思科故障排除手册

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）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器集

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.Windows 系统

ping -s 192.168.0.Unix 环境

记录路由： ping -r 192.168.;0.Windows

ping -s -nRv 192.168.;0.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 章 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 e0/0Cisco缺省的 Ethernet封装方法是 ARPA

show ip interface e0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-lis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，erro和 debug 信息仅发送到 console，telne到路由器上看不到 debug 和 log的信息。

想在 telne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.到 10.1.1.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 erro和其它信息到 console、terminal 路由器内部 buffe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 Alert直接行动

3 Critic紧急情形

4 Error错误信息

5 Warnings警告信息

6 Notificatio正常但重要的情形

7 Informationa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.TFTP 服务器的 IP地址

对 FTP 协议的配置：

Router(config)#exception dump 192.168.1.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.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_protocal/04937.htm" target="_blank">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 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 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 对待组信息

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