

第 35 章

如何解决网络设备之间工 作机制冲突问题



科来官微



CSNA 公众号

☎ 400-6869-069
🌐 www.colasoft.com.cn
✉ support@colasoft.com.cn

在交换机进行数据转发时，对于 Native VLAN 的数据转发都应该是不打 VLAN 标签的，但是不同核心处理系统的交换机在 VLAN 标签的处理上却有不同的处理机制，如果出现工作机制冲突，网络故障也就会随之而来，正如本案例所示。

35.1 问题描述

35.1.1 基本环境描述

某单位计算机网络由内网系统、外网系统两部分组成，内网负责原内部审计系统的资质审批、上报、核准等重要业务。随着此业务不断发展壮大，现有的内网系统不能适应新业务模式的快速发展，于是将此审计系统全部迁移到新建机房系统。原内网系统将用于普通办公使用，为了节省资金内网系统访问互联网借用外网系统的互联网链路。

设计拓扑结构见如下示图。

内、外网核心对接拓扑简图

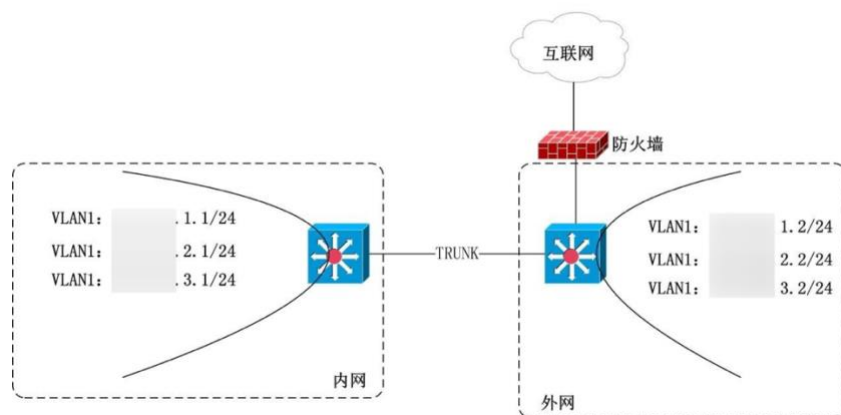


图 35-1

35.1.2 故障现象

内网、外网核心交换机设备对接时启用 TRUNK (802.1q) 链路，VLAN1 为网络管理、VLAN2 和 VLAN3 为正常业务。内、外网核心交换机通过配置后，

TRUNK 链路协商工作正常，但 VLAN1 管理通讯异常，其它 VLAN 正常，此故障严重影响内、外网正常的网络运行维护工作，如下方两图所示。

```
cisco6509#show interfaces trunk

Port      Mode      Encapsulation  Status        Native vlan
Fa1/0     on        802.1q         trunking      1

Port      Vlans allowed on trunk
Fa1/0     1-1005

Port      Vlans allowed and active in management domain
Fa1/0     1-3

Port      Vlans in spanning tree forwarding state and not pruned
Fa1/0     1-3
```

图 35-2

```
cisco6509#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
cisco6509#ping 10.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/80/136 ms
cisco6509#ping 10.3.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.3.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/46/124 ms
cisco6509#
```

图 35-3

35.2 分析方案

35.2.1 分析设备部署

为了能及时、准确分析定位故障原因，现将科来分析系统部署到 TRUNK 链路中，对流经的数据包进行详细分析，部署示意图如下。

内、外网核心对接拓扑简图

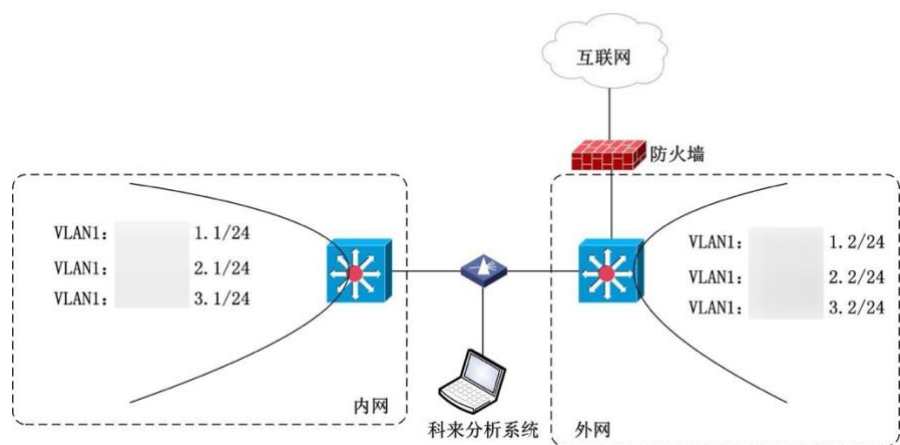


图 35-4

35.2.2 分析过程

从内网核心交换机 Cisco IOS 设备到外网核心交换机 X.X.1.2 地址的数据包抓包结果：

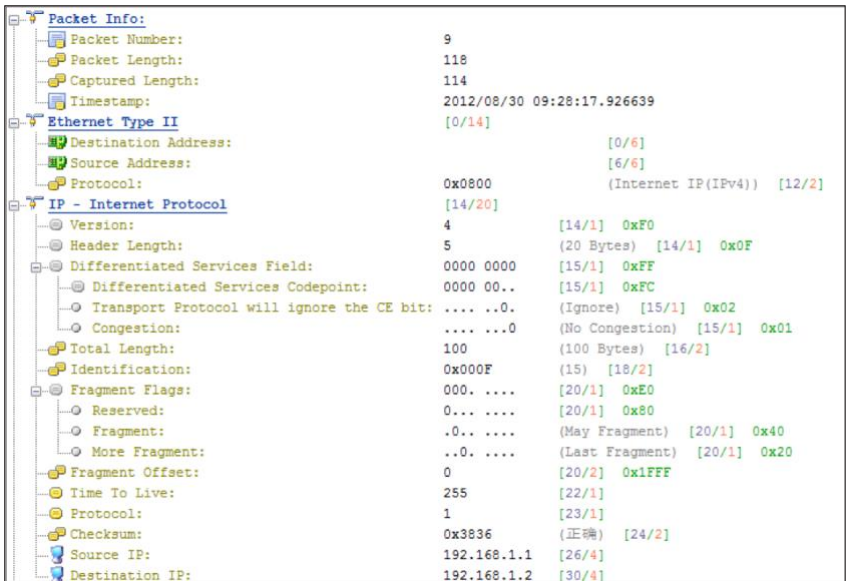
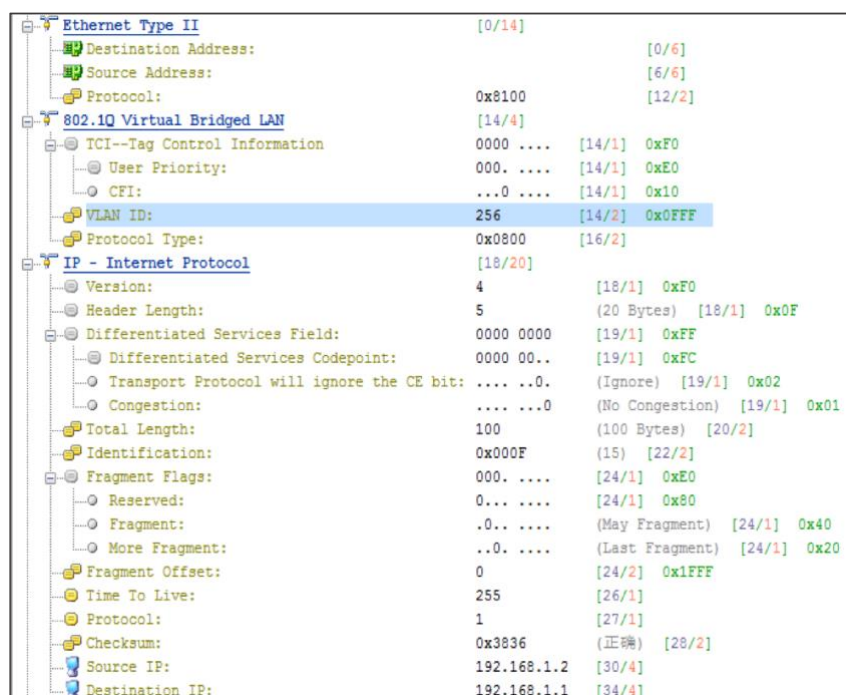


图 35-5

从外网核心交换机 Cisco CatOS 到内网地址 X.X.1.1 的数据包抓包结果：



| | | |
|--|-------------|-----------------------------|
| Ethernet Type II | | [0/14] |
| Destination Address: | | [0/6] |
| Source Address: | | [6/6] |
| Protocol: | 0x8100 | [12/2] |
| 802.1Q Virtual Bridged LAN | | |
| TCI--Tag Control Information | | |
| User Priority: | 0000 | [14/1] 0xF0 |
| CFI: | 000. | [14/1] 0xE0 |
| VLAN ID: | 256 | [14/2] 0x0FFF |
| Protocol Type: | 0x0800 | [16/2] |
| IP - Internet Protocol | | |
| Version: | 4 | [18/1] 0xF0 |
| Header Length: | 5 | (20 Bytes) [18/1] 0x0F |
| Differentiated Services Field: | 0000 0000 | [19/1] 0xFF |
| Differentiated Services Codepoint: | 0000 00.. | [19/1] 0xFC |
| Transport Protocol will ignore the CE bit: |0. | (Ignore) [19/1] 0x02 |
| Congestion: |0 | (No Congestion) [19/1] 0x01 |
| Total Length: | 100 | (100 Bytes) [20/2] |
| Identification: | 0x000F | (15) [22/2] |
| Fragment Flags: | 000. | [24/1] 0xE0 |
| Reserved: | 0... | [24/1] 0x80 |
| Fragment: | .0.. | (May Fragment) [24/1] 0x40 |
| More Fragment: | ..0. | (Last Fragment) [24/1] 0x20 |
| Fragment Offset: | 0 | [24/2] 0x1FFF |
| Time To Live: | 255 | [26/1] |
| Protocol: | 1 | [27/1] |
| Checksum: | 0x3836 | (正确) [28/2] |
| Source IP: | 192.168.1.2 | [30/4] |
| Destination IP: | 192.168.1.1 | [34/4] |

图 35-6

此处的“VLAN ID: 256”实为 VLAN1，Native VLAN 穿越 TRUNK 链路时，CatOS 设备会进行打标。

35.3 分析结论

通过对内、外网核心交换机针对 Native VLAN 数据传输过程的对比，发现导致此次故障的根本原因为 Cisco IOS 和 CatOS 不同处理机制所致。经过查找相关技术文档资料，将 Cisco IOS 调整至为 Native VLAN 也打标后，此故障顺利解决。

35.4 价值

在不同品牌产品对接中，由于各品牌产品的默认处理机制不同，偶尔会出现无法用常规理论解决的问题。通过科来网络分析技术，可以快速发现数据传输过程中的差别，定位到故障根源并解决。

科来网络流量分析解决方案

科来业务性能解决方案

- 科来业务性能管理系统 (UPM)
- 科来网络回溯分析系统 (RAS)
- 科来网络分析系统 (CSNAS)

科来网络安全分析解决方案

- 科来大数据安全态势感知平台 (BAP)
- 科来网络全流量安全分析系统 (TSA)
- 科来APT攻击检测系统 (APT)

CSNA 网络分析认证培训

课程介绍

培训报名

科来网络流量分析技术资料

网络攻击与防范图谱

科来网络通讯协议图

科来网络故障诊断图

CSNA 网络分析经典实战案例

数据包样本

网络分析过滤器

术语表

科来网络流量分析产品下载(免费版)

科来网络分析系统

科来 MAC 地址扫描器

科来 Ping 工具

科来数据包播放器

科来数据包生成器

科来介绍

科来成立于 2003 年，是专注于网络流量分析技术研究与产品开发的高新技术企业，在这一领域有着几十项专利技术和完全独立的自主知识产权。科来研发的产品广泛应用于国内外用户的网络安全分析及网络智能运维等关键领域。科来连续入围 [GartnerNPMD](#) 魔力象限，并荣获“远见者”称号，是唯一入选“远见者”象限的中国企业。科来产品还曾被美国权威评测机构 PC Magazine 评选为《全球最佳科技产品》。

科来专业的技术服务在用户的业务保障上起到关键作用，已经成为对网络时效性高要求的企业的最佳选择，得到了社会各界的广泛认可。同时，科来创办的《CSNA 网络分析认证培训》是我国广具影响力的网络分析认证体系，为国家培养了大量的网络分析技术高级人才。

由于科来公司在网络安全领域的技术优势，受邀为青岛“上合峰会”、多届“两会”、“十九大”、杭州“G20 峰会”、“九三”阅兵、“世界田径锦标赛”、多届“数博会”等重大国家级活动做网络安保工作，做出突出贡献。

- 100 余家世界 500 强企业选择科来
- 为全球 10000 余家商业客户提供网络分析解决方案
- 全球 90 余万用户正在使用科来的产品
- 科来的技术服务于世界 110 个国家和地区