RC-900-C1

ZXR 10 组网案例分析与故障分析处理

故障案例分析

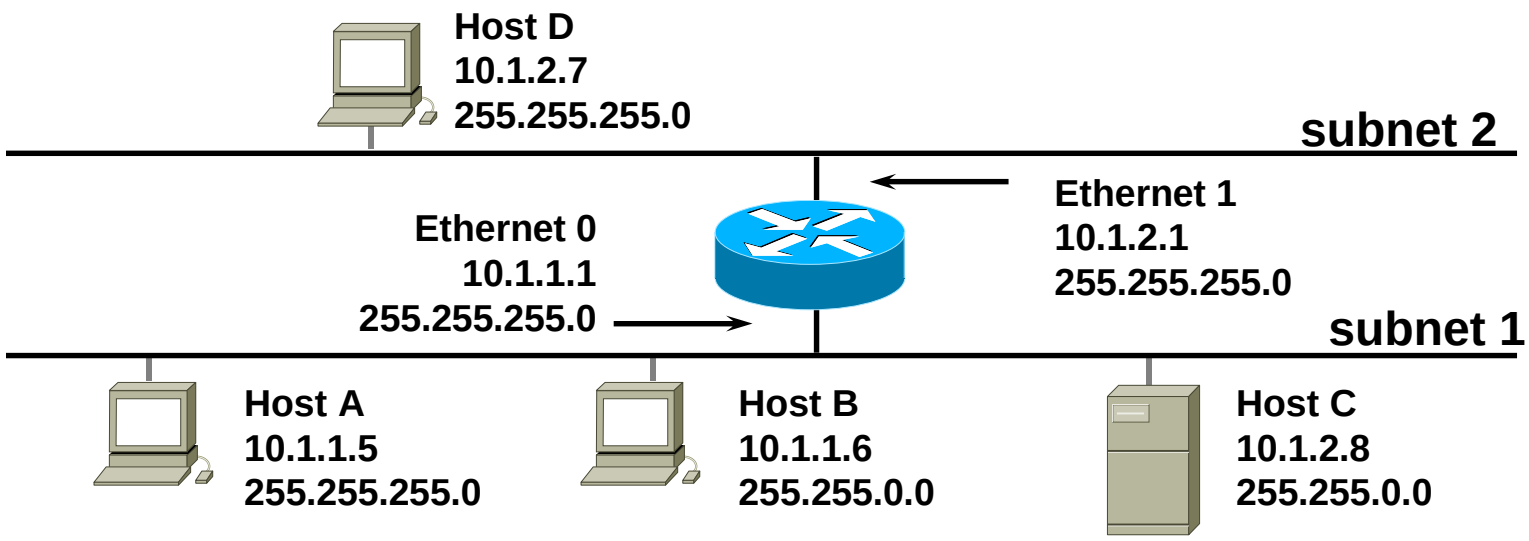
V0504

中兴通讯学院

数据产品课程团队

中兴通讯学院
<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>
univ.zte.com.cn
PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

Users Can Access Some Hosts but Not Others



- Can host A connect to host C?
- Can host A connect to host B?
- Can host D connect to host C?

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析－PVID,VID

- 问题描述： **PVID**和**VID**经常出现于三层交换机里，由于**PVID**和**VID**的设置不合理，造成**VLAN**划分变得混乱。

- 本文结合某地**2826**、**3904**中的故障分析对**PVID**和**VID**进行分析。

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析
—PVID的作用及和VID的区别

- 首先解释一下什么是**PVID**，**PVID**英文解释为**Port-base VLAN ID**，是基于端口的**VLAN ID**。

- **PVID**并不是加在帧头的标记，而是端口的属性，用来标识端口接收到的未标记的帧。

- 也就是说，当端口收到一个未标记的帧时，则把该帧转发到**VID**和本端口**PVID**相等的**VLAN**中去。

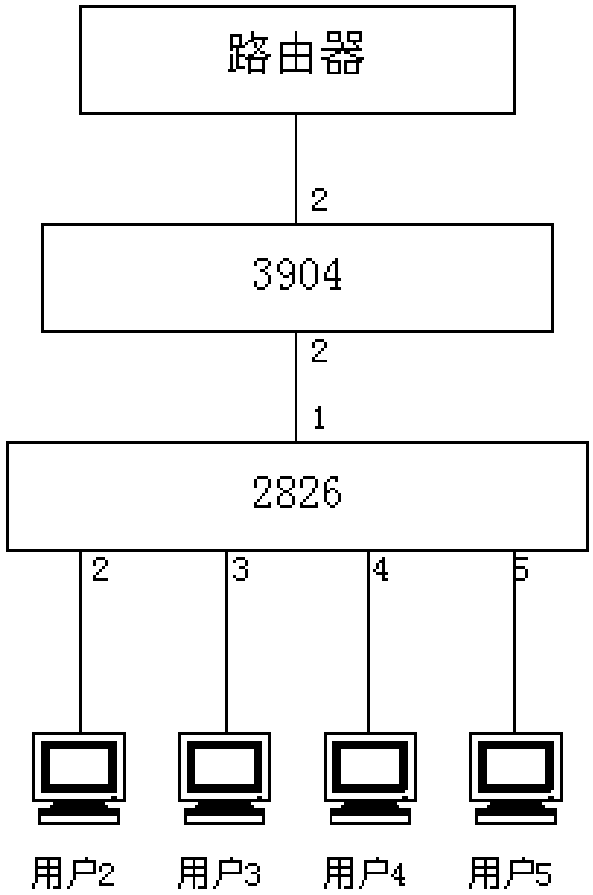
<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

一个故障实例的分析

- 某网组网结构如下图所示，某路由器下挂3904，3904下挂2826，2826下面接了4个用户：
- 其中3904：
  - 接口1上接路由器，打tag标记；
  - 接口2接2826，打tag标记，PVID为1。
- 2826的配置是这样的：
  - 2826的接口1上接3904，打tag标记，属于VLAN 2、3、4、5，PVID为2；
  - 接口2接用户2，属于VLAN 2，PVID为2；
  - 接口3接用户3，属于VLAN 3，PVID为3；
  - 接口4接用户4，属于VLAN 4，PVID为4；
  - 接口5接用户5，属于VLAN 5，PVID为5；



<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

一个故障实例的分析

- 故障现象为：用户2的用户无法上网，而其它的用户可以上网；如果将2826的上连口的PVID值配置为3，那么用户3的用户无法上网，其它的用户可以上网；

- 最后我们将2826的上连口的PVID值设置为1，4个用户的用户就都可以上网了。

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

一个故障实例的分析

- 我们发现，接口1的PVID＝2，故从VLAN 2来的包从接口1出去后不打tag，而此时3904的接口2的PVID＝1，收到未标记得包后，将其送到VLAN 1里。原本VLAN 2的包送到了错误的VLAN里，所以VLAN 2下的用户上不了网。

- 当我们将2826接口1的PVID设为1时，它不等于所属任何VLAN地VID，送出去的包都打了tag，此时3904能根据tag将接受到的包送到正确的VLAN里，故所有VLAN下用户都能上网了。

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

一个故障实例的分析

- 我们可以补充一个实验，将2826的接口1和3904的接口2的PVID都设为2，此时所有用户都能正常上网。

- 原因：2826将VLAN 2的包不打tag的从接口1送出去，3904的接口2收到的包有打tag的（VLAN 3、4、5），也有不打tag的（VLAN 2）。3904的接口2对于打tag的包，能够发往正确的VLAN；不打tag的包，根据接口2的PVID值，送到VID＝PVID的VLAN里，而此时接口2的PVID＝2，也恰巧正确的送到了VLAN 2里。

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析—端口镜像

- 问题描述： 故障现象：一台**T16C**千兆接口连接上光纤后，**LINK**灯不亮

- 解决方案：
- 解决：当时传输设备的网管上显示**T16C**已经发光，对**t16c**做自环测试发现灯也不亮，怀疑灯坏了或者板子有问题，但局方人员说前几天还是好的。原来路由器上做了端口镜像，该千兆口为**target-port**，试验将该配置去掉后，灯亮了。
- 分析：做了端口镜像，千兆接口不能自动进行链路协商了，所以链路起不来

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

CPU占用率高故障一

- 现象描述
- T128路由器的NPCI接口板CPU占用率很高，甚至导致接口板吊死

- 解决方案及步骤
- 执行debug ip icmp看到路由器发出大量的icmp报文，其类型是ttl exceed,这表明路由器收到大量的ttl=1的数据报，这种情况表示网络中存在路由环路，而T128处于环路中间。经过分析，T128上联的cisco7206路由器指过来的静态路由是：

- ip route 222.33.192.0 255.255.248.0 222.62.203.2
- ip route 222.62.203.0 255.255.255.128 222.62.203.2
- 这些都是以后要用到的网段，但目前使用的较少。T128配置了其中几个子网（192.208/28,192.240/28,193-195.0/24,etc）的静态路由，有些配置了静态路由但接口还没有连线使用。而T128是通过缺省路由指向7206的。
- 因此，公网上的病毒扫描(TCP包)这些未用子网，T128就通过缺省路由到7206，7206又通过静态路由返回给T128，因此形成了loop

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

CPU占用率高故障一(续)

- 解决办法，创建一个loopback接口，然后对7206指示的网段做一个静态路由指到loopback接口上，这就是黑洞路由，那么本地没有的路由，数据包都指向loopback扔掉了。

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

CPU占用率高故障二

- 问题描述 T16C的CPU占用率高达90％以上，用户上网感觉慢

- 解决方案 观察上行接口所在槽位的数据流量，system show l3-flow protocol ip module 2；发现有大量的源地址为127.x.x.x的地址向同一个地址发起http连接，连接数量约20多万。启用黑洞路由，ip add route x.x.x.x/32 blackhole，x.x.x.x为被攻击的ip地址。这样cpu占用率下降为2%左右。

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

蠕虫病毒的防范

- 针对可能爆发异常流量的端口应用ACL过滤相应数据包，以控制流量拥塞广域网。

- 1.在全局配置模式下定义ACL：
- zxr10(config)# access-list 101 deny udp any any eq 1434
- zxr10(config)# access-list 101 permit ip any any

- 2.在接口配置模式下，在可能爆发异常流量的端口应用该ACL：
- zxr10(config-if)# ip access-group 101 in

- 此病毒是利用了2002年7月公布的微软SQL Server 2000的一个系统漏洞，对网络上其它系统进行DDos攻击。解决该病毒攻击的根本办法是找到病毒源，进行隔离及并安装相应防漏洞补丁。

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析工具：ping

ping通过向目标主机发送**IP**包并请求目标主机发回一个响应**IP**包以检验本机到一台主机之间的**IP**连接是否可用。一般用法如下：

C:\>ping home.sbell.com.cn ：“**ping**”加主机名
C:\>ping 172.16.2.11 ：“**ping**”加**IP**地址

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析工具:ping

ping完之后，会有下列几种提示信息：

Reply from 172.16.2.11: bytes=32 time=10ms TTL=124
：目标主机发回响应，连接成功
Unknown host www.no.com：无法解析主机名称
Request timed out：主机在指定时间内未响应
Destination host unreachable：无法找到一条通向指定主机的路由

第一种提示信息代表连接成功。
第二种错误提示信息，往往代表了**DNS**服务器设置有问题；
第三种往往代表了目标主机情况不正常；
第四种往往代表了你的路由设置有问题。

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>
univ.zte.com.cn
PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析工具: ipconfig

- **ipconfig**可以查看本机的**IP**设置，如下：

```
C:\>ipconfig

Windows 2000 IP Configuration
Ethernet adapter NE2000:
        Connection-specific DNS Suffix  . : sbell.com.cn
        IP Address. . . . . . . . . . . . : 172.17.4.48
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.17.4.1
```


<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析工具: ipconfig

如果你的PC是通过DHCP的方式来获得IP地址，你可以通过以下命令来释放和重新获得IP地址。

C:\>ipconfig /renew
C:\>ipconfig /release

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析工具: route

route可以查看、管理本机的路由表。使用“**print**”参数可以查看路由表，使用“**add**”、 “**delete**”可以添加、删除路由表。例如：

```
C:\>route print
……
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.17.4.1    172.17.4.48       9
        127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1       1
       172.17.4.0    255.255.255.0    172.17.4.48    172.17.4.48       9
      172.17.4.48  255.255.255.255      127.0.0.1      127.0.0.1       9
   172.17.255.255  255.255.255.255    172.17.4.48    172.17.4.48       9
        224.0.0.0        224.0.0.0    172.17.4.48    172.17.4.48       9
  255.255.255.255  255.255.255.255    172.17.4.48    172.17.4.48       1
Default Gateway:       172.17.4.1
```


<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析工具: tracert

tracert可以跟踪一个**IP**包从本机到目标主机经过的路径，打印经过的每一个路由器的**IP**地址，例如：

C:\>tracert home.sbell.com.cn

Tracing route to bellnet-web2.sbell.com.cn [172.16.2.11]
over a maximum of 30 hops:

1	<10 ms	10 ms	<10 ms	172.17.4.3
2	<10 ms	<10 ms	<10 ms	138.203.220.243
3	20 ms	50 ms	50 ms	138.203.220.253
4	<10 ms	10 ms	10 ms	138.203.221.2
5	30 ms	40 ms	40 ms	bellnet-web2.sbell.com.cn [172.16.2.11]

Trace complete.

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析工具: arp

- 你可以通过以下的命令来显示**arp**表的内容：

D:\>arp -a

Interface: 10.66.1.244 on Interface 0x1000003

Internet Address	Physical Address	Type
10.66.1.48	00-c0-df-b3-30-b9	dynamic
10.66.1.200	00-04-c1-4e-83-c4	dynamic

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析工具－Netstat

- **Netstat**命令可以帮助网络管理员了解网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息，例如显示网络连接、路由表和网络接口信息，可以统计目前总共有哪些网络连接正在运行。

- 利用命令参数，命令可以显示所有协议的使用状态，这些协议包括**TCP**协议、**UDP**协议以及**IP**协议等，另外还可以选择特定的协议并查看其具体信息，还能显示所有主机的端口号以及当前主机的详细路由信息。

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com

故障分析工具－Netstat

- 命令格式：
- **netstat [-r] [-s] [-n] [-a]**
- 参数含义：
- **-r** 显示本机路由表的内容；
- **-s** 显示每个协议的使用状态(包括**TCP**协议、**UDP**协议、**IP**协议)；
- **-n** 以数字表格形式显示地址和端口；
- **-a** 显示所有主机的端口号。

<本文中的所有信息归中兴通讯股份有限公司所有，未经允许，不得外传>

univ.zte.com.cn

PDF 文件以 "FinePrint pdfFactory Pro" 试用版创建 http://www.pdffactory.com