Implementing Traffic Storm Control under a VPLS Bridge

Traffic storm control provides Layer 2 port security under a Virtual Private LAN Services (VPLS) bridge by preventing excess traffic from disrupting the bridge. This module describes how to implement traffic storm control.

Traffic storm control can be configured at the bridge domain level. Support has been added to allow storm control rate to be configured in kbps. For more information about the Traffic Storm Control feature, see the *Implementing Traffic Storm Control under a VPLS Bridge* module in the *System Security Configuration Guide for Cisco ASR 9000 Series Routers*. For complete command reference of Traffic Storm Control commands, see the *Traffic Storm Control Commands* chapter in the *System Security Command Reference for Cisco ASR 9000 Series Routers*.

Prerequisites for Implementing Traffic Storm Control

The following prerequisites are required before implementing traffic storm control:

- The network must be configured with a VPLS bridge domain in an MPLS Layer 2 VPN.
- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Restrictions for Implementing Traffic Storm Control

The restrictions for implementing traffic storm control are as follows:

- Traffic storm control must be applied on a bridge domain, or a bridge port and not on a physical port.

- You can configure storm control on both bridge domain level and bridge port level. In this case, the storm control configured on the bridge port level will always take precedence.
- The ASR 9000 Ethernet Line Card does not support BW-based policing in kbps . However, kbps policing configuration is allowed on the ASR 9000 Ethernet Line Card. Then a conversion is performed from kbps to pps with an assumption of 1000 bytes per packet.
- In an ASR 9000 Enhanced Ethernet Line Card, the storm control is configured with mixed units. For example, broadcast policer is configured with pps and multicast policer with kbps. The policing is done in kbps, such that pps configurations are converted into kbps with an assumption of 1000 bytes per packet.

Information About Implementing Traffic Storm Control

To implement traffic storm control, you should understand the following concepts:

Understanding Traffic Storm Control

A traffic storm occurs when packets flood a VPLS bridge, creating excessive traffic and degrading network performance. Traffic 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 each port under a VPLS bridge.

Traffic storm control monitors incoming traffic levels on a port 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 the 1-second interval is configurable, per port, per traffic type. During this interval, it compares the traffic level with the traffic storm control level that the customer configures.

When the incoming traffic reaches the traffic storm control level configured on the bridge port, traffic storm control drops traffic until the end of storm control interval.

Traffic storm control level can be configured separately for these traffic types:

- Broadcast Traffic
- Multicast Traffic
- Unknown Unicast Traffic

The thresholds are configured using a packet-per-second (pps) and kilobit-per-second (kbps) rate. When the number of packets of the specified traffic type reaches the threshold level on a port, the port drops any additional packets of that traffic type for the remainder of the 1-second interval. At the beginning of a new 1-second interval, traffic of the specified type is allowed to pass on the port.

Traffic storm control has little impact on router performance. Packets passing through ports are counted regardless of whether the feature is enabled. Additional counting occurs only for the drop counters, which monitor dropped packets.

No alarms are produced when packets are dropped.

Note

- Bridge Protocol Data Unit (BPDU) packets are not filtered through the storm control feature.
- Tunneled BPDU packets are filtered as they are forwarded into bridge.
- Traffic storm control is applied to only forwarded packets in the system.

Traffic Storm Control Defaults

- The traffic storm control feature is disabled by default. It must be explicitly enabled on each port for each traffic type.
- The traffic storm control monitoring interval is set in the hardware and is not configurable. On Cisco ASR 9000 Series Router, the monitoring interval is always 1 second.

Supported Traffic Types for Traffic 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 traffic 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.

Traffic storm control does not apply to bridge protocol data unit (BPDU) packets. All BPDU packets are processed as if traffic storm control is not configured.

Supported Ports for Traffic Storm Control

In Cisco IOS XR software Release 3.7.0 FCI, you can configure traffic storm control on the following components under a VPLS bridge domain:

- VPLS bridge domain ACs
- VPLS bridge domain access PWs

Traffic Storm Control Thresholds

Traffic storm control thresholds are configured at a packet-per-second rate. A threshold is the number of packets of the specified traffic type that can pass on a port during a 1-second interval. Valid values for traffic storm control thresholds are integers from 1 to 160000. The maximum value would permit about 19 percent of bandwidth to pass per second on a 10-Gbps link, assuming a 1500-byte packet size.

Traffic Storm Control Drop Counters

Traffic storm control counts the number of packets dropped per port and traffic type. The drop counters are cumulative until you explicitly clear them. Use the **show l2vpn bridge-domain detail** and **show l2vpn forwarding detail** commands to see drop counts. Use the **clear l2vpn forwarding counters** command to clear drop counters.

How to Configure Traffic Storm Control

This section describes how to configure traffic storm control:

Enabling Traffic Storm Control on an AC under a Bridge

Perform this task to enable traffic storm control on an AC under a VPLS bridge. The following task shows how to enable traffic storm control on an AC that is a VLAN on an Ethernet interface.

Note To disable traffic storm control, navigate to the submode you were in when you enabled the feature, and issue the **no** form of the command.

SUMMARY STEPS

1. **configure**
2. l2vpn
3. **bridge group** *bridge-group-name*
4. **bridge-domain** *bridge-domain-name*
5. **interface** *interface-name*
6. **storm-control** {**broadcast** | **multicast** | **unknown-unicast**} **pps** *packet-threshold*
7. **commit**
8. **show l2vpn bridge-domain bd-name** *bridge-name* **detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	

Step 2	l2vpn
	Example:
	`RP/0/0/CPU0:router(config)# l2vpn`
	`RP/0/0/CPU0:router(config-l2vpn)#`
		Enters L2 VPN configuration mode.

Step 3	**bridge group** *bridge-group-name* **Example:**	Enters L2 VPN bridge group configuration mode.

	Command or Action	Purpose
	`RP/0/0/CPU0:router(config-l2vpn)# bridge group csco` `RP/0/0/CPU0:router(config-l2vpn-bg)#`	

Step 4	**bridge-domain** *bridge-domain-name*
	Example:
	`RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain abc`
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd)#`
		Enters L2 VPN bridge domain configuration mode.

Step 5	**interface** *interface-name*
	Example:
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd)# interface GigabitEthernet0/1/0/0.100`
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd-ac)#`
		Names an AC under the bridge domain. In this case, the AC is a VLAN on an Ethernet interface.

Step 6	**storm-control** {**broadcast** | **multicast** | **unknown-unicast**} **pps** *packet-threshold*
	Example:
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd-ac)# storm-control broadcast pps 4500`
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd-ac)# storm-control multicast pps 500`
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd-ac)#`
		Enables traffic storm control on this interface for the specified traffic type. Repeat this command for each traffic type.
		The *packet-threshold* is a packet per second rate and must be an integer between 1 and 160000. It specifies the number of packets that will be allowed to pass on the interface for the specified traffic type during a 1-second interval.

Step 7	**commit**	
Step 8	**show l2vpn bridge-domain bd-name** *bridge-name* **detail** **Example:** `RP/0/0/CPU0:router# show l2vpn bridge-domain bd-name abc detail`	Displays storm control configuration.

Enabling Traffic Storm Control on a PW under a Bridge

Perform this task to enable traffic storm control on a pseudowire under a VPLS bridge.

Note To disable traffic storm control, navigate to the submode you were in when you enabled the feature, and issue the **no** form of the command.

SUMMARY STEPS

1. **configure**
2. l2vpn
3. **bridge group** *bridge-group-name*

4. **bridge-domain** *bridge-domain-name*
5. **neighbor** *address* **pw-id** *id*
6. **storm-control** {**broadcast** | **multicast** | **unknown-unicast**} **pps** *packet-threshold*
7. **commit**
8. **show l2vpn bridge-domain bd-name** *bridge-name* **detail**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	

Step 2	l2vpn
	Example:
	`RP/0/0/CPU0:router(config)# l2vpn`
	`RP/0/0/CPU0:router(config-l2vpn)#`
		Enters L2 VPN configuration mode.

Step 3	**bridge group** *bridge-group-name*
	Example:
	`RP/0/0/CPU0:router(config-l2vpn)# bridge group csco`
	`RP/0/0/CPU0:router(config-l2vpn-bg)#`
		Enters L2 VPN bridge group configuration mode.

Step 4	**bridge-domain** *bridge-domain-name*
	Example:
	`RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain abc`
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd)#`
		Enters L2 VPN bridge domain configuration mode.

Step 5	**neighbor** *address* **pw-id** *id*
	Example:
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd)# neighbor 1.1.1.1 pw-id 100`
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd-pw)#`
		Names an access pseudowire under the bridge domain.
		Note You cannot apply storm control on a forwarding PW (a PW under a VFI).

Step 6	**storm-control** {**broadcast** | **multicast** | **unknown-unicast**} **pps** *packet-threshold*
	Example:
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd-pw)# storm-control broadcast pps 4500`
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd-pw)# storm-control multicast pps 500`
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd-pw)#`
		Enables traffic storm control on this pseudowire for the specified traffic type. Repeat this command for each traffic type.
		The *packet-threshold* is a packet per second rate and must be an integer between 1 and 160000. It specifies the number of packets that will be allowed to pass on the interface for the specified traffic type during a 1-second interval.

Step 7	**commit**	

	Command or Action	Purpose
Step 8	**show l2vpn bridge-domain bd-name** *bridge-name* **detail** **Example:** `RP/0/0/CPU0:router# show l2vpn bridge-domain bd-name csco detail`	Displays storm control configuration settings for the named bridge domain. This command also displays the drop counter values for each configured storm control instance.

Enabling Traffic Storm Control on a Bridge Domain

Perform this task to configure traffic storm control on the bridge domain.

Note To disable traffic storm control, navigate to the submode you were in when you enabled the feature, and issue the **no** form of the command.

SUMMARY STEPS

1. **configure**
2. **l2vpn**
3. **bridge group** *bridge-group-name*
4. **bridge-domain** *bridge-domain-name*
5. **storm-control** {**broadcast** | **multicast** | **unknown-unicast**} {**kbps** | **pps**} *value*
6. **commit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure**	

Step 2	**l2vpn**
	Example:
	`RP/0/0/CPU0:router(config)# l2vpn`
	`RP/0/0/CPU0:router(config-l2vpn)#`
		Enters L2 VPN configuration mode.

Step 3	**bridge group** *bridge-group-name*
	Example:
	`RP/0/0/CPU0:router(config-l2vpn)# bridge group csco`
	`RP/0/0/CPU0:router(config-l2vpn-bg)#`
		Creates a bridge group so that it can contain bridge domains and then assigns network interfaces to the bridge domain..

Step 4	**bridge-domain** *bridge-domain-name*
	Example:
	`RP/0/0/CPU0:router(config-l2vpn-bg)# bridge-domain abc`
	`RP/0/0/CPU0:router(config-l2vpn-bg-bd)#`
		Establishes a bridge domain and enters L2VPN bridge group bridge domain configuration mode.

	Command or Action	Purpose
Step 5	**storm-control** {**broadcast** | **multicast** | **unknown-unicast**} {**kbps** | **pps**} *value* **Example:** `RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# storm-control multicast kbps 77 RP/0/0/CPU0:router(config-l2vpn-bg-bd-pw)#`	Configures storm control for broadcast, multicast, or unicast traffic in kilo bits per second (kbps) or as packes per second (pps).
Step 6	**commit**	

Clearing Traffic Storm Control Drop Counters

Perform this task to reset traffic storm control drop counters to zero.

SUMMARY STEPS

1. clear l2vpn forwarding counters

DETAILED STEPS

	Command or Action	Purpose
Step 1	clear l2vpn forwarding counters **Example:** `RP/0/0/CPU0:router# clear l2vpn forwarding counters`	Clears l2vpn forwarding counters, including storm control drop counters.

Configuration Examples for Traffic Storm Control

This section includes the following configuration examples:

Configuring Traffic Storm Control on an AC: Example

The following example shows broadcast and multicast storm control configuration on an AC under a VPLS bridge.

```
RP/0/RSP0/CPU0:router# show run

[lines deleted]

bridge group 215
  bridge-domain 215
   mtu 9000
   interface GigabitEthernet0/1/0/3.215
    storm-control multicast pps 500
    storm-control broadcast pps 4500
   !
[lines deleted]
```

```
RP/0/RSP0/CPU0:router# show l2vpn bridge-domain bd-name 215 detail
Bridge group: 215, bridge-domain: 215, id: 3, state: up, ShgId: 0, MSTi: 0
  MAC learning: enabled
  MAC withdraw: disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4000, Action: none, Notification: syslog
  MAC limit reached: no
  Security: disabled
  Split Horizon Group: none
  DHCPv4 snooping: disabled
  IGMP Snooping profile: none
  Bridge MTU: 9000
  Filter MAC addresses:
  ACs: 2 (2 up), VFIs: 1, PWs: 1 (1 up)
  List of ACs:
    AC: GigabitEthernet0/1/0/3.215, state is up
      Type VLAN; Num Ranges: 1
     vlan ranges: [100, 100]
      MTU 9008; XC ID 0x440005; interworking none; MSTi 0 (unprotected)
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 4000, Action: none, Notification: syslog
      MAC limit reached: no
      Security: disabled
      Split Horizon Group: none
      DHCPv4 snooping: disabled
      IGMP Snooping profile: none

      Storm Control:
       Broadcast: enabled(4500)
       Multicast: enabled(500)
       Unknown unicast: disabled
      Static MAC addresses:
      Statistics:
        packet totals: receive 36728, send 31
        byte totals: receive 2791284, send 2318
        Storm control drop counters:
          packet totals: broadcast 0, multicast 0, unknown unicast 0
          byte totals: broadcast 0, multicast 0, unknown unicast 0
[lines deleted]
```

Configuring Traffic Storm Control on an Access PW: Example

The following example shows broadcast and multicast storm control configuration on an access PW under a VPLS bridge.

```
RP/0/RSP0/CPU0:router# show run
l2vpn
 bridge group bg_storm_pw
  bridge-domain bd_storm_pw
   interface Bundle-Ether101
   !
   neighbor 10.10.30.30 pw-id 1
    storm-control unknown-unicast pps 120
```

```
    storm-control multicast pps 110
    storm-control broadcast pps 100
   !
  !
 !
!

RP/0/RSP0/CPU0:router# show l2vpn bridge-domain group bg_storm_pw detail
Bridge group: bg_storm_pw, bridge-domain: bd_storm_pw, id: 2, state: up, ShgId: 0, MSTi: 0
  MAC learning: enabled
  MAC withdraw: disabled
  Flooding:
    Broadcast & Multicast: enabled
    Unknown unicast: enabled
  MAC aging time: 300 s, Type: inactivity
  MAC limit: 4000, Action: none, Notification: syslog
  MAC limit reached: no
  Security: disabled
  Split Horizon Group: none
  DHCPv4 snooping: disabled
  IGMP Snooping profile: none
  Bridge MTU: 1500
  Filter MAC addresses:
  ACs: 1 (1 up), VFIs: 0, PWs: 1 (1 up)
  List of ACs:
    AC: Bundle-Ether101, state is up
      Type Ethernet
      MTU 1500; XC ID 0xfffc0003; interworking none
      MAC learning: enabled
      Flooding:
        Broadcast & Multicast: enabled
        Unknown unicast: enabled
      MAC aging time: 300 s, Type: inactivity
      MAC limit: 4000, Action: none, Notification: syslog
      MAC limit reached: no
      Security: disabled
      Split Horizon Group: none
      DHCPv4 snooping: disabled
      IGMP Snooping profile: none
      Storm Control: disabled
      Static MAC addresses:
      Statistics:
        packets: received 0, sent 5205
        bytes: received 0, sent 645420
      Storm control drop counters:
        packets: broadcast 0, multicast 0, unknown unicast 0
        bytes: broadcast 0, multicast 0, unknown unicast 0
  List of Access PWs:
    PW: neighbor 10.10.30.30, PW ID 1, state is up ( established )
      PW class not set, XC ID 0xfffc0006
      Encapsulation MPLS, protocol LDP
      PW type Ethernet, control word disabled, interworking none
      PW backup disable delay 0 sec
      Sequencing not set
    PW Status TLV in use
        MPLS         Local                          Remote
        ------------ ------------------------------ ------------------------------
        Label        16001                          16001
        Group ID     0x2                            0x2
        Interface    Access PW                      Access PW
        MTU          1500                           1500
        Control word disabled                       disabled
        PW type      Ethernet                       Ethernet
        VCCV CV type 0x2                            0x2
```

```
               (LSP ping verification)        (LSP ping verification)
  VCCV CC type 0x6                            0x6
               (router alert label)           (router alert label)
               (TTL expiry)                   (TTL expiry)
  ------------ ------------------------------ --------------------------
Incoming Status (PW Status TLV):
  Status code: 0x0 (Up) in Notification message
Outgoing Status (PW Status TLV):
  Status code: 0x0 (Up) in Notification message
Create time: 16/12/2008 00:06:08 (01:00:22 ago)
Last time status changed: 16/12/2008 00:35:02 (00:31:28 ago)
  MAC withdraw message: send 0 receive 0
Static MAC addresses:
Statistics:
  packets: received 0, sent 0
  bytes: received 0, sent 0
Storm control drop counters:
  packets: broadcast 0, multicast 0, unknown unicast 0
  bytes: broadcast 0, multicast 0, unknown unicast 0
MAC learning: enabled
Flooding:
  Broadcast & Multicast: enabled
  Unknown unicast: enabled
MAC aging time: 300 s, Type: inactivity
MAC limit: 4000, Action: none, Notification: syslog
MAC limit reached: no
Security: disabled
Split Horizon Group: none
DHCPv4 snooping: disabled
IGMP Snooping profile: none
Storm Control:
 Broadcast: enabled(100)
 Multicast: enabled(110)
 Unknown unicast: enabled(120)
```

Configuring Traffic Storm Control on the Bridge Domain: Example

This section contains configuration examples for configuring traffic storm control on the bridge domain:

Configuring Storm Control for Broadcast Traffic: Example

This example shows how to configure storm control for broadcast traffic.

```
(config)# l2vpn
(config-l2vpn)# bridge group grp
(config-l2vpn-bg)# bridge-domain bd
(config-l2vpn-bg-bd)# storm-control broadcast kbps 770
(config-l2vpn-bg-bd)# commit
```

Configuring Storm Control for Multicast Traffic: Example

This example shows how to configure storm control for multicast traffic.

```
(config)# l2vpn
(config-l2vpn)# bridge group grp
(config-l2vpn-bg)# bridge-domain bd
(config-l2vpn-bg-bd)# storm-control multicast pps 88
(config-l2vpn-bg-bd)# commit
```

Configuring Storm Control for Unknown-Unicast Traffic: Example

This example shows how to configure storm control for unknown-unicast traffic.

```
(config)# l2vpn
(config-l2vpn)# bridge group grp
(config-l2vpn-bg)# bridge-domain bd
(config-l2vpn-bg-bd)# storm-control unknown-unicast kbps 1280
(config-l2vpn-bg-bd)# commit
```

Additional References

For additional information related to implementing traffic storm control, refer to the following references.

Related Documents

Related Topic	Document Title
MPLS Layer 2 VPNs	*Implementing MPLS Layer 2 VPNs on Cisco ASR 9000 Series Router* module in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*.
MPLS VPLS bridges	*Implementing Virtual Private LAN Services on Cisco ASR 9000 Series Router* module in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*
Getting started material	*Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*

Standards

Standards [1]	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

[1] Not all supported standards are listed.

MIBs

MIBs	MIBs Link
—	To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport