网络运维纪实文学

36个实例——源自真实
一线运维师的血泪情仇

网络运维

亲历记

王刚耀 著

清華大學出版社

网络运维亲历记

王刚耀 著

清華大學出版社
北京

内 容 简 介

本书共包括 8 章，36 个网络运维实例。首先介绍常用的网络二、三层协议，包括 IP、HSRP、GVRP、VTP 协议和 Trunk 技术及网络运维中的一些技巧，如最简单的 Ping 和 Telnet 工具等。其次介绍当前用户比较关注的网络问题和热门的网络技术，如网络安全、虚拟化、IPv6 和无线网络等。最后介绍与网络运维相关的其他计算机应用技术，如应用系统和网络排查工具等。

本书深入浅出地介绍了计算机网络的多方面知识，注重应用实践，可作为网络从业人员的专业学习和参考用书，也可供高校计算机、通信、网络等专业的师生阅读参考。

图书在版编目(CIP)数据

网络运维亲历记 / 王刚耀著. — 北京：清华大学出版社，2016
ISBN 978-7-302-42984-5

Ⅰ. ①网… Ⅱ. ①王… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2016)第 030499 号

责任编辑：栾大成
装帧设计：杨玉芳
责任校对：徐俊伟
责任印制：沈　露

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 装 者：清华大学印刷厂
经　　销：全国新华书店
开　　本：188mm×260mm　　**印　　张：**20.75　　**字　　数：**340 千字
版　　次：2016 年 7 月第 1 版　　**印　　次：**2016 年 7 月第 1 次印刷
印　　数：1～3500
定　　价：49.00 元

产品编号：066329-01

前　言

计算机技术和网络技术的高速发展，对人类社会各个方面的影响还在不断加深和发酵：从博客、BBS、微博到时下流行的微信；从电脑台式机、一体机、笔记本电脑到现在的平板电脑和移动终端；从现金支付、刷卡支付到网上支付和现在的扫码支付；从商场购物到网上购物等，都能看到计算机技术和网络技术的发展对人们生活的影响无处不在。

笔者从20世纪90年代上大学，及后来攻读硕士学位时，学习的都是计算机专业。毕业后工作直到现在，一直从事计算机和网络相关的工作，接触到了局域网、园区网、城域网和跨区域网的设计、实现和管理的全过程，经历了从局域网到互联网那激动人心的变化。

目前，计算机网络技术方面的书籍往往只介绍某一方面的技术，而且大多数书籍偏重于原理、理论方面知识，这对操作和实践性非常强的网络运维来说，是一个很大的缺憾。尤其对于在校的大学生，因为学校客观环境的限制，不可能拥有像在公司和企业中的实际网络环境，学习的参考书也是包含过多的理论知识，学习起来常常是一头雾水，摸不着头脑。而计算机网络知识的学习，必须通过真实项目的全过程实践，才能真正地掌握网络理论知识。

本书是笔者在多年的网络运维实践中逐渐总结积累下来的经验所得，读者只需对照书中的每一个运维实例的操作步骤，一步步操作，就可以解决相同或类似的网络故障。同时，在操作完成后，包含于其中的计算机网络知识也会了然于胸。

本书共包括8章内容，第1～3章介绍了常用的网络二、三层协议，包括IP、HSRP、GVRP、VTP协议和Trunk技术，以及网络运维中的一些技巧，如最简单的Ping和Telnet工具等。第4～6章介绍了当前用户比较关注的网络问题和热门的网络技术，如网络安全、虚拟化、IPv6和无线网络等。第7～8章介绍了和网络运维相关的其他计算机应用技术，如应用系统和网络排查工具等。

一个人的进步离不开周围人的关心和帮助，在此感谢我的家人，一直以来对我工作的支持；感谢我的同事们，在我工作遇到困难时，总是替我排忧解难；也感谢本书的编辑栾大成，要是没有他的“金点子”及合理的建议，本书也不会这么快和大家见面的。

由于笔者水平和经验有限，书中还存在不少缺点和不足，敬请广大读者批评指正，万分感谢！

网络运维这点事

目前，绝大多数单位运行的计算机网络都是基于TCP/IP协议的，若网络是无线网络，则在二层是基于802.11协议的，例如，使用最普遍的移动终端手机、平板电脑、笔记本电脑等接入到无线局域网WLAN，也就是接入到WIFI，这些终端上肯定会拥有一个IP地址，移动终端和无线路由器或者无线AP的连接通信方式就是使用802.11方式的。

若用户是使用台式机通过网线或光纤连接到网络上网时，台式机上也肯定会有一个IP地址，台式机通过办公室中的信息点再连接到交换机上，台式机和交换机之间的数据通信在二层上就是使用802.3协议的。

上面列举的用户终端通过两种不同的连接方式访问网络时，虽然它们在二层上使用的协议和技术是不一样的，但它们在三层、四层上运行的方式，或使用的协议是完全一致的，三层上主要就是IP协议，它最主要的特征就是每台终端上的IP地址。四层上主要就是TCP和UDP协议，最主要的特征就是端口号，TCP和UDP的端口号范围都是1～65535。

上面说了很多“二、三层”的事，那一层是干什么的？一层就是物理层，像上面说的台式机通过网线或光纤连接到交换机，网线、光纤和交换机上的电口、光口等，这些都是一层即物理层上的。

那网络运维师的日常工作范围，基本上就在这一～四层，如图0-1所示。若是连接到电脑上的网线接触不好导致用户不能访问网络，那就是一层和二层出问题了；若是用户终

端的IP地址有错误，那是三层有问题了；若是有用户反映他访问办公应用系统正常，但是访问不了财务应用系统，那有可能就是四层出问题了，因为应用系统都是和端口进行关联的。有的应用系统能够正常使用，有的不正常，那说明网络没有问题，网络是通的，有一种可能就是网络中的防火墙把财务应用系统的端口进行了限制和阻止，而没有限制和阻止办公应用系统的，所以就有了上面的故障现象。

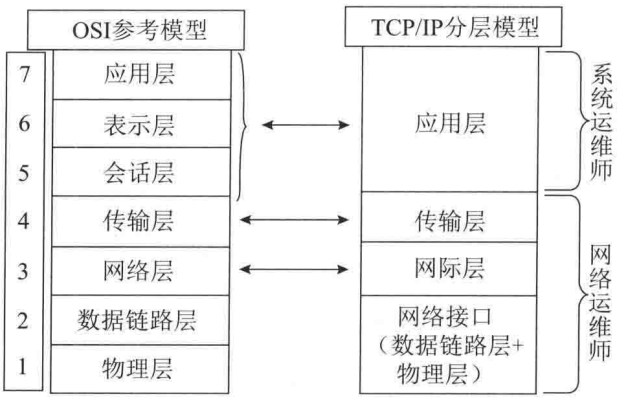
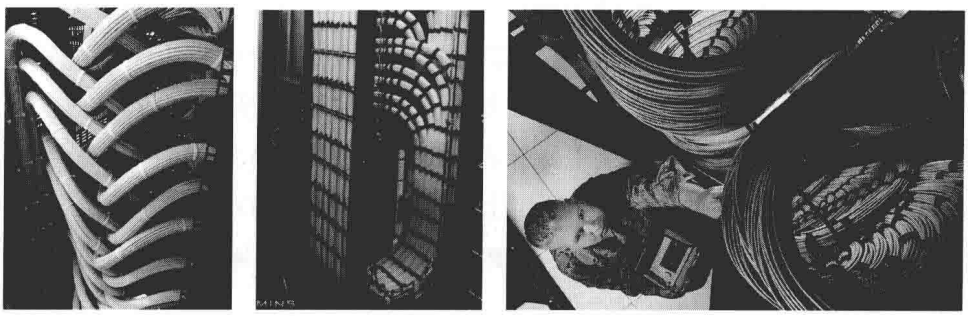


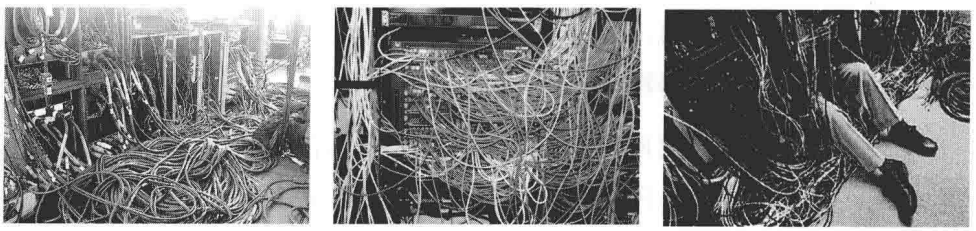
图0-1　运维工程师工作范围

曾经微信上有一篇很火的文章，标题是《有一种机房叫别人家的机房》，文章主要是用图片的形式进行讲述的，我这里拣其中对比明显的几张贴上来：

人家家的



咱家的



对比是很明显的，这也从一个侧面说明，国内一些网络机房确实是存在管理疏松，在布线、接线上不严谨，不按要求和标准来，私拉乱扯。不过这几张图的对比也有些太夸张了，我们大部分的机房布线还是很整齐、很漂亮的，不比国外“人家家的”差，有些甚至还要比他们的好。

另外，我想说的是，就是通过这几张图，能够很直观地呈现出网络运维师的工作环境。这几张图显示的一般都是单位的中心机房，也是网络运维师的主要工作场所。其他的还有各个楼的分中心机房及每栋楼每层的网络设备间。另外，和网络终端用户及网络安全设备供应商的工程师进行交流、沟通和学习，也是网络运维师日常工作的一部分。

好了，说了这么多云里雾里的东西，也不知大家能看明白吗？下面就分8章36个实例具体说说网络运维师都干些什么事。

目 录

第1章 网络三层协议 …… 1

1.1 网络三层协议概述 …… 3

1.1.1 IP协议 …… 3

1.1.2 热备份协议 …… 4

1.1.3 DHCP协议 …… 10

1.1.4 NAT技术 …… 11

1.2 运维实例：莫名奇妙的IP地址冲突 …… 13

1.3 运维实例：双网卡在网络中的实际应用 …… 21

1.4 运维实例：双IP地址引起的网络故障 …… 43

1.5 运维实例：深刻理解HSRP …… 49

1.6 运维实例：网络设备热备部署的3种模式 …… 55

1.7 运维实例：DHCP IP地址池扩充简单方案 …… 72

1.8 运维实例：明明白白NAT …… 73

第2章 网络二层协议 …… 79

2.1 网络二层协议概述 …… 80

2.1.1 MAC地址 …… 80

2.1.2 VLAN技术 …… 81

2.1.3 Trunk技术 …… 81

2.1.4 VTP协议 …… 82

2.2 运维实例：用最简单网络学习二、三层协议 …… 84

2.3 运维实例：实例解析GVRP、VTP协议和Trunk技术 …… 91

2.4 运维实例：用MAC地址定位目标主机 …… 106

2.5 运维实例：交换机虚拟接口应用 …… 115

2.6 运维实例：网络中主机间5种简单通信模式 ····· 121

第3章 网络运维技巧 ····· 129

3.1 运维实例：巧妙利用HOSTS文件替代DNS域名解析 ····· 131
3.2 运维实例：用BAT文件提高维护效率 ····· 136
3.3 运维实例：简单故障，艰难排查 ····· 141
3.4 运维实例：管理路由和交换设备的3种模式 ····· 144
3.5 运维实例：一起连接错误，导致网络崩溃 ····· 157
3.6 运维实例：简单问题，艰难解决 ····· 161
3.7 运维实例：多台电脑共享上网 ····· 166
3.8 运维实例：巧妙利用双绞线中闲置的数据线 ····· 168

第4章 网络安全 ····· 171

4.1 运维实例：网络安全设备的3种管理模式 ····· 172
4.2 运维实例：防火墙部署搭建与故障排除 ····· 184
4.3 运维实例：UTM双机热备和虚拟域功能 ····· 200
4.4 运维实例：SSL VPN部署与排障 ····· 211
4.5 运维实例：IDS在网络中的部署与配置 ····· 215

第5章 虚拟化和IPv6 ····· 221

5.1 运维实例：虚拟化终端防护探讨 ····· 223
5.2 虚拟化网络部署架构 ····· 224
5.2.1 设备间连接和配置情况 ····· 224
5.2.2 虚拟化应用运行过程 ····· 226
5.3 虚拟化客户端安全问题 ····· 227
5.3.1 安全防护五要素 ····· 227
5.3.2 虚拟化应用安全隐患 ····· 228
5.4 虚拟化客户端安全防护措施 ····· 229
5.4.1 手机动态密码验证 ····· 229
5.4.2 扩展USB-Key认证使用范围 ····· 230
5.4.3 远程安全桌面 ····· 231
5.4.4 DMZ区部署七层防火墙 ····· 232

5.5　总结……233
5.6　运维实例：搭建IPv6网络环境……233

第6章　无线网络……247

6.1　运维实例：小型路由器常见问题解析……249
6.2　运维实例：SOHO路由器引起的IP地址冲突……254

第7章　应用系统……261

7.1　运维实例：搭建Linux学习环境的5种方法……263
7.2　运维实例：恢复Windows单系统启动模式……275
7.3　运维实例：BSM提升IT运维效率……280
7.3.1　网络部署架构……280
7.3.2　故障发生过程……281
7.3.3　运用BSM排查故障步骤……282
7.3.4　结束语……286
7.4　运维实例：BSM在企业IT运维中的应用研究……287
7.4.1　BSM基本功能……287
7.4.2　BSM在企业中应用……288
7.5　对IT运维人员进行BSM培训……294
7.5.1　BSM在企业中应用后的效果……295
7.5.2　总结……296

第8章　排查工具应用……297

8.1　运维实例：并不简单的ping故障……298
8.2　运维实例：两则Telnet故障排查实例……307
8.3　运维实例：UDP/TCP调试助手应用……317

第1章 网络三层协议

其实，在互联网中用到的网络协议最多的就是TCP/IP协议，TCP/IP是Transmission Control Protocol/Internet Protocol的简写，中译名为传输控制协议/因特网互联协议。现在我们上班所在的公司和办公室，包括常常拿在手上的手机都连入了互联网。若是还没有联网，那就实在太落伍了。每天一上班，坐在办公桌前，打开电脑浏览器开始看邮箱和今天的新闻时，TCP/IP协议在你的电脑中就开始起作用了。

现在，英语是世界上最通用的语言，无论你到哪一个国家，只要你和对方都会说英语，那你们之间就可以进行对话交流了。同样，在Internet中，只要连入其中的终端遵守TCP/IP协议，它就可以和连入Internet中的其他终端进行通信了。也就是说TCP/IP协议组就类似一门语言。

TCP/IP协议又名网络通信协议，是Internet最基本的协议，也是Internet国际互联网络的基础。TCP/IP 定义了电子设备如何连入因特网及数据如何在它们之间传输的标准。协议采用了4层的层级结构，每一层都呼叫它的下一层所提供的协议来完成自己的需求。通俗而言：TCP负责发现传输的问题，一有问题就发出信号，要求重新传输，直到所有数据安全正确地传输到目的地。而IP是给因特网的每一台联网设备规定一个地址。

TCP/IP协议不是TCP和IP这两个协议的合称，而是指因特网整个TCP/IP协议族。从协议分层模型方面来讲，TCP/IP由4个层次组成：网络接口层、网络层、传输层、应用层。

TCP/IP协议并不完全符合OSI(Open System Interconnect)的7层参考模型，OSI是传统的开放式系统互连参考模型，是一种通信协议的7层抽象的参考模型，其中每一层执行某一特定任务。该模型的目的是使各种硬件在相同的层次上相互通信。这7层是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。而TCP/IP通信协议采用了四层的层级结构，每一层都呼叫它的下一层所提供的网络来完成自己的需求。

1.1　网络三层协议概述

1.1.1　IP协议

IP(Internet Protocol)，网络之间互连的协议，是为计算机网络相互连接进行通信而设计的协议。在因特网中，它是能使连接到网上的所有计算机网络实现相互通信的一套规则，规定了计算机在因特网上进行通信时应当遵守的规则。任何厂家生产的计算机系统，只要遵守IP协议就可以与因特网互连互通。

IPv6是Internet Protocol Version 6的缩写，它是IETF(Internet Engineering Task Force，互联网工程任务组)设计的用于替代现行版本IPv4的下一代IP协议。

IPv4地址分为5类：A类保留给政府机构，B类分配给中等规模的公司，C类分配给任何需要的人，D类用于组播，E类用于实验。各类可容纳的地址数目不同。当将IP地址写成二进制形式时，A类地址的第1位总是0，B类地址的前2位总是10，C类地址的前3位总是110。

1. A类地址

(1)A类地址第1字节为网络地址，其他3个字节为主机地址。它的第1个字节的第1位固定为0。

(2)A类地址网络号范围：1.0.0.0～126.0.0.0。

(3)A类地址中的私有地址和保留地址如下：

①10.X.X.X是私有地址(在互联网上不使用，而被用在局域网络中的地址)。范围为10.0.0.0～10.255.255.255。

②127.X.X.X是保留地址，用作循环测试。

2. B类地址

(1)B类地址第1字节和第2字节为网络地址，其他2个字节为主机地址。它的第1个字节的前2位固定为10。

(2)B类地址网络号范围：128.0.0.0～191.255.0.0。

(3)B类地址的私有地址和保留地址如下：

①172.16.0.0～172.31.255.255是私有地址。

②169.254.X.X是保留地址。如果你的IP地址是自动获取IP地址，而在网络上又没有找到可用的DHCP服务器，就会获取其中一个IP地址。

3. C类地址

(1)C类地址第1字节、第2字节和第3个字节为网络地址，第4个字节为主机地址。另外第1个字节的前3位固定为110。

(2)C类地址网络号范围：192.0.0.0～223.255.255.0。

(3)C类地址中的私有地址如下：

192.168.X.X(192.168.0.0～192.168.255.255)是私有地址。

4. D类地址

(1)D类地址不分网络地址和主机地址，它的第1个字节的前4位固定为1110。

(2)D类地址范围：224.0.0.0～239.255.255.255。

5. E类地址

(1)E类地址不分网络地址和主机地址，它的第1个字节的前5位固定为11110。

(2)E类地址范围：240.0.0.0～255.255.255.254。

IP地址如果只使用ABCDE类来划分，会造成大量的浪费。比如一个有500台主机的网络，无法使用C类地址。但如果使用一个B类地址，6万多个主机地址只有500个被使用，造成IP地址的大量浪费。因此，IP地址还支持VLSM(Variable Length Subnet Mask，可变长子网掩码)技术，可以在ABC类网络的基础上，进一步划分子网。

1.1.2 热备份协议

1. HSRP

HSRP(Hot Standby Router Protocol)热备份路由器协议，是思科的私有协议。

该协议中含有多台路由器，对应一个HSRP组。该组中只有一个路由器承担转发用户流量的职责，这就是活动路由器。当活动路由器失效后，备份路由器将承担该职责，成为新的活动路由器。

但是在本网络内的主机看来，虚拟路由器没有改变。所以主机仍然保持连接，没有受到故障的影响，这样就较好地解决了路由器切换的问题，这就是热备份的原理。

为了减少网络的数据流量，在设置完活动路由器和备份路由器之后，只有活动路由器和备份路由器定时发送HSRP报文。.如果活动路由器失效，备份路由器将接管成为活动路由器。如果备份路由器失效或者变成了活动路由器，将由另外的路由器接管成为备份路由器。

负责转发数据包的路由器称之为活动路由器(Active Router)，一旦主动路由器出现故障，HSRP将激活备份路由器(Standby Routers)取代主动路由器。HSRP协议提供了一种决定使用主动路由器还是备份路由器的机制，并指定一个虚拟的 IP 地址作为网络系统的缺省网关地址。如果主动路由器出现故障，备份路由器(Standby Routers)承接主动路由器的所有任务，并且不会导致主机连通中断现象。

HSRP 运行在UDP上，采用端口号1985。路由器转发协议数据包的源地址使用的是实际IP地址，而并非虚拟地址，正是基于这一点，HSRP 路由器间能相互识别。

HSRP协议利用一个优先级方案来决定哪个配置了HSRP协议的路由器成为默认的主动路由器。如果一个路由器的优先级设置的比所有其他路由器的优先级高，则该路由器成为主动路由器。路由器的缺省优先级是100，所以如果只设置一个路由器的优先级高于100，则该路由器将成为主动路由器。

通过在设置了HSRP协议的路由器之间发组播(地址为224.0.0.2)来得知各自的HSRP优先级，HSRP协议选出当前的主动路由器。当在预先设定的一段时间内主动路由器不能发送Hello消息时，优先级最高的备用路由器变为主动路由器。路由器之间的包传输对网络上的所有主机来说都是透明的。

配置了HSRP协议的路由器交换以下3种组播消息：

Hello消息：Hello消息通知其他路由器发送路由器的HSRP优先级和状态信息，HSRP路由器默认为每3秒钟发送一个Hello消息。

Coup消息：当一个备用路由器变为一个主动路由器时发送一个coup消息。

Resign消息：当主动路由器要宕机或者当有优先级更高的路由器发送Hello消息时，主动路由器发送一个Resign消息。

HSRP的两个定时器：

HSRP使用两个定时器，Hello间隔和Hold间隔。默认的Hello间隔是3秒，默认的Hold间隔是10秒。Hello间隔定义了两组路由器之间交换信息的频率。Hold间隔定义了经过多长时间后，没有收到其他路由器的信息，则活动路由器或者备用路由器就会被宣告为失败。配置计时器并不是越小越好，虽然计时器越小则切换时间越短。计时器的配置需要和STP等的切换时间相一致。另外，Hold间隔最少应该是Hello间隔的3倍。

在任一时刻，配置了HSRP协议的路由器都将处于以下6种状态之一：

Initial状态：HSRP启动时的状态，HSRP还没有运行，一般是在改变配置或端口刚刚启动时进入该状态。

Learn状态：学习状态，不知道虚拟IP，未看到活跃路由器发Hello，等待活动路由器发hello。

Listen状态：路由器已经得到了虚拟IP地址，但是它既不是活动路由器也不是等待路由器。它一直监听从活动路由器和等待路由器发来的Hello报文。

Speak状态：在该状态下，路由器定期发送Hello报文，并且积极参加活动路由器或等待路由器的竞选。

Standby状态：当主动路由器失效时路由器准备接管包传输功能。

Active状态：路由器执行包传输功能。

2. VRRP

VRRP(Virtual Router Redundancy Protocol)虚拟路由冗余协议，是由IETF(国际互联网工程任务组)提出的解决局域网中配置静态网关出现单点失效现象的路由协议。

VRRP是一种选择协议，它可以把一个虚拟路由器的责任动态分配到局域网上的 VRRP 路由器中的一台。控制虚拟路由器IP地址的 VRRP 路由器称为主路由