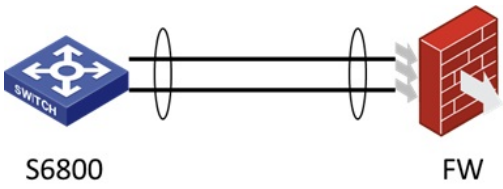
某局点S6800 在某个聚合全部成员口配置bpdu-drop any后导致业务全部中断问题案例

二层链路聚合 STP LLDP 张文宁 2020-04-15 发表

组网及说明

拓扑:如下现场使用S6800跟FW对接，二者使用两根线进行二层动态链路聚合，其中S6800开启了生成树。



问题描述

问题：原本业务一切正常，但是客户为了防止S6800从FW侧收到STP的BPDU攻击，因此在S6800连FW的两个成员口均配置了BPDU拦截功能（bpdu-drop any），发现配置后业务全部中断了。

过程分析

分析：

登录S6800查看日志发现成员接口inactive了：

%Jan 1 12:23:33:418 2013 H3C LAGG/6/LAGG_INACTIVE_PARTNER: Member port GE1/0/10 of aggregation group BAGG1 changed to the inactive state, because the aggregation configuration of its peer port is incorrect.

%Jan 1 12:23:33:422 2013 H3C IFNET/5/LINK_UPDOWN: Line protocol on the interface GigabitEthernet1/0/10 is down.

进一步查看聚合状态发现只剩个参考端口是强制选中状态，而查看对端FW则是两个都是非选中状态：

```
[H3C]dis link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Port Status: S -- Selected, U -- Unselected,
             I -- Individual, * -- Management port
Flags:  A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregate Interface: Bridge-Aggregation1
Aggregation Mode: Dynamic
Loadsharing Type: Shar
Management VLAN : None
System ID: 0x8000, 84d9-31ce-a901
Local:
  Port            Status  Priority Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/0/9         S       32768    1         {ACDEFG}
  GE1/0/10        U       32768    1         {ACG}
Remote:
  Actor           Partner Priority Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/0/9         0       32768    0         0x8000, 0000-0000-0000 {DEF}
  GE1/0/10        0       32768    0         0x8000, 0000-0000-0000 {DEF}
```

因此怀疑该命令将lacp报文也拦截了，开启debug link-aggregation lacp all interface xx发现确实两边没有了lacp的报文交互了，只有单向交互。

根据手册介绍，理解应该是只会拦截stp的bpdu报文：

7. 配置BPDU拦截功能

在开启了生成树协议的网络中，由于设备收到BPDU后会进行STP计算并向其他设备转发，因此恶意用户可借此进行BPDU攻击：通过不停地发送BPDU，使网络中的所有设备都不停地进行STP计算，从而导致设备的CPU占用率过高或BPDU的协议状态错误等问题。

为了避免这种情况，用户可以在端口上配置BPDU拦截功能。开启了该功能的端口将不再接收任何BPDU，从而能够防止设备遭受BPDU攻击，保证STP计算的正确性。

表1-47 配置BPDU拦截功能

操作	命令	说明
进入系统视图	system-view	-
进入二层以太网接口视图	interface interface-type interface-number	-
开启端口的BPDU拦截功能	bpdu-drop any	缺省情况下，端口的BPDU拦截功能处于关闭状态

而且协议类的配置，不应该影响聚合口的选中状态：
协议类配置：是相对于属性类配置而言的，包含的配置内容有MAC地址学习、生成树等。在聚合组中，即使某成员端口与对应聚合接口的协议配置存在不同，也不会影响该成员端口成为选中端口。

最终和后台确认，官网资料写的有歧义，bpdu-drop any指的是拦截所有的二层协议的报文，包括了lldp和lacp和stp这些报文。后续官网资料会更新修改。

定位结论：
bpdu-drop any命令不是只丢弃STP报文，而是二层协议报文（包括LLDP,LACP），资料有歧义，后续会更新改正。

解决方法

解决方法：
1. 去除该命令，换成undo stp enable可以关闭这个接口处理stp报文。
2. 已提需求后续开发bpdu-drop stp功能来单独拦截stp的bpdu报文。（需求电子流单号202004152193）