第3章 数据链路层故障排除

ISSUE 3.0

课程目标

学习完本课程，您应该能够：

- 回顾链路层常见链路类型、协议，回顾物理层故障排除方法
- 了解PPP协议常见故障类型，掌握PPP协议故障排查方法
- 了解VLAN协议常见故障类型，掌握VLAN协议故障排查方法
- 了解STP/RSTP/MSTP协议常见故障类型，掌握STP协议常见故障排查方法

目录

常见链路类型、链路层协议

- 以太网（VLAN、STP）
- 串行链路（PPP、HDLC、FR）
- cPOS/E1链路（PPP）
- MSTP、RPR、DWDM等

相关物理层故障排除

- 以太网链路常见的过度冲突、干扰、异常帧以及性能问题等常见故障，需要从帧格式、接口工作方式、速率匹配以及相应的端口计数查看等方面入手分析。

- 串行链路不通的问题除了排查线缆外，还需要从接口工作方式、时钟选择、波特率设置等方面入手分析。

- 而**cPOS/E1**链路同样需要考虑帧格式、时钟、等问题，同时还需要考虑**CRC**、开销字段、加扰等的设置。

目录

- 链路层协议相关物理层故障排除
- PPP协议故障排除
- VLAN协议故障排除
- STP协议故障排除

PPP协议故障排除

- PPP协议概述
- PPP协议常见故障及排除方法
- PPP协议典型案例分析

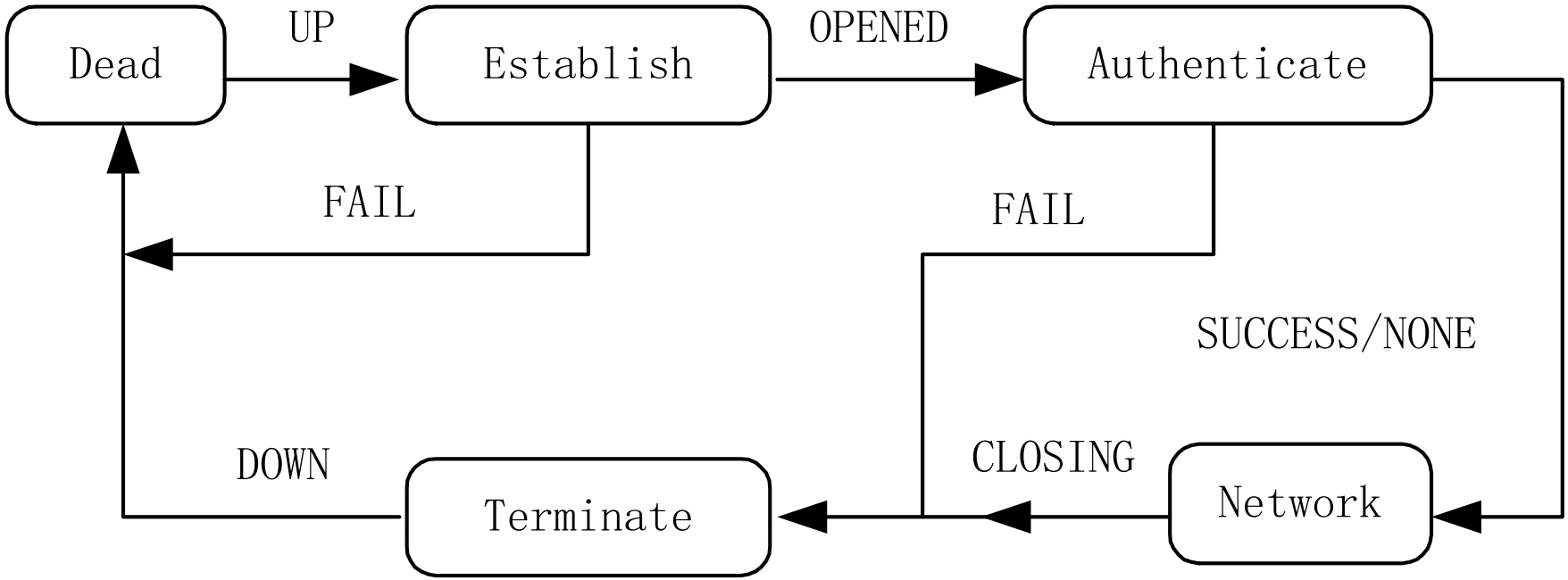
PPP协议概述

- **PPP协议是提供在点到点链路上传递、封装网络层数据包的一种数据链路层协议。**

- **PPP主要由两类协议组成：**
  - → 链路控制协议族(LCP)，主要用于建立，拆除和监控PPP数据链路
  - → 网络控制协议族(NCP)，主要用于协商在该数据链路上所传输的数据包的格式与类型。

- **MP（MultiLink PPP），是将多个PPP链路捆绑使用，目的是增加链路带宽。**

PPP协议协商过程


Dead
UP
Establish
OPENED
Authenticate
FAIL
FAIL
SUCCESS/NONE
DOWN
Terminate
CLOSING
Network

PPP协议常见故障（1）

- 物理接口参数设置不当导致PPP链路故障。常见的参数包括：
  - → 时钟选择（clock）
  - → 时钟反转（invert receive-clock、invert transmit-clock）
  - → 同异步模式选择（physical-mode）
  - → 波特率设置
- 故障常表现为：
  - → 只有发出的报文，而没有接收到的报文；
  - → 大量的接收错误（input errors）

PPP协议常见故障（2）

- **传输线路问题导致PPP链路故障**
  - → 传输线路不通
    - 只有发出的报文，而没有接收到的报文；
    - 线路自环后，收不到自己发出的报文
  - → 传输线路有自环
    - 收发报文的魔术字相同；
  - → 传输线路误码率高
    - 收发报文CRC错误
- **如果一方为非标设备，双方PPP协商项不兼容，可能会导致协商不通过**
  - → 查看ppp调试信息可以看到是哪些项协商不通过

PPP协议常见故障（3）

- **PPP参数配置错误会导致PPP链路故障**
  - → PPP验证配置
  - → MP配置
  - → PPP协商参数配置
- **没有接口路由导致PPP 链路不可用**
  - → LCP已经是Open，但是IP报文无法互通，可考虑路由的原因

PPP协议故障排除的一般步骤（1）

- 物理层问题分析
  - → 设备表现为广域网接口无法正常使用时，首先应该从物理层开始检查。使用display interface命令查看接口信息，根据显示信息中的“物理层状态”和“LCP状态”判断物理层是否正常。
  - → 物理层状态
    - Serial1/0 is up
    - Serial1/0 is down
    - Serial1/0 is administratively down
    - Serial1/0 is standby
- LCP问题分析
  - → 执行命令display interface ，如显示LCP协议未进入OPENED状态，可考虑为LCP的问题；
  - → 打开debugging ppp all查看报文收发的具体信息。

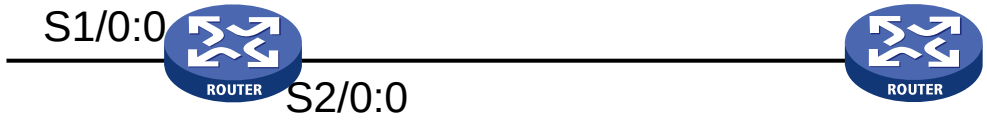
PPP协议故障排除的一般步骤（2）

- 验证问题分析
  - → 使用display interface命令查看接口信息，如显示LCP协议进入OPENED状态，而IPCP依然为Initial状态；或者LCP变为OPENED状态后又很快重新开始协商，可考虑为验证的问题。
  - → 通过debugging ppp all查看提示信息。
- **IPCP问题分析**
  - → 使用display interface命令查看接口信息，如显示LCP协议进入OPENED状态，而IPCP处于REQ_SEND或ACK_RCVD，并观察PPP报文有大量的IPCP报文收发，说明路由器IPCP协商有问题。
  - → 检查IP地址配置
- 其他问题分析
  - → 如LCP、IPCP均已进入OPENED状态，可考虑路由的原因

PPP协议相关的故障诊断命令

- display controller e1
- display interface serial
- debugging ppp
- display ppp mp

PPP案例一（1）



- 现象描述
  - → 两台MSR20-21设备使用E1方式互联，中间封装PPP协议。开始时，通信正常，但是有一天突然不通了。
  - → 通过Console口登录路由器后查看，发现路由器共有两个接口封装PPP，一个是S1/0:0，另一个是S2/0:0，出问题的口是S2/0:0，且两个接口的配置相同。
  - → 试着对S2/0:0口进行shutdown和undo shutdown操作，没有变化。

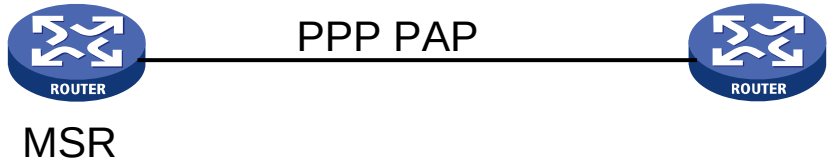
PPP案例一（2）

- 排障过程
  - → 查看接口指示灯亮，与对端网管人员确认物理层参数正确
  - → 用display interface serial 2/0:0命令观察端口状态发现LCP协商未通过
  - → 用display interface serial 2/0:0命令查看端口发现端口下有回环提示：loopback is detected
  - → 观察端口的流量，发现端口的input 和output报文周期性的每次增加20个

PPP案例一（3）

- 排障过程
  - → 联系运营商人员，得知前几天进行过网络改造，使中间的传输设备产生了自环。经过调整，问题解决。
- 建议和总结
  - → 善于使用display interface serial和debugging ppp命令
  - → 以前网络正常但近期突然发生故障，要与现场工程人员多沟通。

PPP案例二（1）



- 现象描述
  - → MSR路由器与某公司路由器之间启用PPP，使用PAP方式进行验证，PPP协商不通。
  - → MSR路由器做被验证方，配置ppp pap local-user xxx password simple xxx。该公司路由器做验证方，配置user xxx password 0 xxx 。

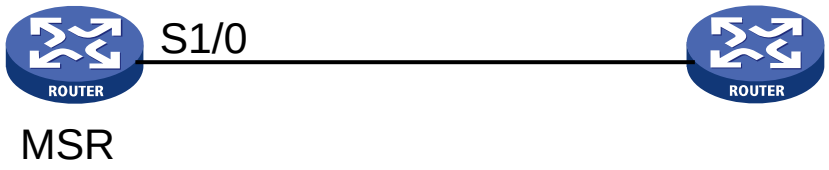
PPP案例二（2）

- 排障过程
  - → 首先查看接口指示灯亮，查看两端端口配置，物理层参数配置正确。说明物理层正常
  - → 通过display interface命令查看接口状态，发现LCP协商通过，但IPCP为Initial状态，且LCP状态不稳定，不断的进行重协商。
  - → 由于未配置验证前通信正常，增加验证配置后出现故障，基本判定是验证的问题
  - → 打开PPP报文调试信息，发现是由于用户名口令错误，验证失败导致PPP协商不过。
  - → 使用display current-configuration查看配置信息，发现两端的用户名和口令是一致的。
  - → 因提示密码错误，所以怀疑是配置有误，于是在路由器上重新配置用户名和密码。之后正常。

PPP案例二（3）

- 原因分析
  - → 配置路由器时，由于操作员对于不熟悉的命令习惯输入“？”来查询帮助信息，在该公司设备上配置user xxx password 0 xxx至最后的密码后，输入一个空格键，再输入？，发现再没有参数了，此时如果输入回车，导致配置的密码就不是xxx了，而是xxx加上一个空格符号。
- 建议和总结
  - → 有些字符（如数字0和字母O）比较相近，查看配置不太容易看得出来。此时，可以在确保不对网络造成危害的前提下重新配置。

PPP案例三（1）



- 现象描述
  - → MSR路由器与某公司路由器使用同步串口连接，两端都使用缺省配置。
  - → MSR路由器的链路层协议不能UP，另外一台路由器的链路层虽然在刚开始是UP状态，但过一分钟左右又会变为DOWN状态 。

PPP案例三（2）

- 排障过程
  - → 在MSR路由器上打开PPP报文调试信息，发现有不可识别的报文输入，发出的CONFREQ报文没有收到回应。
  - → 怀疑物理线路有问题，进行远端环回操作，发现本端发出的报文能够经物理线路返回，说明物理线路无问题。
  - → 怀疑对端路由器有故障，但在本地用另一台某公司路由器与其互连，链路层协议能够UP 。
  - → 查看某公司路由器相关文档，发现其串口的缺省链路层协议是HDLC。修改其成PPP后，故障解决

PPP案例三（3）

- 原因分析
  - → 因为双方的链路层协议不同，所以MSR路由器的链路层协议不能UP。而在另一台路由器上，因为封装了HDLC协议，所以刚开始时协议是UP的。但接口发出的KEEPALVE报文得不到回应，最后导致协议DOWN。
- 建议与总结
  - → 分段排除法和替换法能够更好更快的定位故障 。
  - → 不同公司的产品其缺省配置会有不同

目录

VLAN协议概述

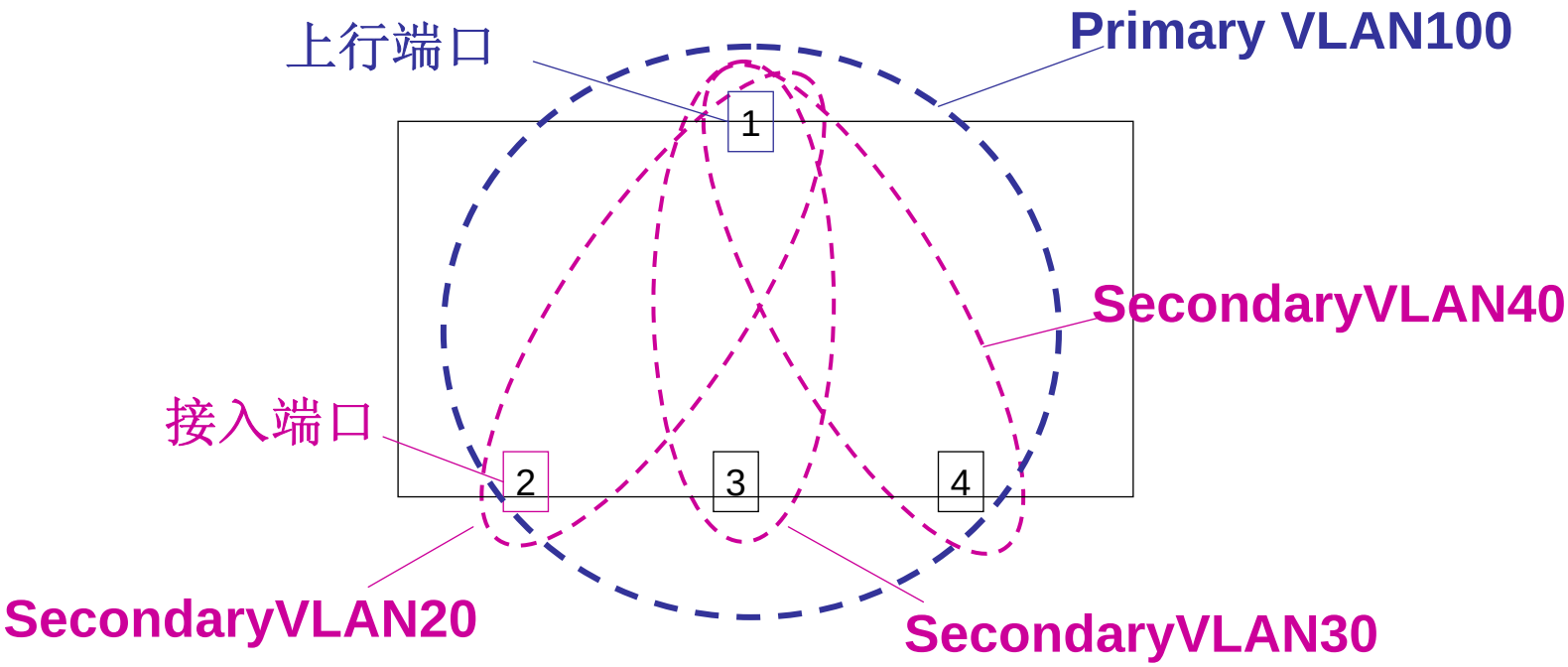
- **VLAN的引入**
  - → 用于隔离网络风暴，增加网络安全性
  - → 增加了4个字节的特殊标注域，用于区别不同用户发送的数据帧，其中VLAN ID占用12个比特位
- **VLAN与端口的关系**
  - → Access端口：这种端口只能属于一个VLAN，并且从该端口进来的数据包都不包含VLAN标签，数据包进入之后，会被加上该端口的VLAN ID（加上VLAN标签）。如果有数据需要从这种接口发送出去，数据帧中的VLAN标签将被删除。这种端口一般用于连接用户主机或路由器。

VLAN协议概述

- **VLAN与端口的关系**
  - → Trunk端口：这种端口可以属于多个VLAN，或者说这种端口可以传送多个VLAN的数据帧。从这种端口发送出去的数据帧都包含有VLAN标签（缺省VLAN ID的数据帧除外）；从这种端口接收到的报文，如果已经有VLAN标签，则直接转发；如果没有VLAN标签，则加上带有缺省VLAN ID的VLAN标签。这种端口一般用于连接交换机或路由器。
  - → Hybrid端口：这种端口可以属于多个VLAN。但是与Trunk端口不同的是它所传送的数据帧，可以包含VLAN标签也可以不包含VLAN标签；而Trunk端口则必须包含VLAN标签（缺省VLAN ID的数据帧除外）。其发送数据帧时根据配置信息进行判断是否加上VLAN标签；接收数据帧时和Trunk端口相同。这种端口一般用于连接交换机或路由器。

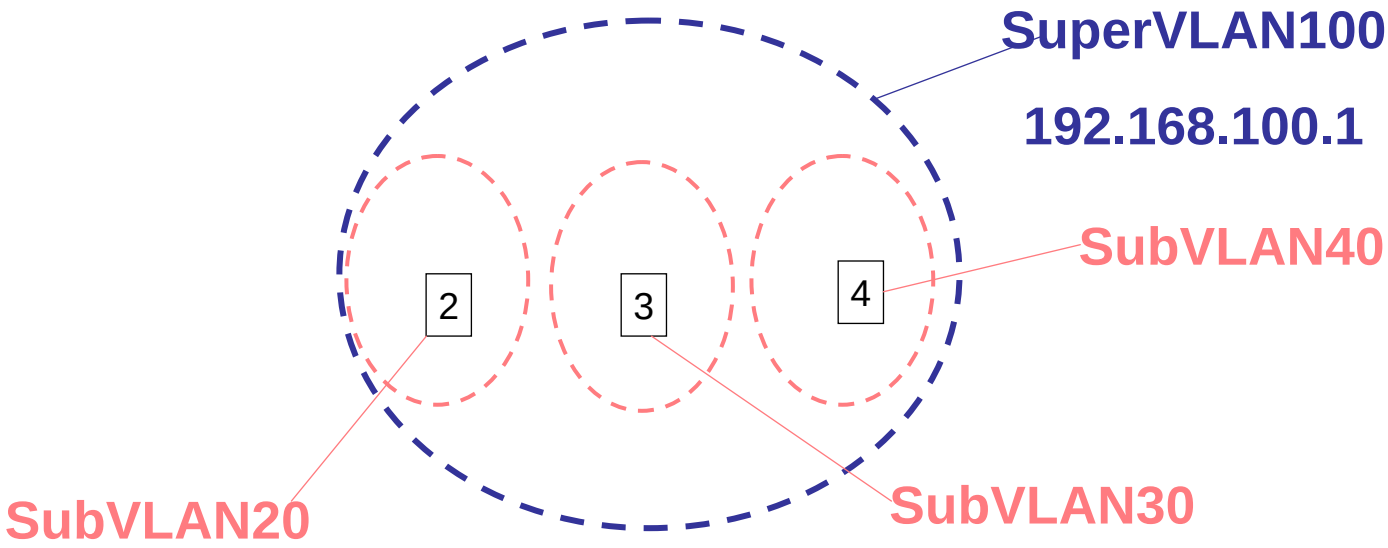
VLAN常用技术简介（1）

- **Isolate-user-vlan技术解决VLAN ID不足**
  - → 采用VLAN ID屏蔽的办法，将接入层的用户VLAN ID对汇聚层设备屏蔽起来，在接入层使用VLAN的方法进行用户二层隔离。
  - → 汇聚层设备只知道Isolate-user-vlan。数据包返回时，根据MAC转发到Isolate-user-vlan所包含的所有Secondary VLAN用户。



VLAN常用技术简介（2）

- **Super VLAN可节省 IP 地址**
  - → Super VLAN 和多个Sub VLAN 关联，Super VLAN 对应的VLAN接口上配置有IP地址；Sub VLAN 不用创建对应的VLAN 接口，不同Sub VLAN 之间二层相互隔离。
  - → 如果想要实现 Sub VLAN 之间的三层互通及Sub VLAN 与其它网络的互通，可以使用设备的本地代理ARP 功能。



VLAN常用技术简介（3）

- **Voice vlan技术简介**
  - → Voice VLAN是为语音数据流而专门划分的VLAN。
  - → 设备可以根据进入端口的数据报文中的源MAC地址字段来判断该数据流是否为语音数据流。
  - → 源MAC地址符合系统设置的语音设备OUI（Organizationally Unique Identifier，全球统一标识符）地址的报文被认为是语音数据流，被划分到Voice VLAN中传输。

- **GVRP技术简介**
  - → GVRP（GARP VLAN Registration Protocol，GARP VLAN注册协议）是GARP（Generic Attribute Registration Protocol，通用属性注册协议）的一种应用，它基于GARP的工作机制，维护设备中的VLAN动态注册信息，并传播该信息到其它的设备中。

VLAN常用技术简介（4）

- **802.1x的Guest VLAN**
  - → 802.1x应用中衍生出的一种VLAN应用
  - → 在用户无法认证或认证失败时进入Guest VLAN，可以访问Guest VLAN内的资源
  - → 访问外部资源仍然需要认证

- **VLAN路由技术简介**
  - → VLAN路由技术模拟路由器的三层接口，在以太网上创建出虚拟局域网三层接口。
  - → 这些接口具有三层报文转发的功能。将二层不能转发的数据帧进行数据帧头的剥离，然后根据IP报文头信息进行转发。

VLAN协议常见故障

- VLAN用户隔离不成功；
- VLAN隔离后不能进行任何通信；
- 采用VLAN技术后，无法进行设备管理。

VLAN协议故障排除的一般步骤

- **首先分析数据帧的转发过程，特别是数据帧携带的VLAN ID的变化。**
  - → 看看在整个数据帧转发的过程中何时删除VLAN标签，何时增加VLAN标签
  - → 在删除和增加的过程中是否变化过VLAN ID，特别是Isolate-user-vlan技术存在的时候。
- **其次分析是否VLAN路由存在问题。**

VLAN协议常见故障排除要点（1）

- **VLAN用户隔离不成功**
  - →检查配置信息，确保没有将用户划分在同一个VLAN下；
  - →分析VLAN用户数据在转发过程中的变化，特别是Isolate-user-vlan技术存在的时候；
  - →检查VLAN路由是否存在问题；
  - →如果需要隔离三层转发的用户，只能借助于包过滤技术来完成。

VLAN协议常见故障排除要点（2）

- **VLAN隔离后不能进行任何通信**
  - →检查配置信息，确保没有做端口的关闭操作或者包过滤等设置；
  - →使用命令display interface vlan-interface检查对应的VLAN虚接口是否存在，状态是否正常；
  - →检查相关的路由信息是否正确

VLAN协议常见故障排除要点（3）

- 采用VLAN技术后，不能进行设备管理

  →解决方法和前两种类似；

  →在某些场合不能彻底将管理VLAN和用户VLAN进行分离的时候，只有采用管理和业务共用VLAN的办法。

VLAN协议相关的故障诊断命令

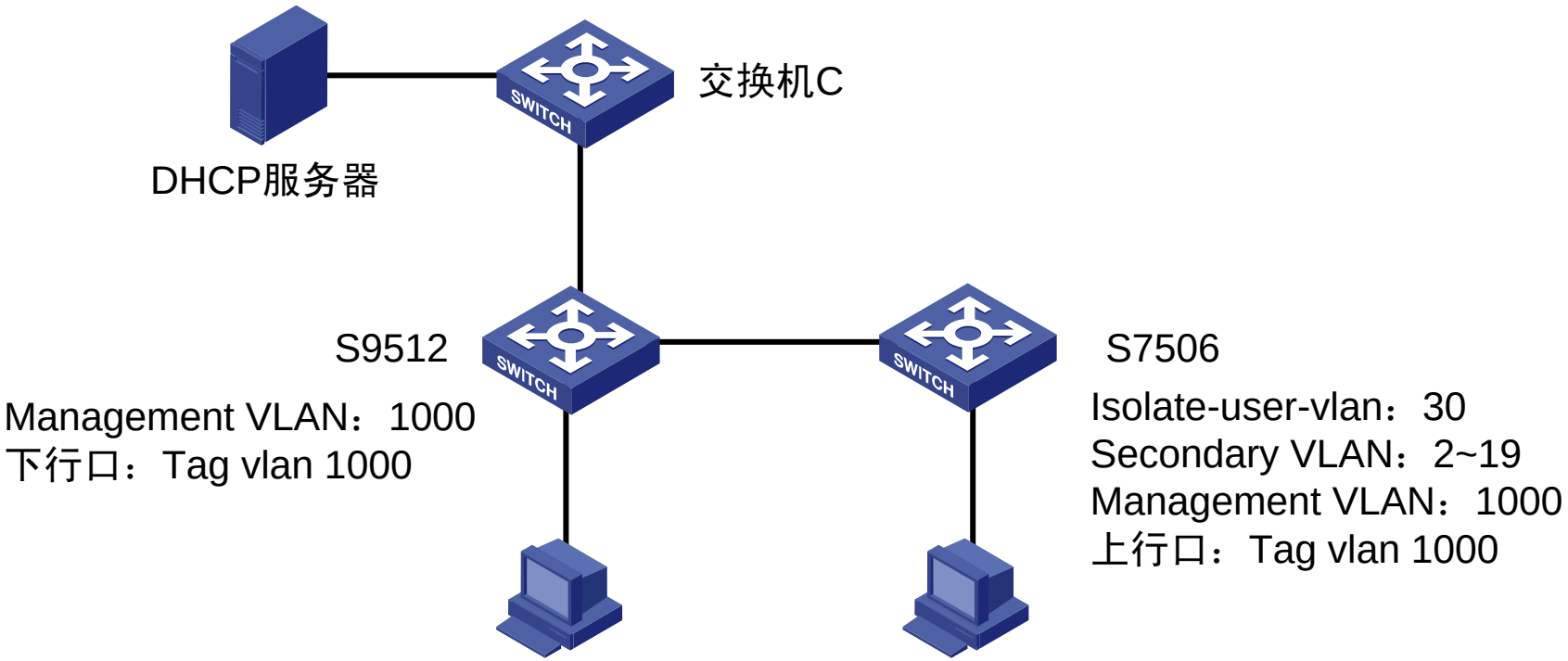
- **display vlan**

  → 用来显示VLAN的相关信息。

- **display interface**

  → 用来显示指定接口当前的运行状态和相关信息。

VLAN案例一（1）

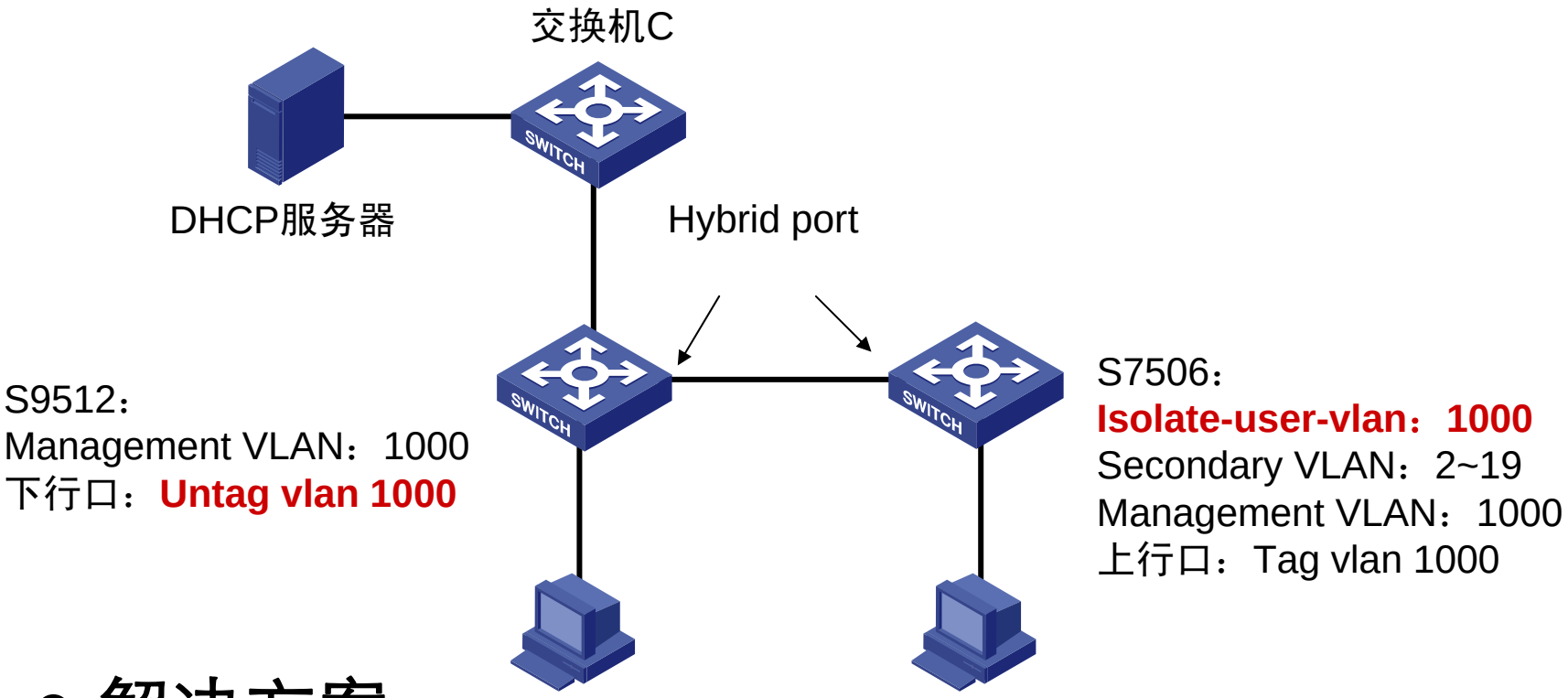


- **S9512所连接的用户可以动态获得IP地址；所有S7506连接的用户都无法动态获得IP地址，也无法与DHCP SERVER通信；在S7506上，可以Ping通DHCP服务器。另外还发现，如果把S7506所连接的用户设置为VLAN 1000用户，则可以通过DHCP服务器获得IP地址，也可以Ping通交换机C。**

VLAN案例一（2）

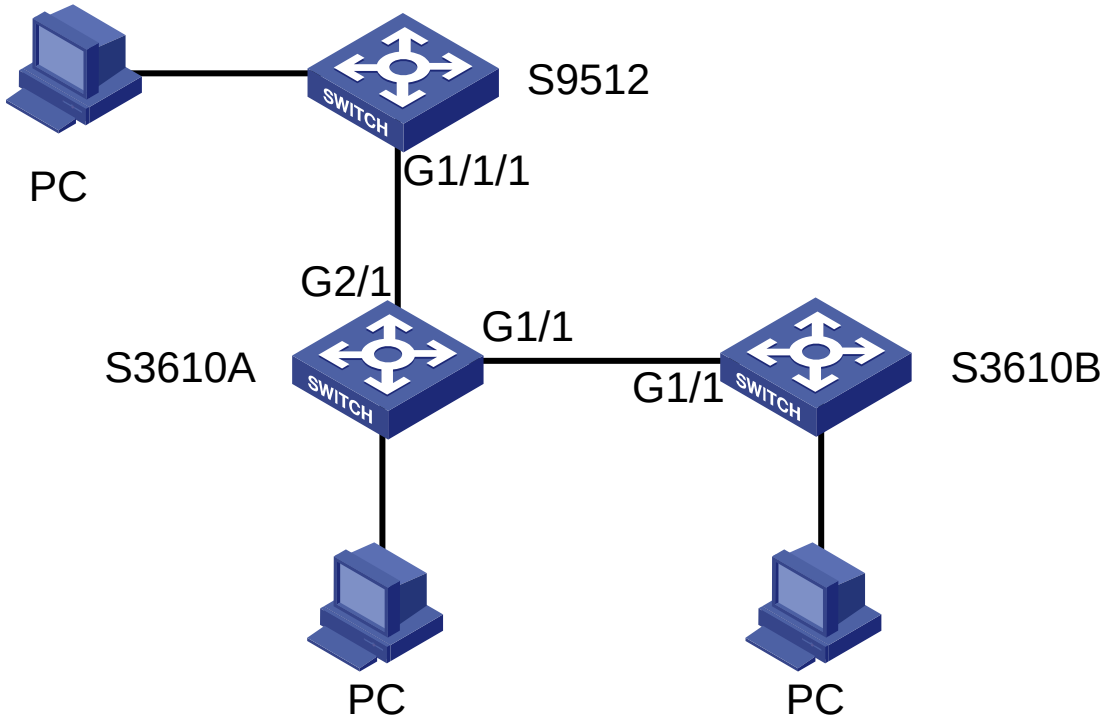
- 排障过程：
  - → S7506下VLAN1000的用户可以正常上网，说明网络物理线路连接正常；
  - → 只有VLAN1000的数据帧得到了转发，其它VLAN数据帧不能通过，说明问题在VLAN配置上；
  - → 帧上行转发过程分析：
    - 用户数据帧通过S7506的上行口去掉VLAN标签后转发到S9512；S9512接收到Untagged帧后，打上端口的PVID，然后从上行口去掉VLAN标签，转发到交换机C。上行没有问题。
  - → 帧下行转发过程分析：
    - Untagged帧进入S9512，打上VLAN1000的标签；因S9512下行口和S7506上行口都为允许VLAN1000数据帧通过且不去掉标签，所有的数据帧都带有VLAN1000标签而转发到S7506，无法到达Secondary VLAN中用户。

VLAN案例一（3）



- 解决方案
  - → S9512下行接S7506的端口配置Untag vlan 1000。
  - → S7506上把Isolate-user-vlan直接设置为1000，包含所有用户端口的Secondary VLAN，同时作为管理VLAN。

VLAN案例二（1）



- 故障现象：
  - → S3610A下的PC机均可以与S9512下的PC互通；而S3610B的VLAN5、VLAN6、VLAN7的PC不能与S9512的VLAN5、VLAN6、VLAN7的PC互通，但VLAN100的PC可以与S9512下VLAN100的PC互通。

VLAN案例二（2）

- 排障过程
  - → VLAN100下的PC机能够正常通信，说明线路无故障；
  - → VLAN5、VLAN6、VLAN7的PC不能互通，说明VLAN配置问题；
  - → 查看S3610B的G1/1的端口状态，发现允许通过的VLAN为5，6，7，100；
  - → 查看S3610A的G1/1和G2/1的端口状态，发现允许通过的VLAN为2，3，4，100，没有VLAN 5，6，7。
  - → 原因找到了，是因为S3610A上没有配置VLAN5、6、7。

VLAN案例二（3）

- 原因分析
  - → S3610A的G2/1和G1/1端口虽然配置了port trunk permit vlan all，但其实是允许本交换机中配置的VLAN通过，而不是允许本交换机没有的VLAN通过。
- 解决方案
  - → 在S3610A手工增加VLAN 5、VLAN6、VLAN7后，故障消失。
- 建议与总结
  - → display interface也是VLAN故障排除中很重要的命令，可以看出端口实际通过哪些VLAN报文。
  - → 还有一种解决方案是在交换机上启用GVRP协议。通过在端口上进行VLAN通告/注册过程，GVRP可以把交换机的VLAN信息传播到全网中。

目录

STP协议概述

- **STP协议的概念**

  → STP（Spanning Tree Protocol，生成树协议）是根据IEEE协会制定的802.1D标准建立的，用于在局域网中消除数据链路层物理环路的协议。

  → STP包含了两个含义，狭义的STP是指IEEE 802.1D中定义的STP协议，广义的STP是指包括IEEE 802.1D定义的STP协议以及各种在它的基础上经过改进的生成树协议。

STP生成树协议的演进（1）

- **STP协议的不足**

  → STP不能快速迁移，即使是在点对点链路或边缘端口也必须等待2倍的Forward Delay的时间延迟，端口才能迁移到转发状态。

- **RSTP协议**

  → RSTP是STP协议的优化版。其“快速”体现在，当一个端口被选为根端口和指定端口后，其进入转发状态的延时在某种条件下大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间。

STP生成树协议的演进（2）

- **RSTP协议的不足**
  - → 虽然RSTP可以快速收敛，但是和STP一样存在以下缺陷：局域网内所有网桥共享一棵生成树，不能按VLAN阻塞冗余链路，所有VLAN的报文都沿着一棵生成树进行转发。

- **MSTP协议**
  - → MSTP（Multiple Spanning Tree Protocol，多生成树协议）可以弥补STP和RSTP的缺陷，它既可以快速收敛，也能使不同VLAN的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。

MSTP协议的特点

- MSTP设置VLAN映射表，把VLAN和生成树联系起来。通过增加“实例”这个概念，将多个VLAN捆绑到一个实例中，以节省通信开销和资源占用率。
- MSTP把一个交换网络划分成多个域，每个域内形成多棵生成树，生成树之间彼此独立。
- MSTP将环路网络修剪成为一个无环的树型网络，避免报文在环路网络中的增生和无限循环，同时还提供了数据转发的多个冗余路径，在数据转发过程中实现VLAN数据的负载分担。
- MSTP兼容STP和RSTP。

MSTP协议故障分类

- **MSTP协议故障分类**
  - → 产生环路导致广播风暴；
  - → 端口无法快速迁移；
  - → 端口长期处于Discarding状态；
  - → 端口处于STP DOWN状态；
  - → 网络流量不稳定；
  - → 设备无法处于同一个MSTP域。

- **MSTP协议兼容STP和RSTP协议，所以MSTP协议的故障排查方法同样适用与STP、RSTP协议。**

MSTP协议故障排除（1）

- 广播风暴故障处理步骤
  - → 检查设备全局MSTP 是否开启
  - → 检查端口MSTP 是否开启
  - → 检查是否发生拓扑改变
  - → 检查端口是否存在STP 报文超时现象
- 端口无法快速迁移故障处理步骤
  - → 检查端口对端连接是否为终端
  - → 检查本设备是否工作在STP 模式
  - → 检查上游设备的工作模式
  - → 检查端口是否为点对点链路
  - → 检查端口的双工模式

MSTP协议故障排除（2）

- **端口长期处于Discarding状态故障处理步骤**
  - → 检查是否收到本端口自己发送的报文
  - → 检查端口收到报文格式是否和配置格式一致
    - 查看系统的日志信息
    - 打开端口报文调试开关查看收到报文的类型
  - → 检查是否端口根保护功能所致
    - 查看系统的日志信息
    - 用display stp abnormal-port查看端口
  - → 检查是否端口环路保护功能所致
- **端口STP DOWN故障处理步骤**
  - → 检查是否BPDU保护功能所致
  - → 检查是否因报文格式频繁切换而被STP关闭

MSTP协议故障排除（3）

- 网络流量不稳定故障处理步骤
  - → 检查端口STP 状态是否震荡
  - → 检查端口STP 角色是否震荡
  - → 检查设备是否频繁收到TC 报文
- 设备无法处于同一个MSTP域故障处理步骤
  - → 检查各设备域配置是否一致正确
  - → 检查本端设备运行模式
  - → 检查对端设备是否支持标准配置摘要计算

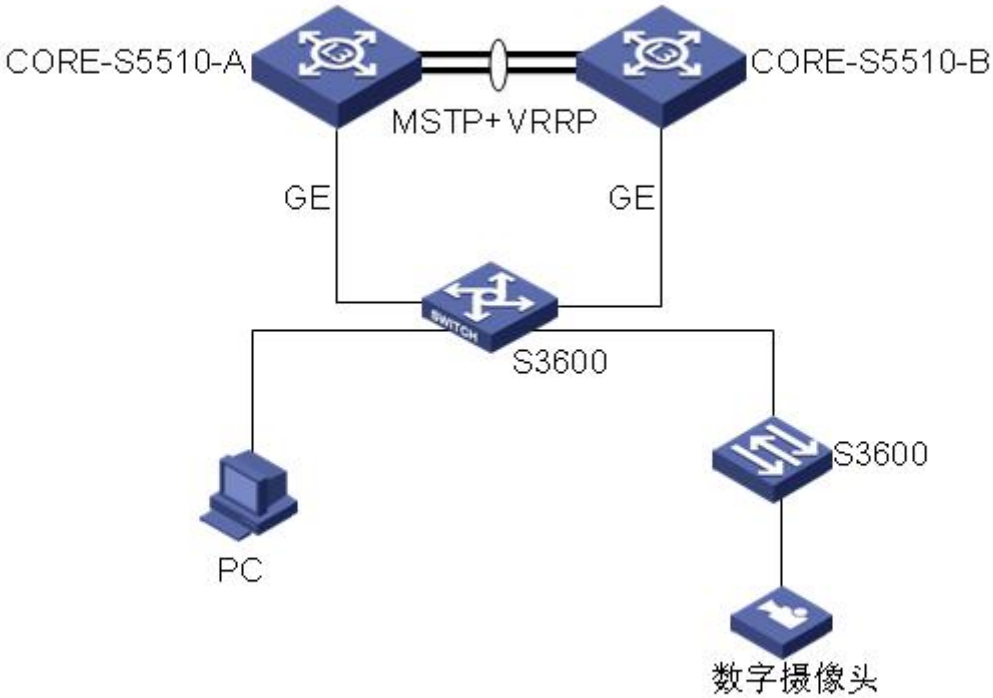
STP协议相关的故障诊断命令

命令	说明
display stp [instance *instance-id*] [interface *interface-list* | slot *slot-number*] [brief]	显示MSTP 的状态信息与统计信息
display stp abnormal-port	显示非正常阻塞的端口信息
display stp down-port	显示被STP 保护功能down 掉的端口信息
display stp [instance *instance-id*] history [slot *slot-number*]	显示MSTP 实例端口角色计算的历史信息
display stp region-configuration	显示已经生效的MST 域的配置信息
display stp root	显示所有MSTP 实例的根桥信息
display stp [instance *instance-id*] tc [slot *slot-number*]	显示MSTP 实例的所有端口发送和接收的TC 或者TCN 报文个数
display logbuffer [reverse] [level *severity* | size *buffersize*] * [| { begin | exclude | include } *regular-expression*]	显示系统日志缓冲区的状态和缓冲区记录的日志信息。

STP协议相关的故障诊断命令

命令	说明
debugging stp all	打开 MSTP 所有的调试信息开关
debugging stp event [interface *interface-type interface-number*]	打开MSTP 的端口事件调试信息开关
debugging stp fsm [instance *instance-id*][interface *interface-type interface-number*]	打开MSTP 状态机调试信息开关
debugging stp global-error	打开MSTP 全局错误调试信息开关
debugging stp global-event	打开 MSTP 全局事件调试信息开关
debugging stp packet [receive | send][interface *interface-type interface-number*][brief | verbose]	打开MSTP 的报文调试信息开关
debugging stp roles	打开MSTP 的端口角色变化调试信息开关
debugging stp tc [interface *interface-type interface-number*]	打开MSTP 的TC 事件调试信息开关

STP案例一（1）



- 故障现象
  - → 在增加级联交换机时，发现级联交换机端口指示灯闪烁两下后即灭，端口也是UP后立即DOWN。经排查线缆良好，更换端口测试故障依旧。

STP案例一（2）

- 排障过程
  - → 由于新增交换机连接的端口为原连接PC机的端口，而原来PC机访问网络正常，说明楼层交换机端口与网线是正常的。
  - → 登录楼层接入交换机，发现楼层交换机日志中有如下提示：

```
#Apr  2 00:43:40:173 2000 F1-S3600-01 MSTP/2/IVBPDU:- 1 -
1.3.6.1.4.1.2011.2.23.1.14.0.5(hwPortMstiBpduGuarded): BPDU-Protection port 2
received BPDU packet!
%Apr  2 00:43:40:361 2000 F1-S3600-01 MSTP/3/IVBPDU:- 1 -BPDU-Protection
port Ethernet1/0/2 received BPDU packet!
```

  - → 进一步查看端口是否被STP DOWN：

```
[ F1-S3600-01]dis stp down-port
Down Port          Reason
Ethernet1/0/2       BPDU-Protection
```

  - → 显示E1/0/2端口处于DOWN状态，原因为BPDU保护导致。

STP案例一（3）

→ 查看交换机上的配置以进一步确认：

```
stp bpdu-protection
stp enable
stp region-configuration
 region-name MGT
 instance 1 vlan 10 999
 instance 2 vlan 20 30
 active region-configuration
 #
interface Ethernet1/0/2
 stp edged-port enable
 port access vlan 30
```

→ 可见交换机开启了BPDU保护功能，并且连接新增交换机的端口设置了edged-port（边缘端口）。

→ 使用undo stp edged-port命令将E1/0/2端口设置为非边缘端口，并使用undo shutdown命令开启E1/0/2端口，故障排除。

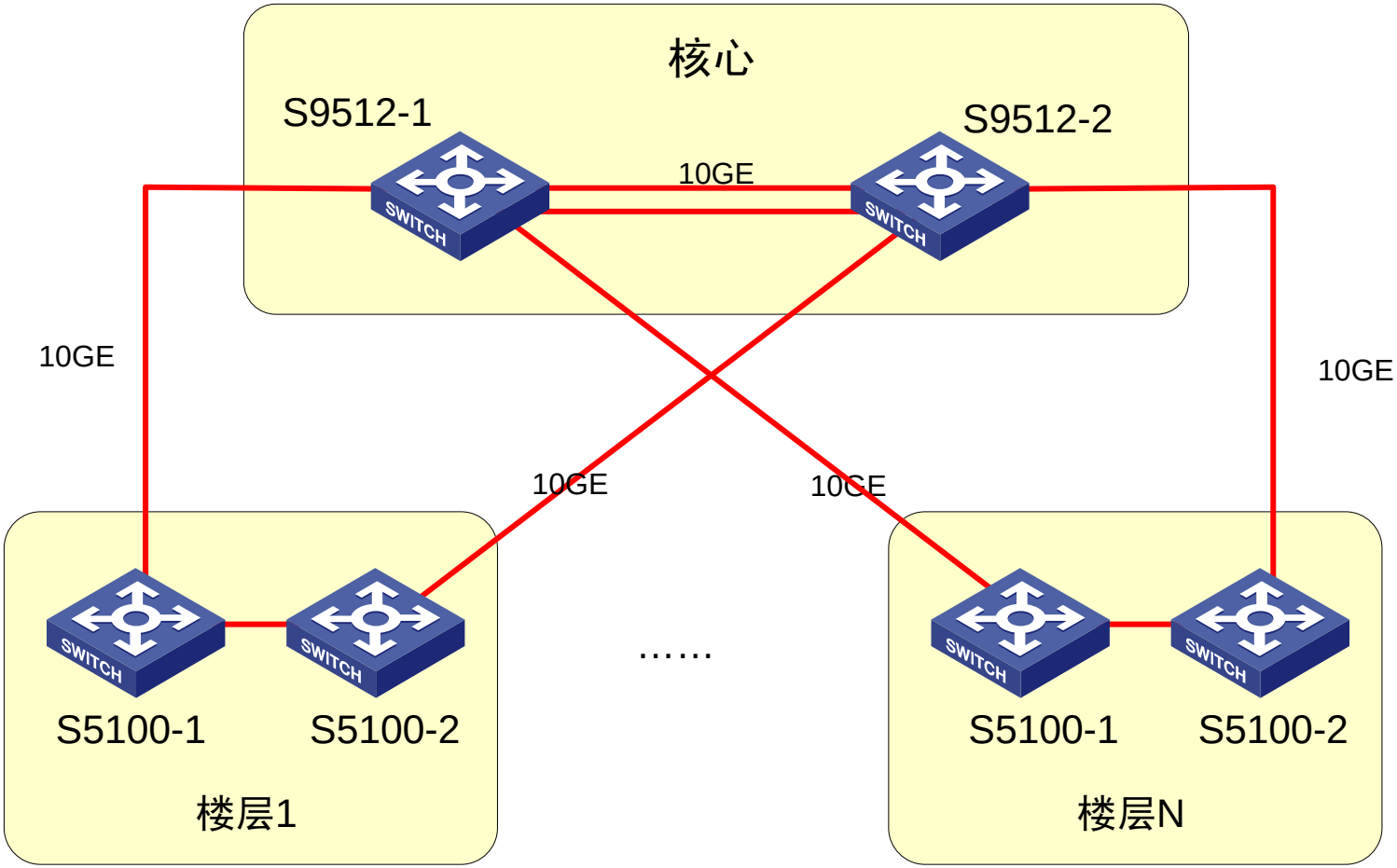
STP案例一（4）

- 原因分析
  - → 接入端口设置为边缘端口后，如果接收到配置消息，系统自动将这些端口设置为非边缘端口，重新计算生成树。
  - → 如果有人伪造配置消息恶意攻击设备，就会引起生成树重新计算，导致网络震荡。
  - → 交换机开启了BPDU保护功能后，如果接收到BPDU，则交换机关闭此端口，以防止可能产生的网络震荡。而被关闭的端口只能由网络管理人员恢复。
  - → 本例中楼层交换机的接入端口配置了边缘端口，同时开启了BPDU保护功能，而新增的交换机开启了STP功能，接入网络后开始发送BPDU报文。此时楼层交换机认为新增交换机为BPDU恶意攻击，将E1/0/2端口关闭。

STP案例一（5）

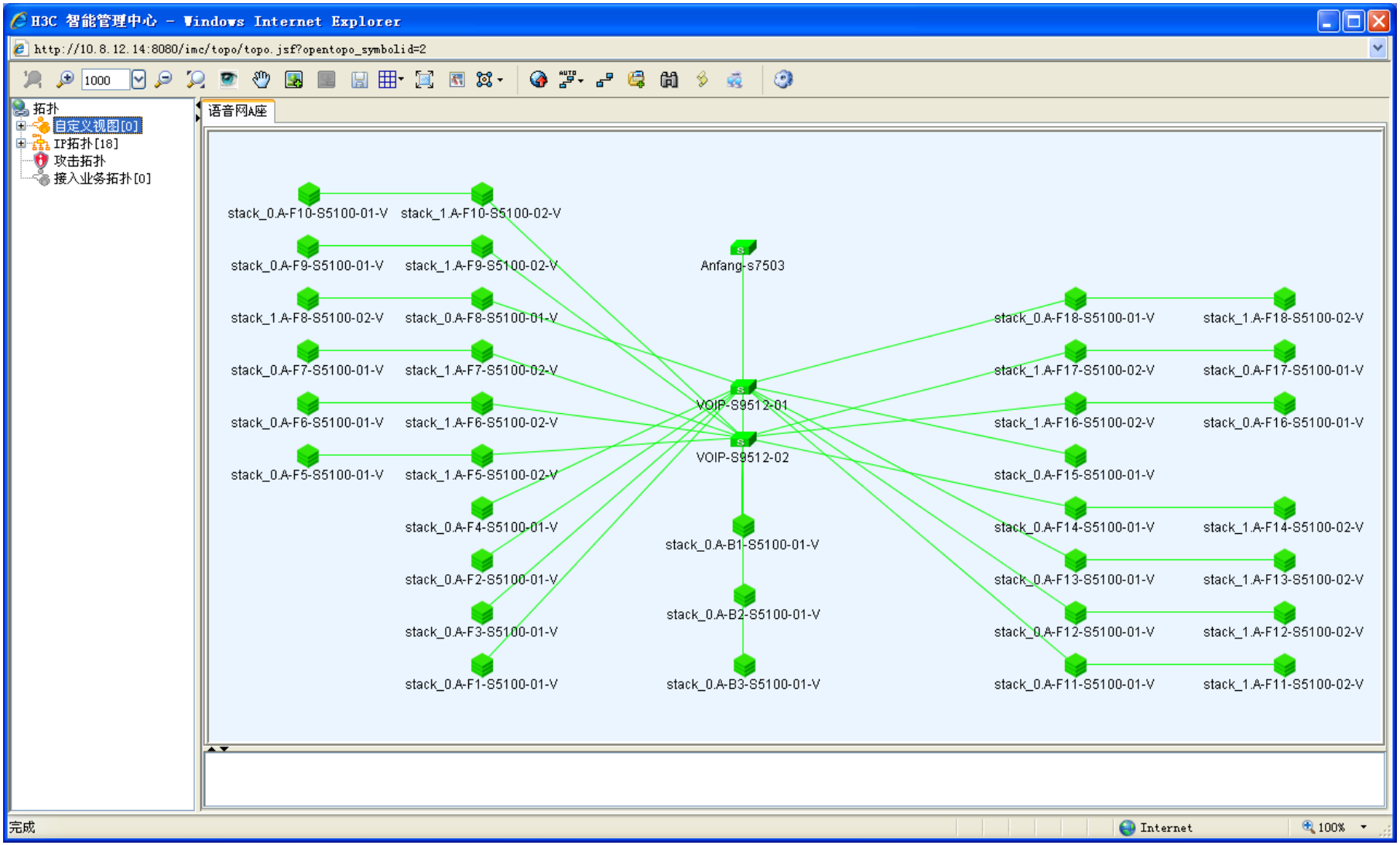
- 建议和总结
  - → 在新增网络设备时，需要充分考虑与现有网络的兼容性，详细分析新增设备对现有网络的影响，并提前做出准备。
  - → 在本例中，除了可以设置楼层交换机的端口为非边缘端口来解决问题外，还可以关闭新增交换机的STP协议，使新增交换机不发出配置消息。

STP案例二（1）



- 故障现象
  - → 某天，部分楼层接入交换机的主用链路切换到了S9512-2这一侧，正常情况下，主用链路应该都在S9512-1这一侧。

STP案例二（2）


H3C 智能管理中心 - Windows Internet Explorer
http://10.8.12.14:8080/imc/topo/topo.jsf?opentopo_symbolid=2
1000
拓扑
自定义视图[0]
IP拓扑[18]
攻击拓扑
接入业务拓扑[0]
语音网A座
stack_0.A-F10-S5100-01-V
stack_1.A-F10-S5100-02-V
stack_0.A-F9-S5100-01-V
stack_1.A-F9-S5100-02-V
stack_1.A-F8-S5100-02-V
stack_0.A-F8-S5100-01-V
stack_0.A-F7-S5100-01-V
stack_1.A-F7-S5100-02-V
stack_0.A-F6-S5100-01-V
stack_1.A-F6-S5100-02-V
stack_0.A-F5-S5100-01-V
stack_1.A-F5-S5100-02-V
stack_0.A-F4-S5100-01-V
stack_0.A-F2-S5100-01-V
stack_0.A-F3-S5100-01-V
stack_0.A-F1-S5100-01-V
Anfang-s7503
VOIP-S9512-01
VOIP-S9512-02
stack_0.A-B1-S5100-01-V
stack_0.A-B2-S5100-01-V
stack_0.A-B3-S5100-01-V
stack_0.A-F18-S5100-01-V
stack_1.A-F18-S5100-02-V
stack_1.A-F17-S5100-02-V
stack_0.A-F17-S5100-01-V
stack_1.A-F16-S5100-02-V
stack_0.A-F16-S5100-01-V
stack_0.A-F15-S5100-01-V
stack_0.A-F14-S5100-01-V
stack_1.A-F14-S5100-02-V
stack_0.A-F13-S5100-01-V
stack_1.A-F13-S5100-02-V
stack_0.A-F12-S5100-01-V
stack_1.A-F12-S5100-02-V
stack_0.A-F11-S5100-01-V
stack_1.A-F11-S5100-02-V
完成
Internet
100%

STP案例二（3）

- 排障过程

→ 查看5楼与8楼交换机配置，发现均有MAST端口，如下：

```
<stack_1.A-F5-S5100-02-V>dis stp bri
 MSTID    Port                Role  STP State     Protection
   0      GigabitEthernet1/0/49    ROOT  FORWARDING    LOOP
   0      TenGigabitEthernet1/1/1* DESI  FORWARDING    LOOP
   1      GigabitEthernet1/0/49    MAST  FORWARDING    LOOP
   1      TenGigabitEthernet1/1/1* DESI  FORWARDING    LOOP
   2      GigabitEthernet1/0/49    MAST  FORWARDING    LOOP
   2      TenGigabitEthernet1/1/1* DESI  FORWARDING    LOOP
(*) means port in aggregation group
```

→ 由于S5100上存在MAST端口，说明S5100为域内的主交换机，MAST端口为连接总根的端口。而S5100的MAST端口上连的设备为S9512，说明S5100与S9512不在同一个域中。

STP案例二（4）

- 排障过程

→设备无法处于MSTP域，最有可能的原因是配置不一致，进一步检查S9512与S5100的MSTP域配置；

S9512上的STP配置：

instance 1 vlan 111 to 112 400 430 440 450 603 800 to 849 900 to 949

instance 2 vlan 113 to 114 401 410 420 431 441 850 to 879 881 to 899 950 to 999

5层S5100上的STP配置：

instance 1 vlan 111 to 112 400 430 440 603 800 to 849 900 to 949

instance 2 vlan 113 to 114 401 410 420 431 441 850 to 899 950 to 999

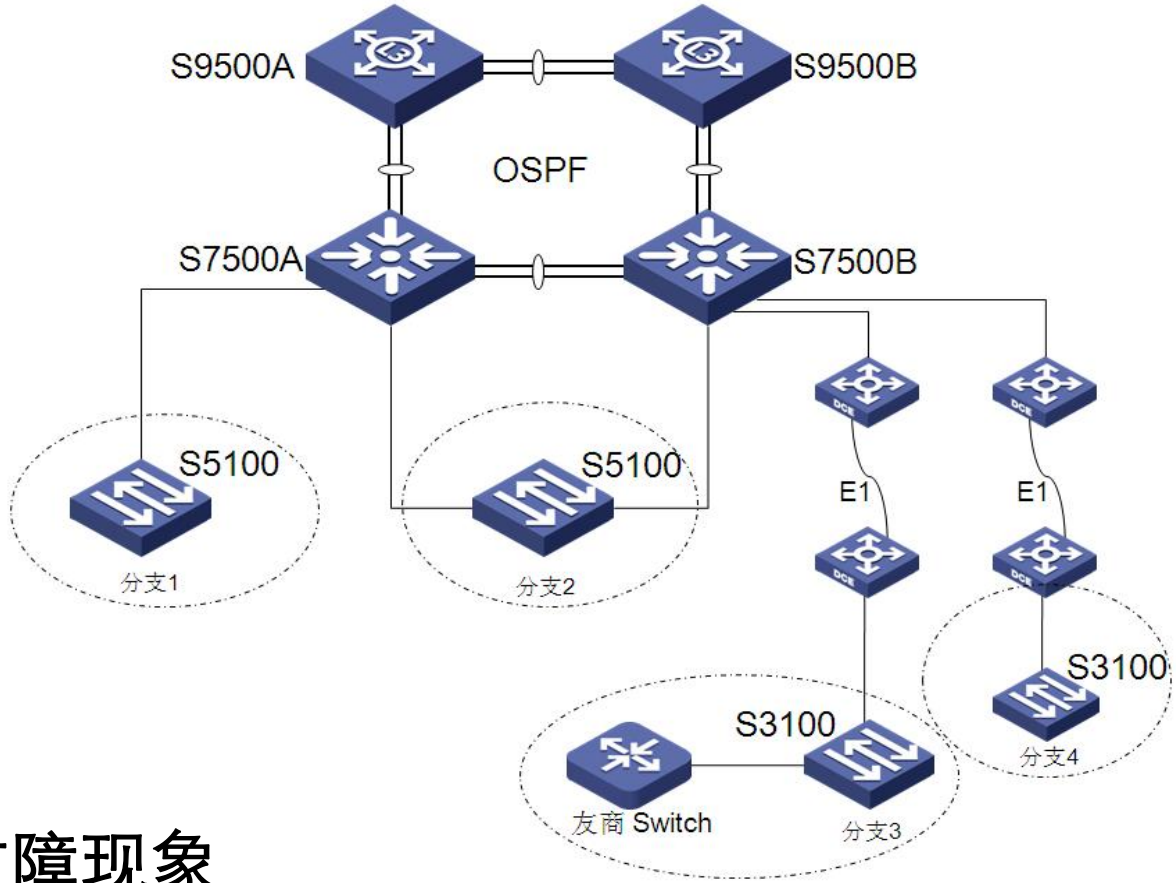
- 解决方案

→将S5100与S9512的配置同步后，问题解决

STP案例二（5）

- 原因分析
  - → 由于实例配置不同，所以每个楼层交换机为一个独立的**MSTP**域
  - → 每个楼层根据域内计算出的域根（可能为**S5100-1**或**S5100-2**）连接至总根
- 建议与总结
  - → 在**MSTP**环境下，如果产生拓扑变化，首先要查看是否由于**MSTP**域配置不同

STP案例三（1）



- 故障现象

  → 网络运行一段时间后，经常出现中断，业务无法正常开展，有时整个网络处于半瘫痪状态。

STP案例三（2）

- 根据现象来看，故障属于网络流量不稳定，重点检查以下三个方面：
  - → 端口STP 状态是否震荡
  - → 端口STP 角色是否震荡
  - → 设备是否频繁收到TC 报文
- 排障过程
  - → 查看S7506的日志信息，发现STP端口状态不停切换，进而导致VRRP组状态不停切换；
  - → 发现S7506连接分支3的接口经常有TC报文收到；
  - → 切断分支3的线路后，网络恢复正常；
  - → 查看S7506端口，发现分支3的协议转换器和S7506端口的工作模式协商为10M、半双工，且端口有大量错包。

STP案例三（3）

- 排障过程
  - → 将协议转换器接在一个备用的二层交换机上测试，发现互连端口不停的up/down。
  - → 查看S3100和友商 3500交换机的日志信息，发现S3100的根端口在不停的迁移，原因终于水落石出了。
- 故障原因
  - → 在S3100下面连接了一台友商的3500交换机。其MAC地址小，成为MSTP实例0的根桥。而S3100和E1协议转换器之间端口协商不稳定，经常出现up/down的情况，导致实例0的STP不停的重新计算，根桥也在不停的切换，从而导致网络动荡。

STP案例三（4）

- 解决方案
  - → 首先将S3100和友商 S3500交换机的STP协议关闭，再把S7506A和S7506B指定为实例0的根桥和备份根桥。避免了S3500成为根桥的问题。
  - → 更换质量更好的E1协议转换器，解决端口协商的问题。
- 建议和总结
  - → 正确的网络规划和部署是协议运行良好的基础。
  - → STP根的稳定性是STP协议运行中非常重要的一部分，如果STP根经常变化，会导致整个网络产生动荡。如果STP网络产生动荡，则首先要查看根是否经常变化，并找出根变化的原因。

本章总结

- 数据链路层回顾
- PPP协议故障排除
- VLAN协议故障排除
- STP协议故障排除

ITоIP解决方案专家

杭州华三通信技术有限公司

www.h3c.com