BPDU PROTECTION AND ITS RELEVANCE
Monday, July 4, 2022
2:26 PM

Introduction

This document describes the Edge port, Bridge Protocol Data Unit (BPDU), BPDU protection function, its relevance, and BPDU filter. Pros and cons of using edge port, BPDU filter and BPDU Protection and how to configure BPDU protection along with edge port.

Edge port / Port Fast

User-side devices such as servers, pc, etc. do not need to run STP. If STP is enabled on switch ports connected to these devices, the ports will alternate between Up and Down or cannot enter the Forwarding state immediately after a topology change on the STP network, which is unacceptable for some services. To prevent the preceding problem, configure the ports that do not need to run STP as edge ports. Edge ports can enter the Forwarding state immediately after they go Up. In addition, edge ports do not send TC (Topology Change) BPDUs and therefore do not affect services on the STP network.

An edge port does not participate in spanning tree calculation. The switch automatically configures an edge port as a non-edge port once the edge port receives a configuration BPDU. Then the spanning tree is recalculated.

Use case scenario of edge port

On a Layer 2 network running a spanning tree protocol, a port connected to terminals does not need to participate in spanning tree calculation. If the port participates in spanning tree calculation, the network convergence speed will be affected. In addition, status changes of the port may cause network flapping, interrupting user traffic. To address this problem, you can run the **stp edged-port enable** command to configure the port as an edge port. Then, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability.

PROS and CONS of enabling edge port

PROS	CONS
Workstation behind the edge port will connect to the network without any delay at the time of STP calculation	If edge port is misconfigured globally or in a specific port can cause loop in the network.
	If a port of a switching device receives a BPDU after being configured as an edge port, the switching device will automatically set the port as a non-edge port and recalculate the spanning tree. This is bad because it can cause change in topology

Configuration of Edge Port

1. Configuration of edge port globally

- The **stp edged-port default** command configures the ports on a switching device as edge ports.
- The **undo stp edged-port default** command restores the default setting.

- **NOTE:** After the stp edged-port default command is run on a device, all ports of the device will be become edge ports.

2. Configuration of edge port in a interface.

- The **stp edged-port enable** command sets the current port as an edge port.
- The **stp edged-port disable** command sets the current port as a non-edge port.
- The **undo stp edged-port** command restores the default attribute of an edge port.
- By default, all the ports on the switching device **are non-edge ports**.

- **NOTE:** If a port of a switching device receives a BPDU after being configured as an edge port, the switching device will automatically set the port as a non-edge port and recalculate the spanning tree.

BPDU

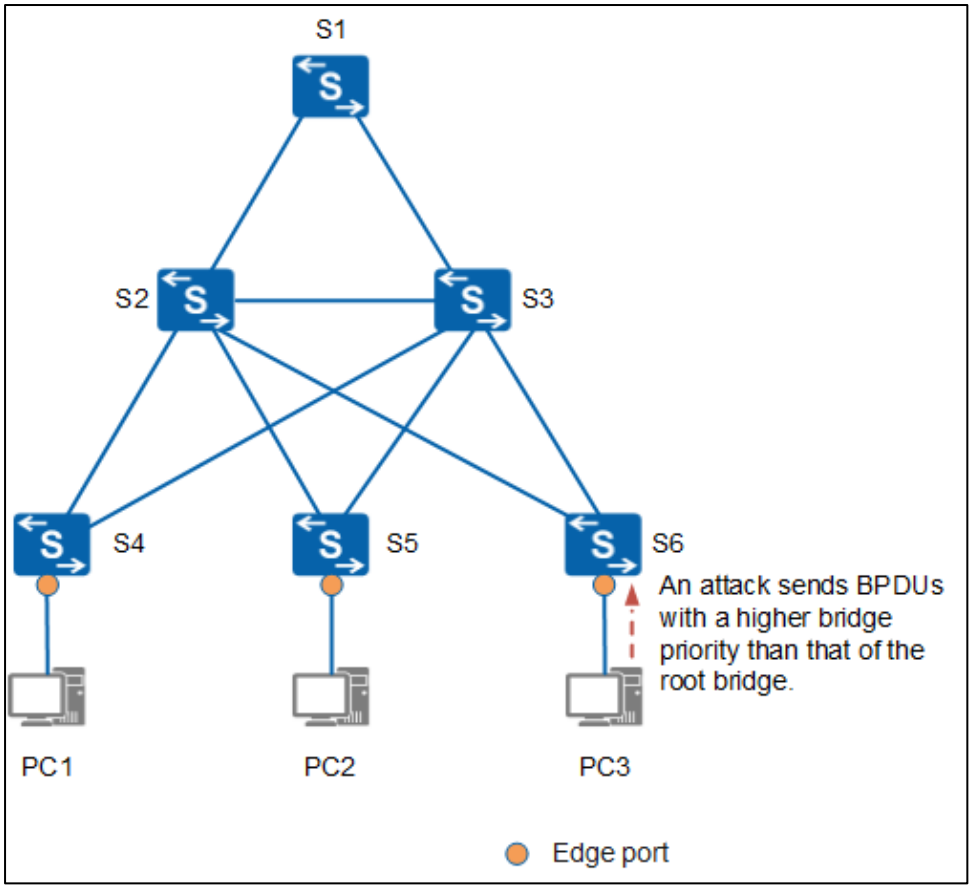
The Spanning Tree Protocol (STP) enabled switches in a redundant Local Area Network (LAN) need to exchange information between each other for Spanning Tree Protocol (STP) to work properly. Bridge Protocol Data Units (BPDUs) are messages, which is transmitted across a local area network to detect loops in network topologies. This message is generated at the time of process of STP.A BPDU contains information regarding ports, switches, port priority and mac addresses.

BPDU PROTECTION

To determine a spanning tree and trim the ring network into a loop-free tree topology, switches running STP, RSTP, MSTP, or VBST exchange BPDUs over a Layer 2 network. Most of the time, while deploying a spanning tree protocol, edge ports are set up to link switches to non-switching devices like user terminals (like PCs) or file servers. Since the spanning tree protocol is not enabled on these ports, they are not included in the spanning tree computation and can go from the Disable state to the Forwarding state instantly. Edge port configuration will stop switches from recalculating the spanning tree topology when user terminals regularly move online and offline, enhancing network reliability.

Best Practices to enable BPDU Guard only on access ports (access ports lead to end user devices) so that any end user devices on these ports that have BPDU Guard enabled are not able to influence the Spanning-tree topology

Relevance and use case scenario of BPDU protection



In the above figure, ports on S4, S5, and S6 connected to PCs are configured as edge ports. Normally, edge ports do not receive BPDUs. If forged BPDUs are sent to attack a device with edge ports and received by them, the device will automatically change the edge ports to non-edge ports and recalculate the spanning tree. If the bridge priority in the BPDUs sent by an attacker is higher than the priority of the root bridge, the network topology will change, thereby interrupting service traffic.

After a switch has activated BPDU protection, the switch will shut down an edge port if it receives a BPDU while maintaining the port attribute. By doing this, it is made sure that the spanning tree topology is not recalculated and that services are not suspended. A notification of this occurrence is sent to the NMS by the switch, which also creates the associated log information:

```
MSTP/4/BPDU_PROTECTION:This edged-port [port-name] that enabled BPDU-Protection will be shutdown, because it received BPDU packet!
```

Pros and Cons of enabling BPDU Protection

PROS	CONS
Bpduguard ensures that if somebody tries to put a L2 device on the network. it is clipped before possible interruption of spanning tree and sends that port to errdisable mode. Hence, there won't be loop in the network	If a switch needs to be plug into an bpdu protection port for whatever reason. Bpdu protection should be disabled in that protection. Because it doesn't participate in STP calculation.
	When the port is in Err Disable State. The switch wont get the mac of that port

Configuration of BPDU

- Run the following command on System-view

```
<Huawei>sy
<Huawei>system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]stp bp
[Huawei]stp bpdu-pr
[Huawei]stp bpdu-protection
[Huawei]
Jul  4 2022 18:43:27-08:00 Huawei DS/4/DATASYNC_CFGCHANGE:OID 1.3.6.1.4.1.2011
.25.191.3.1 configurations have been changed. The current change number is 4,
e change loop count is 0, and the maximum number of records is 4095.0000
        ^
```

- Run display stp in any view to check BPDU PROTECTION

```
<Huawei>display stp
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge          :32768.4c1f-cc87-69e9
Config Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times         :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC       :32768.4c1f-cc87-69e9 / 0
CIST RegRoot/IRPC    :32768.4c1f-cc87-69e9 / 0
CIST RootPortId      :0.0
BPDU-Protection      :Enabled
TC or TCN received   :1
TC count per hello   :0
STP Converge Mode    :Normal
Time since last TC   :0 days 0h:4m:52s
Number of TC         :1
Last TC occurred     :GigabitEthernet0/0/1
```

- **Note:** After bpdu-protection command is enabled. Then its protection is applied to only edge port .
- After BPDU protection is configured, either of the following methods to restore edge ports to the up state:
    - Manually recover an edge port that is shut down after receiving BPDUs.Run the restart or undo shutdown command in the interface view.
    - Enable automatic recovery before any edge port receives BPDUs.
    - Run the error-down auto-recovery cause bpdu-protection interval interval-value command to enable delayed automatic recovery to prevent ports from being stuck in the disabled state.
    - After automatic recovery is configured, an edge port will enter the error-down state after receiving BPDUs and will be restored to the up state after the delay specified by interval-value. A smaller interval-value value indicates a shorter delay for a port to automatically go up and a higher flapping frequency. A larger interval-value value indicates a longer delay for an edge port to automatically go up and a longer traffic interruption.

BPDU FILTER

BPDUfilter on the other hand just filters BPDUs in both directions, which effectively disables STP on the port .Bpdu filter will prevent inbound and outbound bpdu but will remove portfast state on a port if a bpdu is received. Enabling BPDU filtering on an interface is the same as
disabling spanning tree on it and can result in spanning-tree loops.

Use case scenario of BPDU Filter

In an office environment where someone needs another network drop under their desk but you don't have time/budget to run a new line for now. you are been given a small switch but don't want it to break spanning tree. The switch you have lying around for this task is a simple unmanaged switch and will only have one uplink into your network. So on the new switch make sure to enable BPDU filter on the uplink port which will prevent any BPDU's from passing through the interface. This will keep the new switch from causing a BPDU guard error on the existing switch

Pros and Cons of BPDU filter.

PRO	CONS
STP operations can be runned on selected ports of the switch rather than every port of the switch at a time.	If a BPDU is received on edgeport enabled. It changes edgeport to forwarding state and bpdu filter is disabled. Hence it can change Network topology.
Ports that connect to servers and workstations can be configured to remain outside of spanning tree operations.	

Difference between BPDU Protection and BPDU Filter.

Suppose you have a switch with servers connected to it. There is no need to go through all spannig-tree states on these host-facing ports. So, you make port transition with "stp edge port" interface command. One of the benefits is that if your server boots fast, it does not need to wait until port finishes going through all STP port states and can start transmitting data immediately.
Since servers normally should ignore BPDUs coming from a switch, there is no need to send them to a server in the first place. To filter out outgoing BPDUs apply interface command "stp bpdufilter enable".

But when BPDU is received on the port with bpdufilter enabled, the port's portfast status is disabled and port will participate in spanning-tree.

At all times network needs to be protected from unauthorized device that might decide to participate in your spanning-tree topology and cause spanning-tree loop or try to hijack STP root. Command "stp bpdu-protection enable" puts interface in err-disable mode whenever BPDU is received from connected device.

BPDU Protection	BPDU Filter
Prevents accidental connection of switching devices to edgeport-enabled ports.	Restricts the switch from sending unnecessary BPDUs out access ports.
If a BPDU is received on edgeport enabled. It changes edgeport to shutdown state	If a BPDU is received on edgeport enabled. It changes edgeport to forwarding state and bpdu filter is disabled. Hence it can change Network topology.

What happens when both BPDU protection and BPDU Filter is enabled in an interface?

- BPDU Filter takes precedence and BPDU protection doesn't work

Configuration of BPDU filter

Configuration of BPDU Filter globally.

- The stp bpdu-filter default command specifies all ports of a device as BPDU-filter ports.
- The undo stp bpdu-filter default command specifies all ports of a device as non-BPDU-filter ports.
- **By default, a port is a non-BPDU-filter port**

Configuration of BPDU Filter in an interface level.

- The stp bpdu-filter enable command specifies a port as a BPDU-filter port.
- The stp bpdu-filter disable command specifies a port as a non-BPDU-filter port.
- The undo stp bpdu-filter command restores the default attribute of a BPDU-filter port.
- **By default, a port is a non-BPDU-filter port**