control counters are not supported.
- The storm control policer configurations for the L2VPN Attachment Circuit interface can cause traffic rate deviation from the configured rate in bundle-ether and in pw-ether interface.

Configure Storm Control on Bridge Domain

You can configure storm control on a physical port or on a subinterface. The storm control rates that are configured on a subinterface is applied to all the subinterfaces in the main port.

The thresholds are configured using packets per second (pps) or kilobit per second (kbps) rate.

Configuration Example

1. Create a bridge group with bridge domain.
2. Assign an interface or subinterface to the bridge domain.
3. Configure storm control for the interface or subinterface.

```
Router# configure
Router(config)# l2vpn
Router(config-l2vpn)# bridge group bg0
Router(config-l2vpn-bg)# bridge-domain bd0
Router(config-l2vpn-bg-bd)# interface PW-Ether2001.1
```

```
Router(config-l2vpn-bg-bd-ac)# storm-control unknown-unicast pps 10000
Router(config-l2vpn-bg-bd-ac)# storm-control multicast pps 10000
Router(config-l2vpn-bg-bd-ac)# storm-control broadcast pps 10000
Router(config-l2vpn-bg-bd-ac)# commit
```

Running Configuration

```
configure
 l2vpn
  bridge group bg0
   bridge-domain bd0
    interface PW-Ether2001.1
     storm-control broadcast pps 10000
     storm-control multicast pps 10000
     storm-control broadcast pps 10000
```

Verification

The following example shows a truncated output of storm control values configured for broadcast, multicast, and unknown unicast traffic on the PW-Ether interface.

```
Router# show l2vpn bridge-domain bd-name bd0 detail
Legend: pp = Partially Programmed.
Bridge group: bg0, bridge-domain: bd0, id: 0, state: up, ShgId: 0, MSTi: 0

  ...................

  No status change since creation
  ACs: 1 (0 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of ACs:
    AC: PW-Ether2001.1, state is unresolved
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 131072, Action: none, Notification: syslog
      MAC limit reached: no, threshold: 75%
      MAC port down flush: enabled
      MAC Secure: disabled, Logging: disabled
      Split Horizon Group: none
      E-Tree: Root
      Dynamic ARP Inspection: disabled, Logging: disabled
      IP Source Guard: disabled, Logging: disabled
      DHCPv4 Snooping: disabled
      DHCPv4 Snooping profile: none
      IGMP Snooping: disabled
      IGMP Snooping profile: none
      MLD Snooping profile: none
      Storm Control:
        Broadcast: enabled(10000 pps)
        Multicast: enabled(10000 pps)
        Unknown unicast: enabled(10000 pps)
      Static MAC addresses:
      PD System Data: Learn key: 0
```