

# 某网络专业人士排错笔记

## 第1章 故障处理方法

### 一、网络的复杂性

一般网络包括路由、拨号、交换、视频、WAN（ISDN、帧中继、ATM、...）、LAN、VLAN、...

### 二、故障处理模型

#### 1、 界定问题（Define the Problem）

详细而精确地描述故障的症状和潜在的原因

#### 2、 收集详细信息（Gather Facts）R>信息来源：关键用户、网络管理系统、路由器/交换机

##### 1) 识别症状：

##### 2) 重现故障：校验故障依然存在

##### 3) 调查故障频率：

##### 4) 确定故障的范围：有三种方法建立故障范围

？ 由外到内故障处理（Outside-In Troubleshooting）：通常适用于有多个主机不能连接到一台服务器或服务集

？ 由内到外故障处理（Inside-Out Troubleshooting）：

？ 半分故障处理（Divide-by-Half Troubleshooting）

#### 3、 考虑可能情形（Consider Possibilities）考虑引起故障的可能原因

#### 4、 建立一份行动计划（Create the Action Plan）

#### 5、 部署行动计划（Implement the Action Plan）

用于纠正网络故障原因。从最象故障源处，想出处理方法每完成一个步骤，检查故障是否解决

#### 6、 观察行动计划执行结果（Observe Results）

#### 7、 如有行动计划不能解决问题，重复上述过程（Iterate as Needed）

### 三、记录所做修改

在通过行动计划解决问题后，建议把记录作为故障处理的一部分，记录所有的配置修改。

## 第2章 网络文档

### 一、网络基线

解决网络问题的最简单途径是把当前配置和以前的配置相比较。

基线文档由不同的网络和系统文档组成，它包括：

？ 网络配置表

？ 网络拓扑图

? ES 网络配置表

? ES 网络拓扑图

创建网络的注意事项:

- 1) 确定文档覆盖的范围;
- 2) 保持一致: 收集网络中所有设备的相同信息;
- 3) 明确目标: 了解文档的用途;
- 4) 文档易于使用和访问;
- 5) 及时维护更新文档。

## 二、网络配置表

网络配置表的通常目标是提供网络中使用的硬件和软件组成的列表, 其组成有:

分级 项目

杂项信息 设备名、设备型号、CPU 类型、FLASH、DRAM、接口描述、用户名口令

第 1 层 介质类型、速率、双工模式、接口号、连接插座或端口

第 2 层 MAC 地址、STP 状态、STP 根桥、速端口信息、VLAN、Etherchannel 配置、封装、中继状态、接口类型、端口安全、VTP 状态、VTP 模式

第 3 层 IP 地址、IPX 地址、HSRP 地址、子网掩码、路由协议、ACL、隧道信息、环路接口

在多数情形下, 存储这些信息的最佳方式是电子表格或数据库, 电子表格用于较小的网络, 数据库用于较大的网络。

## 三、网络拓扑图

网络拓扑图是图示网络的各组成部分之间如何在逻辑上和物理上相互连接。

### 1、网络拓扑图的组成

分级 项目

杂项信息 设备名、设备型号、设置间连接、接口描述

第 1 层 介质类型、接口号

第 2 层 MAC 地址、VLAN、封装、中继状态、接口类型、DLCI

第 3 层 IP 地址、子网掩码、路由协议

对于大型的网络, 可以制作多个网络拓扑图, 每个网络拓扑图反映一个分离的部分。

### 2、建立网络拓扑图

## 四、发现网络配置信息

### 1、收集路由器和第 3 层交换机网络配置信息

show version ; 显示设备型号、Flash、DRAM、IOS 版本

show ip interface brief ; 显示接口简要信息 (类型、状态、协议状态、IP 地址)

show interface e0/0 ; 显示某接口详细信息 (MAC、IP、MASK、...)

show ip protocols ; 显示 IP 路由协议信息

show ip interface e0/0 ; 显示接口的 IP 协议信息 (状态、IP 地址、ACL、...)

## 2、收集交换机配置信息

交换机网络配置表包含的信息: 设备名、型号、位置、Flash、DRAM、CATOS 版本、管理地址、VTP 域、VTP 模式、端口号、端口速率、端口双工、VLAN、STP 状态、速端口状态、中继状态、...

show version ; 显示 IOS 或 CATOS 版本、DRAM、Flash

show vtp domain ; (CatOS) 显示 VTP 域和 VTP 模式

show vtp status ; (IOS)

show interface ; (CatOS) 显示管理接口信息

show port ; (CatOS) 显示每个端口的简要信息 (号、VLAN、双工、...)

show interface ; (IOS)

show trunk ; (CatOS) 显示中继信息 (模式、封装、允许端口、剪裁、...)

show interface trunk ; (IOS)

show spantree 45 ; (CatOS) 显示端口的 STP 模式、类型、状态、速端口、...)

show spanning-tree 45 ; (IOS)

## 3、发现相邻 CISCO 设备的信息

CDP (Cisco Discovery Protocol) 是 CISCO 的专用协议, 用于识别直接相邻的 CISCO 设备信息, CDP 工作在第 2 层。

Show cdp neighbor ; 显示相邻 CISCO 设备的简要信息 (ID、相邻接口、平台、...)

Show cdp neighbor detail; 显示相邻 CISCO 设备的详细信息 (包含第 3 层信息)

## 五、创建网络文档的过程

- 1、LOGIN ; 登录到设备进入特权模式。
- 2、接口发现 ; 发现关于设备的所需信息
- 3、document ; 在网络配置表中记录发现的信息。
- 4、Diagram ; 从网络配置表传输所需信息到网络拓扑图
- 5、设备发现 ; 判断是否有相邻设备没有记录文档。

## 第 3 章 ES 文档和故障处理

### 一、ES 网络配置表

ES 网络配置表是 ES 的硬件和软件组成的列表。ES 网络配置常包括以下项目:

分级 项目

杂项信息 系统名、系统厂商/型号、CPU 速率、RAM、存储器、系统功能

第 1、2 层 介质类型、接口速率、VLAN、MAC、网络接头

第 3 层 IP 地址、缺省网关、子网掩码、WINS、DNS、

第 7 层 操作系统（版本）、基于网络的应用程序、高带宽应用程序、低延时应用程序、特定考虑

## 二、ES 网络拓扑图

ES 网络拓扑图的典型项目有：系统名、网络连接、物理位置、系统目标、VLAN、IP 地址、子网掩码、操作系统、网络应用程序

大多数 ES 网络拓扑图都建立在网络拓扑图中，其中还可加入 ES 网络配置表数据的子集。

## 三、收集 ES 网络配置信息

通用命令：

- 1) ping host/ip-address ; 发送和接收 ICMP 响应，校验网络的连通性
- 2) arp -a ; 查看修改 ES 的 MAC-IP 映射表（同一子网）
- 3) telnet host/ip-address ; 登录远程 ES 或特定 TCP 端口

Windows 平台命令

- 1) ipconfig /all ; 查看修改 ES 的 IP 信息（适用所有 Windows 平台）
- 2) winipcfg ; 查看修改 ES 的 IP 信息（仅适用于 Win9x 平台）
- 3) tracert host/ip-address ; 校验到主机的连接并显示路径上的设备 IP
- 4) route print ; 显示本设备 IP 路由表的内容
- 5) netstat ; 显示当前网络连接

Unix、Linux 和 Mac OS 系统命令

- 1) ifconfig -a ; 查看 UNIX 和 MAC 主机的 IP 信息
- 2) traceroute host/ip ;
- 3) route -n ;
- 4) cat /etc/resolv.conf ; 查看 DNS 服务器信息

## 四、通用的故障处理过程

1、通用的故障处理过程：

1 收集症状：收集网络、用户、ES 的症状

- 1) 分析现存症状
- 2) 判断所属
- 3) 窄化范围
- 4) 判定症状
- 5) 记录症状

1 分离问题

- 1) Bottom-Up troubleshooting

从物理层开始向上排查，直到应用层。常用于怀疑问题发生在物理层，或在处理复杂网络问题时

使用。

## 2) Top-Down troubleshooting

从应用层开始向下排查故障，用于怀疑问题发生在软件部分。

## 3) Divide-and-Conquer troubleshooting

选择 OSI 模型的特定层（数据链路层、网络层、传输层）开始故障处理，确定问题是在该层、还是上层或下层。适于具有丰富的经验的人员使用。

常用 traceroute 命令检查下 4 层（从物理层到应用层）。

### 1 纠正问题

### 2、ES 故障处理命令

#### 1) ping

连续 Ping: ping -t 192.168.0.1 ; Windows 系统

ping -s 192.168.0.1 ; Unix 环境

记录路由: ping -r 192.168.0.1 ; Windows

ping -s -nRv 192.168.0.1 ; Unix

#### 2) Trace Route

Tracert 10.0.0.1 ; Windows 系统

Tracerout 10.0.0.1 ; Unix

Ping 记录路由器的出接口，而 traceroute 通常记录进入的接口。

#### 3) Arp

显示第 2 层和第 3 层地址的映射表: Arp -a ; Windows/Unix

#### 4) Route

显示路由表: route print ; windows 系统

route -n ; Unix

#### 5) Netstat

显示到 ES 的当前连接及端口: netstat -n ; Windowx & Unix

#### 6) Ipconfig&Ifconfig

显示 ES 的 IP 配置: ipconfig /all ; windows

ifconfig -a ; unix

#### 7) Nbtstat

显示当前名称解析缓存: nbtstat -c ;

清除当前名称解析缓存: nbtstat -r ;

## 第 4 章 协议属性

### 一、OSI 参考模型

应用层

表示层

会话层

传输层

网络层

数据链路层

物理层

## 二、全局协议分类

### 1、面向连接的协议：

windows size：在需要目标系统确认的传输的数据包数。

队列数据传送：对进入和发送的 PDU 指定序号，在目的地再按序号重排数据；

流控：确保发送的速率不超过目标接收的速率，通过为传输建立窗口尺寸实现；

错误控制：确保接收到的数据连续并无错，如有丢失或损失的 PDU，则不发送 ACK 包。

面向连接的协议有：ATM、TCP、Novell SPX、Apple Talk ATP；

### 2、非连接的协议

不包括连接设置和终止，没有流控和错误控制。

非连接的协议有：UDP、Apple Talk DDP、Novell IPX；

## 三、第 2 层：数据链路层

1、Ethernet/IEEE802.3

2、Token Ring/IEEE802.5

四、PPP

五、SDLC

六、Frame Relay

七、ISDN

## 八、第 3、4 层：IP 路由协议

1、IP

2、ICMP

3、TCP

4、UDP

## 第 5 层 Cisco 测试命令和 TCP/IP 连接故障处理

### 一、故障处理命令

1、show 命令：

1) 全局命令：

show version ; 显示系统硬件和软件版本、DRAM、Flash  
show startup-config ; 显示写入 NVRAM 中的配置内容  
show running-config ; 显示当前运行的配置内容  
show buffers ; 详细输出 buffer 的名称和尺寸  
show stacks ; 提供路由器进程和处理器利用率信息, 用 stack decode  
show tech-support ; 显示几个 show 命令的输出  
show access-lists ; 查看访问列表配置  
show memory ; 用于测试内存问题

## 2) 接口相关命令

show queueing [fair|priority|custom]  
show queue e0/1 ; 查看接口上队列的设置和操作  
show interface e0/1 ; Cisco 缺省的 Ethernet 封装方法是 ARPA  
show ip interface e0/1 ; 显示指定接口的 TCP/IP 配置信息

## 3) 进程相关命令

show processes cpu ; 显示路由器 CPU 的使用率和当前的进程  
show processes memory ; 显示路由器当前进程的内存使用情况

## 4) TCP/IP 协议相关命令

Show ip access-list ; 显示 IP 访问列表 (1-199)  
Show ip arp ; 显示路由器的 ARP 缓存 (IP、MAC、封装类型、接口)  
Show ip protocols ; 显示运行在路由器上的 IP 路由协议的信息  
Show ip route ; 显示 IP 路由表中的信息  
Show ip traffic ; 显示 IP 流量统计信息

## 2、debug 命令

DEBUG 不应在 CPU 使用率超过 50% 的路由器上运行。

### 1) 限制 debug 输出

在使用 DEBUG 获得所需数据后, 要关闭 Debug

使路由器对所有消息都配置使用时间戳:

```
Router#service timestamps debug datetime msec localtime
```

```
Router#service timestamp log datetime msec localtime
```

缺省, error 和 debug 信息仅发送到 console, telnet 到路由器上看不到 debug 和 log 的信息。

想在 telnet 中看到 debug 和 log 信息:

```
Router#terminal monitor
```

Router#terminal monitor ; 关闭信息输出

Router#undebug all ; 关闭 debug 进程及所有相关信息的输出

可以应用 ACL 到 debug 以限定仅输出要求的 debug 信息。

如仅查看从 10.0.1.1 到 10.1.1.1 的 ICMP 包:

```
Router(config)#access-list 101 permit icmp host 10.0.1.1 host 10.1.1.1
```

```
Router#debug ip packet detail 101
```

2) 全局 debug 命令:

3) 接口 debug

4) 协议 debug

5) IP debug

```
debug ip packets
```

### 3、logging 命令

输出 error 和其它信息到 console、terminal、路由器内部 buffer 或一台 syslog 服务器:

```
Router>show logging
```

Cisco 路由器有 8 种可能的 logging 级: 0-7

Logging 级别 名称 描述

1 Emergencies 系统不能用的信息

2 Alerts 直接行动

3 Critical 紧急情形

4 Errors 错误信息

5 Warnings 警告信息

6 Notifications 正常但重要的情形

7 Informational 信息

8 Debugging 调试

缺省地, console、monitor、buffer 的 logging 被设置为 debugging 级, 而 trap (syslog) 服务器的 logging 被设置为 informational。

### 4、执行路由核心复制

core dump 包含一份当前系统内存中信息的精确拷贝。捕捉包含在内存中信息的方法有:

1) 配置路由器在崩溃时执行 Core Dump, 存储到 TFTP、FTP、RCP 服务器:

对 TFTP 协议, 只需指定 TFTP 服务器 IP, 不需要任何附加的配置:

```
Router(config)#exception dump 192.168.1.1 ; TFTP 服务器的 IP 地址
```

对 FTP 协议的配置:

```
Router(config)#exception dump 192.168.1.1 ; FTP 服务器的 IP 地址
```

```
Router(config)#ip ftp username Kevin
```

```
Router(config)#ip ftp password aloha
```

```
Router(config)#ip ftp source-interface e0
```

```
Router(config)#exception protocol ftp
```



对 RCP 协议的配置:

```
Router(config)#exception protocol rcp
```

```
Router(config)#exception dump 192.168.1.1 ; RCP 服务器的 IP 地址
```

```
Router(config)#ip rcmd remote-username Kevin
```

```
Router(config)#ip rcmd rcp-enable
```

```
Router(config)#ip rcmd rsh-enable
```

```
Router(config)#ip rcmd remote-host Kevin 192.168.1.1 kevin ;
```

2) 在系统没有崩溃的情况下, 执行 Core Dump 命令。

```
Router#write core
```

Core Dump 仅在 Cisco 工程师测试和解决路由器问题时有用。

## 5、ping 命令

ping 用于测试整个网络可达性和连通性。可在用户 EXEC 模式和特权 EXEC 模式下使用。

IP 的 ping 使用 ICMP 协议提供连通性和可能性信息, 缺省只发送 5 个 echo 信息。

扩展 Ping 的选项有: 源 IP 地址; 服务类型; 数据; 包头选项。

Ping 的响应字符集

字符 解释 字符 解释

! Received an echo-reply message Q Source quench

. Timeout M Unable to fragment

U/H Destination unreachable A Administratively denied

N Network unreachable ? Unknown packet-type

P Protocol unreachable

## 6、traceroute 命令

traceroute 用于显示到达目标的包路径。可在用户模式和特权模式下使用。

Traceroute 的响应:

字符 解释 字符 解释

Xx msec The RTT for each packet \* Timeout

H Host unreachable U Port unreachable

N Network unreachable P Protocol unreachable

A Administratively denied Q Source quench

? Unknown packet type

## 二、LAN 连接问题

### 1、获得 IP 地址

主机可以动态或静态获得 IP 地址。

1) DHCP: DHCP 比 BootP 多了地址池和租期。

2) BootP:

3) Helper Addresses: 指定集中放置的 DHCP 服务器的 IP 地址

Ip helperaddress ip-address ;

No ip forward-protocol udp 137 ;

4) 路由器上的 DHCP 服务: 配置路由器为一台 DHCP 服务器

5) DHCP 和 BootP 故障处理

Show dhcp server ;

Show dhcp lease ;

2、ARP

ARP 映射第 2 层 MAC 地址到第 3 层地址。

Show arp ; 显示路由器的 ARP 表

Debug arp ;

1) ARP 代理: 缺省 Cisco 路由器的 ARP 代理是启用的

在下列情况下, CISCO 路由器将用自身的 MAC 地址响应 ARP 请求:

? 接收到 ARP 的接口上的 Proxy ARP 是启用的;

? ARP 请求的地址不在本地子网;

? 路由器的路由表中包含 ARP 请求地址的子网;

3、TCP 连接示例

三、IP 访问列表

1、标准 ACL: 基于 IP 包的源 IP 地址允许或禁用

2、扩展 ACL: 提供源地址、目标地址、端口号、会话层协议进行过滤。

3、命名 ACL: 可以是标准 ACL, 也可以是扩展 ACL。

命名 ACL 与编号 ACL 的区别: 命名 ACL 有一个逻辑名, 可以删除命名 ACL 中单独一行。

Ip access-list extended Example-Named-ACL

Deny tcp any any eq echo

Deny tcp any any eq 37

Permit udp host 172.16.10.2 any eq snmp

Permit tcp any any

## 第 6 章 TCP/IP 路由协议故障处理

一、缺省网关

当包的目的地址不在路由器的路由表中, 如路由器配置了缺省网关, 则转发到缺省网关, 否则就丢弃。

Show ip route ; 查看 Cisco 路由器的缺省网关

## 二、静态和动态路由

### 三、处理 [k\\_protocol/04937.htm](http://k_protocol/04937.htm) >RIP 故障

RIP 是距离矢量路由协议，度量值是跳数。RIP 最大跳数为 15，如果到目标的跳数超过 15，则为不可达。

RIP V1 是有类别路由协议，RIP V2 是非分类路由协议，支持 CIDR、路由归纳、VLSM，使用多播（224.0.0.9）发送路由更新。

RIP 相关的 show 命令：

Show ip route rip ; 仅显示 RIP 路由表

Show ip route ; 显示所有 IP 路由表

Show ip interface ; 显示 IP 接口配置

Show running-config

Debug ip rip events ;

常见的 RIP 故障：RIP 版本不一致、RIP 使用 UDP 广播更新

## 四、处理 IGRP 故障

IGRP 是 Cisco 专用路由协议，距离矢量协议。IGRP 的度量值可以基于五个要素：带宽、延时、负载、可靠性、MTU，缺省只使用带宽和延时。

IGRP 相关的 show 命令：

Show ip route igrp ; 显示 IGRP 路由表

Debug ip igrp events ;

Debug ip igrp transactions ;

常见的 IGRP 故障：访问列表、不正确的配置、到相邻路由器的 line down

## 五、处理 EIGRP 故障

EIGRP 是链路状态协议和距离矢量混合协议，是 CISCO 专用路由协议。EIGRP 使用多播地址 224.0.0.10 发送路由更新，使用 DUAL 算法计算路由。EIGRP 的度量值可以基于带宽、延时、负载、可靠性、MTU，缺省仅使用带宽和延时。

EIGRP 使用 3 种数据库：路由数据库、拓扑数据库、相邻路由器数据库。

EIGRP 相关的 show 命令：

Show running-config

Show ip route

Show ip route eigrp ; 仅显示 EIGRP 路由

Show ip eigrp interface ; 显示该接口的对等体信息

Show ip eigrp neighbors ; 显示所有的 EIGRP 邻居及其信息

Show ip eigrp topology ; 显示 EIGRP 拓扑结构表的内容

Show ip eigrp traffic ; 显示 EIGRP 路由统计的归纳

Show ip eigrp events ; 显示最近的 EIGRP 协议事件记录

EIGRP 相关的 debug 命令:

Debug ip eigrp as 号

Debug ip eigrp neighbor

Debug ip eigrp notifications

Debug ip eigrp summary

Debug ip eigrp

常见的 EIGRP 故障: 相邻关系、缺省网关等的丢失、老版本 IOS 的路由、stuck in active。

处理 EIGRP 故障时, 先用 show ip eigrp neighbors 查看所有相邻路由器, 然后再用 show ip route eigrp 查看路由器的路由表, 再用 show ip eigrp topology 查看路由器的拓扑结构表, 也可用 show ip eigrp traffic 查看路由更新是否被发送。

## 六、处理 OSPF 故障

OSPF 是链路状态协议, 维护 3 个数据库: 相邻数据库、拓扑结构数据库、路由表。

OSPF 相关的 show 命令:

Show running-config

Show ip route

Show ip route ospf ; 仅显示 OSPF 路由

Show ip ospf process-id ; 显示与特定进程 ID 相关的信息

Show ip ospf ; 显示 OSPF 相关信息

Show ip ospf border-routers ; 显示边界路由器

Show ip ospf database ; 显示 OSPF 的归纳数据库

Show ip ospf interface ; 显示指定接口上的 OSPF 信息

Show ip ospf neighbor ; 显示 OSPF 相邻信息

Show ip ospf request-list ; 显示链路状态请求列表

Show ip ospf summary-address ; 显示归纳路由的再发布信息

Show ip ospf virtual-links ; 显示虚拟链路信息

Show ip interface ; 显示接口的 IP 设置

OSPF 相关的 debug 命令:

Debug ip ospf adj ;

Debug ip ospf events

Debug ip ospf flood

Debug ip ospf lsa-generation

```
Debug ip ospf packet
Debug ip ospf retransmission
Debug ip ospf spf
Debug ip ospf tree
```

常见的 OSPF 故障：OSPF 的每个 area 不超过 100 台路由器，整个网络不超过 700 台路由器；通配符掩码配置不当；

## 七、处理 BGP 故障

BGP（包括 IBGP 和 EBGP）的关键配置是邻居关系，BGP 使用 TCP 建立相邻关系。

BGP 相关的 show 命令：

```
Show ip bgp ; 显示 BGP 所学习到的路由
Show ip bgp network ; 显示特定网络的 BGP 信息
Show ip neighbors ; 显示 BGP 邻居信息
Show ip bgp peer-group ; 显示 BGP 对等组信息
Show ip bgp summary ; 显示所有 BGP 连接的归纳
Show ip route bgp ; 显示 BGP 路由表
```

BGP 相关的 debug 命令：

```
Debug ip bgp 192.1.1.1 updates
Debug ip bgp dampening
Debug ip bgp events
Debug ip bgp keepalives
Debug ip bgp updates
```

典型的 BGP 故障：

## 八、再发布路由协议

## 九、TCP/IP 症状和原因

症状 原因

本地主机不能与远程主机通讯 1) DNS 工作不正常 2) 没有到远程主机的路由 3) 缺少缺省网关 4) 管理拒绝 (ACL)

某个应用程序不能正常工作 1) 管理拒绝 (ACL) 2) 网络没有正常配置以处理该应用程序

启动失败 1) BootP 服务器没有 MAC 地址的实体 2) 缺少 IP helper-address 3) ACL 4) 修改 NIC 或 MAC 地址 5) 重复的 IP 地址 6) 不正常的 IP 配置

不能 ping 远程主机 1) ACL 2) 没有到远程主机的路由 3) 没有设置缺省网关 4) 远程主机 down

缺少路由 1) 没有正确配置路由协议 2) 发布列表 3) 被动接口 4) 没有通告路由的邻居 5)

路由协议版本不一致 6) 邻居关系没有建立

相邻关系没有建立 1) 不正确的路由协议配置 2) 不正确的 IP 配置 3) 没有配置 network 或 neighbor 语句 4) hello 间隔不一致 5) 不一致的 area ID

高的 CPU 利用率 1) 不稳定的路由更新 2) 没有关闭 debug 3) 进程过重

路由触发活跃模式 1) 不一致的间隔 2) 硬件问题 3) 不稳定的链路

## 十、TCP/IP 症状和行动计划

问题 行动计划

DNS 工作不正常 1) 配置 DNS 主机的配置和 DNS 服务器, 可以使用 nslookup 校验 DNS 服务器的工作

没有到远程主机的路由 1) 用 ipconfig /all 检查缺省网关 2) 用 show ip route 查看是否相应路由 3) 如果没有该路由, 用 show ip route 查看是否有缺省网关 4) 如有网关, 检查到目标的下一跳; 如无网关, 修正问题

ACL 有分离的问题与 ACL 相关, 必须分析 ACL、或重写 ACL 并应用。

网络没有配置以处理应用程序 查看路由器配置

Booting 失败 1) 查看 DHCP 或 BootP 服务器, 并查看是否存在故障机的 MAC 实体 2) 使用 debug ip udp 校验从主机接收的包 3) 校验 helper-address 正确配置 4) 查看 ACL 是否禁用包

缺少路由 1) 在第 1 台路由器上用 show ip route 查看所学到的路由 2) 校验相邻路由器 3) 有正确的路由 network 和 neighbor 语句 4) 对 OSPF, 校验通配符掩码 5) 检查应用到接口上的 distribute list 6) 验证邻居的 IP 配置 7) 如果路由被再发布, 验证度量值 8) 验证路由被正常的再发布

没有构成相邻关系 1) 用 show ip protocol neighbors 列表已构成的相邻关系 2) 查看没有构成相邻关系的协议配置 3) 检查路由配置中的 network 语句 4) 用 show ip protocol/interface 查看特定的接口信息, 如 Hello 间隔

## 第 7 章 处理串行线路和帧中继连接故障

### 一、处理串行线路故障

#### 1、HDLC 封装

High-level Data Link Control (HDLC) 是用于串行链路的一种封装方法, HDLC 是 Cisco 路由器串行接口的缺省封装方法。

处理串行链路故障的第一步就是查看链路两端要使用相同的封装类型。

Show interface serial 1 ; 查看接口信息

Clear counters serial number ; 复位接口的计数器到 0

正常情况下, 接口和 line 都是 up 的。

线缆故障、载波故障和硬件故障都可导致接口 down, 通过校验电缆连接、更换硬件 (包括电缆)、

检查载波信令定位问题。

接口 up, line down: CSU/DSU 故障、路由器接口问题、CSU/DSU 或载波的时间不一致、没有从远端路由器接收到 keepalive 信令、载波问题。应验证本地接口和远端接口的配置。

接口重启的原因:

- ? 数秒内排队的包没有被发送;
- ? 硬件问题 (路由器接口、线缆、CSU/DSU);
- ? 时钟信令不一致
- ? 环路接口
- ? 接口关闭
- ? 线协议 down 且接口定期重启

show controllers serial 0 ; 显示接口状态、是否连有电缆、时钟速率

show buffers ; 查看系统 buffer 池, 接口 buffer 设置

debug serial interface ; 显示 HDLC 或 Frame Relay 通信信息

## 2、CSU/DSU 环路测试

有四种类型的环路测试:

- ? 在本地 CSU/DSU 上测试本地环路;
- ? 在远端 CSU/DSU 上测试本地环路;
- ? 从本地 NIU 到远端 CSU/DSU 测试远端环路;
- ? 从远端 NIU 到本地 CSU/DSU 测试远端环路;

用 PPP 封装的串行链路上, PPP 用协商 Magic Number 检测环回网络。

## 3、串行线中总结:

### 1) 症状和问题:

症状或情形 问题

Interface is administratively down;line protocol is down 1) 接口被从命令行关闭 2) 不允许重复的 IP 地址, 两个使用相同 IP 地址的接口将 down

Interface is down;line protocol is down 1) 不合格的线缆 2) 没有本地提供商的信令 3) 硬件故障 (接口或 CSU/DSU、线缆) 4) 时钟

Interface is up;line protocol is down 1) 未配置的接口: 本地或远程 2) 本地提供商问题 3) Keepalive 序号没有增加 4) 硬件故障 (本地或远端接口、CSU/DSU) 5) 线路杂音 6) 时钟不一致 7) 第 2 层 (如 LMI)

Interface is up;line protocol is up(looped) 链路在某处环路

Incrementing carrier transition counter 1) 来自本地提供商的信号不稳定 2) 线缆故障 3) 硬件故障

Incrementing interface resets 1) 线缆故障, 导致 CD 信号丢失 2) 硬件故障 3) 线路拥塞

Input drops, errors, CRC, and framing errors 1) 线路速率超过接口能力 2) 本地提供商问题 3) 线路杂音 4) 线缆故障 5) 不合格线缆 6) 硬件故障

Output drops 接口传输能力超过线路速率

## 2) 问题和行动

问题 解决行动方案

本地提供商问题 1) 检查 CSU/DSU 的 CD 信号和其它信号, 看链路是否在发送和接收信息 2) 如果没有 CD 信号或有其它问题, 联系本地提供商处理故障

不合格或故障的线缆 1) 使用符合设备要求的线缆 2) 使用 breakout 盒检查 3) 交换故障线缆

未配置的接口 1) 使用 show running-config 校验接口配置 2) 确认链路两端使用相同的封装类型

Keepalive 问题 1) 验证 keepalive 被发送 2) 配置了 keepalive 发送, debug keepalive 3) 验证序号在增加 4) 如果序号不增加, 运行环路测试 5) CSU/DSU 环路, 序号仍不增, 则硬件故障

硬件故障 1) 更换硬件

接口在环路模式 1) 检查接口配置 2) 如果在接口配置有环路, 移除 3) 如果接口配置被清除, 清除 CSU/DSU 环路模式 4) 如 CSU/DSU 不在环路模式, 可能是提供商置环

接口 administratively down 1) 检查是否有重复的 IP 地址 2) 进行接口配置模式, 执行 no shutdown

线路速率大于接口能力 1) 使用 hold-queue 减少进入的队列尺寸 2) 增加输出的队列尺寸

接口速率大于线路速率 1) 减少广播流量 2) 增加输出的队列 3) 如有需要, 使用队列算法

## 二、处理帧中继故障

DLCI 用于在帧中继中标识虚拟链路, DLCI 仅仅是本地信令, DLCI 与第 3 层 IP 地址相映射。

处理帧中继的步骤:

- 1) 检查物理层, 线缆或接口问题;
- 2) 检查接口封装;
- 3) 检查 LMI 类型;
- 4) 校验 DLCI 到 IP 的映射;
- 5) 校验 Frame Delay 的 PVC;
- 6) 校验 Frame Delay 的 LMI;
- 7) 校验 Frame Delay 映射;
- 8) 校验环路测试;

### 1、帧中继的 show 命令

show interface

show frame-relay lmi ; 显示 LMI 相关信息 (LMI 类型、更新、状态)

show frame-relay pvc ; 输出 PVC 信息、每条 DLCI 的 LMI 状态、...

show frame-relay map ; 提供 DLCI 号信息和所有 FR 接口的封装

### 2、帧中继的 debug 命令



debug frame-relay lmi ; 显示 LMI 交换信息

debug frame-relay events ; 显示协议和应用程序使用 DLCI 的细节

### 3、帧中继总纳

#### 1) 症状和问题

症状或情形 相关问题

Frame Relay link is down 1) 线缆故障 2) 硬件故障 3) 本地服务商问题 4) LMI 类型不一致 5) Keepalive 没有被发送 6) 封装类型不一致 7) DLCI 不一致

从 Frame Relay 网络不能 ping 远端主机 1) DLCI 指定了错误的接口 2) 封装类型不一致 3) ACL 问题 4) 接口配置错误

#### 2) 问题和行动

问题 解决行动方案

线缆故障 1) 检查线缆并测试接头 2) 更换线缆

硬件故障 1) 执行环路测试, 以分离硬件 2) 将线缆连接到路由器的另一同样配置的接口, 如 OK, 则需更换硬件

本地服务提供商问题 1) 如环路测试使 LMI 状态 up, 但不能连接远端站点, 联系本地载波 2) 包含载波问题, 就好象 FR 配置错误, 如 DLCI 不一致或封装不一致。

LMI 类型不一致 1) 校验路由器的 LMI 类型与 PVC 上的每个设备都一致 2) 如使用公共提供商网络, 不能访问 LMI, 与提供商联系

Keepalive 问题 1) 使用 show interface 查看是否 keepalive 被禁用, 或校验 keepalive 被正常配置 2) 如果 keepalive 设置错误, 进入配置模式并在接口上指定 keepalive 间隔

封装类型 1) 校验两端路由器的封装方式相同, 如有非 Cisco 路由器, 必须用 IETF。用 show frame-relay 命令显示封装信息 2) 用 encapsulation frame-relay ietf 更换封装方式, 与可用 frame-relay map 设置某个 PVC 的封装。

DLCI 不一致 1) 用 show running-config 和 show frame-relay pvc 显示指派给某接口的 DLCI 号 2) 如 DLCI 号配置正常, 联系供应商校验 FR 交换机是否了相同的 DLCI

ACL 问题 1) 使用 show ip interface 显示应用到接口上的 ACL 2) 分析 ACL, 如有需要, 删除或修改它

## 第 8 章 处理 ISDN 故障

### 一、ISDN 基本原理

### 二、常见 ISDN 故障

ISDN 问题分成 3 类: 配置不当的路由器、物理线缆和 ISDN 协议、配置不当的交换机。

#### 1、配置不当的路由器

配置不当由于不同原因: typographical 错误、从服务提供商提供的错误信息、本路由器配置不正确

1) SPID (Service Profile Identifiers) :如 SPID 和 LDN 配置错误, 将有 ISDN 连接问题。SPID 仅用于北美, 只有服务供应商要求时才设置。

2) CHAP: CHAP 认证在使用 PPP 封装的接口上使用。两端路由器的 CHAP 配置一定要相同。在 PPP 中, 用户名和口令是大小写敏感的。

3) Dialer Map 实体: Dialer map 关联高层地址到相关的电话号码。每种协议需要一条 dialer map 语句。

4) 访问列表: ACL 可用于 ISDN 连接以阻止某类型流量触发连接。

5) PPP:

## 2、物理层连接

1) BRI: 在现有电话线上提供数字服务。

2) ISDN BRI 信道:  $2B+D(2*64+16+48=192\text{kbps})$ ; ISDN BRI 的物理帧为 48bits, 链路每秒发送 4000 帧。

3) 本地环路: 客户和 CO 之间的链路, 连接 ISDN 设备到 ISDN 交换机。

4) 物理层: 参考点 (R、S、T、U); 设备 (LT/ET、NT1、NT2、TE1、TE2、TA)

## 三、配置不当的电话交换机

在新安装 ISDN 时, 必须考虑服务供应商 ISDN 交换机配置错误的可能性。

1、第 2 层故障处理:

ISDN 第 2 层故障处理的目标: q.921 协议和 PPP。

1) q.921: ISDN 的第 2 层在 q.921 中定义。Q.921 信令在 D 信道上用 LAPD 协议传输。处理 q.921 故障最常用命令是 debug isdn q921, 问题常与 TEI (terminal endpoint identifier)、SAPI (service access point identifier) 和 SABME (set asynchronous balanced mode extended) 有关。

TEI=127 表示广播; TEI=64-126 保留用于动态分配。

SAPI=0 表示当前第 3 层信令; 63 表示用于 TEI 值分配的管理 SAPI; 64 为呼叫控制。

2) PPP: PPP 使用 LCP 设置和维护链路; NCP 配置和维护网络层协议。

2、第 3 层故障处理:

ISDN 第 3 层也叫 q.931, 使用 debug isdn q931 命令可查看 call setup、connect、release、cancel、status、disconnect 和、user information。

ISDN 第 3 层连接在本地路由器 (TE) 和远端 ISDN 交换机 (ET) 之间。

ISDN 呼叫建立的过程:

1) SETUP: 在本地 TE 和远端 ET 之间发送信息

2) CALL\_PROC: 呼叫处理信令

3) ALERT:

4) CONNECT

5) CONNECT\_ACK:

3、交换机类型:

配置 ISDN 时，必须用 `isdn switch-type` 命令指定本地环路的交换机。

#### 四、ISDN 故障处理命令

- 1、ping: 在 DDR 中，ping 命令触发一个呼叫，在第 2 个 B 信道 up 前，路由器已完成了 ping。
- 2、clear interface bri n: 重置接口上不同的计数器并中止接口上的连接。
- 3、show interface bri n: 显示关于 ISDN BRI D 信道的信息
- 4、show interface bri n 1 2: 显示 ISDN BRI 的 B 信道信息。
- 5、show controller bri: 显示接口硬件控制器信息和 U 接口，供 Cisco 的 TAC 处理故障。
- 6、show isdn status: 显示 ISDN 接口状态和各层详细信息。
- 7、show dialer: 显示关于 DDR 连接的信息，包括拨号、成功的连接、IDLE 时间、呼叫数。
- 8、show ppp multilink:

#### 五、调试 ISDN

- 1、debug bri: 提供有关 BRI B 信道的信息，包括带宽信息
- 2、debug isdn q921: 获取关于接口 D 信道的信息，D 信息用于在交换机和本地 ISDN 设备间传输信令。
- 3、debug dialer: 呼叫连接的原因和连接的状态。
- 4、debug isdn q931: 监视发生在第 3 层的事件。  
Cause ID 显示呼叫被拒绝的原因;  
CallRef ID 发送和返回的信息，用于分析路由器和交换机之间不同呼叫的特定会话。
- 5、debug ppp negotiation: 提供建立 PPP 会话的实时信息，可察看 CHAP 和 PAP 验证
- 6、debug ppp packet: 报告实时 PPP 包流，包括包的类型和所用的 B 信道

### 第 9 章 交换以太网故障处理

#### 一、Switch、Bridge、Hub

广播域: 由 Router 控制

冲突域: 由 Switch 或 Bridge 控制

Switch 和 Hub 比较:

类型 Switch Hub

Unicasts 仅发送到目标 发送到所有端口

Broadcasts 发送同 VLAN 中的所有端口 发送到所有端口

Aggregate bandwidth 等于每个端口的带宽×端口数 等于介质速率

Full/half-duplex 可全双工连接 仅半双工

Support for mixed media:Token Ring,Ethernet,FDDI... 依靠 switch, 可在不同帧类型和物理介质之间传输 仅支持同一介质

混合介质的支持 依赖于桥配置

处理帧 硬件 (ASIC) 软件或

端口数量 从 4 到超过 100 通常 16 个以下

帧类型转换 依靠桥配置

## 二、Catalyst 故障处理工具

### 1、Catalyst 命令行接口：

命令行接口有 Native 模式和 Hybrid 模式。本机模式配置第 3 层和第 2 层在一起；混合模式在不同 CLI 下配置第 3 层和第 2 层，常为基于 set 的 CLI。

### 2、混合模式下的 CLI：

- 1) show system: 关于 switch 的高级总结信息，包括供电状态、uptime 和管理设置
  - 2) show port: 显示指定端口或一个模块上所有端口的信息 (VLAN、速率、双工、状态、类型、...)
  - 3) show log: 报告重要事件，包括所有模块的重启、trap、供电失败、...
  - 4) show logging buffer: 等同于路由器的 show log 命令，根据 logging 级别，报告端口 up 或 down、STP、...
  - 5) show interface: 报告管理模块上 IP 配置和 SC0 接口上 VLAN 信息。(s10、sc0)
  - 6) show cdp: 显示相邻 CISCO 设备信息
  - 7) show config: 等同于 show running-config 命令，显示交换机除 MSFC 等外所有模块上所有设置，仅显示非默认设置。Show config all 显示所有设置。
  - 8) show test: 仅显示 switch 管理模块状态，包括接口卡、供电、内存等。
  - 9) show mac: 显示大量计数，包括每端口帧流量、发出和进入的帧的总数量、丢弃、...
  - 10) show vtp domain:
  - 11) show cam: 显示与端口相关联的 MAC 地址
  - 12) 重复的 MAC 地址
  - 13) show spantree: 显示每个 VLAN 的 SPT 进程状态
  - 14) show version: 显示硬件和软件版本号，包括内存、系统 UP 时间统计等
- ### 3、RMON (Remote Monitoring)

RMON 基于 RMONProbe，从电路（物理介质）上采集数据信息。Router 和 Switch 并不支持所有级别的 RMON 信息，更多的监控可以用 SPAN(Switched Port Analyzer 交换端口分析，也叫 Port Mirroring 端口监控) 实现。

### 4、指示灯：

管理引擎上包含有负载 LED，可以提示交换机的当前负载。在启动过程中，LED 将闪烁；正常情况下，LED 常绿；橙色 LED 提示有问题；红色 LED 提示有故障。

## 三、用 STP 控制环路

STP 算法在 802.1D 中定义，用于在多交换机时控制重复路径，避免网络环路。

Cisco 使用 Port fast 和 Uplink fast 时，要防止产生网络环路。

#### 四、VLAN

VLAN 有基于端口的静态 VLAN 和基于 MAC 的动态 VLAN

1、ISL: Cisco 专用协议，用于连接两台设备以支持多个 VLAN。

? ISL 只能在支持 ISL 的产品上使用

? ISL 必须是点对点的

? ISL 仅用于 100Mb 全双工

? ISL 要求路由器的 IOS 和内存升级;

? ISL 可以支持 Token Ring;

? ISL 添加 30Bit 到原始帧;

? ISL 在帧的末尾包含 CRC。

2、802.1Q: 用于连接非 Cisco 中继到 Cisco 设备

。

3、VTP: VTP 使用多播通知 VTP 域中所有其它交换机关于域中 VLAN 的信息。

? VTP 服务器:

? VTP 客户机

? 透明 VTP:

#### 五、线缆问题

物理层标准:

线缆 10Mb 100Mb

3 类线距离 100m 不可用

5 类距离 100m 100m

多模光纤距离 2000m 2000m

单模光纤距离 高达 100km 高达 100km

1、线缆问题:

1) 万用表 (Multimeters) 和电缆测试器 (Cable Testers)

万用表 (Multimeters) 和伏欧表 (Volt-ohm) 用于验证电缆连通性，只能用于测试铜线或其它基于电信号的电缆，不能用于测试光纤。

电缆测试器 (Cable Testers) 既可测试电缆也可测试光缆，提供给用户更多的被测试电缆的信息，如：连通性、断路、短路、距离过长、噪音、MAC 信息、线路负载、...

2) 时域反射器 (TDRs) 和光时域反射器 (OTDRs)

TDR 是更复杂的电缆测试器，可用于定位电?械奈锢砦侍猓 骸庠谖裁次恢枚下貳 6.塘貳14.砒  
芻斐O室螭?br />

2、交叉线

交叉线用于两台主机直接相连、连接两台网络设备。

以太网使用 1、2、3、6 四芯 (白橙、橙、白绿、绿)，而 T1 电路使用 RJ-45 的 1、2、3、5 四

芯

## 六、交换机连接故障处理

发生在交换机上常见的故障有速率和双工设置，

### 1、SPAN（交换端口分析器）：

也叫 Port Mirroring（端口监视器）交换机拷贝所有被发送到工作站接口的包到另一接口，这个接口没有被指定 VLAN。

Set span enable ; 配置 SPAN

使用 SPAN 既监视接收的、发送的或所有的包。

### 2、多层交换特性卡（MSFC）和 Catalyst 路由：

MSFC 是一个在子板的 Cisco 路由器，安装在管理模块上，提供 VLAN 间路由。

在 CLI 下访问 MSFC: session

### 3、路由器和交换机间 VLAN：

路由器提供 VLAN 间的通信。

#### 1) 广播管理：

路由器不转发广播，交换机控制广播仅转发到是源端口所 VLAN 成员的端口。

#### 2) 策略控制：交换机没有策略，而路由器提供连接 VLAN 的安全和策略控制

#### 3) VLAN 交换：经过路由器转发一个包到同 VLAN 的不同接口

#### 4) VLAN 传输：使用不同 VLAN 协议的两 VLAN 间或 VLAN 协议传输到非 VLAN 第 2 层协议。

#### 5) 路由：在不同 VLAN 或非 VLAN 网络间通信

#### 6) 路由器上 VLAN 故障处理：

show vlans

show arp

show interface

show cdp neighbor

debug vlan packet

debug spantree

7) show vlans：在路由器上执行，显示路由器 VLAN 配置的细节，包括：VLAN 名、接口、IP 地址、VLAN 封装协议、接口协议。

#### 8) debug vlan packet：判定在中继上发送到路由器的数据的 VLAN。

## 3、VLAN 设计和故障处理

VLAN 设计时注意事项：

### 1) 网络直径要少于 8 台交换机；

### 2) VLAN 必须在某个限制内进行编号；

## 七、混合/本地模式命令转换

混合模式 本机模式 解释

Clear vlan No vlan 从配置中删除 VLAN

Set cam agingtime Mac-address-table aging-time 设置保留 MAC 地址的超时值

Set port dulex Duplex 在特定端口上配置双工

Set port name Description 设置端口名

Set port speed speed 设置端口速率

Se tspan Monitor session 设置 SPAN 端口

Set spantree Spanning-tree 设置 STP 信息

Set vlan Switchport access vlan 分配某端口到给定 VLAN

Show cam dynamic Show mac-address-table dynamic 显示 MAC 到端口关系

Show port Show interface 显示端口信息

Show span Show monitor 显示 SPAN 端口

Show test Show diagnostic 显示启动测试结果

Show version Show version 显示交换机 IOS 版本信息

Show vlan Show vlan 显示 VLAN 信息

Show vtp domain Show vtp status 显示 VTP 信息

## 第 10 章 分离并纠正物理层和数据链路层故障

### 1、识别物理层问题的症状

物理层组件包括：接口 / 端口、模块、线缆、中继器、网卡、转换器等。

物理层问题将导致链路上数据完全或间断的丢失，应用程序失败，数据传输速率低。

设备的端口和特定部件的 LED 在正常工作时稳定，故障时 LED 状态将关闭、闪烁或其它颜色。

物理层问题的常见症状：

### 2、识别数据链路层问题的症状

数据链路层问题包括：不正常的帧类型（不相符的封装）、重复的 MAC 地址、换换 鹊?层设备的不当行为。

第 2 层和第 3 层测试工具（CDP、PING）可以帮助检验并校验数据链路层问题。

### 3、用于分离物理层和数据链路层问题的命令和应用程序：

#### 1) ES 命令：

Ping host|ip-address ;

Arp -a ;

Netstat -rn ;

Ipconfig /all ;

Tracert ;

Winipcfg ;

Ifconfig -a ;

Traceroute ;

#### 2) Cisco IOS 命令

```

Ping ;
Traceroute ;
Debug ;
Show version ;
Show ip interface brief ;
Show interface e 1 ;
Show cdp neighbor detail ;
Show controllers ;
Debug ppp|isdn|serial|asynch|frame-relay
Show arp ;
Debug arp|lapb|stun ;

```

#### 4、纠正发生在物理层和数据链路层的命令和应用程序

```

arp -d ;
interface ;
no shutdown ;
encapsulation ;
clock rate ;
controller ;
duplex full|half|auto
speed 10|100|auto

```

##### 1) 纠正 T1/E1 问题的命令

```

channel-group channel-no timeslots timeslot-list speed 56|64
clock source line|internal
framing sf|esf; framing crc4|no-crc4
linecode ami|b8zs; linecode ami|hdb3
pri-group timeslote range

```

## 第 11 章 分离并纠正网络层问题

### 1、网络层问题的症状

### 2、分离网络层问题的 ES 命令

#### 1) 通用命令:

```

ping
arp -a
netstat

```

#### 2) WINDOWS

```

Route print

```



Ipconfig /all

Tracert

Winipcfg

3) UNIX&MAC

Ifconfig -a

Traceroute

Route -n

3、分离网络层问题的 Cisco IOS 命令

1) 通用:

ping

trace

debug

show running-config

2) ARP

Show ip arp

Debug arp

3) 路由表

show ip route

debug ip routing

4) IP 接口

Show ip interface brief

5) BGP

Show ip bgp

Show ip bgp summary

Show ip bgp neighbors

Debug ip bgp

6) IP 流量

Show ip traffic

Debug ip icmp

Debug ip packet

7) IP 访问列表

Show ip access-list