Introduction

This document describes the Bridge Protocol Data Unit (BPDU), BPDU protection function, its relevance and how to configure BPDU protection.

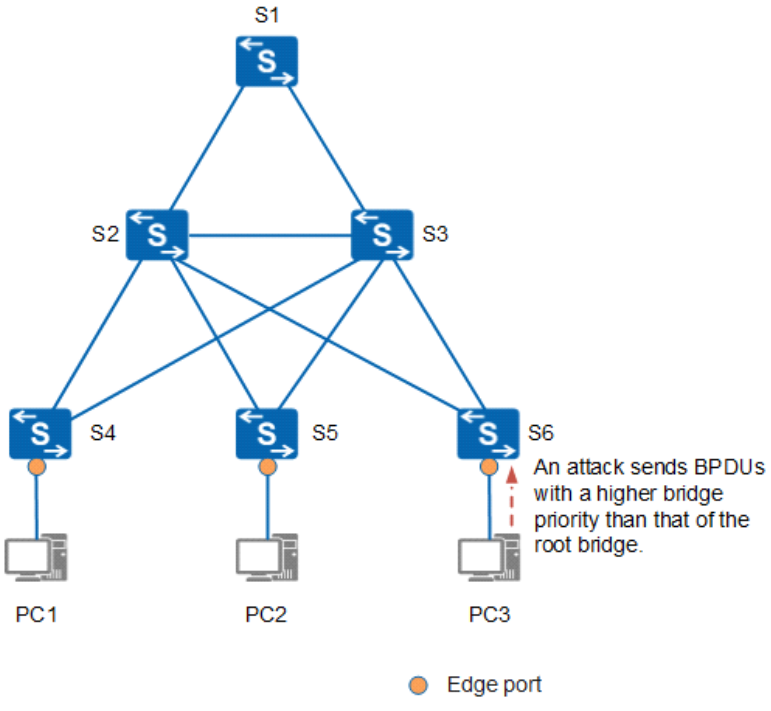
BPDU

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.

Relevance of BPDU



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!
```

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
```