名师助您夯实通向CCIE之路的基础

拨开CCNA迷雾

——重点及疑难解析

◎ 张国清　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http: //www.phei.com.cn

拨开 CCNA 迷雾
——重点及疑难解析

张国清　编著

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本书由资深 Cisco 技术讲师根据多年的教学心得编写而成，针对 CCNA 认证中的重点和难点做了详细的讲解。主要内容包括：OSI 参考模型；TCP/IP 协议；路由基本原理；路由协议工作原理及配置方法（RIPv1，RIPv2，IGRP，EIGRP，OSPF）；访问控制列表；以太网和 WLAN；以太网交换原理；广域网及其接入技术（HDLC、PPP 和帧中继）；动态地址配置；地址翻译；IPsec/SSL VPN；IPv6 简单介绍。

本书的读者对象是：自学 CCNA 者；参加 CCNA 培训者；准备获取 CCNA 认证证书者；工程技术人员。本书既可作为高等院校和思科网络技术学院 CCNA 认证的教材，也可作为企业提高员工技能的培训教材。

图书在版编目（CIP）数据

拨开 CCNA 迷雾——重点及疑难解析 / 张国清编著. —北京：电子工业出版社，2011.1

ISBN 978-7-121-12330-6

Ⅰ.①拨… Ⅱ.①张… Ⅲ.①计算机网络—工程技术人员—资格考核—自学参考资料 Ⅳ.①TP393

中国版本图书馆 CIP 数据核字（2010）第 226505 号

策划编辑：宋 梅
责任编辑：宋 梅
印 刷：北京东光印刷厂
装 订：三河市皇庄路通装订厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1 092 1/16 印张：18.5 字数：473 千字
印 次：2011 年 1 月第 1 次印刷
印 数：4 000 册 定价：49.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

序

仔细阅读了张国清老师的这部新作，我对他能够潜心钻研并不断取得成果表示敬佩。张国清老师把自己对网络技术的热情以及从事第一线教学工作的经验和专业知识倾注于此书。本书摆脱了传统的“应试教育”的思路，完全从掌握实用网络技术的角度出发，引导读者逐步掌握路由技术的精髓。书中所阐述的道理深入浅出，案例充足，实验结果和分析说明详尽，与从国外引进的原版翻译教材相比，更适合中国人的阅读思维和习惯，有助于快速理解和掌握知识。

我相信，张国清老师的努力工作，对于计划参与思科认证考试的人员、学生以及网络工程的技术人员都是非常有帮助的。

思科公司总裁约翰·钱伯斯先生曾说，“互联网和教育是推动社会公平发展的两个核心动力”。秉承这一理念，思科公司积极参与和推动中国教育事业的发展，在中国设立了近400所思科网络技术学院，在校学生超过5万名，累计参加学习的学生人数超过15万名。

思科公司始终坚信，互联网必将改变人们的工作、学习、生活和娱乐方式。而这一理念的实现，是全体支持互联网发展的研究专家、系统厂商、技术与应用开发商、运营商、教育机构和消费者共同努力的结果。在此也感谢张国清老师为此所付出的努力！

思科系统（中国）网络技术有限公司

中国思科网络技术学院总经理

2010年11月1日

前　言

CCNA 认证是世界著名的互联网设备及方案提供商——思科公司推出的系列职业认证之一。思科公司开发的通用职业认证系列包括 CCNA（Cisco Certified Network Associate），CCNP（Cisco Certified Network Professional）和 CCIE（Cisco Certified Internetwork Expert）。除了通用职业认证之外，还有若干专业技术认证。CCNA 是通用职业认证和专业技术认证的基础，因此，广泛受到从事网络技术的人员及大中专学生的青睐。

随着技术的不断进步，CCNA 认证所要求的知识和技能也逐步升级，增加了一些新技术，如 WLAN 技术、VPN 技术和 IPv6 技术。从整体上提升了获取 CCNA 认证的难度，同时也增加了 CCNA 证书的含金量。市场上有许多关于应对 CCNA 考试的书籍，而本书不同于其他书籍的地方在于对 CCNA 涉及的重点和难点进行了深入剖析，在 CCNA 要求的知识层面上，使读者对相关理论和技术有一个较深刻的理解。

本书适合以下人员阅读：

- 自学 CCNA 者；
- 参加 CCNA 培训者；
- 准备获取 CCNA 认证证书者；
- 工程技术人员。

全书共 13 章。

第 1 章　开放系统互连：讲述了 OSI 参考模型理论。

第 2 章　TCP/IP 协议介绍：详细讲解了 IP 地址、子网划分、VLSM、ARP 和 ICMP 协议等内容。

第 3 章　路由原理：阐述了路由原理，分别介绍了距离矢量型路由协议和链路状态型路由协议的工作原理和特性。

第 4 章　配置静态和动态路由：介绍了如何在路由器上配置 RIPv1，RIPv2 和 IGRP 协议及静态路由。

第 5 章　访问控制列表：介绍了在路由器上实现数据和网络安全的技术。

第 6 章　OSPF 路由协议：介绍了 OSPF 路由协议原理及配置。

第 7 章　EIGRP 原理及配置：介绍了 EIGRP 协议的原理及配置。

第 8 章　以太网技术：介绍了以太网工作原理和 CSMA/CD。

第 9 章　以太网交换技术：介绍了以太网交换原理和以太网交换机的配置方法。

第 10 章　广域网及其接入技术：介绍了广域网的概念和广域网接入技术。

第 11 章　DHCP 和 NAT 技术：介绍了 DHCP 工作原理和 NAT 技术。

第 12 章　VPN 技术：介绍了隧道原理和加密技术，以及 IPSec VPN 和 SSL VPN。

第 13 章　IPv6 概述：介绍了 IPv6 地址、ICMPv6、实现 IPv6 的方案和 IPv6 路由协议等。

本书由张国清编著，参加编写工作的还有张运欣。

鉴于作者水平有限，书中难免出现错误和纰漏之处，欢迎读者批评指正，作者不胜感激。欢迎访问作者博客：http://gooltsing.blog.chinaunix.net。

编著者

2010 年 9 月 9 日

目　录

第1章　开放系统互连

本章重点

- 分层原则
- 层与层之间的关系
- 数据封装
- 对等层通信原则
- 各层定义的内容

国际标准化的制定始于电气技术行业，由成立于1906年的IEC（International Electrotechnical Commission）制定。1946年，来自25个国家的代表聚集伦敦，决定成立一个新的国际化组织，其目标是“推动国际间工业标准的协调和统一”。这个新的组织就是ISO，于1947年2月23号开始正式运作。

1.1　ISO与OSI

国际标准化组织是一个非政府组织机构，是世界上最大的制定标准的实体，现今由世界上140多个国家的标准化组织机构组成。尽管国际标准化组织主要制定技术方面的标准，但它对经济和社会方面的标准化也有重要的影响。

由于不同的语言对国际标准化组织（International Organization for Standardization）的名称有不同的缩写方法，后来决定使用来自希腊语的一个词——ISOS，该词在希腊语中是平等的意思（Equal），把这个词的前3个字符——ISO，作为该组织在任何语言中的缩写。

国际标准就是ISO成员体间的一个协定。成员体可以原封不动地使用原始的协定，也可以与本国的标准结合使用。

所有的协议最少每隔5年重新评议一次，决定它是否继续使用、改版或者取消。

最初的计算机网络的研究是分散进行的，没有一个统一的组织机构或实体统一协调此事，一般情况下是由各大著名公司按照自己的想法去研究和实现的，如IBM和DEC公司等。这样就存在一个潜在的问题：各种网络之间并不兼容，因此不同网络之间的通信就成了问题。随着计算机网络在数量上的增加和范围上的扩大，20世纪70年代末期，这些公司开始意识到：由于网络规范的不同，它们之间的信息交换变得不可能。

为了解决这个问题，ISO研究了DEC NET，SNA和TCP/IP等，试图发现它们的问题所在。利用这些研究成果，ISO于1984年发布了一套描述性的网络模型——开放系统互连参考模型（Open System Interconnection Reference Model，OSI），为生产商们提供了一个大家共同遵守的标准。该标准最大程度上解决了不同网络间的相互兼容性和互操作性。由于

该参考模型非常详细地描述了网络应该具有的功能模块及其互连，所以该模型成为当今最主要的参考标准。

1.2　OSI 参考模型

OSI 参考模型（见图 1-1）是一个纯的理论分析模型，也就是说，OSI 参考模型本身并不是一个具体协议的真实分层。在该模型出现之前，也没有任何一个具体的协议栈具有完整的 7 个功能分层，这与网络的历史发展有关。虽然今天使用的协议没有严格按照 OSI 七层分层，但人们仍然使用 OSI 的理论来指导自己的工作，尤其在研究和教学方面。这正是体现了 OSI 的理论指导功能。

图 1-1　OSI 参考模型

从图 1-1 中可以看到，整个参考模型分成 7 层（Layer），为了便于描述，为每层编了序号，起了名字。从下到上依次是：

第 1 层，物理层；
第 2 层，数据链路层；
第 3 层，网络层；
第 4 层，传输层；
第 5 层，会话层；
第 6 层，表示层；
第 7 层，应用层。

分层是为了降低复杂程度。不难想象，把一个复杂的事物分解成若干个部分去分析就会简单得多。分层也有利于加速协议的发展和优化，更好地体现开放性。针对某一层所进行的优化和修改并不影响其他层的功能。

根据功能不同而分层是 OSI 分层的原则。如果功能相同或相近，就把它们划分在同一个层上，如果不同，就要分层。不同的层所完成的工作是不同的。层与层之间并不是孤立的，它们的关系是：下层为上层服务（请参阅 1.3 节）。

常见的协议如 TCP/IP、以太网、FDDI、IEEE 802.3 和 IEEE 802.5 等与 OSI 参考模型的对应（对比）关系，如图 1-2 所示。

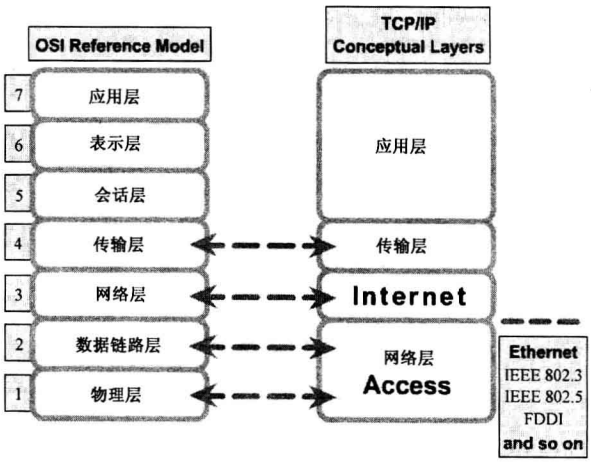

图 1-2　常见协议与 OSI 参考模型的对应关系

1.2.1　物理层

物理层：物理层主要定义物理和电气规范。组网使用的电缆规范就属于物理层的范畴。如双绞线和光纤等。

物理层涉及比特流的传输问题，例如，用什么样的电流、电脉冲、光或者电磁场来代表逻辑的二进制信息。由于在数据通信中用二进制组合来表示字符，所以，用什么样的脉冲信号来表示数字“0”和“1”，对于各种通信场合下保证通信的可靠性和经济性是十分重要的。我们把用直流信号表示“0”和“1”的信号形式叫做码型；将二进制数转换成电或光信号的方式称为编码。理论上，任意的二进制码的组合方式都可以形成数据传输代码，因此，可用于数据的传输代码很多。

在常用的网络中，10BASE-T 使用曼彻斯特编码；令牌环网络使用差分曼彻斯特编码；100BASE-TX 采用 MLT-3 编码机制；1000BASE-T 采用 PAM-5 编码机制。

网络接口卡与网络连接以及网络的物理拓扑结构也属于物理层的范畴。网络的物理拓扑结构描述了网络的物理布局。

1.2.2　数据链路层

物理层处理的对象是比特，原始的比特流对于主机识别其所代表的实际信息是没有什么帮助的，所以，数据链路层要解决一些更现实的问题，如网络上的计算机如何被定位，即寻址等问题。数据链路层建议应该为网络上的主机定义一个可以标志它的地址，在制造网卡时就在网卡里烧结了一个编号，该编号被称为主机的物理地址。计算机安装了网卡，网卡的编号就代表了这台主机。有了这个地址，网络上的主机之间的通信就有了目标，也就知道了数据从哪里来到哪里去，哪一台主机应该接收数据，不是数据目标的主机就会忽略它。

当两台主机进行通信时，一台主机把连续的比特流通过物理媒介在网络上传播。对于目的地主机来说，它必须知道什么时候应该开始接收，什么时候接收应该结束；哪些是有用的比特，哪些是无用的比特；哪些是有效信息，哪些是无效信息（其他用途）等一系列问题。例如，前面讲过的地址，代表主机地址的比特肯定在源主机发送出的比特流中。对于网络上的其他主机来说，为了确定该数据是否是给自己的，必须比较代表目的地地址的那些比特。可是，并不能随便从比特流中截取一些比特来比较，因为这些比特可能不是代表地址的。

数据链路层的另一个重要功能是要把一系列连续的比特流形成一系列称为帧（Frame）的数据段，该数据段具有一定的数据结构，每部分都有特定的含义，如图 1-3 所示，这样主机就能够知道其代表的含义了。成帧（Framing）是第 2 层的重要功能，只有成了帧，原本没有实际意义的比特就有了含义了。

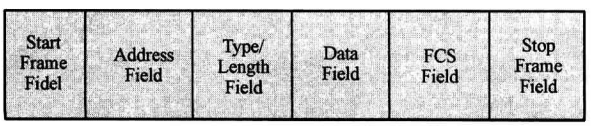

图 1-3　帧结构

一个完整的帧应该包括如下字段：

- 帧起始字段（Start Frame Field）——表示一个帧的开始。
- 地址字段（Address Field）——源计算机物理地址及目的地计算机物理地址。
- 长度 / 类型控制字段（Length/Type Field）——帧（长度）字段，说明帧的确切长度。（类型）字段，指出第 3 层协议。
- 数据字段（Data Field）——第 3 层的信息。
- 帧校验序列（Frame Check Sequence，FCS）字段——用以校验数据字段，可以帮助目的地计算机判断收到的帧是否正确。
- 帧结束字段（Stop Frame Field）——表示帧的结束。

在数据传输过程中，难免会因为各种原因造成数据被破坏。数据链路层定义，使用帧校验序列的方法，使目标主机判断接收到的数据是否在传输过程中被破坏了。图 1-3 中的 FCS 字段就是用做此目的的。发送端主机对发送的数据采用某种校验算法进行计算，把计算的值写入 FCS 字段。目标主机收到数据后采用同样方法进行校验，然后和预先写入的值比较，如果相同，表明数据在传输过程中没有被破坏，如果不同则表明数据被破坏了。

计算帧校验序列的方式常用的有以下 3 种：

- 循环冗余校验（CRC）；
- 奇偶校验；
- 校验和。

对于被破坏了的数据，目标主机请求对方重传。重传体现了数据链路层为数据传输提供可靠性的功能。除此之外，数据链路层还提供数据的流量控制，使通信双方的会话顺利、可靠地进行。

数据链路层定义的第 3 个功能是媒介访问控制方法（Media Access Control Method）。媒介访问控制方法定义了网络上的计算机如何获得物理通道的使用权，只有获得使用权的计算机才可以向网络上发送数据。从计算机组网来看，网络中的计算机是共享同一个物理传输通道的，如果没有一定的方法管理计算机使用该传输通道，势必造成数据碰撞，使得哪一台设备也不能通信。媒介访问控制方法可以分为以下 3 类。

- 竞争方式：也称为争用方式，如 CSMA/CD。这种方式没有确定性，抢到通道就使用，抢不到就不用。
- 令牌传递方式：如 Token Passing。这种方式有确定性，那就是拥有令牌的使用通道。
- 轮询方式：这种方式也有确定性，网络上的设备被轮流询问，优先级高的设备拥有使用通道的优先权。

1.2.3　网络层

网络层可以看做一座桥梁，这座桥梁把不同规范的网络连通起来。把网络层的数据作为不同网络间交换的数据单元。当数据到达目标网络时再转换成特定网络规范的帧格式。如图 1-4 所示，两种不同规范的网络互连，一种是以太网，一种是令牌环网络，它们在 Internet 上交换的是网络层数据，如 IP 数据包，当它们接收到数据，需要往自己网络内部传输时，路由器就转换成它们识别的以太数据帧或者令牌帧。

网络层有两个重要的功能：定义逻辑地址；为数据传输提供路由，也就是确定路径。

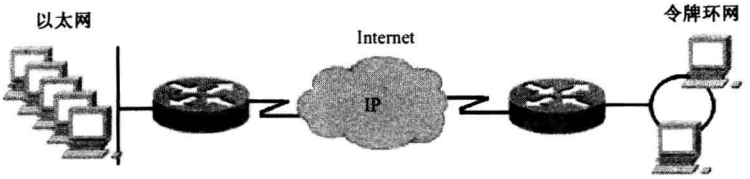

图 1-4　IP 作为通用的交换数据

与数据链路层地址相比，网络层定义的逻辑地址的最大特点是具有层次结构，而物理地址则是一个平面结构。网络层定义的逻辑地址分为两部分，一部分为网络；另一部分为该网络中的节点，代表一台主机。当需要查找某台主机时，先找到该主机所在的网络，再找到该网络中代表该主机的节点即可，如同身份证编号。这样，为管理网络中的计算机提供了极大的方便。

逻辑地址有多种，不同的协议集有不同的逻辑地址，例如，192.168.20.2 是 IP 地址，192.168.20 代表一个网络，2 是该网络上的一个节点（有关 IP 地址的详细介绍请参阅第 3 章相关内容）。

网络层的另外一个重要功能是路由，也就是为被转发的数据找一条到达目的地的最佳路径。完成此项功能需要两方面的信息：一个是已知的最佳路径信息——路由表；另一个是被转发数据携带的网络层逻辑地址。路由器是完成这项功能的设备。当路由器从它的某个接口收到数据后，读取数据中携带的逻辑地址，然后查阅路由表，作出如何转发该数据的决定。

1.2.4　OSI 的其他层

OSI 的上层与操作系统和应用程序有密切的关系。

① 传输层的主要功能是提供端到端的可靠传输；第一次对上层传送来的数据进行分段，把信息划分为适合被传输的数据段。传输层还负责区分上层不同的应用服务（详细介绍请参阅第 2 章相关内容）。

② 会话层在应用程序间建立会话、管理会话和终止会话，包括初始化、停止及重新同步两台会话的主机。

③ 表示层负责将数据转换成接收端设备可以理解的格式。下面这个简单的例子可以说明表示层的功能。当两个不同语言体系的人要交谈时，唯一方法就是找一个人帮他们翻译。表示层即为网络通信设备的翻译员。主要提供以下 3 种功能：

- 翻译数据格式；
- 数据加密；
- 数据压缩。

④ 应用层不对其他的 OSI 层提供服务，但是对位于 OSI 模型以外的应用程序提供服务。此外，应用层也使用应用程序（如 WWW，E-mail，FTP 和 Telnet）为 OSI 模型的其余各层提供一个直接的接口，或利用单独的应用程序［如文书处理器、表达管理器（Presentation Managers）和网络重定向器（Network Redirector）］提供一个间接的接口。

具体的协议集在实现时往往把上 4 层与操作系统一起实现，它们的功能主要在主机上完