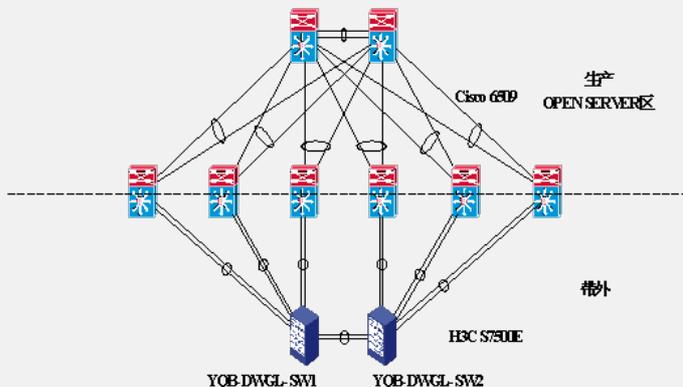


思科交换机出现强制Err-disable引起的全网中断的案例

一、组网：



用户网络分为带外网管和生产网两张网络，其中带外网管网络的网关是两台7500E交换机，下联思科的6509交换机作为二层设备，两张网络通过访问控制进行物理业务隔离。

两台7500E交换机配置了VRRP协议用于网关冗余，下联的思科6509交换机采用链路聚合将两根千兆链路捆绑后上行，全网为了避免环路，开启了STP协议，根桥在生产网最上端的6509交换机上

二、问题描述：

用户网络在运行过程中，出现突发的网络中断，7500E交换机中的SW2出现频繁的端口UP/Down，现场工程师检查思科交换机发现光模块没有发光，同时查看到思科6509交换机上有如下日志告警，继而上游思科多台设备同时将两台S7500E交换机互链路端口强制Down掉，最终导致业务彻底中断。

```
049364: Aug 23 15:10:48.281 Beijing: %PM-SP-4-ERR_DISABLE: channel-misconfig error detected on Po2, putting Gi7/2 in err-disable state
```

```
049365: Aug 23 15:10:48.309 Beijing: %EC-SP-5-UNBUNDLE: Interface GigabitEthernet net7/2 left the port-channel Port-channel2
```

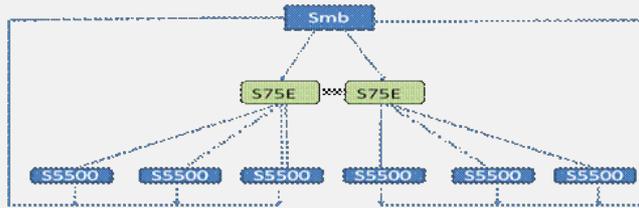
```
049366: Aug 23 15:10:48.313 Beijing: %PM-SP-4-ERR_DISABLE: channel-misconfig error detected on Po2, putting Gi8/2 in err-disable state
```

```
049367: Aug 23 15:10:48.313 Beijing: %PM-SP-4-ERR_DISABLE: channel-misconfig error detected on Po2, putting Po2 in err-disable state
```

三、过程分析：

- 1, 根据故障现象，我们首先怀疑光模块可能存在问题，将存在UP/Down的端口光模块返回我司进行分析，但经过实验室测试，证明除一个光模块发送光功率出现问题外，其他光模块没有问题。但正常情况下，一个光口故障不会导致全网其他交换机之间互通存在问题，而且用户设备之间已经配置链路聚合和端口自协商，这两个协议的本质就是对链路的单点故障进行全面的保护，所以即使出现单个光模块故障，按理不可能对网络有任何的实质影响，所以问题的焦点是为何单点失效引起整网的故障，并且可以判定光模块存在问题，但不是全网中断的根本原因。
- 2, 据此，我们对比所有交换机的log日志，我们将用户网络出现问题的现象和特点整理如下：
 - 1)首先单个S75E端口出现down/up。
 - 2)思科多台设备上几乎同时上报端口异常，提示“channel-misconfig error detected”。随之出现主动端口down。是思科设备的ERR-DETECT功能导致。
 - 3) 手动聚合的聚合端口也出现该错误并报down。
 - 4) 故障时两台S75E上的友商设备均有部分设备报错误并主动down。
 - 5) S7500E交换机上端口的报文统计看，未见明显的广播和多播流量。也即是没有形成长时间的网络环路，否则端口上应该有较为明显的额广播和多播统计。

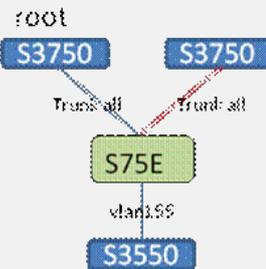
- 6) S7500E交换机上没有启动任何能影响网络运行的协议，芯片上均为没有任何明显的丢包记录。软件运行状态也正常。
- 3, 根据以上现象，很难解释清楚故障原因，因此我们在实验室搭建了测试环境，用以模拟用户现网情况
- 1) 测试网络拓扑



- 2) 模拟光模块故障端口由于瞬间故障导致单通。在实验室通过debug命令强行让S75E端UP,S5500端芯片逻辑端口Down。测试发现S75E设备上lACP上报无法收到lACP报文而解聚合，其它设备均正常工作。其它交换机上流量并未中断。
- 3) 模拟光模块故障端口由于瞬间定位故障导致环路。在实验室通过debug命令强行解开S75E一端聚合。测试发现第三台S5500设备上STP回上报告警，聚合端口block掉，其它设备均正常工作。
- 4) 模拟光模块故障端口频繁快速down/up。在实验室通过给设备使用debug版本模拟端口频繁down/up。测试发现第三台S5500设备上概率出现无法收到lACP报文告警，其它设备均正常工作。
- 5) 挂起S75E-1的LACP 软件模块，模拟相关软件挂死。测试发现与S75E-1设备上互联的所有设备，动态lACP设备出现无法收到LACP报文而告警，端口均被block。但是S75E-2互联的其它设备均正常工作。
- 6) 我们将上图中6台S5500更换为2台友商的S3750。测试结果一样。

至此可以判定，无论S7500E产生何种严重的故障，都不可能扩散故障区域。

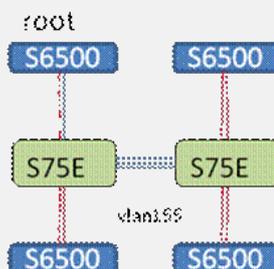
- 7) 实验室发现的存在类似问题的组网：接入S3550,右侧S3750 报misconfig down, 当Root的设备，突然收到S3550发送的报文为access属性导致



- 8) 实验室发现的存在类似问题的组网SMB模拟两台设备发送正常BPDU报文，特点是让这两个BPDU分别走聚合端口的两个端口，S3750 报misconfig down



- 9) 结合用户问题网络情况



S7500E上配置的聚合为手动聚合，当到root的一个端口处在单通（由于配置强制模式，所以处在单通的概率），其它S6509设备报misconfig down。而此次down按照标准协议分析，是不应该采取该动作的。此故障很明显，根据我们推断，S6509的err detect功能集成到stp中，可能处在如下两种判断条件，会主动down端口。

1) 当S75E到root的S6500聚合一个端口出现单通，S75E实际并无感知，所以状态也不会变化，而此时为根的S6500感知端口down，会将stp的BPDU报文的cost改变为1G带宽的开销值。但是其它设备，由于聚合没用变化，所以还是2G的开销值，这样收到的报文和自己的不一致，就主动报mis config错误。

2) 当S75E到root的S6500聚合一个端口出现单通，S6500发送bpdu报文端口从1迁移到2，这样可能出现的一种情况是，root发送的报文到其它S6500，时和S75E发送的stp报文分两个端口发给其它S6500，S6500认为这样的不正确而报misconfig。

四、解决方法：

由于问题的现象需要详细了解65上err detect功能才能有突破，但查阅了相关文档，思科对于err detect功能采取动作的原因，没有一个完整的文档进行阐述。但根据这个问题的处理经验，可以通过配置修改来杜绝此类问题。

1，根据6509上的日志信息，采取相应的对策，我们高度怀疑stp和erdetect联合机制导致，可以请评估在65与S75E的端口上配置BPDU过滤功能。防止STP检测导致影响全网。

2：尽可能不要跨设备配置聚合和STP混用。

3: 请考量评估是否能关闭err detect的子项misconfig功能。