

[美] Michael Valentine Andrew Whitaker 著

徐 宏 程代伟 等译 薛荣华 审校

CCNA Exam Cram Third Edition

The Smart Way to Study

que®

CCNA

考试精要

(第三版)(640-802)



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>



光碟内有新的模拟试题

CCNA Exam Overview: Andrew Chiswick ©

© 2008, 2010, 2012, 2014, 2016, 2017

CCNA Exam Overview Third Edition

The Smart Way to Study

CCNA

CCNA

考试精要

(第三版) (640-802)

CCNA Exam Cram Third Edition

CCNA 考试精要 (第三版) (640-802)

[美] Michael Valentine Andrew Whitaker 著

徐宏程代伟等译
薛荣华 审校

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书是一本 CCNA 应试必备的学习指南,由 Cisco 技术的知名培训师编写。CCNA 考试的内容已几度变化,本书编写的考试目标是最新的考试内容。本书针对新的考试目标帮助应试者全面复习、掌握新的考试内容。附带的光碟上有新 CCNA 考试(640-802)的大量准备工具和资料。为了有助于准备 Cisco 模拟考试,光碟上包含 CCNA 考试目标、正确和不正确答案的解释和多种模式的考试。最后还有 PC 机、便携机和 Palm 手持机的电子闪存卡以及本书的电子版。相信通过本书的学习,应试者定能顺利地通过这一考试。

读者对象:CCNA # 640-802 考试的应试者、Cisco 网络工程技术人员和销售人员、大专院校计算机通信专业师生。

que®

Copyright © 2008 by Que Publishing, Inc., Indianapolis, Indiana. All rights reserved.

No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein. 本书英文版由美国 Que 公司出版,Que 公司已将中文版独家版权授予中国电子工业出版社及北京美迪亚电子信息有限公司。未经许可,不得以任何形式和手段复制或抄袭本书内容。

版权贸易合同登记号 图字:01-2008-2040

图书在版编目(CIP)数据

CCNA 考试精要:第3版. 640-802/(美)威里蒂那(Valentine, M.)等著;徐宏,程代伟等译. —北京:电子工业出版社,2008. 9

书名原文:CCNA Exam Cram. Exam 640-802, 3rd Edition

ISBN 978-7-121-07110-2

I. C… II. ①威…②徐…③程… III. 计算机网络—工程技术人员—资格考核—自学参考资料 IV. TP393

中国版本图书馆 CIP 数据核字(2008)第 106632 号

责任编辑:吴 源

印 刷:北京天竺颖华印刷厂

装 订:三河市金马印装有限公司

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

北京市海淀区翠微东里甲 2 号 邮编:100036

开 本:787×1092 1/16 印张:24.75 字数:630 千字

印 次:2008 年 9 月第 1 次印刷

定 价:59.00 元(含 CD-ROM 一张)

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。

CCNA 考试精要要点

这个 CCNA 考试精要要点包括有关 CCNA 考试的关键要点。复习这些信息作为进入考试中心前要做的最后一件事，特别注意你感到需要复习的部分。开始考试前你可以立即把头脑中的这些要点写在空白纸上。

OSI 模型

层	名称	协议和设备	PDU
7	应用	FTP、Telnet、TFTP、SMTP、POP3、SNMP、DNS、NTP、HTTP、HTTPS、DHCP	数据
6	表示	ASCII、.jpg、.doc	数据
5	会话	RPC、SQL/Telnet（仅为登录）	数据
4	传输	TCP——面向连接的，可靠使用 PAR UDP——无连接的、不可靠的、为可靠性使用上层协议	段
3	网络	IP、ICMP、RIP、IGRP、EIGRP、OSPF 路由和路径决定、逻辑寻址	包
2	数据链路	以太网、帧中继、PPP、HDLC 物理（硬件）地址（MAC 地址）	帧
1	物理	媒介上的比特传输 集线器、转发器、连接器	比特

TCP 和 UDP

知道下列协议和端口号：

TCP		UDP	
FTP	20、21	DNS	53
Telnet	23	DHCP	67、68
SMTP	25	TFTP	69
DNS	53	NTP	123
HTTP	80	SNMP	161
POP	101		
NNTP	119		
HTTPS	443		

TCP 采用主动确认和重传（PAR）：

- ▶ 源设备为每个字段启动定时器；如果定时器到期前没有收到确认则重传。
- ▶ 源设备记录发送的所有字段并期望得到每一个的确认。
- ▶ 目的地设备通过发送一个 ack 信号作为其期待下一个序列号而确认接受一个字段。

能够识别一个 TCP 头部

源端口	目的端口
序列号	
确认号	
混杂标记	窗口 (流控)
校验和	紧急指针
选项	

能够识别一个 UDP 头部

源端口	目的端口
长度	校验和

CDP

- ▶ 专用的 (仅 Cisco) 数据链路 (第 2 层) 协议
- ▶ L3 协议, 及媒介独立
- ▶ 使用 L2 组播收集直连设备的硬件和协议信息
- ▶ 默认启用; 能由 no cdp run 全局禁用
- ▶ 要学习远程设备 L3 地址、硬件平台和 IOS 版本, 使用 show cdp neighbor detail 或 show cdp entry

LAN 技术

- ▶ 以太网物理地址=MAC 地址。
 - ▶ 12 个十六进制数字
 - ▶ 前 6 个数字是 NIC 制造商的 OUI
- ▶ PC 到交换机/集线器=直通电缆。
- ▶ 集线器-集线器、交换机-交换机、PC-PC、路由器-路由器、PC-路由器直接 (没有交换机/集线器: 使用交叉电缆)。
- ▶ 交换机、网桥和路由器分段一个网络。集线器和转发器扩展一个网络。
- ▶ 交换机增加冲突域数目, 不分段广播域。路由器、L3 交换机和 VLAN 分段广播域。

交换

- ▶ 交换机是一个多端口网桥。交换机使用硬件 ASIC 转发帧, 使得它们比网桥快。每个端口专用带宽。
- ▶ 网桥和交换机通过读每个帧的源 MAC 来学习 MAC。
- ▶ 交换机以三种模式之一操作:
 - ▶ 存储转发: 整个帧被缓存。运行 FCS (差错校验)。
 - ▶ 直通: 只读目的地 MAC、帧被转发。
 - ▶ 碎片丢弃: 帧的前 64 字节被缓存, 帧被转发。Cisco 专用。

- ▶ 半双工：共享冲突域和较低的吞吐量。
- ▶ 全双工：点到点和更高的吞吐量。
- ▶ 要远程管理一台交换机，需要一个 IP 地址、子网掩码和默认网关。该交换机必须在它的管理 VLAN 中一个端口上是可达的。

虚拟 LANS (VLANs)

VLANs:

- ▶ 逻辑上将一台交换机划分成多个独立的第 2 层交换机
- ▶ 在一台交换机中创建分隔的广播域，增加广播域的数目
- ▶ 使用中继跨越多个交换机
- ▶ 允许将用户按功能逻辑分组
- ▶ 简单地添加、移动和改变网络中的主机
- ▶ 增强安全性

VLAN 配置步骤:

1. 该 VLAN 必须创建。
2. 该 VLAN 可被命名。
3. 需要的端口必须添加到新的 VLAN。VLAN 间的路由选择需要一台路由器或第 3 层交换机。

中继

中继承载从一个连接上（交叉电缆）VLAN 来的多个通信量。VLAN ID 使用两种方法之一标记：

1. ISL
2. IEEE 802.1q

一个中继可以在 5 种模式之一中操作：

- ▶ 动态自动
- ▶ 动态合意
- ▶ 开
- ▶ 关
- ▶ 强制

VTP (VLAN 中继协议)

VTP 简化 VLAN 管理。VLAN 的配置从一台服务器模式的交换机分配到一个 VTP 域中的所有交换机。

3 个 VTP 模式如下：

- ▶ 服务器
- ▶ 客户机
- ▶ 透明
- ▶ 交换机必须在同一个 VTP 域而且必须使用同样的口令交换 VTP 信息

- ▶ 生成树协议 (STP IEEE 802.1d)
- ▶ L2 协议防止在具有冗余交换路径的网络中的交换环路。
- ▶ 根交换机是具有最低 STP 优先级的交换机; 如果优先级相同, 低 MAC 就是根。
- ▶ 根端口包含到根交换机最低开销路径。
- ▶ STP 路径开销由基于带宽的开销总和来决定。

生成树拓扑端口状态:

1. 阻塞: 不发送数据, 侦听 BPDU
2. 侦听: 发送和接收 BPDU
3. 学习: 记录 MAC 地址
4. 转发: 正常操作

收敛: 50 秒 (20 秒最大老化 + 15 秒转发延迟 + 15 秒转发延迟)

路由器/交换机的引导顺序

1. POST——设备发现硬件并执行硬件检查例程。
2. 找到 IOS。
3. 装载 IOS。
4. 找到配置 (startup-config)。
5. 装载配置 (running-config)。

配置寄存器设置:

- ▶ 0x2102 (默认): 检查 NVRAM 中“引导系统”命令; 如果没有, 则首先装载闪存中有效的 IOS。
- ▶ 0x2100: 引导进入 ROM 监视器模式 (ROMMON)。
- ▶ 0x2101: 引导进入 ROM RxBoot 模式。RxBoot 可以连接到一台 TFTP 服务器来下载一个 IOS 到闪存中。
- ▶ 0x2142: 引导时忽略 NVRAM 中的启动配置 (为了恢复口令)。

路由器/交换机的存储器组件:

- ▶ ROM: 开始和维护上电自检 (POST)、bootstrap、ROM Monitor (ROMMON) 和 RXBOOT
- ▶ 闪存内存: 存储 IOS
- ▶ NVRAM: 存储 startup-config (引导时装入的配置)
- ▶ RAM: 运行 IOS 和 running-config (启动后的活动配置)

使路由器安全

在所有 5 条 telnet 线路上配置口令, 该配置将类似如下:

```
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# login
```

配置 SSH

要在路由器或交换机上配置 SSH, 需要的元素如下:

- ▶ 一个主机名
- ▶ 一个域名
- ▶ 一个 RSA 密钥
- ▶ 一个本地认证的用户名和口令

示例 SSH 配置：

```
Switch>enable
Switch#config t
Switch(config)#hostname Branch_2960
Branch_2960(config)#ip domain-name
ExamCram2.net
Branch_2960(config)#crypto key
generate rsa
Branch_2960(config)#username admin
password ciscocisco
Branch_2960(config)#line vty 0 4
Branch_2960(config-line)#login
Branch_2960(config-line)#login local
Branch_2960(config-line)#transport
input ssh
Branch_2960(config-line)#exit
```

路由选择

默认管理距离：

连接的接口	0
静态路由	1
EIGRP (内部)	90
IGRP	100
OSPF	110
RIPv1 和 v2	120
EIGRP (外部)	170

静态路由

```
Router(config)#ip route 192.168.1.0
255.255.255.0 10.1.1.1
```

默认路由语法是：

```
Router(config)#ip route 0.0.0.0
0.0.0.0 192.168.1.1
```

距离矢量路由选择协议

将整个路由表通告给直连邻居并且不管是否有变化出现都要发送更新（每 x 秒）。

RIPv1、RIPv2、IGRP。

链路状态路由选择协议

- 发送包含它们自己的链路状态的更新到网络上的所有其他路由器。例子是 OSPF、ISIS。
- 触发网络中变化通告的交换。
- 建立和维护从其他路由器来的 hello 包和链路状态通告（LSA）的逻辑数据库。
- 计算从该逻辑数据库到每个目的地的路径并把最佳路径放入路由表。

有类（FLSM）与无类（VLSM）

- 有类（默认 RIPv1、IGRP、EIGRP）：不通告子网掩码。
- 无类（RIPv2、IS-IS、OSPF、EIGRP）：通告子网掩码。

路由汇总

路由汇总/聚合/超网通过缩短子网掩码，只包括所有网络共同比特将几个网络子网描绘成一个大的网络地址。

RIP

语法：直接连接、有类网络：

```
Router(config)#router rip
Router(config-router)#network
192.168.111.0
Router(config-router)#network
192.168.165.0
```

EIGRP

- EIGRP：快收敛、VLSM 支持。
多协议支持：IP, IPX, AppleTalk。EIGRP 为每个协议维护路由选择、拓扑和邻居表。
- EIGRP 度量与 IGRP 相同，但为 32 比特，IGRP 为 24 比特。
- 后继路由是最佳路由，装入路由表。可行后继路由是拓扑结构表中的备份路由。
- EIGRP 最大跳计数=224。

OSPF

- 可缩放（不限制跳计数）、厂商中立的、链路状态、VLSM 支持。

OSPF 区域：

- 区域可被指定为从 0 到 65535 的任意数。
- 区域 0 是骨干区。

OSPF RouterID 标准：

- 一个环回（逻辑）接口上最高的 IP 地址。
- 如果没有环回，则最高 IP 地址在物理接口上。

DR/BDR 只在下列拓扑中推举：

► 广播多路访问（例如以太网）。

► 非广播多路访问（例如帧中继）。

为区域 0 中的网络 192.168.16.0/24 配置 OSPF：

```
Router(config)#router ospf 7
Router(config-router)#network
192.168.16.0 0.0.0.255 area 0
```

OSPF 度量 = 开销。开销 = 10^8 / 带宽 b/s

访问表

- 尾部暗示 deny any：每个访问表必须至少有一个是允许的，否则它会拒绝所有通信量。
- 标准型 IP 访问表基于源 IP 地址/网络过滤整个 IP 协议。数目范围 1~99。放在尽可能接近目的地的地方。
- 扩展型 IP 访问表基于源 IP 地址/网络、目的地 IP 地址/网络、指定协议（TCP、UDP、ICMP...）和端口号过滤。放在尽可能接近源的地方。
- 每个协议的每个接口的每个方向上有一个访问表。
- 通配符掩码：0 匹配；1 忽略地址中的相应比特。

扩展访问表语法：

```
access-list list# [permit | deny]
[protocol] [source ip]
[WCmask] [dest.
ip] [WCmask] [operator] [operand]
```

WAN

常见的 WAN 串行封装是：

- HDLC
- PPP
- 帧中继
- 链路两端的封装类型必须匹配

IPSec

IPSec 组件	描述	示例
安全协议	使用安全算法使通信安全的方法	认证报头 (AH) 封装安全有效载荷 (ESP)
密钥管理	负责交换在算法中使用的使 IP-sec VPN 安全的秘密密钥	因特网安全协会和密钥管理协议 (ISAKMP) 因特网密钥交换 (IKE) 安全密钥交换机制 (SKEME) Oakley
安全算法	用来使通信安全的数学算法	数据加密标准 (DES) 三重 DES (3DES) 高级加密标准 (AES) 报文摘要 (MD5) 安全散列算法 (SHA-1)

基本安全性

目标	描述	例子	缓解步骤
机密性	防止数据私密性被窃听	包捕获和重放	使用加密隐藏传输中数据的内容
完整性	防止数据被改变	中间人 (MitM) 攻击	使用散列获取数据指纹, 这样你就可以验证它没有从它的原始形式改变
可用性	保证数据、主机或服务能为它们的意图使用	拒绝服务 (DoS) 攻击	使用速率限制来阻止额外通信流量并安装最新的补丁

无线 LANs

为了增加安全性的无线安全方法:

- ▶ WEP——静态预共享密钥, 弱加密
- ▶ Cisco 过渡方案——动态密钥交换, 802.1x/EAP 认证, 每个包唯一密钥; 专用的
- ▶ WPA——带有 TKIP 的动态密钥; 预共享密钥或 802.1x 认证; Wi-Fi 联盟产品证书
- ▶ 802.11i/WAP2——AES 加密 (强); 动态密钥; 预共享密钥或 802.1x 认证; Wi-Fi 联盟产品证书

特性	802.11	802.11a	802.11b	802.11g	802.11n *
标准的日期	1997	1999	1999	2003	2008
最大速度 (DSSS)	不适用 1 或 2Mb/s FHSS	不适用	11Mb/s	不适用	每个数据流 11Mb/s
最大速度 (OFDM)	不适用	54Mb/s	不适用	54Mb/s	600Mb/s
分配的频段	2.4GHz	5GHz	2.4GHz	2.4GHz	2.4 和/或 5.0GHz
可用信道	11	23	11	11	11 或 23
近似范围	75 英尺	75 英尺	105 英尺	150 英尺	500 英尺

* 对于 802.11n, 这个标准批准前所有值为假定的。

网络地址转换

- ▶ NAT 将私有 IP 地址映射到公共注册的地址
- ▶ 静态: `ip nat inside source static [inside ip] [outside ip]`

术语

- ▶ 内部本地：分配给内部网络上一台主机的一个私有 IP 地址
- ▶ 内部全局：一个注册的因特网地址，它代表到一个外部网络的一台内部主机
- ▶ 外部全局：一台因特网主机的注册地址
- ▶ 外部本地：当出现在内部网络上时，因特网主机的地址

示例 PAT 配置，使用一个地址池（名为 MyPool，从 24.17.5.1 开始到 24.17.5.14 结束）转换：

```
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat pool MyPool 24.17.5.1 24.17.5.14 netmask 255.255.255.240
ip nat inside source list 1 pool MyPool overload
interface Ethernet 0
ip nat inside
interface serial 0
ip nat outside
```

PPP

- ▶ 厂商中立：Cisco 到非 Cisco
- ▶ 在单个 L2 链路上能封装多个 L3 协议

PPP 的配置

```
RtrA(config)#username RtrB password
samepass
RtrA(config)#interface bri 0
RtrA(config-if)#encapsulation ppp
RtrA(config-if)#ppp authentication chap

RtrB(config)#username RtrA password
samepass
RtrB(config)#interface bri 0
RtrB(config-if)#encapsulation ppp
RtrB(config-if)#ppp authentication chap
```

帧中继

- ▶ DLCI 识别路由器和帧交换机之间的电路（PVC）；DLCI 是帧中继中的 L2 地址。
- ▶ LMI 是路由器和本地帧中继交换机之间的信令。LMI 类型如下：
 - ▶ Cisco (DEFAULT)
 - ▶ ANSI
 - ▶ Q.933a
- ▶ 两个帧中继封装（两个路由器必须匹配）：
 - ▶ Cisco (默认)
 - ▶ IETF
- ▶ 点到点子接口解决水平分割问题并将一个子网映射到一个 DLCI。

- ▶ 如果使用子接口，则删除物理接口上的 IP 地址。
- ▶ 必须指定 sub-if 作为点到点或点到多点——自 IOS 12.0 以来无默认设置。
- ▶ 要映射第 3 层 IP 地址到第 2 层 DLCI，帧中继使用反向 ARP，或静态映射：

```
(config-if)#frame-relay map ip
    [next-hop-address] [local DLCI]
```

broadcast

broadcast 关键字允许在 PVC 上路由更新。

排错命令和输出

show interface serial 0

- ▶ 串口 0 是 Up/线路协议是 up：接口工作。
- ▶ 串口 0 是 Up/线路协议是 down：第 1 层是 up，第 2 层是 down（时钟或不匹配的帧类型）。
- ▶ 串口 0 是 down/线路协议是 down：第 1 层为 down（失效或远程端关闭）。
- ▶ 管理性 down/线路协议是 down：接口被关闭且必须没有不关闭的。

IPv6

IPv6 一般信息：

- ▶ IPsec 支持是强制和内置的。
- ▶ 报头大小固定为 40 字节/320 比特。
- ▶ 移动性内置但不强制。
- ▶ 过渡策略包括隧道、双栈和协议转换。

IPv6 地址：

- ▶ 128 比特长。
- ▶ 写成 8 组 4 个十六进制字符。
- ▶ 2001::/16=6to4 隧道地址。
- ▶ 单播地址分配给一台主机。
- ▶ 组播地址一次分配给一台或多台主机；以 FF00::/8 开始。
- ▶ 任播地址类似于组播，除了单播包将进入一台主机外，这台主机它是按路由选择度量确定的最靠近的。
- ▶ IPv6 决不广播；由组播代替。

IPv6 地址压缩：

给定地址 1010:0000:BBBB:000C:D000:0000:0000:0001

下面的地址表示是可能的：

- ▶ 丢弃打头的零：

1010:0:BBBB:C:D000:0:0:1

- ▶ 用:: 压缩连续全零的组的每个地址一次：

1010:0:BBBB:C:D000:1

关于作者

Andrew Whitaker (M.Sc.、CISSP、CCVP、CCNP、CCSP、CCNA、CCDA、MCSE、MCTS、CNE、CEI、CEH、ECSA、Security+、A+、Network+、Convergence+、CTP) 是 InfoSec 和网络公司的主任, Training Camp 公司的高级培训讲师。Training Camp 是一家国际培训公司, 通过它独一无二的加速学习模式, 它每年帮助数千 IT 专业人员通过认证。为 Training Camp 的专家教学已被华尔街杂志、Philadelphia 调查者、证书杂志和商业周刊收集。除了合著本书之外, Andrew 还合著了 Cisco 出版社题为《渗透考试和网络防线》一书, 并合著了关于 Cisco 认证的文章 CertificationZone。Andrew 目前正对其他图书进行著作和技术编辑。

drew 目前正在对其他图书进行著作和技术编辑。

献词

Mike Valentine: 本书献给既是绅士又是学者的 Rus Healy。

Andrew Whitaker: 献给 Reagan 和 Makayla。爸爸爱你们。

致谢

Mike Valentine: 我喜欢感谢我在 Skyline 的新朋友, 使我在权威 Cisco 培训的世界里受到欢迎。Andy、Frank、Dave 和 Toby 一直欣赏我的教学和专业经验, 并给我极大的机会学习和成长。这是我成为 Skyline 人的特权。

在 Pearson 的好人总是尽力热情指导不谦恭的著者。Brett、Vanessa、Chris 和所有背后工作的人们, 感谢你们出色的工作。

Steve Kalman 的指导是无价的, 没有什么能逃过他锐利的眼睛对本书仔细的评判。谢谢, Steve。

Liana 和 Jaine, 你们给我的生活带来乐趣。感谢你, 苹果土豆片和海盗公主。

最后, 感谢所有我的学生。记住我说的一切。

Andrew Whitaker: Brett Bartow 和 Chris Cleveland, 感谢继续信任我的工作。

Steve Kalman、Brian D' Andrea 和 Tami Day-Orsatti, 你们有惊人的知识财富并注重细节。我想我现在需要发给你们所有出错的新的补充。

Chris Porter、Steve Guadino 和 Dave Minutella, 别担心——这回不用着急了。

Jennifer, 让我有机会为 Que 工作。

192 号星巴克, 感谢你让我靠一杯咖啡一天工作八小时。

告诉我们你想什么

作为这本书的读者, 你是我们最重要的批评家和评论员。我们重视你的意见并想知道我们什么地方做得对、什么地方可以做得更好、你喜欢看我们出版的什么书和任何你愿意传递给我们的至理名言。

作为 Que 出版社的一名副主编, 我欢迎你的评论。你可以发电子邮件或直接给我写信让我知道你喜不喜欢这本书——以及我们怎样能把我们的书做得更好。

请注意, 对本书有关课题的技术问题我无法帮助你。但是, 我们有一个用户服务组, 我会把有关本书的技术问题转发到那里。

当你写信时请一定写明本书的书名和作者以及你的姓名、电子邮件地址和电话号码。我将仔细阅读你的评论并与本书的作者和编辑共享。

Email: feedback@quepublishing.com

Mail: Dave Dusthimer

Associate Publisher

Que Publishing
800 East 96th Street
Indianapolis, IN 46240 USA

青 春 的 活

读者服务

为了便于读者访问本书的任何更新、下载或可能有用的勘误表，请访问我们的网站并在 www.informit.com/title/0789737124 上注册这本书。