软考课程
5天通关

朱小平 编著

# 网络工程师的5天修炼

- 一线火爆网络工程师考试培训师、网络规划设计师朱小平老师激情分享
- 5天修炼，博一生精彩；名师一句，胜题海万千
- 5天精华，浓缩10年网络工程师培训经验
- 独特的方法，精辟的提炼，完整的内容，让3000余名考生轻松通过网络工程师考试

中国水利水电出版社
www.waterpub.com.cn

实现技术自由的梦想

# 网络工程师的5天修炼

修练5天 软考不难

**第1天**

“打好基础，掌握理论”。先掌握网络工程师考试最基础的内容，以网络体系结构的层次思想为指导，对网络有初步的认识。

**第2天**

“夯实基础，再学理论”。在了解网络基本通信模型的基础上，进一步学习网络安全、无线网络、存储技术和计算机的软硬件知识，涵盖了考试中的前十道非网络部分试题。

**第3天**

“动手操作，案例配置”。掌握网络工程中操作系统和服务器的各种实际操作，对Windows系统和Linux系统的基本配置有深入了解。

**第4天**

“再接再厉，案例实践”。学习网络工程中最核心的设备配置及综合应用的知识，包括交换机、路由器、防火墙的实际配置案例和网络规划设计，充分掌握考试中设备配置和网络设计的各知识点。

**第5天**

“模拟测试，反复操练”。进入全真的模拟考试，检验自己的学习效果，熟悉考试的题型和题量，进一步提升修炼成果。

ISBN 978-7-5084-9495-1
9 787508 494951 >
定价:38.00元

销售分类：认证考试/国家软考

软考课程5天通关

# 网络工程师的5天修炼

朱小平　编著

中国水利水电出版社
www.waterpub.com.cn

## 内 容 提 要

网络工程师考试是计算机技术与软件专业技术资格（水平）考试系列中一个重要的考试，它是计算机专业技术人员获得网络工程师职称的一个重要途径。但网络工程师考试涉及的知识点极广，几乎涵盖了本科计算机专业课程的全部内容，并且有一定的难度。

本书以作者多年从事软考教育培训和试题研究的心得体会建立了一个5天的复习架构。本架构通过深度剖析考试大纲并综合历年的考试情况，将网络工程师考试涉及的各知识点高度概括、整理，以知识图谱的形式将整个考试分解为一个个相互联系的知识点逐一讲解，并附以典型的考试试题和详细的试题分析解答以确保做到触类旁通。读者通过对本书中知识图谱的了解可以快速提高复习效率和准确度，做到复习有的放矢，考试便得心应手。最后还给出了一套全真的模拟试题并详细作了点评。

本书可作为参加网络工程师考试考生的自学用书，也可作为软考培训班的教材。

**图书在版编目（CIP）数据**

网络工程师的5天修炼 / 朱小平编著. -- 北京 : 中国水利水电出版社, 2012.3
（软考课程5天通关）
ISBN 978-7-5084-9495-1

Ⅰ. ①网… Ⅱ. ①朱… Ⅲ. ①计算机网络－工程技术人员－资格考试－自学参考资料 Ⅳ. ①TP393

中国版本图书馆CIP数据核字(2012)第030270号

**策划编辑：周春元　责任编辑：陈　洁　加工编辑：孙　丹　封面设计：李　佳**

| | |
|---|---|
| 书　名 | 软考课程5天通关<br>**网络工程师的5天修炼** |
| 作　者 | 朱小平　编著 |
| 出版发行 | 中国水利水电出版社<br>（北京市海淀区玉渊潭南路1号D座　100038）<br>网址：www.waterpub.com.cn<br>E-mail：mchannel@263.net（万水）<br>sales@waterpub.com.cn<br>电话：（010）68367658（发行部）、82562819（万水） |
| 经　售 | 北京科水图书销售中心（零售）<br>电话：（010）88383994、63202643、68545874<br>全国各地新华书店和相关出版物销售网点 |
| 排　版 | 北京万水电子信息有限公司 |
| 印　刷 | 北京蓝空印刷厂 |
| 规　格 | 184mm×240mm　16开本　21.625印张　556千字 |
| 版　次 | 2012年4月第1版　2012年4月第1次印刷 |
| 印　数 | 0001—3000册 |
| 定　价 | 38.00元 |

# I

# 前言

通过网络工程师考试已成为IT技术人员获得薪水和职称提升的必要条件，在企业和政府的信息化过程中也需要大量拥有网络工程师资质的专业人才，因此，每年都会有大批的“准网络工程师”参加这个考试。我们每年在全国各地进行的考前辅导中，与很多“准网络工程师”交流过，他们都反映出一个心声：“考试面涉及太广，通过考试不容易”。在这些学员当中，有的基础扎实，有的薄弱；有的是计算机专业科班出身，有的是学其他专业转行的；为什么都会有这样一个感觉呢？有的认为工作很忙，没有工夫来学习；有的认为年纪大了，理论性的知识不用多年，重新拾起不容易；有的认为理论扎实，但是经验欠缺。据此，考生最希望能得到老师给出的所谓的当次考试重点。但软考作为严肃的国家级考试不可能会在考前出现所谓的重点。因此，在这里我给各位准备考试的学员一个真诚的建议，与其等待所谓的重点，不如静下心来，看一看书，将工作的心得体会结合考试来理一理，或许就会有柳暗花明的感觉。考试能不能过关，主要还在于个人的修为。

为了帮助“准网络工程师”们，给合多年来辅导的心得，我想就以历次培训经典的5天时间、30个学时作为学习时序，取名为“网络工程师的5天修炼”，寄希望于考生能在5天的时间里有所飞跃。5天的时间很短，但真正深入学习也挺不容易。真诚地希望“准网络工程师”们能抛弃一切杂念，静下心来，花仅仅5天的时间，当作一个修炼项目来做，相信您一定会有意外的收获。

然而，考试的范围十分广泛，从信息化的基础知识到软件工程、操作系统、项目管理、知识产权、计算机网络基础，再到网络安全技术等领域知识，甚至这里的一个知识块在大学或研究生课程里就是一门功课。好在考试涉及的非网络部分知识深度不深，侧重点还在网络技术；好在考试毕竟有章可循，有一定的技巧和方法。

本书的“5天修炼”是这样来安排的：

第1天“打好基础，掌握理论”。先掌握网络工程师考试最基础的内容，以网络体系结构的层次思想为指导，对网络有初步的认识。

第2天“夯实基础，再学理论”。在了解网络基本通信模型的基础上，进一步学习网络安全、无线网络、存储技术和计算机的软硬件知识，涵盖了考试中的前十道非网络部分试题。

第3天“动手操作，案例配置”。掌握网络工程中操作系统和服务器的各种实际操作，对Windows

系统和 Linux 系统的基本配置有深入了解。

第 4 天“再接再厉，案例实践”。学习网络工程中最核心的设备配置及综合应用知识，包括交换机、路由器、防火墙的实际配置案例和网络规划设计，充分掌握考试中设备配置和网络规划设计的知识点。

第 5 天“模拟测试，反复操练”。进入全真的模拟考试，检验自己的学习效果，熟悉考试的题型和题量，进一步提升修炼成果。

不过也提醒“准网络工程师”们，不要只是为了考试而考试，一定是要抱着“修炼”的心态，通过考试只是目标之一，更多是要提高自身水平，将来在工作岗位上有所作为。

此外，要感谢中国水利水电出版社万水分社总编雷顺加、策划编辑周春元，他们的辛勤劳动和真诚约稿，也是我能编写此书的动力之一。感谢和我共事多年的邓子云和刘毅先生对本书的编写给出许多宝贵的意见，感谢湖南农业大学网络信息中心罗益荣主任和我的同事们、助手们，是他们帮助我做了大量的资料整理，甚至参与了部分编写工作。

然而，虽经多年锤炼，本人毕竟水平有限，敬请各位考生、各位培训师批评指正，不吝赐教。我的联系邮箱是：zhuxiaoping@hunau.net。

编 者

2012 年 2 月

# II

# 目　录


前言

**第 1 天　打好基础，掌握理论** …… 1

◎冲关前的准备 …… 1

◎考试形式解读 …… 1

◎答题注意事项 …… 1

◎制定复习计划 …… 2

**第 1 学时　网络体系结构** …… 3

1.1　OSI 参考模型 …… 4

1.1.1　考点分析 …… 4

1.1.2　知识点精讲 …… 4

1.2　TCP/IP 参考模型 …… 7

1.2.1　考点分析 …… 7

1.2.2　知识点精讲 …… 8

**第 2 学时　物理层** …… 9

2.1　数据通信理论知识 …… 9

2.1.1　考点分析 …… 9

2.1.2　知识点精讲 …… 10

2.2　数字传输系统 …… 19

2.2.1　考点分析 …… 19

2.2.2　知识点精讲 …… 19

2.3　接入技术 …… 20

2.3.1　考点分析 …… 20

2.3.2　知识点精讲 …… 20

2.4　有线传输介质 …… 23

2.4.1　考点分析 …… 23

2.4.2　知识点精讲 …… 23

2.5　其他知识点 …… 24

2.5.1　考点分析 …… 24

2.5.2　知识点精讲 …… 25

**第 3 学时　数据链路层** …… 25

3.1　检错与纠错 …… 26

3.1.1　考点分析 …… 26

3.1.2　知识点精讲 …… 26

3.2　点对点协议 …… 31

3.2.1　考点分析 …… 31

3.2.2　知识点精讲 …… 31

3.3　常见广播方式的数据链路层 …… 32

3.3.1　考点分析 …… 32

3.3.2　知识点精讲 …… 32

**第 4 学时　网络层** …… 40

4.1　IP 协议与 IP 地址 …… 40

4.1.1 考点分析 …… 40
4.1.2 知识点精讲 …… 41
4.2 地址规划与子网规划 …… 45
4.2.1 考点分析 …… 45
4.2.2 知识点精讲 …… 45
4.3 ICMP …… 49
4.3.1 考点分析 …… 49
4.3.2 知识点精讲 …… 49
4.4 ARP 和 RARP …… 51
4.4.1 考点分析 …… 51
4.4.2 知识点精讲 …… 51
4.5 IPv6 …… 53
4.5.1 考点分析 …… 53
4.5.2 知识点精讲 …… 53
4.6 NAT …… 55
4.6.1 考点分析 …… 55
4.6.2 知识点精讲 …… 55
**第 5 学时 传输层** …… 56
5.1 TCP …… 56
5.1.1 考点分析 …… 56
5.1.2 知识点精讲 …… 56
5.2 UDP …… 60
5.2.1 考点分析 …… 60
5.2.2 知识点精讲 …… 60
**第 6 学时 应用层** …… 62
6.1 DNS …… 63
6.1.1 考点分析 …… 63
6.1.2 知识点精讲 …… 63
6.2 DHCP …… 67
6.2.1 考点分析 …… 67
6.2.2 知识点精讲 …… 67
6.3 WWW 与 HTTP …… 69
6.3.1 考点分析 …… 69
6.3.2 知识点精讲 …… 69
6.4 Email …… 71
6.4.1 考点分析 …… 71
6.4.2 知识点精讲 …… 71
6.5 FTP …… 72
6.5.1 考点分析 …… 72
6.5.2 知识点精讲 …… 72
6.6 SNMP …… 74
6.6.1 考点分析 …… 74
6.6.2 知识点精讲 …… 74
6.7 其他应用协议 …… 79
6.7.1 考点分析 …… 79
6.7.2 知识点精讲 …… 79
**第 2 天 夯实基础，再学理论** …… 81
**第 1 学时 网络安全** …… 81
7.1 安全设计、原则与审计 …… 82
7.1.1 考点分析 …… 82
7.1.2 知识点精讲 …… 82
7.2 可靠性 …… 83
7.2.1 考点分析 …… 83
7.2.2 知识点精讲 …… 83
7.3 网络安全威胁 …… 85
7.3.1 考点分析 …… 85
7.3.2 知识点精讲 …… 86
7.4 加密算法与信息摘要 …… 87
7.4.1 考点分析 …… 87
7.4.2 知识点精讲 …… 88
7.5 数字签名与数字证书 …… 90
7.5.1 考点分析 …… 90
7.5.2 知识点精讲 …… 90
7.6 密钥分配 …… 92
7.6.1 考点分析 …… 92
7.6.2 知识点精讲 …… 92
7.7 SSL、HTTPS …… 94
7.7.1 考点分析 …… 94

7.7.2 知识点精讲 ····· 94
7.8 RADIUS ····· 95
7.8.1 考点分析 ····· 95
7.8.2 知识点精讲 ····· 95
7.9 VPN ····· 97
7.9.1 考点分析 ····· 97
7.9.2 知识点精讲 ····· 97
7.10 网络隔离与入侵检测 ····· 100
7.10.1 考点分析 ····· 100
7.10.2 知识点精讲 ····· 100
**第 2 学时 无线基础知识** ····· 102
8.1 无线局域网 ····· 102
8.1.1 考点分析 ····· 102
8.1.2 知识点精讲 ····· 102
8.2 无线局域网安全 ····· 106
8.2.1 考点分析 ····· 106
8.2.2 知识点精讲 ····· 106
8.3 无线局域网配置 ····· 107
8.3.1 考点分析 ····· 107
8.3.2 知识点精讲 ····· 107
8.4 3G ····· 110
8.4.1 考点分析 ····· 110
8.4.2 知识点精讲 ····· 110
**第 3 学时 存储技术基础** ····· 111
9.1 RAID ····· 111
9.1.1 考点分析 ····· 111
9.1.2 知识点精讲 ····· 111
9.2 NAS 和 SAN ····· 112
9.2.1 考点分析 ····· 112
9.2.2 知识点精讲 ····· 112
**第 4 学时 网络规划与设计** ····· 113
10.1 网络生命周期 ····· 113
10.1.1 考点分析 ····· 113
10.1.2 知识点精讲 ····· 113
10.2 网络需求分析 ····· 114
10.2.1 考点分析 ····· 114
10.2.2 知识点精讲 ····· 114
10.3 通信规范 ····· 114
10.3.1 考点分析 ····· 114
10.3.2 知识点精讲 ····· 115
10.4 逻辑网络设计 ····· 115
10.4.1 考点分析 ····· 115
10.4.2 知识点精讲 ····· 116
10.5 物理网络设计 ····· 117
10.5.1 考点分析 ····· 117
10.5.2 知识点精讲 ····· 117
**第 5 学时 计算机硬件知识** ····· 119
11.1 CPU 体系结构 ····· 119
11.1.1 考点分析 ····· 119
11.1.2 知识点精讲 ····· 119
11.2 流水线技术 ····· 122
11.2.1 考点分析 ····· 122
11.2.2 知识点精讲 ····· 122
11.3 内存结构与寻址 ····· 124
11.3.1 考点分析 ····· 124
11.3.2 知识点精讲 ····· 124
11.4 数的表示与计算 ····· 126
11.4.1 考点分析 ····· 126
11.4.2 知识点精讲 ····· 126
11.5 总线与中断 ····· 128
11.5.1 考点分析 ····· 128
11.5.2 知识点精讲 ····· 128
**第 6 学时 计算机软件知识** ····· 129
12.1 操作系统概念 ····· 130
12.1.1 考点分析 ····· 130
12.1.2 知识点精讲 ····· 130
12.2 软件开发 ····· 133
12.2.1 考点分析 ····· 133

12.2.2 知识点精讲……133
12.3 项目管理基础……140
12.3.1 考点分析……140
12.3.2 知识点精讲……141
12.4 软件知识产权……143
12.4.1 考点分析……143
12.4.2 知识点精讲……144
**第 3 天 动手操作，案例配置**……148
**第 1 学时 必考题 1——Windows 管理**……148
13.1 域与活动目录……148
13.1.1 考点分析……148
13.1.2 知识点精讲……149
13.2 用户与组……152
13.2.1 考点分析……152
13.2.2 知识点精讲……152
13.3 文件系统与分区管理……153
13.3.1 考点分析……153
13.3.2 知识点精讲……154
**第 2 学时 上、下午考试共同考点 1——Windows 命令**……155
14.1 IP 配置网络命令……155
14.1.1 考点分析……155
14.1.2 知识点精讲……155
14.2 系统管理命令……165
14.2.1 考点分析……165
14.2.2 知识点精讲……165
**第 3 学时 案例难点 1——Windows 配置**……166
15.1 DNS 服务器配置……166
15.1.1 考点分析……166
15.1.2 知识点精讲……166
15.2 DHCP 服务器配置……171
15.2.1 考点分析……171
15.2.2 知识点精讲……172
15.3 Web 服务器配置……175
15.3.1 考点分析……175
15.3.2 知识点精讲……175
15.4 FTP 服务器配置……180
15.4.1 考点分析……180
15.4.2 知识点精讲……180
15.5 远程访问与路由配置……186
15.5.1 考点分析……186
15.5.2 知识点精讲……186
**第 4 学时 必考题 2——Linux 管理**……190
16.1 分区与文件管理……190
16.1.1 考点分析……190
16.1.2 知识点精讲……191
16.2 系统启动过程……193
16.2.1 考点分析……193
16.2.2 知识点精讲……193
16.3 系统运行级别……196
16.3.1 考点分析……196
16.3.2 知识点精讲……196
16.4 守护进程……198
16.4.1 考点分析……198
16.4.2 知识点精讲……198
16.5 常见配置文件……199
16.5.1 考点分析……199
16.5.2 知识点精讲……200
**第 5 学时 上、下午考试共同考点 2——Linux 命令**……201
17.1 系统与文件管理命令……201
17.1.1 考点分析……201
17.1.2 知识点精讲……201
17.2 网络配置命令……209
17.2.1 考点分析……209
17.2.2 知识点精讲……210
**第 6 学时 案例难点 2——Linux 配置**……217
18.1 DNS 服务器配置……217

18.1.1 考点分析 ····· 218
18.1.2 知识点精讲 ····· 218
18.2 DHCP 服务器配置 ····· 223
18.2.1 考点分析 ····· 223
18.2.2 知识点精讲 ····· 223
18.3 FTP 服务器配置 ····· 227
18.3.1 考点分析 ····· 227
18.3.2 知识点精讲 ····· 227
18.4 Web 服务器配置 ····· 231
18.4.1 考点分析 ····· 231
18.4.2 知识点精讲 ····· 231
**第 4 天 再接再厉，案例实践** ····· 234
**第 1 学时 交换基础** ····· 234
19.1 交换机概述 ····· 234
19.1.1 考点分析 ····· 234
19.1.2 知识点精讲 ····· 235
19.2 交换机工作原理 ····· 238
19.2.1 考点分析 ····· 238
19.2.2 知识点精讲 ····· 238
**第 2 学时 案例重点 1——交换机配置** ····· 239
20.1 交换机基础配置 ····· 239
20.1.1 考点分析 ····· 239
20.1.2 知识点精讲 ····· 240
20.2 端口配置 ····· 243
20.2.1 考点分析 ····· 243
20.2.2 知识点精讲 ····· 243
20.3 VLAN、VTP 配置 ····· 246
20.3.1 考点分析 ····· 246
20.3.2 知识点精讲 ····· 246
20.4 STP ····· 253
20.4.1 考点分析 ····· 253
20.4.2 知识点精讲 ····· 253
20.5 HSRP ····· 257
20.5.1 考点分析 ····· 257
20.5.2 知识点精讲 ····· 258
**第 3 学时 路由基础** ····· 258
21.1 路由器概述 ····· 258
21.1.1 考点分析 ····· 258
21.1.2 知识点精讲 ····· 258
21.2 路由器原理 ····· 259
21.2.1 考点分析 ····· 259
21.2.2 知识点精讲 ····· 259
21.3 端口种类 ····· 260
21.3.1 考点分析 ····· 260
21.3.2 知识点精讲 ····· 260
**第 4 学时 案例重点 2——路由配置** ····· 262
22.1 路由器基础配置 ····· 262
22.1.1 考点分析 ····· 262
22.1.2 知识点精讲 ····· 262
22.2 RIP ····· 266
22.2.1 考点分析 ····· 266
22.2.2 知识点精讲 ····· 266
22.3 OSPF ····· 268
22.3.1 考点分析 ····· 268
22.3.2 知识点精讲 ····· 268
22.4 BGP ····· 272
22.4.1 考点分析 ····· 272
22.4.2 知识点精讲 ····· 272
22.5 IGRP 和 EIGRP ····· 274
22.5.1 考点分析 ····· 274
22.5.2 知识点精讲 ····· 274
22.6 IPv6 ····· 274
22.6.1 考点分析 ····· 274
22.6.2 知识点精讲 ····· 275
22.7 NAT ····· 276
22.7.1 考点分析 ····· 276
22.7.2 知识点精讲 ····· 277
**第 5 学时 案例难点 3——防火墙配置** ····· 278

23.1 防火墙基本知识……279
23.1.1 考点分析……279
23.1.2 知识点精讲……279
23.2 ACL……280
23.2.1 考点分析……280
23.2.2 知识点精讲……280
23.3 防火墙基本配置……283
23.3.1 考点分析……283
23.3.2 知识点精讲……283
**第 6 学时 案例难点 4——VPN 配置**……284
24.1 IPSec VPN 配置基本知识……285
24.2 IPSec VPN 配置……286
**第 5 天 模拟测试，反复操练**……289
第 1～2 学时 模拟测试 1（上午试题）……289
第 3～4 学时 模拟测试 1（下午试题）……298
第 5～6 学时 模拟测试 1 点评（上午试题）303
第 7～8 学时 模拟测试 1 点评（下午试题）315
**后记**……319
**附录一 网络工程师考试常考公式、要点汇总表**……320
**附录二 网络工程师考试常用术语汇总表**……326
**参考文献**……335

# 第1天

# 打好基础，掌握理论

## 冲关前的准备

不管基础如何、学历如何，拿到这本书的就算是有缘人。5天的关键学习并不需要准备太多的东西，不过还是在此罗列出来，以做一些必要的简单准备。

（1）本书。如果看不到本书那真是太遗憾了。

（2）至少20张草稿纸。

（3）1支笔。

（4）处理好自己的工作和生活，以使这5天能静下心来学习。

## 考试形式解读

网络工程师考试有两场，分为上午考试和下午考试，两场在同一天的考试中都过关才能算这个级别的考试过关。

上午考试的内容是计算机与网络知识，考试时间为150分钟，笔试，选择题，而且全部是单项选择题，其中含5分的英文题。上午考试总共75道题，共计75分，按60%计，45分算过关。

下午考试的内容是网络系统设计与管理，考试时间为150分钟，笔试，问答题。一般为5道大题，每道大题15分，有若干个小问，总计75分，按60%计，45分算过关。

## 答题注意事项

上午考试答题时要注意以下事项：

（1）记得带2B以上的铅笔和一块比较好的橡皮。上午考试答题采用填涂答题卡的形式，阅卷是由机器阅卷的，所以需要使用2B以上的铅笔；带好一点的橡皮是为了修改选项时擦得比较干净。

（2）注意把握考试时间，虽然上午考试时间有150分钟，但是题量还是比较大的，一共75道题，做一道题还不到2分钟，因为还要留出10分钟左右来填涂答题卡和检查核对。笔者的考

试经验是做20道左右的试题就在答题卡上填涂完这20道题，这样不会慌张，也不会明显地影响进度。

（3）做题先易后难。上午考试一般前面的试题会容易一点，大多是知识点性质的题目，但也会有一些计算题，有些题还会有一定的难度，个别试题还会出现新概念题（即在教材中找不到答案，平时工作也可能很少接触），这些题常出现在60～70题之间。考试时建议先将容易做的和自己会的做完，其他的先跳过去，在后续的时间中再集中精力做难题。

下午考试答题采用的是专用答题纸，既有选择题，也有填空题。下午考试答题要注意以下事项：

（1）先易后难。先大致浏览一下5道考题，考试往往既会有知识点问答题，也会有计算题，同样先将自己最为熟悉和最有把握的题先完成，再重点攻关难题。

（2）问答题最好以要点形式回答。阅卷时多以要点给分，不一定要与参考答案一模一样，但常以关键词语或语句意思表达相同或接近为判断是否给分或给多少分的标准。因此答题时要点要多写一些，以涵盖到参考答案中的要点。比如，如果题目中某问题给的是5分，则极可能是5个要点，一个要点1分，回答时最好能写出7个左右的要点。

（3）配置题分数一定要拿住。网络工程师的配置题分值大、形式固定、内容变化也不大，熟悉基本和常见的配置命令和配置流程就能拿高分。

## ◎制定复习计划

5天的关键学习对于每个考生来说都是一个挑战，这么多的知识点要在短短的5天时间内翻个底朝天，是很不容易的，也是非常紧张的，但也是值得的。学习完这5天，相信您会感到非常充实，考试也会胜券在握。先看看这5天的内容是如何安排的吧（如表1-1所示）。



表1-1　5天修炼学习计划表

| 时间 | | 学习内容 |
|---|---|---|
| 第1天　打好基础，掌握理论 | 第1学时 | 网络体系结构 |
| | 第2学时 | 物理层 |
| | 第3学时 | 数据链路层 |
| | 第4学时 | 网络层 |
| | 第5学时 | 传输层 |
| | 第6学时 | 应用层 |
| 第2天　夯实基础，再学理论 | 第1学时 | 网络安全 |
| | 第2学时 | 无线基础知识 |
| | 第3学时 | 存储技术基础 |
| | 第4学时 | 网络规划与设计 |
| | 第5学时 | 计算机硬件知识 |
| | 第6学时 | 计算机软件知识 |

续表

| 时间 | | 学习内容 |
| --- | --- | --- |
| 第 3 天 动手操作，案例配置 | 第 1 学时 | Windows 管理 |
| | 第 2 学时 | Windows 命令 |
| | 第 3 学时 | Windows 配置 |
| | 第 4 学时 | Linux 管理 |
| | 第 5 学时 | Linux 命令 |
| | 第 6 学时 | Linux 配置 |
| 第 4 天 再接再厉，案例实践 | 第 1 学时 | 交换机基础 |
| | 第 2 学时 | 交换机配置 |
| | 第 3 学时 | 路由基础 |
| | 第 4 学时 | 路由配置 |
| | 第 5 学时 | 防火墙 |
| | 第 6 学时 | VPN |
| 第 5 天 模拟测试，反复操练 | 第 1～2 学时 | 模拟测试 1（上午试题） |
| | 第 3～4 学时 | 模拟测试 1（下午试题） |
| | 第 5～6 学时 | 模拟测试 1（上午试题点评） |
| | 第 7～8 学时 | 模拟测试 1（下午试题点评） |

从笔者这几年的考试培训经验来看，不怕您基础不牢，怕的就是您不进入状态。闲话不多说了，开始第 1 天的复习吧。

## 第 1 学时　网络体系结构

第 1 天的第 1 学时主要学习网络体系结构。“网络体系结构”是计算机网络技术的基础知识点，是现代网络技术的整体蓝图，是学习和复习网络工程师考试的前提。根据历年考试的情况来看，每次考试涉及相关知识点的分值在 0～5 分之间，且只有上午考试部分涉及。本章考点知识结构图如图 1-1 所示。

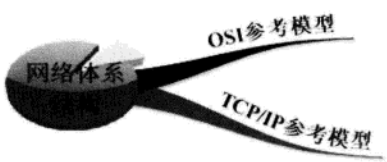



图 1-1　考点知识结构图

## 1.1 OSI参考模型

主要讲述OSI参考模型、OSI各层功能的作用、协议组成等重要基础知识。

### 1.1.1 考点分析

历年网络工程师考试试题中，涉及本部分的相关知识点有：服务访问点的定义和组成；OSI参考模型各层的定义、功能和数据单位；OSI参考模型各子层对应的具体协议。

### 1.1.2 知识点精讲

设计一个好的网络体系结构是一个复杂的工程，好的网络体系结构使得相互通信的计算终端能够高度协同工作。ARPANET 在早期就提出了分层方法，把复杂问题分割成若干个小问题来解决。1974年，IBM第一次提出了**系统网络体系结构**（System Network Architecture，SNA）概念，SNA第一个应用了分层的方法。

随着网络飞速发展，用户迫切要求能在不同体系结构的网络间交换信息，不同网络能互连起来。**国际标准化组织**（International Standard Organized，ISO）从1977年开始研究这个问题，并与1979年提出了一个互联的标准框架，即著名的**开放系统互连参考模型**（Open System Interconnection/Reference Model，OSI/RM），简称OSI模型。1983年形成了OSI/RM的正式文件，即**ISO 7498标准**，即常见的七层协议的体系结构。网络体系结构也可以定义为计算机网络各层及协议的集合，这样，OSI本身就算不上一个网络体系结构，因为没有定义每一层所用到的服务和协议。体系结构是抽象的概念，实现是具体的概念，实际运行的是硬件和软件。

开放系统互连参考模型分七层，从低到高分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。

1. *物理层*（Physical Layer）

物理层位于OSI/RM参考模型的最底层，为数据链路层实体提供建立、传输、释放所必须的物理连接，并且提供**透明的比特流传输**。物理层的连接可以是全双工或半双工方式，传输方式可以是异步或同步方式。物理层的数据单位是**比特**，即一个二进制位。物理层构建在物理传输介质和硬件设备相连接之上，向上服务于紧邻的数据链路层。

物理层通过各类协议定义了网络的机械特性、电气特性、功能特性和规程特性。

- **机械特性**：规定接口的外形、大小、引脚数和排列、固定位置。
- **电气特性**：规定接口电缆上各条线路出现的电压范围。
- **功能特性**：指明某条线上出现某一电平的电压表示何种意义。
- **规程特性**：指明各种可能事件出现的顺序。

物理层的两个重要概念：DCE和DTE。

- **数据终端设备**（Data Terminal Equipment，DTE）：具有一定的数据处理能力和数据收发能

力的设备，用于提供或接收数据。常见的 DTE 设备有路由器、PC、终端等。

- **数据通信设备**（Data Communications Equipment，DCE）：在 DTE 和传输线路之间提供信号变换和编码功能，并负责建立、保持和释放链路的连接。常见的 DCE 设备有 CSU/DSU、NT1、广域网交换机、MODEM 等。

两者的区别是：**DEC提供时钟**，而**DTE不提供时钟**；DTE的接头是针头（俗称公头），而DCE的接头是孔头（俗称母头）。

2. 数据链路层（Data Link Layer）

数据链路层将原始的传输线路转变成一条逻辑的传输线路，实现实体间二进制信息块的正确传输，为网络层提供可靠的数据信息。数据链路层的数据单位是**帧**，具有流量控制功能。**链路**是相邻两节点间的物理线路。数据链路与链路是两个不同的概念。**数据链路**可以理解为数据的通道，是物理链路加上必要的通信协议而组成的逻辑链路。

数据链路层应具有的功能：

- 链路连接的建立、拆除和分离：数据传输所依赖的介质是长期的，但传输数据的实体间的连接是有生存期的。在连接生存期内，收发两端可以进行不等的一次或多次数据通信，每次通信都要经过建立通信联络、数据通信和拆除通信联络这三个过程。
- 帧定界和帧同步：数据链路层的数据传输单元是帧，由于数据链路层的协议不同，帧的长短和界面也不同，所以必须对帧进行定界和同步。
- 顺序控制：对帧的收发顺序进行控制。
- 差错检测、恢复：差错检测多用方阵码校验和循环码校验来检测信道上数据的误码，而帧丢失等用序号检测。各种错误的恢复则常靠反馈重发技术来完成。
- 链路标识、流量/拥塞控制。

局域网中的数据链路层可以分为**逻辑链路控制**（Logical Link Control，LLC）和**介质访问控制**（Media Access Control，MAC）两个子层。其中 LLC 只在使用 802.3 格式的时候才会用到，而如今很少使用 802.3 格式，取而代之的是以太帧格式，而使用以太帧格式则不会有 LLC 存在。

3. 网络层（Network Layer）

网络层控制子网的通信，其主要功能是提供**路由选择**，即选择到达目的主机的最优路径并沿着该路径传输数据包。网络层还应具备的功能有：路由选择和中继；激活和终止网络连接；链路复用；差错检测和恢复；流量/拥塞控制等。

4. 传输层（Transport Layer）

传输层利用实现可靠的**端到端的数据传输**能实现数据**分段、传输和组装**，还提供差错控制和流量/拥塞控制等功能。

5. 会话层（Session Layer）

会话层允许不同机器上的用户之间建立会话。会话就是指各种服务，包括对话控制（记录该由谁来传递数据）、令牌管理（防止多方同时执行同一关键操作）、同步功能（在传输过程中设置检查点，以便在系统崩溃后还能在检查点上继续运行）。

建立和释放会话连接还应做以下工作：

- 将会话地址映射为传输层地址。
- 进行数据传输。
- 释放连接。

6. *表示层*（Presentation Layer）

表示层提供一种通用的数据描述格式，便于不同系统间的机器进行信息转换和相互操作，如会话层完成EBCDIC编码（大型机上使用）和ASCII码（PC机器上使用）之间的转换。表示层的主要功能有：数据语法转换、语法表示、数据加密和解密、数据压缩和解压。

7. *应用层*（Application Layer）

应用层位于OSI/RM参考模型的最高层，直接针对用户的需要。应用层向应用程序提供服务，这些服务按其向应用程序提供的特性分成组并称为服务元素。应用层服务元素又分为公共应用服务元素（Common Application Service Element，CASE）和特定应用服务元素（Specific Application Service Element，SASE）。

下面再介绍几个网络工程师考试涉及的重要考点及概念：

（1）封装。OSI/RM参考模型的许多层都使用特定方式描述信道中来回传送的数据。数据在从高层向低层传送的过程中，每层都对接收到的原始数据添加信息，通常是附加一个报头和报尾，这个过程称为封装。

（2）网络协议。网络协议（简称**协议**）为网络中的数据交换建立的一系列规则、标准或约定。协议是控制两个（或多个）对等实体进行通信的集合。

网络协议由**语法、语义和时序关系**三个要素组成。

- 语法：数据与控制信息的结构或形式。
- 语义：根据需要发出哪种控制信息，依据情况完成哪种动作以及做出哪种响应。
- 时序关系：又称为同步，即事件实现顺序的详细说明。

（3）PDU。协议数据单元（Protocol Data Unit，PDU）是指对等层次之间传送的数据单位。如在数据从会话层传送到传输层的过程中，传输层把数据PDU封装在一个传输层数据段中。如图1-2所示描述了OSI参考模型数据封装流程及各层对应的PDU。

（4）实体。任何可以接收或发送信息的硬件/软件进程通常是一个特定的软件模块。

（5）服务。在协议的控制下，两个对等实体间的通信使得本层能为上一层提供服务。要实现本层协议，还需要使用下一层所提供的服务。

协议和服务区别是：本层服务实体只能看见服务而无法看见下面的协议。协议是“水平的”，是针对两个对等实体的通信规则；服务是“垂直的”，是由下层向上层通过层间接口提供的。只有能被高一层实体“看见”的功能才能称为服务。

（6）服务原语。上层使用下层所提供的服务必须通过与下层交换一些命令，这些命令就称为服务原语。

（7）服务数据单元。OSI把层与层之间交换的数据的单位称为服务数据单元（Service Data

Unit，SDU）。相邻两层的关系如图 1-3 所示。

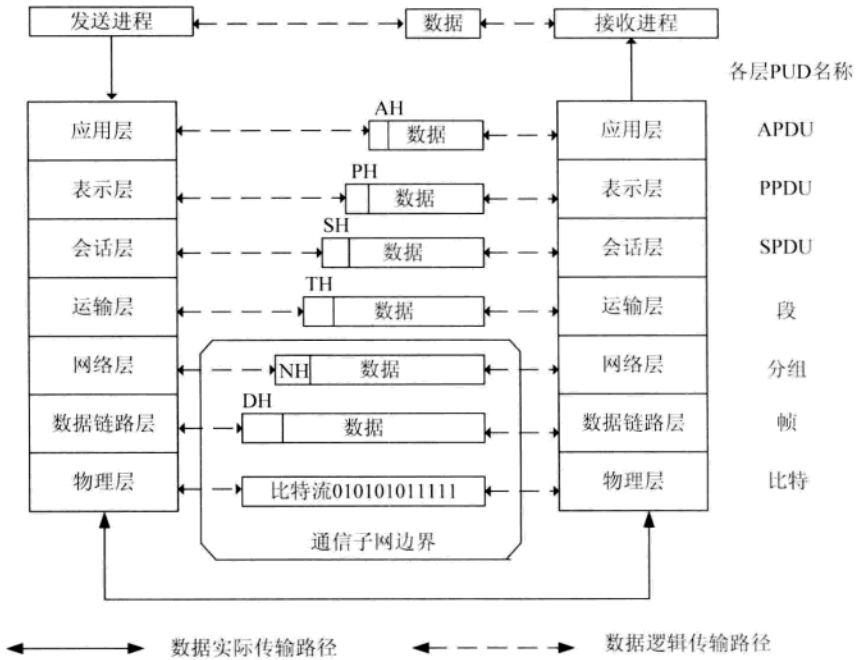



图 1-2 OSI 参考模型通信示意图

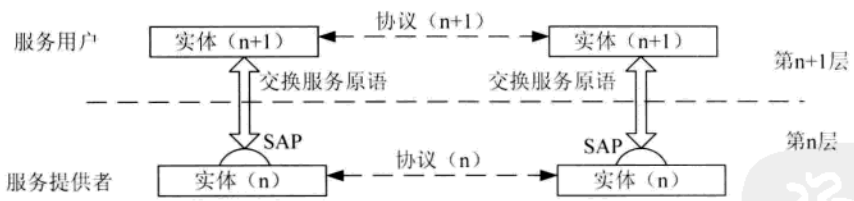



图 1-3 相邻两层关系

## 1.2 TCP/IP 参考模型

主要讲述 TCP/IP 参考模型和 TCP/IP 参考模型各层功能的作用等重要基础知识。

### 1.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：各种常见的协议对应的层次关系。

### 1.2.2 知识点精讲

OSI 参考模型虽然完备，但是太过复杂，不实用。而之后的 TCP/IP 参考模型经过一系列的修改和完善得到了广泛的应用。TCP/IP 参考模型包含应用层、传输层、网络层和网络接口层。TCP/IP 参考模型与 OSI 参考模型有较多相似之处，各层也有一定的对应关系，具体对应关系如图 1-4 所示。

| OSI | TCP/IP |
|---|---|
| 应用层 | 应用层 |
| 表示层 | |
| 会话层 | |
| 传输层 | 传输层 |
| 网络层 | 网络层 |
| 数据链路层 | 网络接口层 |
| 物理层 | |

图 1-4　TCP/IP 参考模型与 OSI 参考模型的对应关系

（1）应用层。TCP/IP 参考模型的应用层包含了所有高层协议。该层与 OSI 的会话层、表示层和应用层相对应。

（2）传输层。TCP/IP 参考模型的传输层与 OSI 的传输层相对应。该层允许源主机与目标主机上的对等体之间进行对话。该层定义了两个端到端的传输协议：TCP 协议和 UDP 协议。

（3）网络层。TCP/IP 参考模型的网络层对应 OSI 的网络层。该层负责为经过逻辑互联网络路径的数据进行路由选择。

（4）网络接口层。TCP/IP 参考模型的最低层是网络接口层，该层在 TCP/IP 参考模型中并没有明确规定。

TCP/IP 参考模型是一个协议族，各层对应的协议已经得到广泛应用，具体的各层协议对应 TCP/IP 参考模型的哪一层往往是考试的重点。TCP/IP 参考模型主要协议的层次关系如图 1-5 所示。

TCP/IP 参考模型与 OSI 参考模型有很多相同之处，都是以协议栈为基础的，对应各层功能也大体相似。当然也有一些区别，如 OSI 模型最大的优势是强化了服务、接口和协议的概念，这种做法能明确什么是规范、什么是实现，侧重理论框架的完备。TCP/IP 模型是事实上的工业标准，而改进后的 TCP/IP 模型却没有做到，因此其并不适用于新一代网络架构设计。TCP/IP 模型没有区分物理层和数据链路层这两个功能完全不同的层。OSI 模型比较适合理论研究和新网络技术研究，而 TCP/IP 模型真正做到了流行和应用。

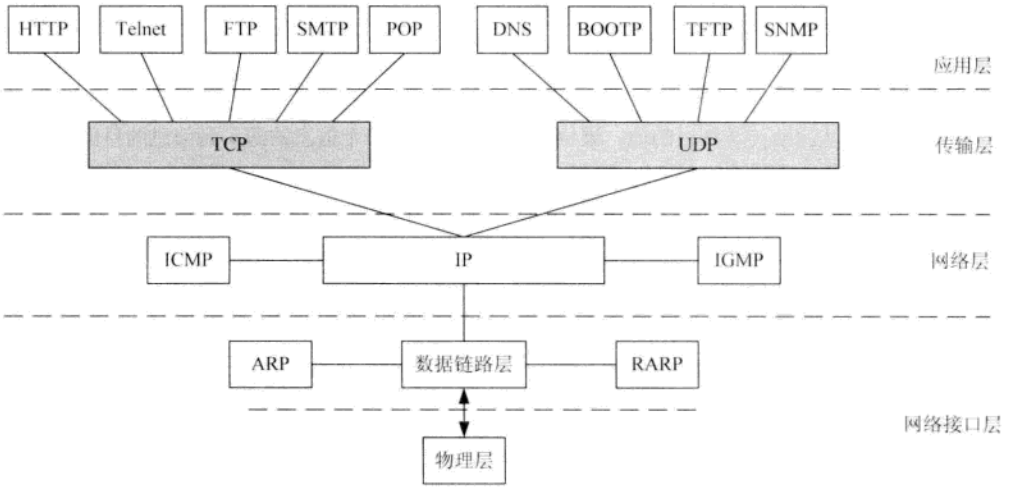



图 1-5 TCP/IP 参考模型主要协议的层次关系图

# 第 2 学时 物理层

第 1 天的第 2 学时主要学习物理层所涉及的重要知识点。物理层是协议模型的最底层，因此包含相当多的理论知识和应用性技术，是历年考试的核心考点之一。根据历年考试的情况来看，每次考试涉及的相关知识点的分值约在 3～20 分之间。物理层知识的考察主要集中在上午的考试中，下午的考试更偏向于对综合布线知识、ADSL、HFC 等知识点的考察。本章考点知识结构图如图 2-1 所示。

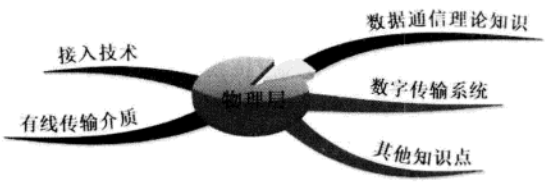



图 2-1 考点知识结构图

## 2.1 数据通信理论知识

### 2.1.1 考点分析

历年网络工程师考试试题涉本此部分的相关知识点有：数据通信基本概念、传输速率、调制与

编码、数据传输方式、数据交换方式、多路复用。

### 2.1.2 知识点精讲

**通信**就是将信息从源地传送到目的地。**通信研究**就是解决从一个信息的源头到信息的目的地整个过程的技术问题。**信息**是通过通信系统传递的内容，其形式可以是声音、动画、图像、文字等。

通信信道上传输的电信号编码、电磁信号编码、光信息编码叫做**信号**。信号可以分为模拟信号和数字信号两种。**模拟信号**是在一段连续的时间间隔内，其代表信息的特征量可以在任意瞬间呈现为任意数值的信号；**数字信号**是信息用若干个明确定义的离散值表示的时间离散信号。可以简单地认为，模拟信号值是连续的，而数字信号值是离散的。

传送信号的通路称为**信道**，信道也可以是模拟或数字方式，传输模拟信号的信道叫做**模拟信道**；传输数字信号的信道叫做**数字信道**。

信息传输过程可以进行抽象，通常称为数据通信系统模型，具体如图 2-2 所示。

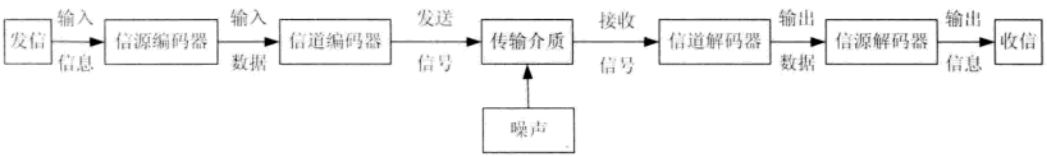



图 2-2 数据通信系统模型

（1）发信是信息产生的源头，可以是人，也可以是硬件。

（2）信源编码器的作用是进行**模/数转换**（A/D 转换），即将文字、声音、动画、图像等转换为数字信号或模拟信号。计算机或终端可以看作信源编码器。由计算机或终端产生的数字信号的频谱都是从零开始的，这种**未经调制**的信号所占用的频率范围叫做**基本频带**（这个频带从直流起可以高到数百千赫兹，甚至数千赫兹），简称为**基带**。局域网中的信源编码器发出的信号往往是基本频带信号，简称为**基带信号**。

另外，当采用模拟信号传输数据时往往只占用**有限的频带**，使用频带传输的信号简称为**频带信号**。通过借助将基带划分为多个频带方式可以将链路容量分解成两个或更多信道，每个信道可以携带不同的信号，这就是**宽带传输**。

（3）信道编码器的作用是将信号转换为合适的形式对传输介质进行数据传输。

（4）信道解码器将传输介质和传输数据转换为接收信号。

（5）信源解码器的作用是进行**数/模转换**（D/A 转换），即将数字信号或模拟信号转换为文字、声音、动画、图像等。

1. 传输速率

数字通信系统的有效程度可以用码元传输速率和信息传输速率来表示。

码元：在数字通信中常用时间间隔相同的符号来表示一个二进制数字，这样的时间间隔内的信号称为二进制码元。另一种定义是，在使用时间域（时域）的波形表示数字信号时，代表不同离散

数值的基本波形就称为码元。网络工程师考试中常用的是第二种定义。

码元速率（波特率）：即单位时间内载波参数（相位、振幅、频率等）变化的次数，单位为波特，常用符号 Baud 表示，简写成 B。

比特率（信息传输速率、信息速率）：指单位时间内在信道上传送的数据量（即比特数），单位为比特每秒（bit/s），简记为 b/s 或 bps。

比特率与波特率关系：

波特率与比特率有如下换算关系：

$$\text{比特率} = \text{波特率} \times \text{单个调制状态对应的二进制位数} = \text{波特率} \times \log_2^N \qquad (2\text{-}1)$$

其中，N 是码元总类数。

带宽：传输过程中信号不会明显减弱的一段频率范围，单位为赫兹（Hz）。对于模拟信道而言，信道带宽计算公式如下：

$$\text{信道带宽 W=最高频率–最低频率} \qquad (2\text{-}2)$$

信噪比与分贝：信号功率与噪声功率的比值称为信噪比，通常将信号功率记为 S，噪声功率记为 N，则信噪比为 S/N。通常人们不使用信噪比本身，而是使用 10lgS/N 的值，即分贝（dB 或 decibel）。

$$1\text{dB} = 10 \times \log_{10} S/N \qquad (2\text{-}3)$$

无噪声时的数据速率计算：在无噪声情况下应依据尼奎斯特定理来计算最大数据速率。尼奎斯特定理为：

$$\text{最大数据速率} = 2W\log_2 N = B\log_2 N \qquad (2\text{-}4)$$

其中，W 表示带宽，B 代表波特率，N 是码元总的种类数。

有噪声时的数据速率计算：在有噪声情况下应依据香农公式来计算极限数据速率。香农公式为：

$$\text{极限数据速率} = \text{带宽} \times \log_2(1+S/N) \qquad (2\text{-}5)$$

其中，S 为信号功率，N 为噪声功率。

**误码率**：指接收到的错误码元数在总传送码元数中所占的比例。

$$P_C = \frac{\text{错误码元数}}{\text{码元总数}} \qquad (2\text{-}6)$$

2. 调制与编码

由于模拟信号和数字信号的应用非常广泛，日常生活中的模拟数据和数字数据也很多，因此数据通信中就面临模拟数据和数字数据与模拟信号和数字信号之间相互转换的问题，这就要用到调制和编码。**编码**就是用数字信号承载数字或模拟数据；**调制**就是用模拟信号承载数字或模拟数据。

调制可以分为基带调制和带通调制。

- **基带调制**。基带调制只对基带信号波形进行变换，并不改变其频率，变换后仍然是基带信号。

- **带通调制（频带调制）**。带通调制使用载波将基带信号的频率迁移到较高频段进行传输，解决了很多传输介质不能传输低频信息的问题，并且使用带通调制信号可以传输得更远。

（1）模拟信号调制为模拟信号。

由于基带信号包含许多低频信息或直流信息，而很多传输介质并不能传输这些信息，因此需要使用调制器对基带信号进行调制。

模拟信号调制为模拟信号的方法有：

- **调幅（AM）**：依据传输的原始模拟数据信号变化来调整载波的振幅。
- **调频（FM）**：依据传输的原始模拟数据信号变化来调整载波的频率。
- **调相（PM）**：依据传输的原始模拟数据信号变化来调整载波的初始相位。

（2）模拟信号编码为数字信号。

模拟信号编码为数字信号最常见的就是脉冲编码调制（Pulse Code Modulation，PCM）。脉冲编码的过程为采样、量化和编码。

- 采样，即对模拟信号进行周期性扫描，把时间上连续的信号变成时间上离散的信号。采样必须遵循奈奎斯特采样定理才能保证无失真地恢复原模拟信号。

举例：模拟电话信号通过 PCM 编码成为数字信号。语音最大频率小于 4KHz（**约为 3.4KHz**），根据采样定理，采样频率要大于 2 倍语音最大频率，即 8KHz（采样周期=125us），就可以无失真地恢复语音信号。

- 量化，即利用抽样值将其幅度离散，用先规定的一组电平值把抽样值用最接近的电平值来代替。规定的电平值通常用二进制表示。

举例：语音系统采用 128 级（7 位）量化，采用 8KHz 的采样频率，那么有效数据速率为 56kb/s，又由于在传输时，每 7bit 需要添加 1bit 的信令位，因此语音信道数据速率为 64kb/s。

- 编码，即用一组二进制码组来表示每一个有固定电平的量化值。然而实际上量化是在编码过程中同时完成的，故编码过程也称为模/数变换，记作 A/D。

（3）数字信号调制为模拟信号。

模拟信号传输的都是在数字载波信号上完成的，与模拟信号调制为模拟信号的方法类似，可以利用调制频率、振幅和相位三种载波特性之一或组合。

基本调制方法有：

- **幅移键控（Amplitude Shift Keying，ASK）**：载波幅度随着基带信号的变化而变化，方式还可称作通-断键控或开关键控。
- 如图 2-3 所示显示了 ASK 调制器的输入和对应的输出波形，对于输入二进制数据流的每个变化，ASK 波形都有一个变化。对于二进制输入为 1 的整个时间，输出为一个振幅恒定、频率恒定的信号；对于二进制输入为 0 的整个时间，载波处于关闭状态。

**注意**：1 和 0 时的 ASK 波形表示方式可以相反。

- 频移键控（Frequency Shift Keying，FSK）：载波频率随着基带信号的变化而变化。

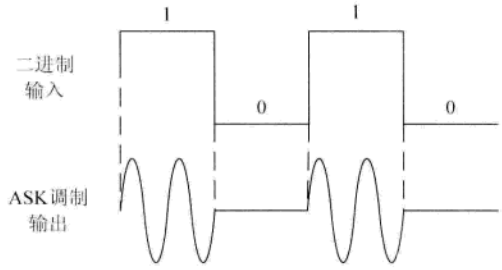



图 2-3 ASK 的输入和输出波形

- 如图 2-4 所示显示了 FSK 调制器的输入和对应的输出波形，从中可以发现二进制 0 和 1 的输入对应不同频率的波形输出。

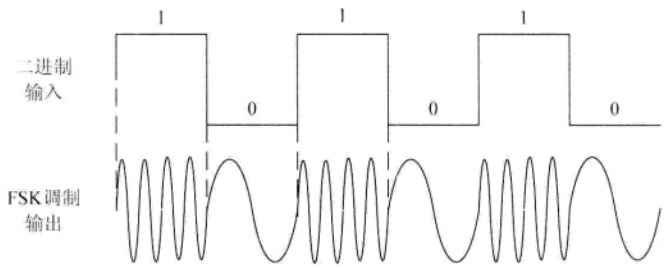



图 2-4 FSK 的输入和输出波形

- **相移键控（Phase Shift Keying，PSK）**：载波相位随着基带信号的变化而变化。PSK 最简单的形式是 BPSK，载波相位有 2 种，分别表示逻辑 0 和 1。

如图 2-5 所示显示了 BPSK 调制器的输入和对应的输出波形，二进制 1 和 0 分别用不同相位的波形表示。

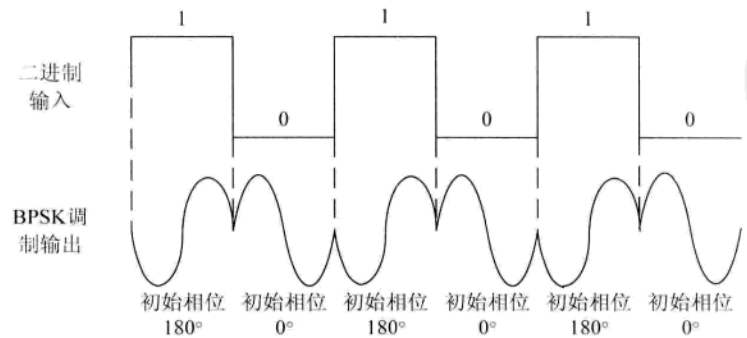



图 2-5 BPSK 的输入和输出波形

较为复杂的是高阶 PSK，即用多个输入相位来表示多个信息位。**4PSK** 又称为 QPSK，使用 4 个输出相位表示 2 个输入位；**8PSK** 使用 8 个输出相位表示 3 个输入位；**16 PSK** 使用 16 个输出相位表示 4 个输入位。

**DPSK** 称为相对相移键控调制，记作 2DPSK。信息是通过连续信号之间的载波信号的初始相位是否变化来传输的。

如图 2-6 所示显示了 DPSK 调制器的输入和对应的输出波形，对于输入位 0，初始有相位变化；对于输入位 1，初始无相位变化。

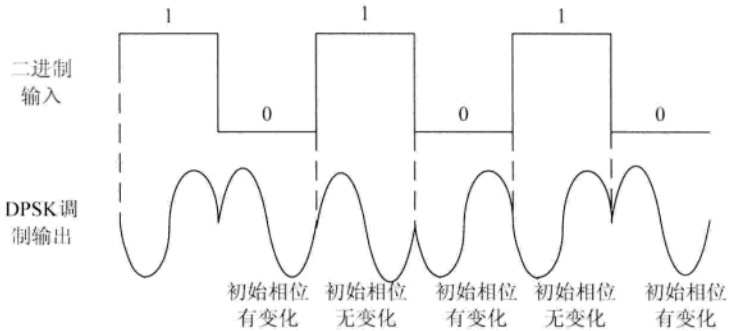



图 2-6　DPSK 的输入和输出波形

当然结合使用振幅、频率和相位方式可以表示更多的信号，QAM 就是其中的一种。

- **正交幅度调制（Quadrature Amplitude Modulation，QAM）。**若利用正交载波调制技术传输 ASK 信号，可使频带利用率提高一倍。如果再把其他技术结合起来还可以进一步提高频带利用率。能够完成这种任务的技术称为正交幅度调制（QAM），通常有 4QAM、8QAM、16QAM、64QAM 等，如 16QAM 是指包含 16 种符号的 QAM 调制方式。

如表 2-1 所示总结了常见的调制技术，并给出了对应的码元数。

**表 2-1　常见调制技术汇总表**

| 调制技术 | 码元种类/比特位 | 特性 |
|---|---|---|
| 幅移键控（ASK） | 2/1 | 恒定振幅表示 1，载波关闭表示 0；抗干扰性差，容易实现 |
| 频移键控（FSK） | 2/1 | 不同的两个频率分别代表 0 和 1 |
| 相移键控（PSK） | 2/1 | 不同的两个相位分别代表 0 和 1 |
| QPSK（4PSK） | 4/2 | +45°、+135°、-45°、-135° 分别代表 00、01、10、11 |
| 8PSK | 8/3 | 8 个相位分别代表 000、…、111 的 8 个值 |
| DPSK | 2/1 | 遇到位 0，初始有相位变化；遇到位 1，初始无相位变化 |
| 4QAM | 4/2 | 结合了 ASK 和 PSK 的调制方法 |

（4）数字信号调制为数字信号。

数字信号调制的方法比较多，下面讲述考试所涉及的所有数字信号调制方法，如图 2-7 所示。

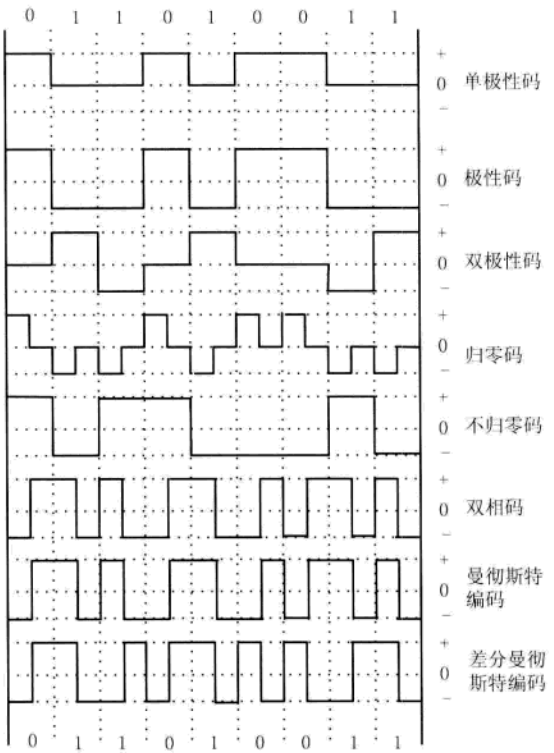



图 2-7　各种常见编码

- 极性编码

使用正负电平和零电平来表示的编码。**极性码**使用正电平表示 0，负电平表示 1；**单极性码**使用正电平表示 0，零电平表示 1；**双极性码**使用正负电平和零电平共 3 个电平表示信号。典型的信号交替反转编码（Alternate Mark Inversion，AMI）就是一种双极性码，数据流中遇到 1 时，电平在正负电平之间交替翻转，遇到 0 则保持零电平。

极性编码使用恒定的电平表示数字 0 或 1，因此需要使用时钟信号定时。

- 归零码（Return to Zero，RZ）

码元中间信号回归到零电平，从正电平到零电平表示 0，从负电平到零电平表示 1。这种中间信号都有电平变化的方式，使得编码可以自同步。

- 不归零码（Not Return to Zero，NRZ）

码元中间信号不回归到 0，遇到 1 时，电平翻转；遇到 0 时，电平不翻转。这种翻转的特性称

为差分机制。**不归零反相编码（No Return Zero-Inverse，NRZ-I）**，在NRZ-I编码中，编码后电平只有正负电平之分，没有零电平，属于不归零编码。NRZ-I遇到0时，电平翻转；遇到1时，电平不翻转。

- 双相码

双相码的每一位中有电平转换，如果中间缺少电平翻转，则认为是违例代码，既可以同步，也可以用于检错。负电平到正电平代表0，正电平到负电平代表1。

- 曼彻斯特编码

曼彻斯特编码属于一种双相码，负电平到正电平代表0，高电平到负电平代表1；也可以是负电平到正电平代表1，正电平到负电平代表0。常用于10M以太网。传输一位信号需要有两次电平变化，因此编码效率为50%。

- 差分曼彻斯特编码

差分曼彻斯特编码属于一种双相码，中间电平只起到定时的作用，不用于表示数据。信号开始时有电平变化则表示0，没有电平变化则表示1。

- 4B/5B、8B/10B、8B/6T编码

由于曼彻斯特编码的效率不高，只有50%，因此在高速网络中，这种编码方式显然就不适用了。在高速率的局域网和广域网中采用m位比特编码成n位比特编码方式，即mB/nB编码。常见的mB/nB编码如表2-2所示。

表2-2 常见的mB/nB编码

| 编码 | 定义 | 应用领域 |
|---|---|---|
| 4B/5B | 将4个比特数据编码成5个比特符号的方式<br>编码效率为4bit/5bit=80% | FDDI、100Base-TX、100Base-FX |
| 8B/10B | 8B/10B编码是将一组连续的8位数据分解成两组数据，一组3位，一组5位，经过编码后分别成为一组4位的代码和一组6位的代码，从而组成一组10位的数据发送出去。编码效率为8bit/10bit=80% | USB 3.0、1394b、Serial ATA、PCI Express、Infini-band、Fiber Channel、RapidIO、千兆以太网（注：1000base-t与100base-Tx采用PAM-5编码） |
| 64/66B | 将64位信息编码为66位符号。编码效率为64bit/66bit=97% | 万兆以太网 |
| 8B/6T | 将8位映射为6个三进制位 | 100Base-T4（3类UTP） |

3. 数据传输方式

数据传输方式可以按多种方式进行分类。

（1）按信号类型分类。

1）**模拟通信**：利用正弦波的幅度、频率或相位的变化，或利用脉冲的幅度、宽度或位置变化来模拟原始信号，以达到通信的目的。

2）**数字通信**：用数字信号作为载体来传输消息，或用数字信号对载波进行数字调制后再传输的通信方式。

（2）按照一次传输的数据位数分类。

1）**串行通信**：串行通信是指使用一条数据线将数据一位一位地依次传输，每一位数据占据一个固定的时间长度。常见的串行通信技术标准有 EIA－232（RS-232）、EIA-422（RS-422）、EIA－485（RS-485），通用串行总线（Universal Serial Bus，USB）、IEEE 1394。

2）**并行通信**：一组数据的各数据位在多条线上同时被传输，这种传输方式称为并行通信。常见应用了并行通信技术有磁盘并口线和打印机并口。

（3）按照信号传送的方向与时间的关系分类。

1）**单工通信**：数据只能在一个方向上流动，如无线电波和有线电视。

2）**半双工**：可以切换方向的单工通信，但不能同时或双向通信，如对讲机。

3）**全双工通信**：允许数据同时在两个方向上进行传输，如电话和手机通信。

（4）按照数据的同步方分类。

1）**同步通信**：通信双方必须先建立同步，即双方时钟要调整到同一频率。同步方式可以分为两种：一种是使用**全网同步**，用一个非常精确的主时钟对全网所有结点上的时钟进行同步；另一种是使用**准同步**，各结点的时钟之间允许有微小的误差，然后采用其他措施实现同步传输。同步通信是一种连续串行传送数据的通信方式，一次通信只传送一帧信息。这里的信息帧与异步通信中的字符帧不同，通常含有若干个数据字符，它们均由**同步字符**、**数据字符**和**校验字符（CRC）**组成。

2）**异步通信**：发送端和接收端可以由各自的时钟来控制数据的发送和接收，这两个时钟源彼此独立、互不同步。发送端可以在任意时刻开始发送字符，因此必须在每一个字符的开始和结束的地方加上标志，即加上起始位和终止位，用于正确接收每一个字符。异步通信中，数据通常以字符或字节为单位组成字符帧传送。

$$\text{异步通信数据速率} = \text{每秒钟传输字符数} \times (\text{起始位} + \text{终止位} + \text{校验位} + \text{数据位}) \quad (2\text{-}6)$$

$$\text{异步通信有效数据速率} = \text{每秒钟传输字符数} \times \text{数据位} \quad (2\text{-}7)$$

4. *数据交换方式*

通信网络数据的交换方式有多种，主要分为电路交换、报文交换、分组交换和信元交换，具体方式如表 2-3 所示。

表 2-3 数据交换方式及其特性

| 数据交换方式 | 定义 | 特点 |
| --- | --- | --- |
| 电路交换 | 通信开始之前，主呼叫和被呼叫之间建立连接，之后建立通信，期间独占整个链路，结束通信时释放链路。电路交换是面向连接的 | 优点：时延小<br>缺点：链路空闲率高，不能进行差错控制 |
| 报文交换 | 结点把要发送的信息组织成一个报文（数据包），该报文中含有目标结点的地址，完整的报文在网络中一站一站地向前传送。每一个结点接收**整个报文**并检查目标结点地址，然后根据网络中的拥塞情况在适当的时候转发到下一个结点 | 优点：不用建立专用通路；可以校验，也可以将一个报文发至多个目的地<br>缺点：中间节点需要先存储，再转发报文，时间延时较大；中间节点的存储空间也需要较大 |

续表

| 数据交换方式 | | 定义 | 特点 |
|---|---|---|---|
| 分组交换（确定最大报文长度） | 数据报 | 数据报服务类似于邮政系统的信件投递。每个分组都携带完整的源和目的节点的地址信息，独立地进行传输，每当经过一个中间节点时都要根据目标地址和网络当前的状态，按一定的路由选择算法选择一条最佳的输出线，直至传输到目的节点 | 优点：不需要建立连接<br>缺点：每个分组独立选路，不完全走一条路；可靠性差 |
| | 虚电路 | 在虚电路服务方式中，为了进行数据的传输，网络的源主机和目的主机之间先要建立一条逻辑通道，所有报文沿着逻辑通道传输数据。在传输完毕后，还要将这条虚电路释放。虚电路的服务方式是网络层向传输层提供的一种使所有分组按顺序到达目的主机的可靠的数据传送方式。虽然用户感觉到好像占用了一条端到端的物理线路，但实际上并没有真正地占用，即这一条线路不是专用的，所以称之为“虚电路” | 优点：相对数据报可以进行流控和差错控制，提高了可靠性，适合远程控制和文件传送<br>缺点：不如数据报方式灵活 |
| 信元交换 | | 信元交换又叫ATM（异步传输模式），是一种面向连接的快速分组交换技术，它是通过建立虚电路来进行数据传输的。信元交换技术是一种快速分组交换技术，它结合了电路交换技术延迟小和分组交换技术灵活的优点。信元是固定长度的分组，ATM采用信元交换技术，其信元长度为53字节，其中信元头为5字节，数据为48字节 | 结合了电路交换技术延迟小和分组交换技术灵活的优点 |

5. 多路复用

多路复用（信道复用）的实质是在发送端将多路信号组合成一路信号，然后在一条专用的物理信道上实现传输，接收端再将复合信号分离出来。多路复用技术有：时分复用（Time Division Multiplexing，TDM）、波分复用（Wavelength Division Multiplexing，WDM），、频分复用（Frequency Division Multiplexing，FDM）。具体各复用的技术特性如表2-4所示。

表2-4 各类复用及其技术特性

| 复用技术 | | 特点 | 应用 |
|---|---|---|---|
| 时分复用 | 同步时分复用 | 固定时隙的时分复用，即使无数据传输的各子信道轮流按时间独占带宽 | E1、T1、SDH/ SONET、DDN、PON下行 |
| | 统计时分复用 | 对同步时分复用进行改进，通过动态地分配时隙来进行数据传输的 | ATM |
| 波分复用 | | 所谓波分复用就是将整个波长频带被划分为若干个波长范围，每路信号占用一个波长范围来进行传输。属于特殊的频分复用 | 光纤通信 |
| 频分复用 | | 频分复用是指多路信号在频率位置上分开，但同时在一个信道内传输。频分复用信号在频谱上不会重叠，但在时间上是重叠的 | 宽带有线电视、无线广播、ADSL、无线局域网 |

## 2.2 数字传输系统

### 2.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：脉冲编码调制 PCM 体制、同步光纤网、同步数字系列。

### 2.2.2 知识点精讲

1. 脉冲编码调制 PCM 体制

前面介绍了脉冲编码调制 PCM 的原理，下面讲述 PCM 两个重要国际标准：北美的 24 路 PCM（T1，速率为 1.544Mb/s）和欧洲的 30 路 PCM（E1，速率为 2.048Mb/s）。

（1）E1。E1 有成帧、成复帧与不成帧三种方式，考试主要考成复帧方式。

1）E1 的成复帧方式。E1 的一个时分复用帧（长度为 T=125us）共划分为 32 个相等的时隙，时隙的编号为 CH0～CH31。其中时隙 CH0 用作帧同步，时隙 CH16 用来传送信令，剩下 CH1～CH15 和 CH17～CH31 共 30 个时隙用作 30 个语音话路，E1 载波的控制开销占 6.25%。每个时隙传送 8bit（7bit 编码加上 1bit 信令），因此共用 256bit。每秒传送 8000 个帧，因此 PCM 一次群 E1 的数据率就是 2.048Mb/s，其中每个话音信道的数据速率是 64kb/s。

2）E1 的成帧方式。E1 中的第 0 时隙用于传输帧同步数据，其余 31 个时隙可以用于传输有效数据。

3）E1 的不成帧方式。所有 32 个时隙都可用于传输有效数据。

E1 有以下三种使用方法：

- 2M 的 DDN 方式：将整个 2M 用作一条链路。
- CE1 方式：将 2M 用作若干个 64k 线路的组合。
- PRA 信令方式：也是 E1 最原本的用法，把一条 E1 作为 32 个 64K 来用，但是时隙 0 和时隙 16 用作信令，一条 E1 可以传 30 路话音。

我国和欧洲等国家使用 E1。

（2）T1。T1 系统共有 24 个语音话路，每个时隙传送 8bit（7bit 编码加上 1bit 信令），因此共用 193bit（192bit 加上 1bit 帧同步位）。每秒传送 8000 个帧，因此 PCM 一次群 **T1 的数据率=8000×193b/s=1.544Mb/s**，其中的每个话音信道的数据速率是 **64kb/s**。

美国、加拿大、日本和新加坡使用 T1。

如表 2-5 所示给出了 T1 和 E1 的常考点。

E1 和 T1 可以使用复用方法，4 个一次群可以构成 1 个二次群（分别称为 E2 和 T2），4 个二次群构成 1 个三次群（分别称为 E3 和 T3）。

表 2-5 T1 和 E1 的常考点

| 名称 | 总速率 | 话路组成 | 每个话音信道的数据速率 |
|---|---|---|---|
| T1 | 1.544Mb/s | 30 条语音话路和 2 条控制话路 | 64kb/s |
| E1 | 2.048Mb/s | 24 条语音话路 | 64kb/s |

2. 同步光纤网

由于 PCM 速率不统一（T1 和 E1 共存）、属于准同步方式，因此人们提出同步光纤网（Synchronous Optical Network，SONET）解决上述问题。SONET 使用非常精确的铯原子钟提供时间同步。

SONET 和 PCM 都是每秒钟传送 8000 帧，STS-1 帧长为 810 字节，因此基础速率为 8000×810×8=51.84Mb/s。该速率对电信号称为第 1 级同步传送信号（Synchronous Transport Signal，STS-1）；对光信号称为第 1 级光载波（Optical Carrier，**OC-1**）。

**SONET 中，OC-1 为最小单位，值为 51.84Mb/s，OC-N 代表 N 倍的 51.84Mb/s，**如 OC-3=OC-1×3=155.52Mb/s。

3. 同步数字系列

同步数字系列（Synchronous Digital Hierarchy，SDH）是 ITU-T 以 SONET 为基础制定的国际标准。SDH 和 SONET 的不同主要在于基本速率不同，SDH 的基本速率是第 1 级同步传递模块（Synchronous Transfer Module，STM-1）。**STM-1 的速率为 155.2Mb/s**，与 OC-3 的速率相同，STM-N 则代表 N 倍的 STM-1。

当数据传输速率较小时，可以使用 SDH 提供的准同步数字系列（Plesiochronous Digital Hierarchy，PDH）兼容传输方式。**该方式在 STM-1 中封装了 63 个 E1 信道**，可以同时向 63 个用户提供 2Mb/s 的接入速率。PDH 兼容方式有两种接口，一种是传统的 E1 接口，如路由器上的 G.703 转 V.35 接口；另一种是封装了多个 E1 信道的 CPOS（Channel POS）接口。



## 2.3 接入技术

### 2.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：xDSL、HFC、FTTx。

### 2.3.2 知识点精讲

1. xDSL

xDSL 技术就是利用电话线中的高频信息传输数据，高频信号损耗大，容易受噪声干扰。xDSL 的速率越高，传输距离越近。如表 2-6 所示给出了 xDSL 的常见类型。

表 2-6 常见的 xDSL

| 名称 | 对称性 | 上、下行速率（受距离影响有变化） | 极限传输距离 | 复用技术 |
|---|---|---|---|---|
| ADSL（非对称数字用户线路） | 不对称 | 上行：640～1Mb/s<br>下行：1～8Mb/s | 3～5km | 频分复用 |
| VDSL（甚高速数字用户线路） | 不对称 | 上行：1.6～2.3Mb/s<br>下行：12.96～52Mb/s | 0.9～1.4km | QAM 和 DMT |
| HDSL（高速数字用户线路） | 对称 | 上行：1.5Mb/s<br>下行：1.5Mb/s | 2.7～3.6km | 时分复用 |
| G.SHDSL（对称的高比特数字用户环路） | 对称 | 一对线上、下行可达 192kb/s～2.312Mb/s | 3.7～7.1km | 时分复用 |

注：DSL 就是 ISDN 技术，已经被淘汰。

常见的 ADSL 接入方式有以下两种：

（1）ADSL 虚拟拨号。

采用专门的协议 PPP over Ethernet，拨号后直接由验证服务器进行检验，用户需输入用户名和密码，检验通过后就建立起一条高速的用户数字并分配相应的动态 IP。

（2）ADSL 专线接入。

类似于专线的接入方式，用户配置好 ADSL MODEM 后，PC 设定固定的 IP 地址、掩码、网关之后就可以和局端自动建立起一条链路。

2. HFC

混合光纤一同轴电缆（Hybrid Fiber-Coaxial，HFC）。HFC 通常由光纤干线、同轴电缆支线和用户配线网络三部分组成，从有线电视台出来的节目信号先变成光信号在干线上传输，到用户区域后把光信号转换成电信号，经分配器分配后通过同轴电缆送到用户。

常考的 HFC 网络结构如图 2-8 所示。

电缆调制解调器（Cable Modem，CM）是用户设备和同轴电缆网络的接口，**是有线电视网络（Cable TV，CATV）网络用户端必须安装的设备**。在下行方向接收前端设备，即电缆调制解调器终端系统（Cable Modem Terminal Systems，CMTS）发送来的 **64QAM** 信号，经解调后传送给 PC 的以太网接口。在上行方向把 PC 发送的以太帧封装在时隙中，经 **QPSK** 调制后，通过上行数据通路传送给 CMTS。

3. FTTx

FTTx 技术主要用于接入网络光纤化，范围从区域电信机房的局端设备到用户终端设备，局端设备为光线路终端（Optical Line Terminal，OLT）、用户端设备为光网络单元（Optical Network Unit，ONU）或光网络终端（Optical Network Terminal，ONT）。

（1）FTTx 分类。

根据光纤到用户的距离来分类，可分成光纤到交换箱（Fiber To The Cabinet，FTTCab）、光纤

到路边（Fiber To The Curb，FTTC）、光纤到大楼（Fiber To The Building，FTTB）及光纤到户（Fiber To The Home，FTTH）等服务形态。常考的 HFC 设计结构如图 2-8 所示。

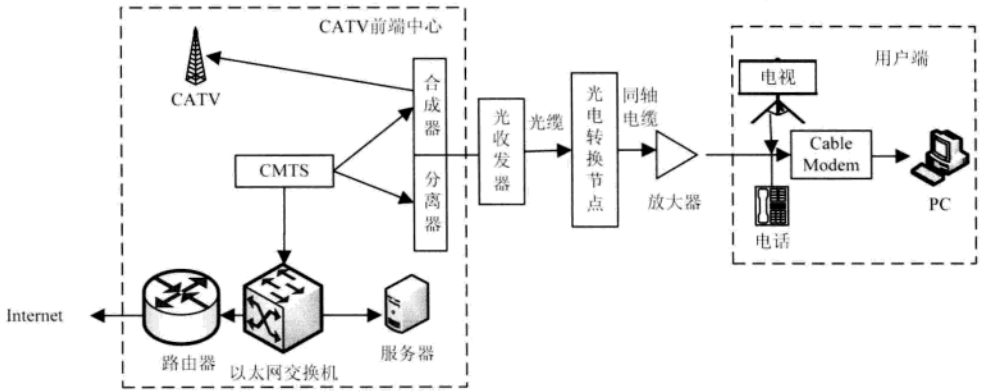



图 2-8　常考的 HFC 设计结构

（2）PON 技术。

无源光纤网络（Passive Optical Network，PON）是指 ODN（光配线网）中不含有任何电子器件和电子电源，ODN 全部由光分路器（Splitter）等无源器件组成，不需要贵重的有源电子设备。一个无源光纤网络包括一个安装于中心控制站的 OLT 及一批配套的安装于用户场所的光网络单元 ONU。在 OLT 与 ONU 之间的光配线网包含了光纤和无源分光器/耦合器。PON 原理拓扑如图 2-9 所示。

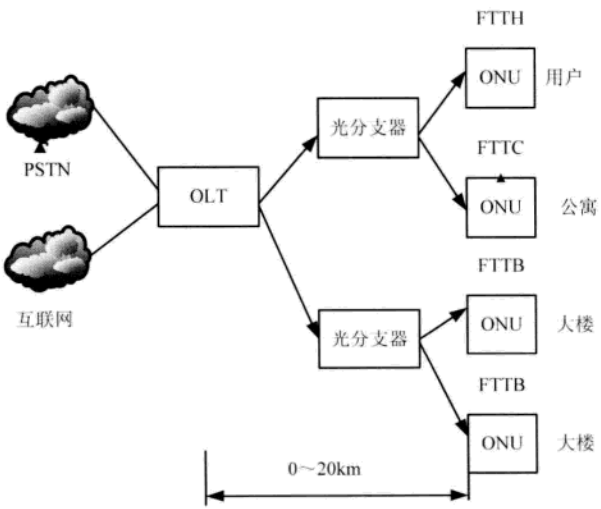



图 2-9　PON 原理拓扑

PON 技术主要有：以太网无源光网络（Ethernet Passive Optical Network，EPON）和千兆以太网无源光网络（Gigabit-Capable PON，GPON）。

**注意：基于 ATM 的 PON 技术（即 APON 技术）已经被淘汰。**

## 2.4 有线传输介质

### 2.4.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：同轴电缆、屏蔽双绞线、非屏蔽双绞线、光纤。

### 2.4.2 知识点精讲

1. 同轴电缆

同轴电缆由内到外分为四层：中心铜线、塑料绝缘体、网状导电层和电线外皮。电流传导与中心铜线和网状导电层形成回路。同轴电缆因中心铜线和网状导电层为同轴关系而得名。

同轴电缆从用途上分，可分为**基带同轴电缆**和**宽带同轴电缆**（即网络同轴电缆和视频同轴电缆）。同轴电缆分 50Ω 基带电缆和 75Ω 宽带电缆两类。基带电缆又分**细同轴电缆**和**粗同轴电缆**，基带电缆仅仅用于数字传输，数据率可达 10Mb/s。

2. 屏蔽双绞线

根据屏蔽方式的不同，屏蔽双绞线可分为两类，即 STP（Shielded Twisted-Pair）和 FTP（Foil Twisted-Pair）。STP 是指每条线都有各自屏蔽层的屏蔽双绞线，而 FTP 则是采用整体屏蔽的屏蔽双绞线。

**注意：屏蔽只在整个电缆有屏蔽装置，并且两端正确接地的情况下才起作用。所以要求整个系统全部是屏蔽器件，包括电缆、插座、水晶头和配线架等，同时建筑物需要有良好的地线系统。**

屏蔽双绞线电缆的外层由铝箔包裹以减小辐射，但这并不能完全消除辐射。屏蔽双绞线的价格相对较高，安装时要比非屏蔽双绞线电缆困难。类似于同轴电缆，它必须配有支持屏蔽功能的特殊连结器和相应的安装技术。但屏蔽双绞线有较高的传输速率，100 米内可以达到 155Mb/s，比相应的非屏蔽双绞线高。

3. 非屏蔽双绞线

非屏蔽双绞线由 8 根不同颜色的线分成 4 对绞合在一起，成对扭绞的作用是尽可能减少电磁辐射与外部电磁干扰的影响。将双绞线按电气特性区可分为三类线、四类线、五类线、超五类线、六类线。网络中最常用的是五类线、超五类和六类。

（1）双绞线的线序标有标准 568A 和标准 568B。

**标准 568A** 线序为绿白、绿、橙白、蓝、蓝白、橙、棕白、棕；**标准 568B** 线序为橙白、橙、绿白、蓝、蓝白、绿、棕白、棕。

在实际应用中，大多数都使用568B的标准，通常认为该标准对电磁干扰的屏蔽更好。

（2）交叉线与直连线。

**交叉线**是指一端是568A标准，另一端是568B标准的双绞线；**直连线**是指两端都是568A或568B标准的双绞线。

综合布线中对五类线、超五类线、六类线测试的参数有：衰减量、近端串扰、远端串扰、回波损耗、特性阻抗、接线方式。

4. 光纤

光纤是光导纤维的简称，光纤传输介质由可以传送光波的**玻璃纤维或透明塑料**制成，**外包一层比玻璃折射率低的材料**。进入光纤的光波在两种材料的介面上形成**全反射**，从而不断地向前传播。光纤可以分为单模光纤和多模光纤。

光波在光纤中的传播模式与**芯线和包层的相对折射率**、**芯线的直径**以及**工作波长**有关。如果芯线的直径小到光波波长大小，则光纤就成为波导，光在其中无反射地沿直线传播，这种光纤叫**单模光纤**。

光波在光导纤维中以多种模式传播，不同的传播模式有不同波长的光波和不同的传播和反射路径，这样的光纤叫**多模光纤**。

如表2-7所示给出了单模光纤和多模光纤的特性。

表2-7 单模光纤和多模光纤的特性

| | 单模光纤 | 多模光纤 |
|---|---|---|
| 光源 | 激光二极管 | LED |
| 光源波长 | 1310nm和1550nm两种 | 850nm和1300nm两种 |
| 纤芯直径/包层外径 | 8.3/125μm | 50/125μm和62.5/125μm |
| 距离 | 2～10km | 2km |
| 速率 | 100～10Gb/s | 1～10Gb/s |
| 光种类 | 一种模式的光 | 不同模式的光 |

光纤布线系统的测试指标包括：最大衰减限值、波长窗口参数和回波损耗限值。网络工程师考试的下午题中一般考单模和多模的距离，通常多模传输距离为500m左右，而单模的传输距离一般是500m以上到2～5km。

## 2.5 其他知识点

### 2.5.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：RS-232-C、帧中继、ATM。

### 2.5.2 知识点精讲

1. RS-232-C

RS-232-C 是美国电子工业协会（Electrical Industrial Association，EIA）于 1973 年提出的串行通信接口标准，主要用于 DTE（如计算机和终端等设备）与 DCE（如调制解调器、中继器、多路复用器等）之间通信的接口规范。RS-232-C 的电气特性采用 V.28 标准电路。信号电平-3V～-15V 代表逻辑 1，+3V～+15V 代表逻辑 0。在传输距离小于 15m 时，最大数据速率为 19.2kb/s，在传输距离小于 50m 时，最大数据速率为 9.6kb/s；在传输距离小于 100m 时，最大数据速率为 1.2kb/s。标准的 RS-232-C 接口使用 25 针 DB 连接器（插头/插座），接口可简化为 9 针和 15 针两种。

2. 帧中继

帧中继最初是作为 ISDN 的一种承载业务而定义的。帧中继在第二层建立虚电路，用帧方式承载数据业务，因而第三层就被简化掉了。帧中继提供虚电路业务，其业务面向连接的网络服务。在帧中继的虚电路上可以提供不同的服务质量。在帧中继网上，用户的**数据速率可以在一定的范围内变化**，从而**既可以适应流式业务**，又可以**适应突发式业务**。帧中继提供两种虚电路：交换虚电路和永久虚电路。帧长可变，可以承载各种局域网的数据传输。

3. ATM

异步传输模式（Asynchronous Transfer Mode，ATM）是一项数据传输技术，是实现 B-ISDN 业务的核心技术之一。ATM 是以信元为基础的一种分组交换和复用技术，是一种为了多种业务设计的通用的面向连接的传输模式。ATM 的传送单元是固定长度为 53byte 的 CELL（信元），其中 5B 为信元头，用来承载该信元的控制信息；48B 为信元体，用来承载用户要分发的信息。信头部分包含了选择路由用的 VPI（虚通道标识符）/VCI（虚通路标识符）信息，因而它具有分组交换的特点。

ATM 用户业务分为 4 类，即 CBR、VBR、ABR 和 UBR。

- 固定比特率（Constant Bit Rate，CBR）：采用固定比特率业务适合于交互式语音和视频流。
- 可变比特率（Variable Bit Rate，VBR）：可变比特率业务适合交互式压缩视频信号。
- 有效比特率（Available Bit Rate，ABR）：采用有效比特率业务用于突发通信。
- 不定比特率（Unspecified Bit Rate，UBR）：采用不定比特率业务可用于传送 IP 分组，包括文件传输、电子邮件业务潜在的应用领域。

## 第 3 学时　数据链路层

第 1 天的第 3 学时主要学习数据链路层所涉及的重要知识点。数据链路层是 OSI 参考模型中的第二层，处于物理层和网络层之间。数据链路层在物理层提供的服务的基础上向网络层提供服务，其最基本的服务是将源主机网络层传来的数据可靠地传输到相邻节点的目标机网络层。为达到这一目的，数据链路必须具备一系列相应的功能。在网络工程师的考试中主要考查这些功能的特性、技

术原理、校验计算等。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在3～8分之间。数据链路层知识的考察主要集中在上午的考试中。本章考点知识结构图如图3-1所示。


图3-1　考点知识结构图

## 3.1　检错与纠错

### 3.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：基本概念、海明码、CRC编码。

### 3.1.2　知识点精讲

1. 基本概念

通信链路都不是完全理想的。比特在传输的过程中可能会产生**比特差错**，即1可能会变成0，0也可能变成1。

一帧包含m个数据位（即报文）和r个冗余位（校验位）。假设帧的总长度为n，则有n=m+r。包含数据和校验位的n位单元通常称为n位**码字**（codeword）。

**海明码距（码距）**是两个码字中不相同的二进制位的个数；**两个码字的码距**是一个编码系统中任意两个合法编码（码字）之间不同的二进数位数；**编码系统的码距**是整个编码系统中任意两个码字的码距的最小值。**误码率**是传输错误的比特占所传输比特总数的比率。

例1：如图3-2所示给出了一个编码系统，用两个比特位表示4个不同信息。任意两个码字之间不同的比特位数从1到2不等，但最小值为1，故该编码系统的码距为1。

| | 二进码字 | |
|---|---|---|
| | a2 | a1 |
| 0 | 0 | 0 |
| 1 | 0 | 1 |
| 2 | 1 | 0 |
| 3 | 1 | 1 |

图3-2　码距为1的编码系统

如果任何码字中的一位或多位被颠倒或出错了，结果中的码字仍然是合法码字。例如，如果传送信息 10，而被误收为 11，因 11 是合法码字，所以接收方仍然认为 11 是正确的信息。

然而，如果用 3 个二进位来编 4 个码字，那么码字间的最小距离可以增加到 2，如图 3-3 所示。

| | 二进码字 | | |
|---|---|---|---|
| | a3 | a2 | a1 |
| 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 |
| 2 | 1 | 1 | 0 |
| 3 | 1 | 1 | 1 |

图 3-3 改进后码距为 2 的编码系统

这里任意两个码字相互间最少有两个比特位的差异。因此，如果任何信息中的一个比特位出错，那么将成为一个不用的码字，接收方能检查出来。例如信息是 001，因出错成为了 101，101 不是合法码字，这样接收方就能发现出错了。

海明研究发现，**检测 d 个错误**，则编码系统**码距≥d+1**；**纠正 d 个错误**，则编码系统**码距>2d**。

2. *海明码*

海明码是一种多重奇偶检错系统，它具有检错和纠错的功能。海明码中的全部传输码字是由原来的信息和附加的奇偶校验位组成的。每一个这种奇偶校验位和信息位被编在传输码字的特定位置上。这种系统组合方式能找出错误出现的位置，无论是原有信息位，还是附加校验位。

设海明码校验位为 k，信息位为 m，则它们之间的关系应满足 $m+k+1\leqslant 2^k$。

下面以原始信息 101101 为例，讲解海明码的推导与校验的过程。

（1）确定海明码校验位长。

m 是信息位长，则 m=6。根据关系式 $m+k+1\leqslant 2^k$，得到 $7+k\leqslant 2^k$。解不等式得到最小 k 为 4，即校验位为 4。信息位加校验的总长度为 10 位。

（2）推导海明码。

1）填写原始信息。

从理论上讲，海明码校验位可以放在任何位置，但习惯上校验位被从左至右安排在 1、2、4、8、…的位置上。原始信息则从左至右填入剩下的位置。如图 3-4 所示，校验位处于 B1、B2、B4、B8 位，剩下位为信息位，信息位依从左至右的顺序先行填写完毕。

| 校验位编号 | P1 | P2 | | P3 | | | P4 | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | | 0 | 1 | 1 | | 0 | 1 |
| 位置编号 | B1 | B2 | B3 | B4 | B5 | B6 | B7 | B8 | B9 | B10 |

图 3-4 填入原始信息位

2）计算校验位。

依据公式得到校验位：

$$P1=B3\oplus B5\oplus B7\oplus B9=1\oplus 0\oplus 1\oplus 0=0$$
$$P2=B3\oplus B6\oplus B7\oplus B10=1\oplus 1\oplus 1\oplus 1=0$$
$$P3=B5\oplus B6\oplus B7=0\oplus 1\oplus 1=0$$
$$P4=B9\oplus B10=0\oplus 1=1 \qquad (3\text{-}1)$$

注：⊕ 表示异或运算。

这个公式常用，但是直接死记硬背比较困难，只能换个方式进行理解记忆。

把除去 1、2、4、8（校验位位置值编号）之外的 3、5、6、7、9、10 值转换为二进制位，如表 3-1 所示。

表 3-1　二进制与十进制转换表

| 信息位 | 信息位编号的十进制 | 信息位编号的二进制 | | | |
|---|---|---|---|---|---|
| | | 第 4 位 | 第 3 位 | 第 2 位 | 第 1 位 |
| B3 | 3 | 0 | 0 | 1 | 1 |
| B5 | 5 | 0 | 1 | 0 | 1 |
| B6 | 6 | 0 | 1 | 1 | 0 |
| B7 | 7 | 0 | 1 | 1 | 1 |
| B9 | 9 | 1 | 0 | 0 | 1 |
| B10 | 10 | 1 | 0 | 1 | 0 |



将所有信息编号的二进制的第 1 位为 1 的 Bi 进行“异或”操作，结果填入 P1。即上面讲的 P1=B3⊕B5⊕B7⊕B9=1⊕0⊕1⊕0=0；

所有信息编号的二进制的第 2 位为 1 的 Bi 进行“异或”操作，结果填入 P2。即上面讲的 P2=B3⊕B6⊕B7⊕B10=1⊕1⊕1⊕1=0；

依此类推，将所有信息编号的二进制的第 3 位为 1 的 Bi 进行“异或”操作，结果填入 P3；将所有信息编号的二进制的第 4 位为 1 的 Bi 进行“异或”操作，结果填入 P4。

填入校验位后得到图 3-5。

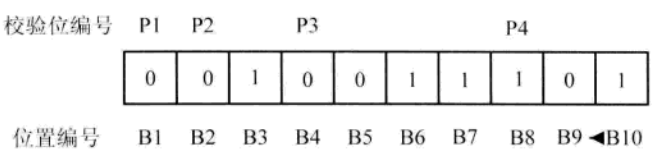



图 3-5　加入校验码后的信息

（3）校验。

将所有信息位位置编号 1～10 的值转换为二进制位，如表 3-2 所示。

表 3-2 二进制与十进制转换表

| 信息位 | 信息位编号的十进制 | 信息位编号的二进制 | | | |
|---|---|---|---|---|---|
| | | 第 4 位 | 第 3 位 | 第 2 位 | 第 1 位 |
| B1 | 1 | 0 | 0 | 0 | 1 |
| B2 | 2 | 0 | 0 | 1 | 0 |
| B3 | 3 | 0 | 0 | 1 | 1 |
| B4 | 4 | 0 | 1 | 0 | 0 |
| B5 | 5 | 0 | 1 | 0 | 1 |
| B6 | 6 | 0 | 1 | 1 | 0 |
| B7 | 7 | 0 | 1 | 1 | 1 |
| B8 | 8 | 1 | 0 | 0 | 0 |
| B9 | 9 | 1 | 0 | 0 | 1 |
| B10 | 10 | 1 | 0 | 1 | 0 |

将所有信息编号的二进制的第 1 位为 1 的 Bi 进行“异或”操作，得到 X1；

将所有信息编号的二进制的第 2 位为 1 的 Bi 进行“异或”操作，得到 X2；

将所有信息编号的二进制的第 3 位为 1 的 Bi 进行“异或”操作，得到 X4；

将所有信息编号的二进制的第 4 位为 1 的 Bi 进行“异或”操作，得到 X8。

即公式：

$$X1=B1\oplus B3\oplus B5\oplus B7\oplus B9$$

$$X2=B2\oplus B3\oplus B6\oplus B7\oplus B10$$

$$X4=B4\oplus B5\oplus B6\oplus B7$$

$$X8=B8\oplus B9\oplus B10 \quad (3\text{-}2)$$

得到一个形式为 X8X4X2X1 的二进制，转换为十进制时，结果为 0，则无错；结果非 0（假设为 Y），则错误发生在第 Y 位。

假设起始端发送加了上述校验码信息之后，目的端收到的信息为 0010111101，如图 3-6 所示。

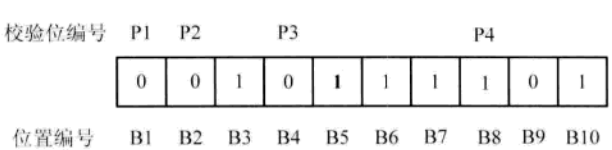



图 3-6 接收信息为 0010111101

依据公式（3-2），得到

$$X1=B1\oplus B3\oplus B5\oplus B7\oplus B9=0\oplus 1\oplus 1\oplus 1\oplus 0=1$$

$$X2=B2\oplus B3\oplus B6\oplus B7\oplus B10=0\oplus 1\oplus 1\oplus 1\oplus 1=0$$

$$X4=B4\oplus B5\oplus B6\oplus B7=0\oplus 1\oplus 1\oplus 1=1$$

$$X8=B8\oplus B9\oplus B10=1\oplus 0\oplus 1=0$$

则将 X4X3X2X1=0101 的二进制转换为十进制为 5。结果为 0，则错误发生在第 5 位。

3. CRC 编码

纠错码广泛用于无线通信中，因为无线线路比有线噪声更多、容易出错。有线线路上的错误率非常低，所以对于偶然的错误，利用错误检测和重传机制更为有效。数据链路层广泛使用循环冗余校验码（Cyclical Redundancy Check，CRC）进行错误检测。CRC 编码又称为多项式编码（polynomial code）。CRC 的基本思想是把位串看成系数为 0 或 1 的多项式，一个 k 位的帧看成是一个 k-1 次多项式的系数列表，该多项式有 k 项，从 $x^{k-1}$ 到 $x^0$。这样的多项式就是 k-1 阶多项式，该多项式形为 $A_1x^{k-1}+A_2x^{k-2}+\cdots+A_{n-2}x^1+A_{n-1}x^0$：。例如，1101 有 4 位，可以代表一个 3 阶多项式，系数为 1、1、0、1，即 $x^3+x^2+1$。

使用 CRC 编码，需要先商定一个**生成多项式（generator polynomial）G(x)**。生成多项式的最高位和最低位必须是 1。假设原始信息有 m 位，则对应多项式 M(x)。生成校验码思想就是在原始信息位后追加若干校验位，使得追加的信息能被 G(x)整除。接收方接收到带校验位的信息，然后用 G(x)整除。余数为 0，则没有错误；反之则发生错误。

（1）生成 CRC 校验码。

这里以 2009 年 5 月网络工程师考试题为例，讲述 CRC 校验码生成的过程。假设原始信息串为 10110，CRC 的生成多项式为 $G(x)=x^4+x+1$，求 CRC 校验码。

1）原始信息后“添 0”。

假设生成多项式 G(x)的阶为 r，则在原始信息位后添加 r 个 0，新生成的信息串共 m+r 位，对应多项式设定为 $x^rM(x)$。

$G(x)=x^4+x+1$ 的阶为 4，即 10011，则在原始信息 10110 后添加 4 个 0，新信息串为 10110 0000。

2）使用生成多项式除。

利用模 2 除法，用对应的 G(x)位去除串 $x^rM(x)$对应的位串，得到长度为 r 位的余数。除法过程如图 3-7 所示。

```
          1010000
      ┌──────────
10011 │101100000
      │ 10011
      ├──────
      │  11100
      │  10011
      ├──────
      │   1111
```

图 3-7　CRC 计算过程

得到余数 1111。注意：余数不足 r，则余数左边用若干个 0 补齐。如求得余数为 11，r=4，则补两个 0 得到 0011。

3）将余数添加到原始信息后。

上例中，原始信息为 10110，添加余数 1111 后，结果为 10110 1111。

（2）CRC 校验。

CRC 校验过程与生成过程类似，接收方接收了带校验和的帧后，用多项式 G(x)来除。余数为 0，则表示信息无错；否则要求发送方进行重传。

**注意**：收发信息双方需使用相同的生成多项式。

（3）常见的 CRC 生成多项式。

CRC–16=$x^{16}+x^{15}+x^2+1$。该多项式用于 FR、X.25、HDLC、PPP 中，用于校验除帧标志位外的全帧。

CRC–32=$x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1$。该多项式用于校验以太网（802.3）帧（不含前导和帧起始符）、令牌总线（802.4）帧（不含前导和帧起始符）、令牌环（802.5）帧（从帧控制字段到 LLC 层数据）、FDDI 帧（从帧控制字段到 INFO）和 ATM 全帧和 PPP 除帧标志位外的全帧。

## 3.2 点对点协议

### 3.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：PPP 和 PPPOE。

### 3.2.2 知识点精讲

1. PPP

点到点协议（the Point-to-Point Protocol，PPP）提供了一种在点到点链路上封装网络层协议信息的标准方法。PPP 也定义了可扩展的链路控制协议（Link Control Protocol，LCP），使用验证协议磋商在链路上传输网络层协议前验证链路的对端。

PPP 有以下三个主要的组成部分：

- 在串行链路上封装数据报的方法。
- 建立、配置和测试数据链路链接（the data-link connection）的 LCP 协议。
- 建立和配置不同网络层协议的一组网络控制协议（Network Control Protocol，NCP）。

为了在点到点链路（point-to-point link）上建立通信，PPP 链路的一端必须在建立阶段（Establishment Phase）首先发送 LCP 包（packets）配置数据链路。链路建立后，在进入到网络层协议阶段前，PPP 提供一个可选择的验证阶段。

PPP 支持两种验证协议：密码验证协议（Password Authentication Protocol，PAP）和挑战一握

手验证协议（Challenge Handshake Authentication Protocol，CHAP）。

（1）PAP。

PAP 提供了一种简单的方法，可以使对端（peer）使用 2 次握手建立身份验证，这个方法仅仅在链路初始化时使用。链路建立阶段完成后，对端不停地发送 Id/Password 对给验证者，一直到验证被响应或连接终止为止。

PAP 不是一个健全的身份验证方法。密码在电路上是明文发送的，并且对回送、重复验证和错误攻击没有保护措施。

（2）CHAP。

CHAP 用于使用 3 次握手验证，这种验证可以在链路建立初始化时进行，也可以在链路建立后的任何时间内重复进行。

在链路建立完成后，验证者向对端发送一个 challenge 信息，对端使用一个 one-way-hash 函数计算出的值响应这个信息。验证者使用自己计算的 hash 值校验响应值。如果两个值匹配，则验证通过；否则连接应该终止。

2. PPPOE

PPPOE（Point-to-Point Protocol over Ethernet）可以使以太网的主机通过一个简单的桥接设备连到一个远端的接入集中器上。通过 PPPOE 协议，远端接入设备能够实现对每个接入用户的控制和计费。PPPOE 协议的工作流程包括发现和会话两个阶段，发现阶段是无状态的，目的是获得 PPPOE 终结端（在局端的 ADSL 设备或其他接入设备上）的以太网 MAC 地址，并建立一个唯一的 PPPOE SESSION-ID。发现阶段结束后就进入标准的 PPP 会话阶段。

## 3.3 常见广播方式的数据链路层



### 3.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：局域网的数据链路层结构、CSMA/CD、IEEE 802 系列协议、802.3 规定的传输介质特性。

### 3.3.2 知识点精讲

1. 局域网的数据链路层结构

802 标准把数据链路层分为两个子层：①逻辑链路控制（Logical Link Control，LLC），该层与硬件无关，实现流量控制等功能；②媒体接入控制层（Media Access Control，MAC），该层与硬件相关，提供硬件和 LLC 层的接口。局域网数据链路层结构如图 3-8 所示，LLC 层目前不常使用。

（1）MAC。

MAC 子层的主要功能包括数据帧的封装/卸装、帧的寻址和识别、帧的接收与发送、链路的管

理、帧的差错控制等。MAC 层的主要访问方式有 CSMA/CD、令牌环和令牌总线三种。

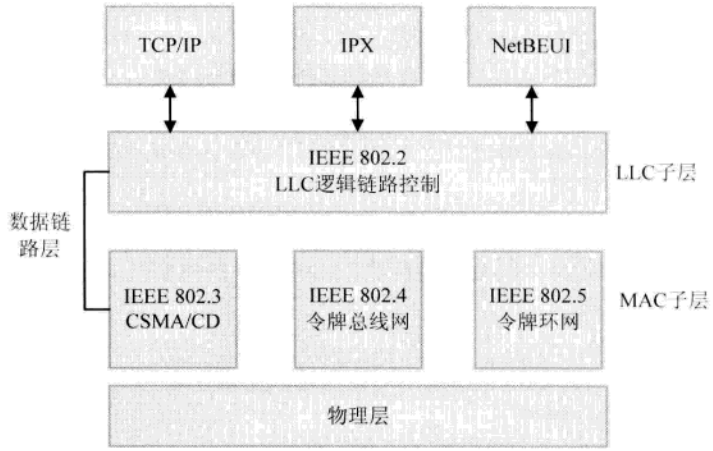



图 3-8　局域网数据链路层结构

以太网发送数据需要遵循一定的格式，以太网中的 MAC 帧格式如图 3-9 所示。

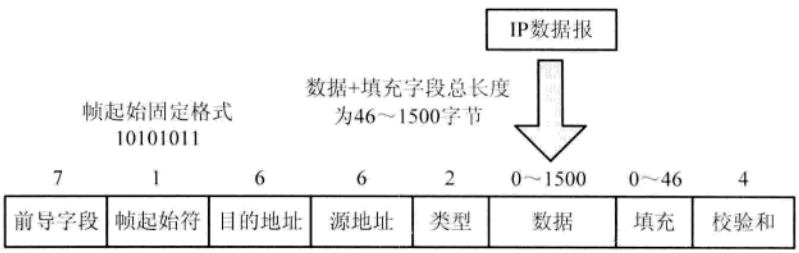



图 3-9　MAC 帧格式

帧由 8 个字段组成，每一个字段有一定含义和用途。每个字段长度不等，下面分别加以简述。

- 前导字段：形为 1010…1010，长度为 7 个字节。
- 帧起始符字段：固定格式为 10101011，长度为 1 个字节。
- 目的地址、源地址字段：可以是 6 个字节。最高位为 0，代表普通地址；最高位为 1，代表组地址；全 1 的目标地址是广播地址。
- 类型字段：标识上一层使用什么协议，以便把收到的 MAC 帧数据上交给上一层协议，也可以表示长度。

类型字段是 DIX 以太网帧的说法，而 IEEE 802.3 帧中的该字段被称为长度字段。由于该字段有两个字节，可以表示 0～65535，因此该字段可以赋予多个含义，0～1500 可以表示长度值，1536～65535（0x0600～0xFFFF）被用于描述类型值。考试中，该字段常标识为长度字段。

- 数据字段：上一层的协议数据，长度为0～1500字节。
- 填充字段：确保最小帧长为64个字节，长度为0～46字节。
- 校验和字段：32位的循环冗余码，检验算法见本书的CRC部分。

**注意**：以太网的最小帧长为64字节，这个帧长是指从**目的地址到校验和**的长度。

很多资料中往往提到泛洪一词，容易和广播混淆。广播和泛洪是不同的。广播帧形式为FF.FF.FF.FF.FF.FF，广播是向子网所有端口（含自身端口）发送广播帧；泛洪是向所有端口（除自身端口）发送普通数据帧。

（2）MAC地址。

**MAC地址**，也叫硬件地址，又叫链路地址，**由48比特组成。**MAC地址结构如图3-10所示。

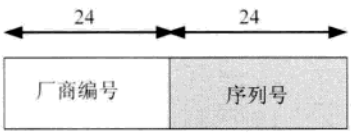



图3-10　MAC地址结构

MAC地址的前24位是厂商编号，由IEEE分配给生产以太网网卡的厂家；后24位是序列号，由厂家自行分配，用于表示设备地址。网卡的物理地址通常是由网卡生产厂家烧入网卡的EPROM（一种闪存芯片，通常可以通过程序擦写），它存储的是真正表示主机的地址，用于发送和接收的终端传输数据。也就是说，在网络底层的物理传输过程中是通过物理地址来识别主机的，一般也是全球唯一的。

（3）LLC。

LLC子层能向上提供以下四种不同类型的服务：

- 不确认的无连接服务：即数据报服务 ，适用于点对点通信、广播通信、多播通信（组播通信）。
- 面向连接服务：即虚电路服务，这种方式特别适合于传送很长的数据文件。
- 带确认的无连接服务：即可靠的数据报服务，这种方式特别适合于过程控制或自动化工厂环境中的告警信息或控制信号的传输。带确认的无连接服务只用在令牌总线网中。
- 高速传送服务：这种方式专为城域网使用。

2. CSMA/CD

载波监听多路访问/冲突检测（Carrier Sense Multiple Access/Collision Detect，CSMA/CD）是一种争用型的介质访问控制协议，起源于美国夏威夷大学开发的ALOHA网所采用的争用型协议，并对其进行了改进，具有更高的介质利用率。

CSMA/CD的工作原理是：发送数据前先监听信道是否空闲，若空闲，则立即发送数据。在发送数据时，边发送边继续监听。若监听到冲突，则立即停止发送数据，等待一段随机时间再重新尝试。

CSMA/CD 是一种解决访问冲突的协议，技术上易实现，网络中各工作站处于平等地位，不需要集中控制，不提供优先级控制。**在网络负载较小时，CSMA/CD 协议的通信效率很高；但在网络负载增大时，发送时间增加，发送效率急剧下降。这种网络协议适合传输非实时数据。**如图 3-11 所示描述了 CSMA/CD 和令牌环线路利用率与延时的关系。

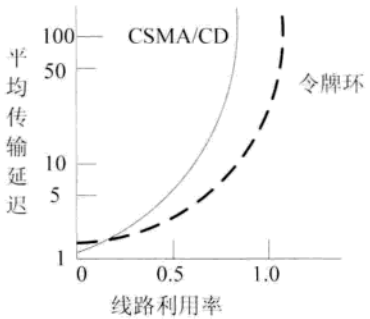



图 3-11 CSMA 特性

**注意**：万兆以太网标准（IEEE 802.3ae）采用了全双工方式，彻底抛弃了 CSMA/CD。

下面讲解 CSMA/CD 的重要组成和重要概念。

（1）多路访问。

表明多路计算机连接在一根总线上。

（2）载波监听（CSMA）。

表明发送数据前检测总线中是否有数据发送，如果有，则进入类似退避算法的程序，进而反复进行载波监听工作；如果没有，则依据一定的坚持算法决定如何发送。

这里要注意一个重要时间参数，以太网规定了**帧间最小间隔为 9.6μs**，使接收方在接收完数据后清理缓存，做好接收下一帧的准备。

坚持算法可以分为以下三类：

1）**1-持续 CSMA（1-persistent CSMA）**。当信道忙或发生冲突时，要发送帧的站一直持续监听，一旦发现信道有空闲（即在帧间最小间隔时间内没有检测到信道上有信号）便可发送。

特点：有利于抢占信道，减少信道空闲时间；较长的传播延迟和同时监听会导致多次冲突，降低系统性能。

2）**非持续 CSMA**。发送方并不持续侦听信道，而是在冲突时等待随机的一段时间 N，再发送。

特点：有更好的信道利用率，由于随机时延后退，从而减少了冲突的概率；然而，可能出现的问题是因后退而使信道闲置一段较长时间，这会使信道的利用率降低，而且增加了发送时延。

3）**p-持续 CSMA（p-persistent CSMA）**。发送方按 P 概率发送帧，即信道空闲时（即在帧间最小间隔时间内没有检测到信道上有信号），发送方不一定发送数据，而是按照 P 概率发送。以 1-P

概率不发送，若不发送数据，下一时间间隔 τ 仍空闲，同理进行发送；若信道忙，则等待下一时间间隔 τ；若冲突，则等待随机的一段时间重新开始。**τ 为单程网络传输时延。**

特点：P 的取值比较困难，大了会产生冲突，小了会延长等待时间。假定 n 个发送站等待发送，此时发现网络中有数据传送，当数据传输结束时，则有可能出现 n×P 个站发送数据。如果 n×P>1，则必然出现多个站点发送数据，这也必然导致冲突。有的站传输数据完毕后产生新帧与等待发送的数据帧竞争，很可能加剧冲突。如果 P 太小，例如 P=0.01，则表示一个站点中 100 个时间单位才会发送一次数据，这样 99 个时间单位就空闲了，造成浪费。

（3）冲突检测。

CSMA/CD 采用“边发送边监听”方式，即边发送边检测信道信号电压变化，如果发现信号变化幅度超过一定限度，则认为总线上发生“冲突”。以下介绍几个重要定义和数据：

- **电磁波在 1km 电缆传播的时延约为 5μs。**
- **冲突检测最长时间为两倍的总线端到端的传播时延（2τ），2τ 称为争用期（contention period），又称为碰撞窗口。**经过争用期还没有检测到碰撞时，才能肯定发送不会出现碰撞。
- **10M 以太网争用期定为 51.2μs。**对于 10Mb/s 网络，时间 51.2μs 可以发送 512bit 数据，即 64 字节。
- 以太网规定 10Mpbs 以太网**最小帧长为 64 字节，最大帧长为 1518 字节，最大传输单元（MTU）为 1500 字节**。小于 64 字节的都是由于冲突而异常终止的**无效帧**，接收这类帧时应将其**丢弃（千兆以太网和万兆以太网最小帧长为 512 字节）。**
- **最小帧长=网络速率×2×（最大段长/信号传播速度）**
- **吞吐率**：单位时间实际传送的数据位数。

**吞吐率=帧长/（传输数据帧所花费的时间+1 帧发送到网络所花费的时间））=帧长/（网络段长/传播速度+1 帧长/网络数据速率）**

- **网络利用率=吞吐率/网络数据速率**
- **强化碰撞，**当发生碰撞时，发送数据的站除了立刻停止发送当前数据外，还需要发送 32bit 或 48bit 的**干扰信号（Jamming Signal）**，所有站都会收到阻塞信息（连续几个字节的全 1）。

（4）退避算法。

CSMA 只能减少冲突，不能完全避免冲突，只有当经过争用期这段时间还没有检测到碰撞时，才能肯定本次发送的数据不会发生碰撞。以太网使用退避算法中的一种（**截断的二进制指数退避算法**）来解决发送数据的碰撞问题。这种算法规定：发生碰撞的站在信道空闲后并不立即发送数据，而是推迟一个随机时间再进入发送流程。这种方法减少了重传时再次发生碰撞的概率。

算法如下：

1）设定基本退避时间为争用期 2τ。

2）从整数集合[0, $2^k$–1]中随机取一个整数 r，则 r×2τ 为发送站等待时间。其中，k=Min[重传次

数,10]。

3）重传次数大于 16 次，则丢弃该帧数据并汇报高层。

从流程可知，**该算法的特点是网络负载越重，可能后退的时间越长，没有对优先级进行定义，不合适突发性业务和流式业务。该算法考虑了网络负载对冲突的影响，在重负载下能有效分解冲突。**

3. IEEE 802 系列协议

IEEE 802 协议包含了以下多种子协议。把这些协议汇集在一起就叫 802 协议集，该协议集合的组成如图 3-12 所示。

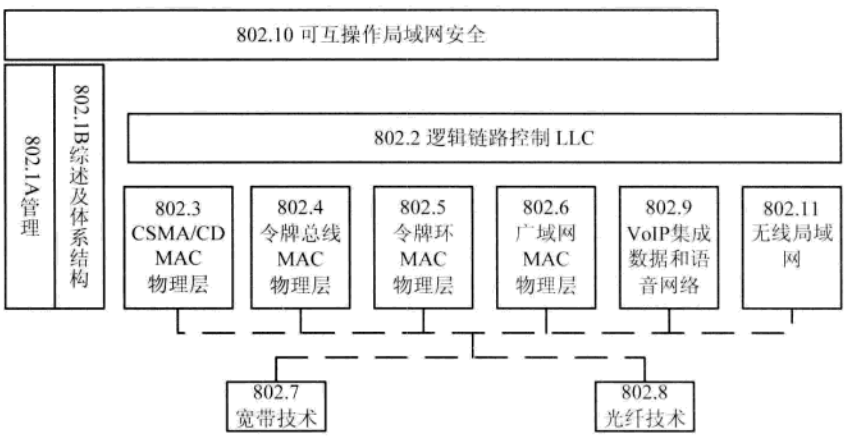



图 3-12 802 体系结构

（1）IEEE 802.1 系列。

IEEE 802.1 协议提供高层标准的框架，包括端到端协议、网络互连、网络管理、路由选择、桥接和性能测量。

- IEEE 802.1d：生成树协议（Spanning Tree Protocol，STP）。
- IEEE 802.1P：是交换机与优先级相关的流量处理的协议。
- IEEE 802.1q：虚拟局域网（Virtual Local Area Network，VLAN）协议定义了 VLAN 和封装技术，包括 GARP 协议及其源码、GVRP 协议及其源码。
- **IEEE 802.1s**：多生成树协议（Multiple Spanning Tree Protocol，MSTP）。
- **IEEE 802.1w**：快速生成树协议（Rapid Spanning Tree Protocol，RSTP）。
- **IEEE 802.1x**：基于端口的访问控制(Port Based Network Access Control)协议起源于 802.11 协议，目的是为了解决无线局域网用户的接入认证问题。802.1x 协议提供了一种用户接入认证的手段，并简单地通过控制接入端口的开/关状态来实现，不仅适用于无线局域网的接入认证，还适用于点对点物理或逻辑端口的接入认证。

（2）IEEE 802.2。

**IEEE 802.2**：逻辑链路控制（Logical Link Control，LLC）提供 LAN 和 MAC 子层与高层协议间的一致接口。

（3）IEEE 802.3 系列。

IEEE 802.3 是考试的重中之重。802.3 是以太网规范，定义 CSMA/CD 标准的媒体访问控制（MAC）子层和物理层规范。

- **IEEE 802.3ab**：该标准针对实体媒介部分制定的 1000 Base-T 规格，使得超高速以太网不再只限制于光纤介质。这是一个传输介质为4对 CAT-5 双绞线、100m 内达到以 1 Gb/s 传输数据的标准。
- **IEEE 802.3u**：快速以太网（Fast Ethernet）的最小帧长不变，数据速率提高了 10 倍，所以冲突时槽缩小为 5.12μs。以太网的计算冲突时槽的公式为

$$slot \approx 2S/0.7C+2tphy$$

其中，S 表示网络的跨距（最长传输距离），0.7C 为 0.7 倍光速（信号传播速率），tphy 是发送站物理层时延（由于往返需通过站点两次，所以取其时延的两倍值）。

- **IEEE 802.3z**：千兆以太网（Gigabit Ethernet）。千兆以太网标准 802.3z 定义了一种帧突发方式（frame bursting），这种方式是指一个站可以连续发送多个帧，用以保证传输站点连续发送一系列帧而不中途放弃对传输媒体的控制，该方式仅适用于半双工模式。在成功传输一帧后，发送站点进入突发模式以允许继续开始传输后面的帧，直到达到每次 65536 比特的突发限制。
- **IEEE 802.3ae**：万兆以太网（10 Gigabit Ethernet）。该标准仅支持光纤传输，提供两种连接：一种是和以太网连接，速率为 10Gb/s 物理层设备，即 LAN PHY；另一种是与 SHD/SONET 连接，速率为 9.58464Gb/s 的 WAN 设备，即 WAN PHY。通过 WAN PHY 可以与 SONETOC-192 结合，通过 SONET 城域网提供端到端连接。该标准支持 10Gbase-s（850nm 短波）、10Gbase-l（1310nm 长波）、10Gbase-E（1550nm 长波）三种规格，最大传输距离分别为 300m、10km 和 40km。802.3ae 支持 802.3 标准中定义的最小帧长和最大帧长，不采用 CSMA/CD 方式，只用全双工方式**（千兆以太网和万兆以太网的最小帧长为 512 字节）**。

**（4）IEEE 802.4**：令牌总线网（Token-Passing Bus）。

**（5）IEEE 802.5**：令牌环线网。

**（6）IEEE 802.6**：城域网 MAN，定义城域网的媒体访问控制（MAC）子层和物理层规范。

**（7）IEEE 802.7**：宽带技术咨询组，为其他分委员会提供宽带网络技术的建议和咨询。

**（8）IEEE 802.8**：光纤技术咨询组，为其他分委员会提供使用有关光纤网络技术的建议和咨询。

**（9）IEEE 802.9**：集成数据和语音网络（Voice over Internet Protocol，VoIP）定义了综合语音

/数据终端访问综合语音/数据局域网（包括 IVD LAN、MAN、WAN ）的媒体访问控制（MAC）子层和物理层规范。

**（10）IEEE 802.10**：可互操作局域网安全标准，定义局域网互连安全机制。

**（11）IEEE 802.11**：无线局域网标准，定义了自由空间媒体的媒体访问控制（MAC）子层和物理层规范。

**（12）IEEE 802.12**：按需优先定义使用按需优先访问方法的 100Mp/s 以太网标准。

**（13）没有 802.13 标准**：13 不吉利。

**（14）IEEE 802.14**：有线电视标准。

**（15）IEEE 802.15**：无线个人局域网（Personal Area Network，PAN），适用于短程无线通信的标准（如蓝牙）。

**（16）IEEE 802.16**：宽带无线接入（Broadband Wireless Access，BWA）标准。

4. 802.3 规定的传输介质特性

前面介绍了以太网传输介质，下面介绍传输介质的选用方案。传输介质一般使用 10Base-T 形式进行描述。其中 10 是速率，即 10Mb/s；Base 表示传输速率，Base 是基带，Broad 是宽带；而 T 则代表传输介质，T 是双绞线，F 是光纤。

常见的传输介质如表 3-3 所示。

**表 3-3 常见的传输介质及其特性**

| 名称 | 电缆 | 最大段长 | 特点 |
|---|---|---|---|
| 100Base-T4 | 4 对 3 类 UTP | 100m | 3 类双绞线，8B/6T，NRZ 编码 |
| 100Base-TX | 2 对 5 类 UTP 或 2 对 STP | 100m | 100Mb/s 全双工通信，MLT-3 编码 |
| 100Base-FX | 1 对光纤 | 2000m | 100Mb/s 全双工通信，4B/5B、NRZI 编码 |
| 1000Base-CX | 2 对 STP | 25m | 2 对 STP |
| 1000Base-T | 4 对 UTP | 100m | 4 对 UTP |
| 1000Base-SX | 62.5μm 多模 | 220m | 模式带宽 160MHz*km，波长 850nm |
| | | 275m | 模式带宽 200MHz*km，波长 850nm |
| | 50μm 多模 | 500m | 模式带宽 400MHz*km，波长 850nm |
| | | 550m | 模式带宽 500MHz*km，波长 850nm |
| 1000Base-LX | 62.5μm 多模 | 550m | 模式带宽 500MHz*km，波长 850nm |
| | 50μm 多模 | | 模式带宽 400MHz*km，波长 850nm |
| | | | 模式带宽 500MHz*km，波长 850nm |
| | 单模 | 5000m | 波长 1310nm 或 1550nm |

续表

| 名称 | 电缆 | 最大段长 | 特点 |
| --- | --- | --- | --- |
| 10Gbase-S | 50μm 多模 | 300m | 波长 850nm |
| | 62.5μm 多模 | 65m | 波长 850nm |
| 10Gbase-L | 单模 | 10km | 波长 1310nm |
| 10Gbase-E | 单模 | 40km | 波长 1550nm |
| 10Gbase-LX4 | 单模 | 10km | 波长 1310nm<br>波分多路复用 |
| | 50μm 多模 | 300m | |
| | 62.5μm 多模 | | |

注：通常用光纤传输信号的速率与其传输长度的乘积来描述光纤的模式带宽特性，用 B*L 表示，单位为 MHz*km。

# 第 4 学时　网络层

第 1 天的第 4 学时主要学习网络层所涉及的重要知识点。网络层是 OSI 参考模型中的第三层，本层知识点相当重要，而且也很多。由于网络路由协议知识在上、下午考试中均考到，因此该知识点统一放入路由器部分进行集中讲解。根据历年考试的情况来看，每次考试涉及相关知识点的分值（除去路由知识外）约在 2～8 分之间。网络层知识的考查在上午和下午的考试中均有涉及。本章考点知识结构图如图 4-1 所示。



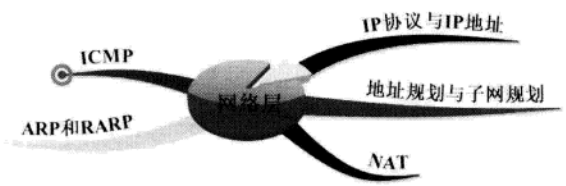



图 4-1　考点知识结构图

## 4.1　IP 协议与 IP 地址

### 4.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：IP 协议、IPv4 地址、IP 地址分类、几类特殊的 IP 地址。

### 4.1.2 知识点精讲

1. IP 协议

网络之间的互连协议（Internet Protocol，IP）是方便计算机网络系统之间相互通信的协议，是各大厂家遵循的计算机网络相互通信的规则。如图 4-2 所示给出了 IP 数据报头（Packet Header）结构，有些教材称为 IP 数据报头。

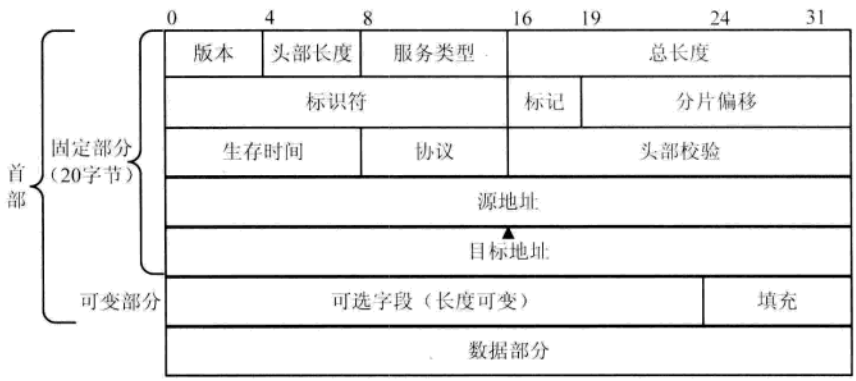



图 4-2 IP 数据报报头格式

（1）版本。

长度为 4 位，标识数据报的 IP 版本号，值为二进制 0100，则表示 IPv4。

（2）头部长度（Internet Header Length，IHL）。

长度为 4 位。该字段表示数的单位是 32 位，即 4 字节。常用的值是 5，也是可取的最小值，表示报头为 20 字节；可取的最大值是 15，表示报头为 60 字节。

（3）区分服务（Type of Service，ToS）。

长度为 8 位，指定特殊数据处理方式。该字段分为两部分：优先权和 ToS。后来该字段被 IETF 改名为区分服务（Differentiated Services，DS）。该字段的前 6 位构成了区分代码点（DiffServ Code Point，DSCP）和显式拥塞通知（Explicit Congestion Notification，ECN）字段，DSCP 用于定义 64 个不同服务类别，而 ECN 用于通知拥塞，具体如图 4-3 所示。

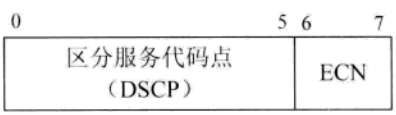



图 4-3 ECN 字段

（4）总长度（Total Length）。

该字段长度为 16 位，单位是字节，指的是首部加上数据之和的长度。所以，数据报的最大长

度为 $2^{16}-1=65535$ 字节。由于有 MTU 限制（如以太网单个 IP 数据报就不能超过 1500 字节），所以超过 1500 字节的 IP 数据报就要分段，而总长度是所有分片报文的长度和。

（5）标识符（Identifier）。

该字段长度为 16 位。同一数据报分段后，其标识符一致，这样便于重装成原来的数据报。

（6）标记字段（Flag）。

该字段长度为 3 位，第 1 位不使用；第 2 位是不分段（DF）位，值为 1 表示不能分片，为 0 表示允许分片；第 3 位是更多分片（MF）位，值为 1 表示之后还有分片，为 0 表示最后一个分片。

（7）分片偏移字段（Fragment Offset）。

该字段长度为 13 位，单位 8 字节，即每个分片长度是 8 字节的整数倍。该字段是标识所分片的分组，分片之后在原始数据中的相对位置。

（8）生存时间（Time to Live，TTL）。

该字段长度为 8 位，用来设置数据报最多可以经过的路由器数。由发送数据的源主机设置，通常为 16、32、64、128 个。每经过一个路由器，其值减 1，直到为 0 时该数据报被丢弃。

（9）协议字段（Protocol）。

该字段长度为 8 位，指明 IP 层所封装的上层协议类型，如 ICMP（1）、IGMP（2）、TCP（6）、UDP（17）等。

（10）头部校验（Header Checksum）。

该字段长度为 16 位，是根据 IP 头部计算得到的校验和码。计算方法没有采用复杂的 CRC 编码，而是对头部中每个 16 比特进行二进制反码求和（与 ICMP、IGMP、TCP、UDP 不同，IP 报头不对 IP 报头后面的数据进行校验）。

（11）源地址、目标地址字段（Source and Destination Address）。

该字段长度均为 32 位，用来标明发送 IP 数据报文的源主机地址和接收 IP 报文的目标主机地址，都是 IP 地址。

（12）可选字段（Options）。

该字段长度可变，从 1 字节到 40 字节不等，用来定义一些任选项，如记录路径、时间戳等。这些选项很少被使用，并且并不是所有主机和路由器都支持这些选项。可选项字段的长度必须是 32 位（4 字节）的整数倍，如果不足，必须填充 0 以达到此长度要求。

2. IPv4 地址

IP 地址就好像电话号码：有了某人的电话号码，你就能与他通话了。同样，有了某台主机的 IP 地址，你就能与这台主机通信了。TCP/IP 协议规定，IP 地址使用 32 位的二进制来表示，也就是 4 个字节。例如，采用二进制表示方法的 IP 地址形式为 00010010 00000010 10101000 00000001，这么长的地址，网络工程师操作和记忆起来太费劲。为了方便使用，IP 地址经常被写成十进制的形式，中间使用符号“.”分开不同的字节。于是，上面的 IP 地址可以表示为 18.2.168.1。IP 地址的这种表示法叫做**点分十进制表示法**，这显然比 1 和 0 容易记忆得多。如图 4-4 所示将 32 位的地址映射到用点分十进制表示法表示的地址上。

| 00010010 | 00000010 | 10101000 | 00000001 |
|---|---|---|---|
| 18 . 2 . 168 . 1 | | | |

图 4-4 点分十进制与 32 地址的对应表示形式

3. IP 地址分类

IP 地址分为五类：A 类用于大型网络，B 类用于中型网络，C 类用于小型网络，D 类用于组播，E 类保留用于实验。每一类有不同的网络号位数和主机号位数。各类地址特征如图 4-5 所示。

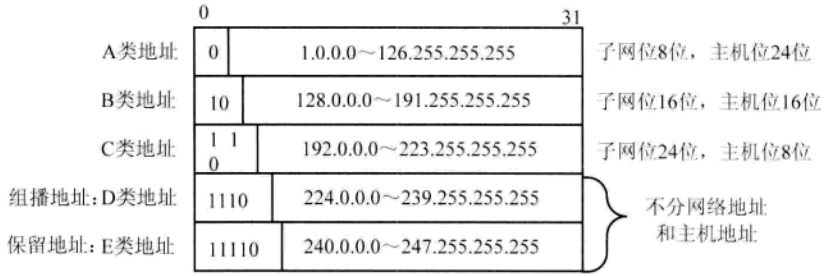



图 4-5 五类地址特征

（1）A 类地址。

IP 地址写成二进制形式时，A 类地址的第一位总是 0。A 类地址的第 1 字节为网络地址，其他 3 个字节为主机地址。

A 类地址范围：1.0.0.0～126.255.255.255。

A 类地址中的私有地址和保留地址：

1）10.X.X.X 是私有地址，就是在互联网上不使用，而只用在局域网络中的地址。网络号为 10，网络数为 1 个，地址范围为 10.0.0.0～10.255.255.255。

2）127.X.X.X 是保留地址，用做环回（Loopback）地址，环回地址（典型的是 127.0.0.1）向自己发送流量。发送到该地址的数据不会离开设备到网络中，而是直接回送到本主机。该地址既可以作为目标地址，又可以作为源地址，是一个虚 IP 地址。

（2）B 类地址。

IP 地址写成二进制形式时，B 类地址的前两位总是 10。B 类地址的第 1 和第 2 字节为网络地址，第 3 和第 4 字节为主机地址。

B 类地址范围：128.0.0.0～191.255.255.255。

B 类地址中的私有地址和保留地址：

1）172.16.0.0～172.31.255.255 是私有地址。

2）**169.254.X.X 是保留地址**。如果 PC 机上的 IP 地址设置自动获取，而 PC 机又没有找到相应的 DHCP 服务，那么最后 PC 机可能得到保留地址中的一个 IP。没有获取到合法 IP 后的 PC 机地

址分配情况如图 4-6 所示。

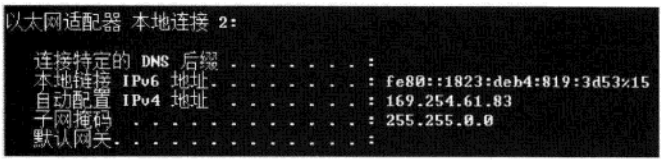



图 4-6　在断开的网络中，PC 机被随机分配了一个 169.254.X.X 保留地址

（3）C 类地址。

IP 地址写成二进制形式时，C 类地址的前三位固定为 110。C 类地址第 1、第 2 和第 3 字节为网络地址，第 4 字节为主机地址。

C 类地址范围：192.0.0.0～223.255.255.255。

C 类地址中的私有地址：192.168.X.X 是私有地址，地址范围：192.168.0.0～192.168.255.255。

（4）D 类地址。

IP 地址写成二进制形式时，D 类地址的前四位固定为 1110。D 类地址不分网络地址和主机地址，该类地址用作组播。

D 类地址范围：224.0.0.0～239.255.255.255。

（5）E 类地址。

IP 地址写成二进制形式时，E 类地址的前四位固定为 11110。E 类地址不分网络地址和主机地址。

E 类地址范围：240.0.0.0～247.255.255.255。

4. 几类特殊的 IP 地址

几类特殊的 IP 地址的结构和特性如表 4-1 所示。

表 4-1　特殊地址特性

| 地址名称 | 地址格式 | 特点 | 可否作为源地址 | 可否作为目标地址 |
|---|---|---|---|---|
| 有限广播 | 255.255.255.255（网络字段和主机字段全 1） | 不被路由，会被送到相同物理网络段上的所有主机 | N | Y |
| 直接广播 | 主机字段全 1，如 192.1.1.255 | 广播会被路由，并会发送到专门网络上的每台主机 | N | Y |
| 网络地址 | 主机位全 0，如 192.168.1.0 | 表示一个子网 | N | N |
| 全 0 地址 | 0.0.0.0 | 代表任意主机 | Y | N |
| 环回地址 | 127.X.X.X | 向自己发送数据 | Y | Y |

## 4.2 地址规划与子网规划

### 4.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：子网掩码、IP地址结构、VLSM和CIDR、IP地址和子网规划。

### 4.2.2 知识点精讲

1. 子网掩码

子网掩码用于区分网络地址、主机地址、广播地址，是表示网络地址和子网大小的重要指标。子网掩码的形式是网络号部分全1，主机号部分全0。掩码也能像IPv4地址一样使用点分十进制表示法书写，但掩码不是IP地址。掩码还能使用“/从左到右连续1的总数”形式表示，这种描述方法称为**建网比特数**。

如表4-2和表4-3所示给出了B类和C类网络可能出现的子网掩码以及对应网络数量和主机数量。

表4-2 B类子网掩码特性

| 子网掩码 | 建网比特数 | 子网络数 | 可用主机数 |
|---|---|---|---|
| 255.255.255.252 | /30 | 1，6382 | 2 |
| 255.255.255.248 | /29 | 8，192 | 6 |
| 255.255.255.240 | /28 | 4，096 | 14 |
| 255.255.255.224 | /27 | 2，048 | 30 |
| 255.255.255.192 | /26 | 1，024 | 62 |
| 255.255.255.128 | /25 | 512 | 126 |
| 255.255.255.0 | /24 | 256 | 254 |
| 255.255.254.0 | /23 | 128 | 510 |
| 255.255.252.0 | /22 | 64 | 1022 |
| 255.255.248.0 | /21 | 32 | 2046 |
| 255.255.240.0 | /20 | 16 | 4094 |
| 255.255.224.0 | /19 | 8 | 8190 |
| 255.255.192.0 | /18 | 4 | 16382 |
| 255.255.128.0 | /17 | 2 | 32766 |
| 255.255.0.0 | /16 | 1 | 65534 |

表 4-3 C 类子网掩码特性

| 子网掩码 | 建网比特数 | 子网络数 | 可用主机数 |
|---|---|---|---|
| 255.255.255.252 | /30 | 64 | 2 |
| 255.255.255.248 | /29 | 32 | 6 |
| 255.255.255.240 | /28 | 16 | 14 |
| 255.255.255.224 | /27 | 8 | 30 |
| 255.255.255.192 | /26 | 4 | 62 |
| 255.255.255.128 | /25 | 2 | 126 |
| 255.255.255.0 | /24 | 1 | 254 |

**注意**：（1）主机数=可用主机数+2。

（2）A 类地址的默认掩码是 255.0.0.0；B 类地址的默认掩码是 255.255.0.0；C 类地址的默认掩码是 255. 255. 255.0。

2. 地址结构

早期 IP 地址结构为两级地址：

IP 地址::={<网络号>,<主机号>} （4-1）

RFC 950 文档发布后增加一个子网号字段，变成三级网络地址结构

IP 地址::={<网络号>,<子网号>,<主机号>} （4-2）

3. VLSM 和 CIDR

（1）可变长子网掩码（Variable Length Subnet Masking，VLSM）。

传统的 A 类、B 类和 C 类地址使用固定长度的子网掩码，分别为 8 位、16 位、24 位，这种方式比较死板、浪费地址空间，VLSM 则是对部分子网再次进行子网划分，允许一个组织在同一个网络地址空间中使用多个不同的子网掩码。VLSM 使寻址效率更高，IP 地址利用率也更高。所以 VLSM 技术被用来节约 IP 地址，该技术可以理解为把大网分解成小网。

（2）无类别域间路由（Classless Inter-Domain Routing，CIDR）。

在进行网段划分时，除了有将大网络拆分成若干个小网络的需求外，也有将小网络组合成大网络的需求。在一个有类别的网络中（只区分 A、B、C 等大类的网络），路由器决定一个地址的类别，并根据该类别识别网络和主机。而在 CIDR 中，路由器使用前缀来描述有多个位是网络位（或称前缀），剩下的位则是主机位。CIDR 显著提高了 IPv4 的可扩展性和效率，通过使用路由聚合（或称超网）可有效地减小路由表的大小，节省路由器的内存空间，提高路由器的查找效率。该技术可以理解为把小网合并成大网。

4. IP 地址和子网规划

IP 地址和子网规划是历次网络工程师考试的重点，每次考试的分值大约在 3～6 分，而且上、下午考试都有可能考到。IP 地址和子网规划类的题目可以分为以下几种形式：

（1）给定 IP 地址和掩码，求网络地址、广播地址、子网范围、子网能容纳的最大主机数。

【例 4-1】已知 8.1.72.24，子网掩码是 255.255.192.0。计算网络地址、广播地址、子网范围、子网能容纳的最大主机数。

1）计算子网的步骤如图 4-7 所示。

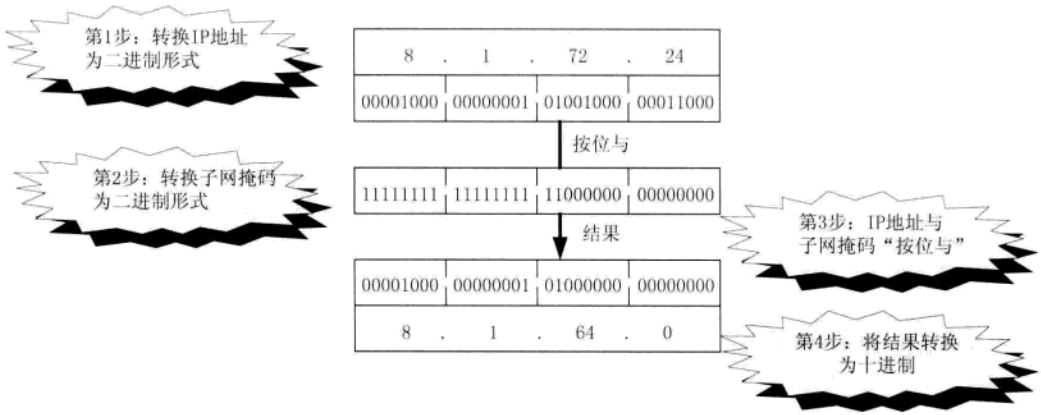



图 4-7 计算子网

2）计算广播地址的步骤如图 4-8 所示。

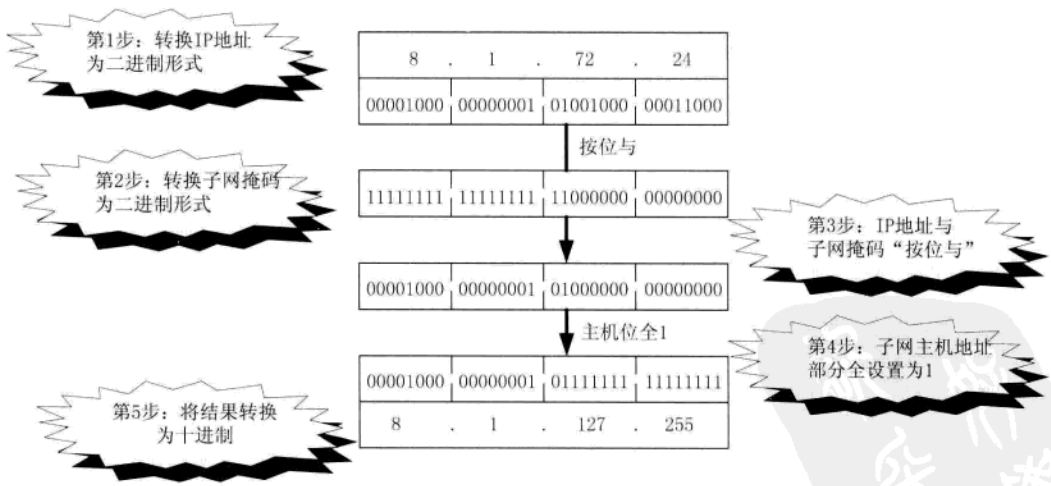



图 4-8 计算广播地址

3）子网范围。

子网范围=[子网地址]～[广播地址]=8.1.64.0～8.1.127.255。

4）子网能容纳的最大主机数。

子网能容纳的最大主机数=$2^{\text{主机位}}-2=2^{14}-2=16382$。

（2）给定现有的网络地址和掩码并给出子网数目，计算子网掩码及子网可分配的主机数。

【例 4-2】某公司网络的地址是 200.100.192.0，掩码为 255.255.240.0，要把该网络分成 16 个子网，则对应的子网掩码应该是多少？每个子网可分配的主机地址数是多少？

1）计算子网掩码。

计算子网掩码的步骤如图 4-9 所示。

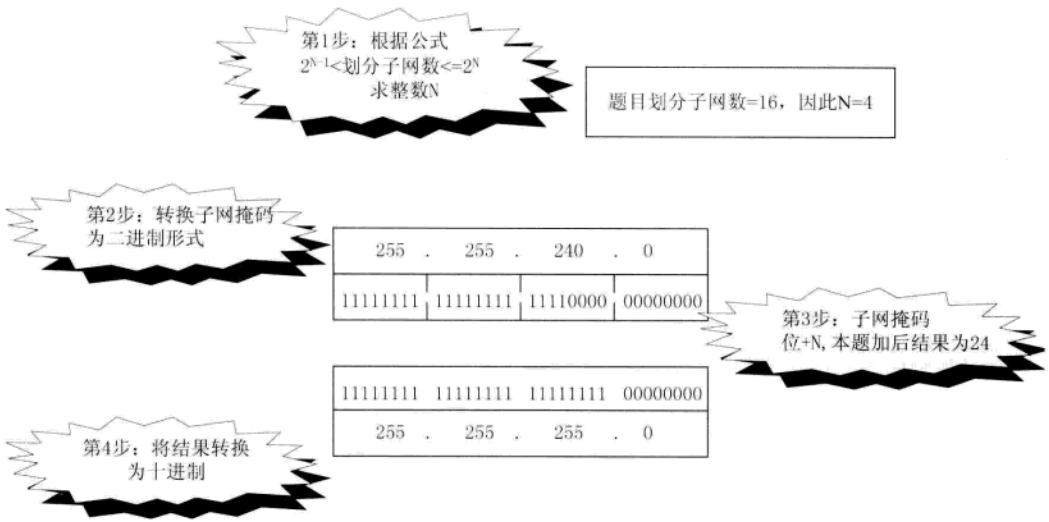



图 4-9　计算子网掩码

可以得到，本题的子网掩码为 255.255.255.0。

2）计算子网可分配的主机数。

子网能容纳的最大主机数=$2^{\text{主机位}}-2=2^8-2=254$。

（3）给出网络类型及子网掩码，求划分子网数。

【例 4-3】一个 B 类网络的子网掩码为 255.255.192.0，则这个网络被划分成了多少个子网？

1）根据网络类型确定网络号的长度。

本题网络类型为 B 类网，因此网络号为 16 位。

2）转换子网掩码为建网比特数。

本题中的子网掩码 255.255.192.0 可以用/18 表示。

3）子网号=建网比特数-网络号，划分的子网个数=$2^{\text{子网号}}$。

本题子网号=18–16=2，因此划分的子网个数=$2^2=4$。

（4）使用子网汇聚将给出的多个子网合并为一个超网，求超网地址。

【例 4-4】路由汇聚（Route Summarization）是把小的子网汇聚成大的网络，将 172.2.193.0/24、172.2.194.0/24、172.2.196.0/24 和 172.2.198.0/24 子网进行路由汇聚后的网络地址是多少？

**1）将所有十进制的子网转换成二进制。**

本题转换结果如表 4-4 所示。

表 4-4 转换结果

| | 十进制 | 二进制 |
|---|---|---|
| 子网地址 | 172.2.193.0/24 | **10101100.0000010.11000** 001.00000000 |
| | 172.2.194.0/24 | **10101100.0000010.11000** 010.00000000 |
| | 172.2.196.0/24 | **10101100.0000010.11000** 100.00000000 |
| | 172.2.198.0/24 | **10101100.0000010.11000** 110.00000000 |
| 合并后的超网地址 | 172.2.192.0/21 | **10101100.0000010.11000** 000.00000000 |

2）从左到右找连续的相同位和相同位数。

从表 4-4 中可以发现，相同位为 21 位，即 10101100.0000010.11000　000.00000000 为新网络地址，将其转换为点分十进制得到的汇聚网络为 172.16.192.0/21。

## 4.3 ICMP

### 4.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：ICMP 报文格式、ICMP 报文分类、ICMP 报文应用。

### 4.3.2 知识点精讲

Internet 控制报文协议（Internet Control Message Protocol，ICMP）是 TCP/IP 协议族的一个子协议，是网络层协议，用于 IP 主机和路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对用户数据的传递起着重要的作用。

（1）ICMP 报文格式。

ICMP 报文是**封装在 IP 数据报**内传输，封装结构如图 4-10 所示。由于 IP 数据报首部校验和并不检验 IP 数据报的内容，因此不能保证经过传输的 ICMP 报文不产生差错。

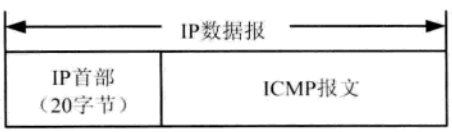



图 4-10 ICMP 报文封装在 IP 数据报内部

ICMP 报文如图 4-11 所示。


图 4-11　ICMP 报文格式

（2）ICMP 报文分类。

ICMP 报文分为 **ICMP 差错报告报文**和 **ICMP 询问报文**，具体如表 4-5 所示。

表 4-5　常考的 ICMP 报文

| 报文种类 | 类型值 | 报文类型 | 报文定义 | 报文内容 |
|---|---|---|---|---|
| 差错报告报文 | 3 | 目的不可达 | 路由器与主机不能交付数据时就向源点发送目的不可达报文 | 包括网络不可达、主机不可达、协议不可达、端口不可达、需要进行分片却设置了部分片、源路由失败、目的网络未知、目的主机未知、目的网络被禁止、目的主机被禁止、由于服务类型 TOS 网络不可达、由于服务类型 TOS 主机不可达、主机越权、优先权中止生效 |
| | 4 | 源点抑制 | 由于拥塞而丢弃数据报时就向源点发送抑制报文，降低发送速率 | |
| | 5 | 重定向（改变路由） | 路由器将重定向报文发送给主机，优化或改变主机路由 | 包括网络重定向、主机重定向、对服务类型和网络重定向、对服务类型和主机重定向 |
| | 11 | 时间超时 | 丢弃 TTL 为 0 的数据，向源点发送时间超时报文 | |
| | 12 | 参数问题 | 发现数据报首部有不正确字段时丢弃报文，并向源点发送参数问题报文 | |
| 询问报文 | 0 | 回送应答 | 收到**回送请求报文**的主机必须回应源主机**回送应答报文** | |
| | 8 | 回送请求 | | |
| | 13 | 时间戳请求 | 请求对方回答当前日期和时间 | |
| | 14 | 时间戳应答 | 回答当前日期和时间 | |

（3）ICMP 报文应用。

ICMP 报文应用有 Ping 命令（使用回送应答和回送请求报文）和 Traceroute 命令（使用时间超时报文和目的不可达报文）。

## 4.4 ARP 和 RARP

### 4.4.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：ARP 和 RARP 定义、ARP 病毒、ARP 病毒的发现和解决手段。

### 4.4.2 知识点精讲

1. ARP 和 RARP 定义

地址解析协议（Address Resolution Protocol，ARP）是将 32 位的 IP 地址解析成 48 位的以太网地址；而反向地址解析（Reverse Address Resolution Protocol，RARP）则是将 48 位的以太网地址解析成 32 位的 IP 地址。ARP 报文**封装在以太网帧**中进行发送。ARP 的请求过程如下：

（1）发送 ARP 请求。

请求主机以**广播方式**发出 **ARP 请求分组**。ARP 请求分组主要由**主机本身的 IP 地址、MAC 地址**以及**需要解析的 IP 地址**三个部分组成。具体发送 ARP 请求的过程如图 4-12 所示，该图要求找到 1.1.1.2 对应的 MAC 地址。

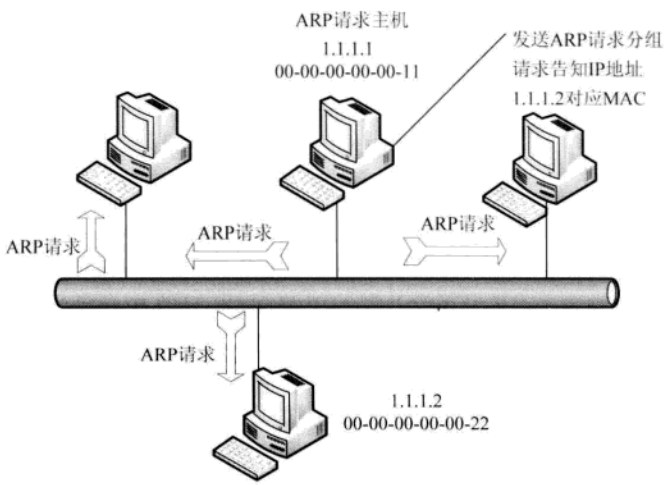



图 4-12 发送 ARP 请求分组

（2）ARP 响应。

所有主机都能收到 ARP 请求分组，但只有与请求解析的 IP 地址一致的主机响应，并以**单播方式**向 ARP 请求主机发送 ARP 响应分组。ARP 响应分组由**响应方的 IP 地址**和 **MAC 地址**组成。具体过程如图 4-13 所示，地址为 1.1.1.2 的主机发出响应报文。

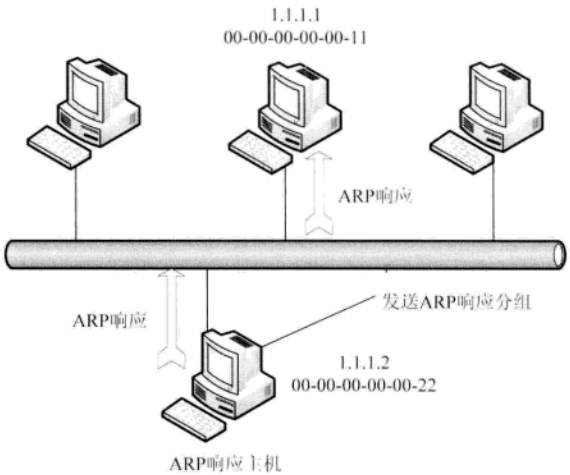



图 4-13　发送 ARP 响应分组

（3）A 主机写高速缓存。

A 主机收到响应分组后，将 1.1.1.2 和 MAC 地址 00-00-00-00-00-22 对应关系写入 ARP 高速缓存。**ARP 高速缓存**纪录了 IP 地址和 MAC 地址的对应关系，避免了主机进行一次通信就发送一次 ARP 请求分组的情况出现，减少了网络中 ARP 请求带来的广播报文。当然高速缓存中的每个 IP 地址和 MAC 地址的对应关系都有一定的**生存时间**，大于该时间的对应关系将被删除。

2. ARP 病毒

ARP 病毒是一种破坏性极大的病毒，利用了 ARP 协议设计之初没有任何验证功能这一漏洞而实施破坏。ARP 木马使用 ARP 欺骗手段破坏客户机建立正确的 IP 地址和 MAC 地址对应关系，把虚假的网关 MAC 地址发送给受害主机。达到盗取用户账户、阻塞网络、瘫痪网络的目的。

ARP 病毒利用感染主机的方法向网络发送大量虚假的 ARP 报文，**主机没有感染 ARP 木马时也有可能导致网络访问不稳定**。例如：向被攻击主机发送的虚假 ARP 报文中，目的 IP 地址为**网关 IP 地址**，目的 MAC 地址为**感染木马的主机 MAC 地址**。这样会将同网段内其他主机发往网关的数据引向发送虚假 ARP 报文的机器，并抓包截取用户口令信息。

ARP 病毒还能在局域网内产生大量的广播包，造成广播风暴。

3. 一类 ARP 病毒的发现和解决手段

网管员经常使用的发现和解决 ARP 病毒的手段有：接入交换机端口绑定固定的 MAC 地址、查看接入交换机的端口异常（一个端口短时间出现多个 MAC 地址）、安装 ARP 防火墙、发现主机

ARP 缓存中的 MAC 地址不正确时可以执行 arp-d 命令清除 ARP 缓存、主机使用“arp-s 网关 IP 地址/网关 MAC 地址”命令设置静态绑定。

通常还可以通过安装杀毒软件、给各类终端系统打补丁、交换机启用 ARP 病毒防治功能等组合方式阻挡攻击并去除 ARP 病毒。

## 4.5 IPv6

### 4.5.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：IPv6 的书写规则、单播地址。

### 4.5.2 知识点精讲

IPv6（Internet Protocol Version 6）是 IETF 设计的用于替代现行 IPv4 的下一代 IP 协议。IPv6 地址长度为 128 位，但通常写作 8 组，每组为 4 个十六进制数的形式，如 2002:0db8:85a3:08d3:1319:8a2e:0370:7345 是一个合法的 IPv6 地址。

1. IPv6 的书写规则

（1）任何一个 16 位段中起始的 0 不必写出来；任何一个 16 位段如果少于 4 个十六进制的数字，就认为忽略了起始部分的数字 0。

例如，2002:0db8:85a3:08d3:1319:8a2e:0370:7345 的第 2、第 4 和第 7 段包含起始 0。使用简化规则，该地址可以书写为 2002:db8:85a3:8d3:1319:8a2e:370:7345。

**注意**：只有起始的 0 才能被忽略，末尾的 0 不能忽略。

（2）任何由全 0 组成的 1 个或多个 16 位段的单个连续字符串都可以用一个双冒号“::”来表示。

例如：2002:0:0:0:0:0:0:0001 可以简化为 2002::5。

**注意**：双冒号只能用一次。

2. 单播地址

单播地址用于表示单台设备的地址。发送到此地址的数据包被传递给标识的设备。单播地址和多播地址的区别在于高八位不同，多播地址的高八位总是十六进制的 FF。单播地址有以下几类：

（1）**全球单播地址**。

全球单播地址是指这个单播地址是全球唯一的，其地址格式如图 4-14 所示。

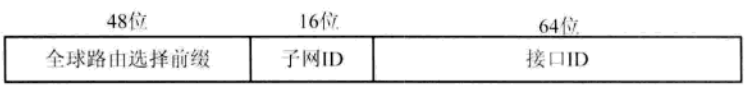



图 4-14 全球单播地址格式

当前分配的全球单播地址最高位为001（二进制）。

（2）**链路本地单播地址**。

链路本地单播地址在邻居发现协议等功能中很有用，该地址主要用于启动时及系统尚未获取较大范围的地址时，链路节点的自动地址配置。该地址的起始10位固定为1111111010（FE80::/10）。

（3）地区本地单播地址。

这个地址仅在一个给定区域内地址是唯一的，其他区域内可以使用相同的地址。但这类方式争议较大，地区本地单播地址的起始10位固定为1111111011（FE8C::/10）。

（4）任意播地址。

任意播地址更像一种服务，而不是一台设备，并且相同的地址可以驻留在提供相同服务的一台或多台设备中。任意广播地址取自单播地址空间，而且在语法上不能与其他地址区别开来。寻址的接口依据其配置确定单播和任意广播地址之间的差别。使用任意播地址的好处是路由器总选择到达最近的或代价最低的服务器路由。因此，提供一些通用服务的服务器能够通过一个大型的网络进行传播，并且流量可以由本地传送到最近的服务器，这样可以使得流量模型变得更加有效。

（5）组播地址。

多播地址标识不是一台设备，而是多台设备组成一个多播组。发送给一个多播组的数据包可以由单台设备发起。一个多播数据包通常包括一个单播地址作为它的源地址，一个多播地址作为它的目的地址。一个数据包中，多播地址从来不会作为源地址出现。IPv6中的组播在功能上与IPv4中的组播类似：表现为一组接口可以同时接受某一类的数据流量。IPv6的组播地址格式如图4-15所示。

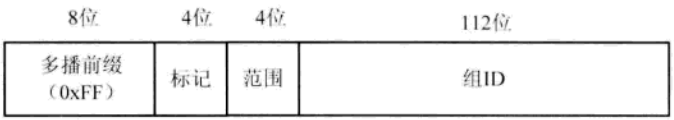



图4-15　IPv6的组播地址格式

组播分组前8比特设置为1，十六进制值为FF。接下来的4比特是地址生存期：0是永久的，1是临时的。接下来的4比特说明了组播地址范围（分组可以达到多远）：1为节点、2为链路、5为站点、8为组织、E为全局（整个因特网）。

如表4-6所示给出了IPv6高位数字代表的地址类型。

表4-6　IPv6地址类型

| 地址类型 | 高位数字（二进制） | 高位数字（十六进制） |
|---|---|---|
| 未指定 | 00…0 | ::/128 |
| 环回地址 | 00…1 | ::1/128 |
| 多播地址 | 11111111 | FF00::/8 |
| 链路本地单播地址 | 1111111010 | FE80::/10 |

续表

| 地址类型 | 高位数字（二进制） | 高位数字（十六进制） |
| --- | --- | --- |
| 地区本地单播地址（有争议） | 1111111011 | FEC0::/10 |
| 全球单播地址（当前分配的） | 001 | 2xxx::/4 或者 3xxx::/4 |
| 剩下作为未来全球单播地址分配 | | |

## 4.6 NAT

### 4.6.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：基本 NAT、NAPT。

### 4.6.2 知识点精讲

网络地址转换（Network Address Translation，NAT）将数据报文中的 IP 地址替换成另一个 IP 地址，一般是私有地址转换为公有地址来实现访问公网的目的。这种方式只需要占用较少的公网 IP 地址，有助减少 IP 地址空间的枯竭。传统 NAT 包括基本 NAT 和 NAPT 两大类。

（1）基本 NAT。

NAT 设备配置多个公用的 IP 地址，当位于内部网络的主机向外部主机发起会话请求时，把内部地址转换成公用 IP 地址。如果内部网络中主机的数目不大于 NAT 所拥有的公开 IP 地址的数目，则可以保证每个内部地址都能映射到一个公开的 IP 地址，否则允许同时连接到外部网络的内部主机的数目会受到 NAT 公开 IP 地址数量的限制。也可以使用静态映射的方式把特定内部主机映射为一个特定的全球唯一的地址，保证了外部对内部主机的访问。基本 NAT 可以看成一对一的转换。

基本 NAT 又可以分为静态 NAT 和动态 NAT。静态 NAT 中，内、外网 IP 地址映射是固定的；动态 NAT 中，内、外网 IP 地址映射是动态的。

（2）NAPT。

网络地址端口转换（Network Address Port Translation，NAPT）是 NAT 的一种变形，它允许多个内部地址映射到同一个公有地址上，也可称之为**多对一地址转换**或地址复用。NAPT 同时映射 IP 地址和端口号，来自不同内部地址的数据报的源地址可以映射到同一个外部地址，但它们的端口号被转换为该地址的不同端口号，因而仍然能够共享同一个地址，即 NAPT 出口数据报中的内网 IP 地址被 NAT 的公网 IP 地址代替，出口分组的端口被一个高端端口代替。外网进来的数据报根据对应关系进行转换。NAPT 将**内部的所有地址映射到一个外部 IP 地址（也可以是少数外部 IP 地址），这样做的好处是隐藏了内部网络的 IP 配置、节省了资源**。

# 第5学时　传输层

第1天的第5学时主要学习传输层所涉及的重要知识点。传输层是OSI参考模型中的第四层，重要知识点围绕TCP和UDP协议展开。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在2～5分之间。传输层知识点的考察主要集中在上午考试中。本章考点知识结构图如图5-1所示。


图5-1　考点知识结构图

## 5.1　TCP

### 5.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：面向连接和无连接服务、TCP。

### 5.1.2　知识点精讲

1. 面向连接和无连接服务

网络服务分为面向连接和无连接服务两种方式。

（1）面向连接服务。

面向连接的服务是双方通信的前提，即先要建立一条通信线路，这个过程分为三步：建立连接、使用连接和释放连接。面向连接服务的工作方式与电话系统类似。其特点也是打电话必须经过建立拨号、通话和挂电话这3个过程。

数据传输过程前必须经过建立连接、使用连接和释放连接3个过程；建立之后，一个虚拟的电话联系信道就建立了。当数据正式传输时，数据分组不需要再携带目的地址。面向连接需要通信之前建立连接，但是这种方式比较复杂，相对无连接的效率不高。

（2）无连接服务。

无连接的服务就是通信双方不需要事先建立一条通信线路，而是把每个带有目的地址的数据包（数据分组）送到线路上，由系统选定路线进行传输。IP协议和UDP协议就是一种无连接协议；邮政系统可以看成一个无连接的系统。

无连接收发双方之间通信时，其下层资源只需在数据传输时动态地进行分配，不需预留。收发双方只有在传输数据时候才处于激活状态。

无连接服务通信比较迅速、使用灵活、连接开销小，但是这种方式可靠性低，不能防止报文丢失、重复或失序。

2. TCP

传输控制协议（Transmission Control Protocol，TCP）是一种可靠的、面向连接的字节流服务。源主机在传送数据前需要先和目标主机建立连接。然后在此连接上，被编号的数据段按序收发。同时要求对每个数据段进行确认，这样保证了可靠性。如果在指定的时间内没有收到目标主机对所发数据段的确认，源主机将再次发送该数据段。

（1）TCP 的三种机制。

TCP 建立在无连接的 IP 基础之上，因此使用了 3 种机制实现面向连接的服务。

1）使用序号对数据报进行标记。

这种方式便于 TCP 接收服务在向高层传递数据之前调整失序的数据包。

2）TCP 使用确认、校验和定时器系统提供可靠性。

当接收者按照顺序识别出数据报未能到达或发生错误时，接收者将通知发送者；当接收者在特定时间没有发送确认信息时，那么发送者就会认为发送的数据包并没有到达接收方，这时发送者就会考虑重传数据。

3）TCP 使用窗口机制调整数据流量。

窗口机制可以减少因接收方缓冲区满而造成丢失数据报文的可能性。

（2）TCP 报文首部格式。

TCP 报文首部格式如图 5-2 所示。

<table>
<tr><td colspan="5">源端口（16）</td><td colspan="4">目的端口（16）</td></tr>
<tr><td colspan="9">序列号（32）</td></tr>
<tr><td colspan="9">确认号（32）</td></tr>
<tr><td>报头长度（4）</td><td>保留(6)</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>YSN</td><td>FIN</td><td>窗口（16）</td></tr>
<tr><td colspan="5">校验和（16）</td><td colspan="4">紧急指针（16）</td></tr>
<tr><td colspan="6">选项（长度可变）</td><td colspan="3">填充</td></tr>
<tr><td colspan="9">TCP 报文的数据部分（可变）</td></tr>
</table>

图 5-2 TCP 报文首部格式

- 源端口（Source Port）和目的端口（Destination Port）

该字段长度均为 16 位。TCP 协议通过使用端口来标识源端和目标端的应用进程，端口号取值范围为 0～65535。

- 序列号（Sequence Number）

该字段长度为32位。因此序号范围为[0,$2^{32}$–1]。序号值是进行mod $2^{32}$运算的值，即序号值为最大值$2^{32}$–1后，下一个序号又回到0。

【例5-1】本段数据的序号字段为1024，该字段长100字节，则下一个字段的序号字段值为1125。这里序列号字段又称为**报文段序号**。

- 确认号（Acknowledgement Number）

该字段长度为32位。期望收到对方下一个报文段的第一个数据字段的序号。

【例5-2】接收方收到了序号为100、数据长度为300字节的报文，则接收方的确认号设置为301。

**注意**：如果确认号=N，则表示N-1之前（包含N-1）的所有数据都已正确收到。

- 报头长度（Header Length）

报头长度又称为数据偏移字段，长度为4位，单位32位。没有任何选项字段的TCP头部长度为20字节，最多可以有60字节的TCP头部。

- 保留字段（Reserved）

该字段长度为6位，通常设置为0。

- 标记（Flag）

该字段包含的字段有：紧急（URG）——紧急有效，需要尽快传送；确认（ACK）——建立连接后的报文回应，ACK设置为1；推送（PSH）——接收方应该尽快将这个报文段交给上层协议，不需等缓存满；复位（RST）——重新连接；同步（SYN）——发起连接；终止（FIN）——释放连接。

- 窗口大小（Windows Size）

该字段长度为16位。因此序号范围为[0,$2^{16}$–1]。该字段用来进行流量控制，单位为字节，是作为接收方让发送方设置其发送窗口的依据。这个值是本机期望一次接收的字节数。

- 校验和（Checksum）

该字段长度为16位，对整个TCP报文段（即TCP头部和TCP数据）进行校验和计算，并由目标端进行验证。

- 紧急指针（Urgent Pointer）

该字段长度为16位。它是一个偏移量，和序号字段中的值相加表示紧急数据最后一个字节的序号。

- 选项（Option）

该字段长度可变到40字节。可能包括窗口扩大因子、时间戳等选项。为保证报头长度是32位的倍数，因此还需要填充0。

（3）TCP建立连接。

TCP会话通过**三次握手**来建立连接。三次握手的目标是使数据段的发送和接收同步，同时也向其他主机表明其一次可接收的数据量（窗口大小）并建立逻辑连接。这三次握手的过程可以简述如下：

双方通信之前均处于 **CLOSED** 状态。

**1）第一次握手。**

源主机发送一个同步标志位 SYN=1 的 TCP 数据段。此段中同时标明初始序号（Initial Sequence Number，ISN）。ISN 是一个随时间变化的随机值，即 **SYN=1，SEQ=x**。源主机进入 **SYN-SENT** 状态。

**2）第二次握手。**

目标主机接收到 SYN 包后发回确认数据报文。该数据报文 ACK=1，同时确认序号字段表明目标主机期待收到源主机下一个数据段的序号，即 ACK=x+1（表明前一个数据段已收到且没有错误）。

此外，在此段中设置 SYN=1，并包含目标主机的段初始序号 y，**即 ACK=1，确认序号 ACK=x+1，SYN=1，自身序号 SEQ=y**。此时目标主机进入 **SYN-RCVD** 状态，源主机进入 **ESTABLISHED** 状态。

**3）第三次握手。**

源主机再回送一个确认数据段，同样带有递增的发送序号和确认序号（**ACK=1，确认序号 ACK=y+1，自身序号 SEQ**），TCP 会话的三次握手完成。接下来，源主机和目标主机可以互相收发数据。三次握手的过程如图 5-3 所示。

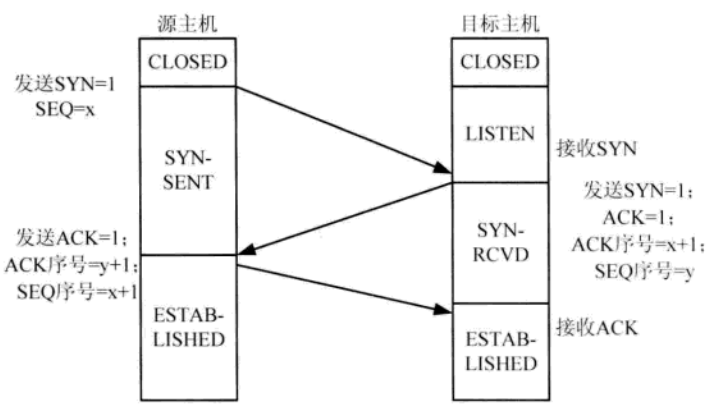



图 5-3 三次握手

（4）TCP 释放连接。

TCP 释放连接可以分为四步，具体过程如下：

双方通信之前均处于 **ESTABLISHED** 状态。

**1）第一步**：源主机发送一个释放报文（**FIN=1，自身序号 SEQ =x**），源主机进入 **FIN-WAIT** 状态。

**2）第二步**：目标主机接收报文后发出确认报文（**ACK=1，确认序号 ACK=x+1，自身序号 SEQ =y**），目标主机进入 **CLOSE-WAIT** 状态。此时，源主机停止发送数据，但是目标主机仍然可以发送数据，此时 TCP 连接为半关闭状态（**HALF-CLOSE**）。源主机接收到 ACK 报文后等待目标主机

发出 FIN 报文，这可能会持续一段时间。

**3）第三步：**目标主机确定没有数据，向源主机发送后，发出释放报文（**FIN=1，ACK=1，确认序号 ACK =x+1，自身序号 SEQ =z**）。目标主机进入 **LAST-ACK** 状态。

**注意：**这里由于处于半关闭状态（HALF-CLOSE），目标主机还会发送一些数据，其序号不一定为 y+1，因此可设为 z。而且，目标主机必须重复发送一次确认序号 ACK=x+1。

**4）第四步：**源主机接收到释放报文后，对此发送确认报文（**ACK=1，确认序号 ACK=z+1，自身序号 SEQ=x+1**），在等待一段时间确定确认报文到达后，源主机进入 **CLOSED** 状态。目标主机在接收到确认报文后，也进入 **CLOSED** 状态。释放连接的过程如图 5-4 所示。

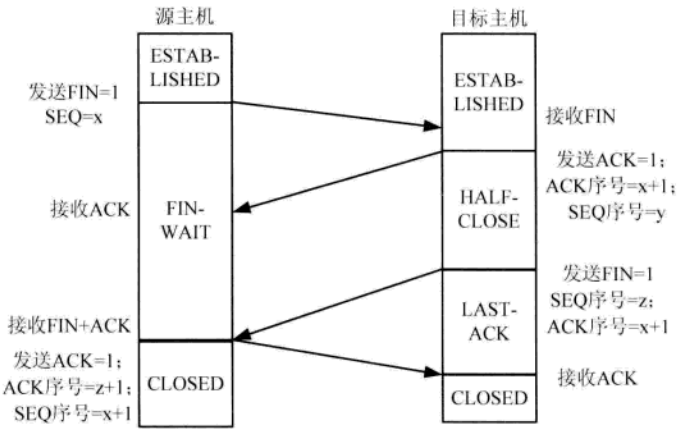



图 5-4　释放连接



## 5.2　UDP

### 5.2.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：UDP、端口。

### 5.2.2　知识点精讲

1. UDP

用户数据报协议（User Datagram Protocol，UDP）是一种不可靠的、无连接的数据报服务。源主机在传送数据前不需要和目标主机建立连接。数据附加了源端口号和目标端口号等 UDP 报头字段后直接发往目的主机。这时，每个数据段的可靠性依靠上层协议来保证。在传送数据较少且较小的情况下，UDP 比 TCP 更加高效。

如图 5-5 所示给出了 UDP 的头部结构。

| 源端口号（16 位） | 目的端口号（16 位） |
| --- | --- |
| 长度（16 位） | 校验和（16 位） |
| 数据 | |

图 5-5 UDP 协议格式

- 源端口号字段

该字段长度为 16 位。作用与 TCP 数据段中的端口号字段相同，用来标识源端的应用进程。在需要对方回信时用，不需要时可用全 0。

- 目标端口号字段

该字段长度为 16 位。作用与 TCP 数据段中的端口号字段相同，用来标识目标端的应用进程。在目标交付报文时必须用到。

- 长度字段

该字段长度为 16 位。标明 UDP 头部和 UDP 数据的总长度字节。

- 校验和字段

该字段长度为 16 位。用来对 UDP 头部和 UDP 数据进行校验，有错就丢弃。和 TCP 不同的是，对 UDP 来说，此字段是可选项，而 TCP 数据段中的校验和字段是必须有的。

2. 端口

协议端口号（Protocol Port Number，Port）是标识目标主机进程的方法。TCP/IP 使用 16 位的端口号来标识端口，所以端口的取值范围为[0,65535]。

端口可以分为系统端口、登记端口、客户端使用端口。

（1）系统端口。

该端口的取值范围为[0,1023]，常见端口如表 5-1 所示。

表 5-1 常见端口

| 端口号 | 名称 | 功能 |
| --- | --- | --- |
| 20 | FTP-DATA | FTP 数据传输 |
| 21 | FTP | FTP 控制 |
| 22 | SSH | SSH 登录 |
| 23 | TELNET | 远程登录 |
| 25 | SNMP | 简单邮件传输协议 |
| 53 | DNS | 域名解析 |
| 67 | DHCP | DHCP 服务器开启，用来监听和接收客户请求消息 |

续表

| 端口号 | 名称 | 功能 |
| --- | --- | --- |
| 68 | DHCP | 客户端开启，用于接收 DHCP 服务器的消息回复 |
| 69 | TFTP | 简单 FTP |
| 80 | HTTP | 超文本传输 |
| 110 | POP3 | 邮局协议 |
| 143 | IMAP | 交互式邮件存取协议 |
| 161 | SNMP | 简单网管协议 |
| 162 | SNMP（trap） | SNMP Trap 报文 |

（2）登记端口。

登记端口是为没有熟知端口号的应用程序使用的，端口范围为[1024,49151]。这些端口必须在 IANA 登记以避免重复。

（3）客户端使用端口。

这类端口仅在客户进程运行时候动态使用，使用完毕后，进程会释放端口。该端口范围为[49152,65535]。

## 第 6 学时　应用层

第 1 天的第 6 学时主要学习应用层所涉及的重要知识点。应用层是 OSI 参考模型中的最高层。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 2～6 分之间。应用层知识的考察主要集中在上午考试中，而下午考的则是这些知识点的应用配置，将在后面的章节中介绍。本章考点知识结构图如图 6-1 所示。



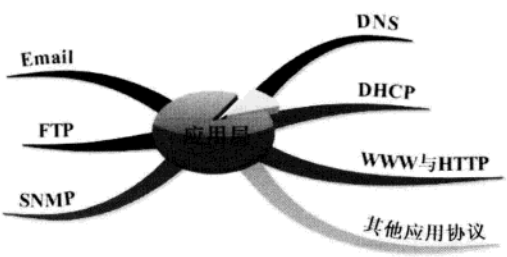



图 6-1　考点知识结构图

## 6.1 DNS

### 6.1.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：DNS 名字空间、域名服务器、资源记录、域名解析。

### 6.1.2 知识点精讲

域名系统（Domain Name System，DNS）是把主机域名解析为 IP 地址的系统，解决了 IP 地址难记的问题。该系统是由解析器和域名服务器组成的。**DNS 主要基于 UDP 协议，较少情况下使用 TCP 协议，端口号均为 53。**域名系统由三部分构成：DNS 名字空间、域名服务器、DNS 客户机。

1. DNS 名字空间

DNS 系统属于分层式命名系统，即采用的命名方法是层次树状结构。连接在 Internet 上的主机或路由器都有一个唯一的层次结构名，即域名（Domain Name）。域名可以由若干个部分组成，每个部分代表不同级别的域名并使用“.”号分开。完整的结构为：**主机.…三级域名.二级域名.顶级域名.**

**注意：**域名的每个部分不超过 63 个字符，整个域名不超过 255 个字符。顶级域名后的“.”号表示根域，通常可以不用写。

Internet 上域名空间的结构如图 6-2 所示。

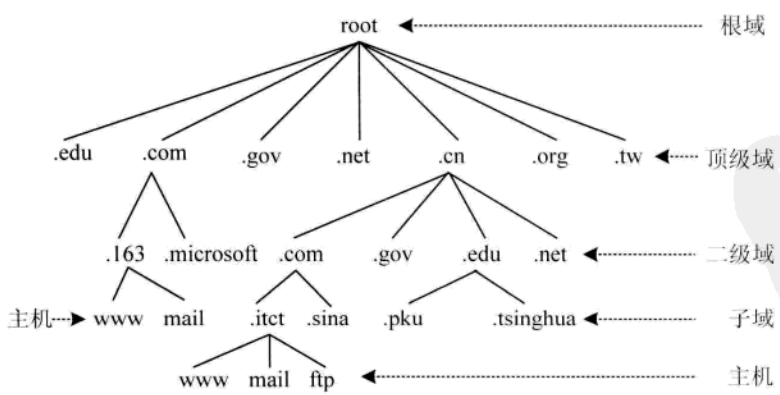



图 6-2 Internet 上域名空间的结构

（1）根域：根域处于 Internet 上域名空间结构树的最高端，是树的根，提供根域名服务。根

域用“.”来表示。

（2）顶级域名（Top Level Domain，TLD）：顶级域名在根域名之下，分为三大类：国家顶级域名、通用顶级域名和国际顶级域名。常用域名如表6-1所示。

表6-1 常用域名

| 域名名称 | 作用 |
| --- | --- |
| .com | 商业机构 |
| .edu | 教育机构 |
| .gov | 政府部门 |
| .int | 国际组织 |
| .mil | 美国军事部门 |
| .net | 网络组织（如因特网服务商和维修商），现在任何人都可以注册 |
| .org | 非盈利组织 |
| .biz | 商业 |
| .info | 网络信息服务组织 |
| .pro | 会计、律师和医生 |
| .name | 个人 |
| .museum | 博物馆 |
| .coop | 商业合作团体 |
| .aero | 航空工业 |
| 国家代码 | 国家（如cn代表中国） |

（3）主机：属于最低层域名，处于域名树的叶子端，代表各类主机提供的服务。

2. 域名服务器

域名服务器运行模式为客户机/服务器模式（C/S模式）。

（1）按域名空间层次可以分为根域名服务器、顶级域名服务器、权限域名服务器、本地域名服务器。具体功能如表6-2所示。

表6-2 按域名空间层次划分的服务器

| 名称 | 定义 | 作用 |
| --- | --- | --- |
| 根域名服务器 | 最高层次域名服务器，该服务器保存了全球所有顶级域名服务器的IP地址和域名。全球有100多个 | 本地域名无法解析域名时，直接向根域名服务器请求 |
| 顶级域名服务器 | 管理本级域名（如.cn）上注册的所有二级域名 | 可以解析本级域名下的二级域名的IP地址；提交下一步所寻域名服务器地址 |

续表

| 名称 | 定义 | 作用 |
| --- | --- | --- |
| 权限域名服务器 | 一个域可以分为多个区，每一个区都设置服务器，即权限服务器 | 该区域管理主机的域名和 IP 地址的映射、解析 |
| 本地域名服务器 | 主机发出的 DNS 查询报文最初送到的服务器 | 查询本地域名和 IP 地址的映射、解析。向上级域名服务器进行域名查询 |

（2）按域名服务器的作用可以分为主域名服务器、辅域名服务器、缓存域名服务器、转发域名服务器。具体功能如表 6-3 所示。

**表 6-3 按作用划分的域名服务器**

| 名称 | 定义 | 作用 |
| --- | --- | --- |
| 主域名服务器 | 维护本区所有域名信息，信息存于磁盘文件和数据库中 | 提供本区域名解析，区内域名信息的权威。**具有域名数据库。一个域有且只有一个主域名服务器** |
| 辅域名服务器 | 主域名服务器的备份服务器提供域名解析服务，信息存于磁盘文件和数据库中 | 主域名服务器备份，可进行域名解析的负载均衡。**具有域名数据库** |
| 缓存域名服务器 | 向其他域名服务器进行域名查询，将查询结果保存在缓存中的域名服务器 | 改善网络中 DNS 服务器的性能，减少反复查询相同域名的时间，提高解析速度，节约出口带宽。**获取解析结果耗时最短，没有域名数据库** |
| 转发域名服务器 | 负责**非本地和缓存中**无法查到的域名。接收域名查询请求，首先查询自身缓存，如果找不到对应的，则转发到指定的域名服务器查询 | 负责域名转发，由于转发域名服务器同样可以有缓存，因此可以减少流量和查询次数。**具有域名数据库** |

3. 资源记录

DNS 数据库包括 DNS 服务器所使用的一个或多个区域文件，每个区域都拥有一组结构化的资源记录。资源记录的格式为

[Domain] [TTL] [class] record-type record-specific-data

- Domain：资源记录引用的域对象名。可以是单台主机，也可以是整个域。Domain 字串用“.”分隔，只要没有用一个“.”标示结束，就与当前域有关系。
- TTL：生存时间记录字段。以秒为单位定义该资源记录中的信息存放在高速缓存中的时间长度。通常该字段为空，表示生存周期在授权资源记录开始中指定。
- class：指定网络的地址类。对于 TCP/IP 网络使用 IN。
- record-type：记录类型。标识这是哪一类资源记录，常见的记录类型如表 6-4 所示。
- record-specific-data：指定与这个资源记录有关的数据。这个值是必要的。数据字段的格式取决于类型字段的内容。

4. 域名解析

域名解析就是将域名解析为 IP 地址。域名解析的方法分为：递归查询和迭代查询。

表 6-4　常见资源记录

| 资源记录名称 | 作用 | 举例（Windows 系统下的 DNS 数据库） |
|---|---|---|
| A | 将 DNS 域名映射到 IPv4 的 32 位地址中 | host1.itct.com.cn. IN　A　202.0.0.10 |
| AAAA | 将 DNS 域名映射到 IPv4 的 128 位地址中 | ipv6_ host2.itct.com.cn. IN　AAAA 2002:0:1:2:3:4:567:89ab |
| CNAME | 规范名资源记录，允许多个名称对应同一主机 | aliasname.itct.com.cn. CNAME truename.itct.com.cn |
| MX | 邮件交换器资源记录，其后的数字首选参数值（0～65535）指明与其他邮件交换服务器有关的邮件交换服务器的优先级。较低的数值被授予较高的优先级 | example.itct.com.cn. MX 10 mailserver1.itct.com.cn |
| NS | 域名服务器记录，指明该域名由哪台服务器来解析 | example.itct.com.cn. IN NS nameserver1.itct.com.cn. |
| PTR | 指针，用于将一个 IP 地址映射为一个主机名 | 202.0.0.10.in-addr.arpa. PTR host.itct.com.cn |

（1）递归查询。

递归查询为最主要的域名查询方式。主机有域名解析的需求时，首先查询本地域名服务器，如果成功，则由本地域名服务器反馈结果；如果失败，则查询上一级的域名服务器，然后由上一级域名服务器完成查询。如图 6-3 所示是一个递归查询，表示主机 123.abc.com 要查询域名为 www.itct.com.cn 的 IP 地址。

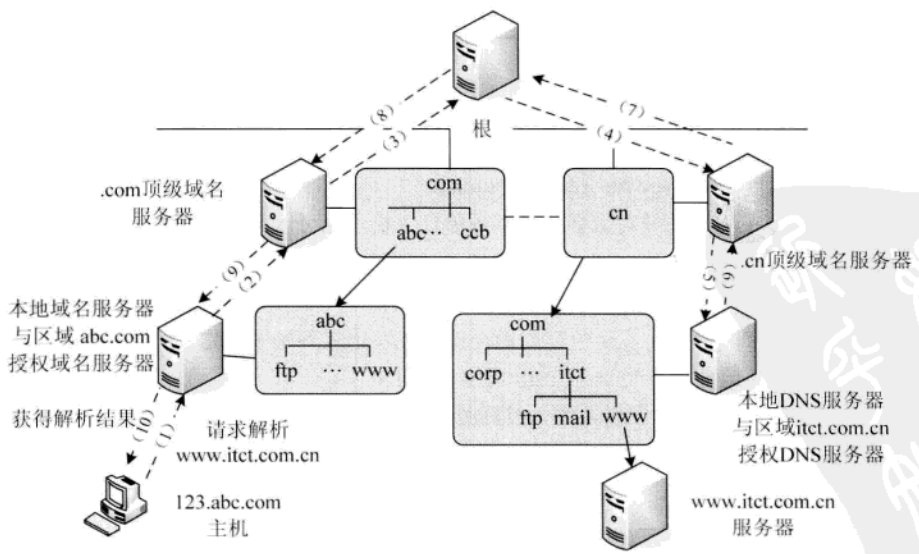



图 6-3　本地与区域域名服务器的递归查询

（2）迭代查询。

当主机有域名解析的需求时，首先查询本地域名服务器，如果成功，则由本地域名服务器反馈结果；如果失败，本地域名服务器则直接向根域名服务器发起查询请求，由其给出一个顶级域名服务器的 IP 地址 A.A.A.A；然后，本地域名服务器则直接向 A.A.A.A 顶级域名服务器发起查询请求，由其给出一个本地域名服务器（或者权限服务器）地址 B.B.B.B；如此迭代下去，直到得到结果 IP。如图 6-4 所示是一个迭代查询，表示主机 123.abc.com 要查询域名为 www.itct.com.cn 的 IP 地址。

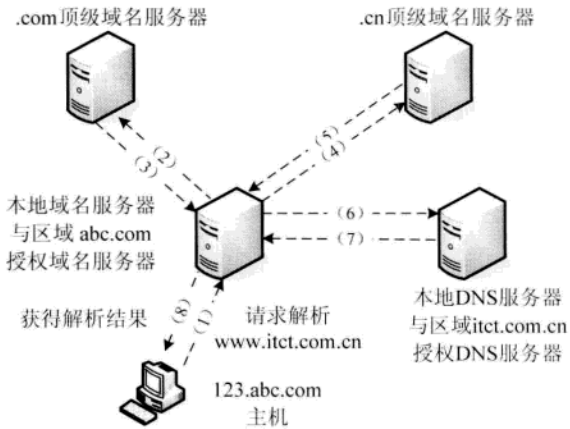



图 6-4 本地与区域域名服务器的迭代查询

另外，稳定的 DNS 系统是保证网络正常运行的前提。网络管理员可以通过使用防火墙控制对 DNS 的访问、避免 DNS 的主机信息（HINFO）记录被窃取、限制区域传输等手段来加强 DNS 的安全。

## 6.2 DHCP

### 6.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：DHCP 基本知识、DHCP 工作过程、DHCP 管理。

### 6.2.2 知识点精讲

BOOTP 是最早的主机配置协议。动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）则是在其基础之上进行了改良的协议，是一种用于简化主机 IP 配置管理的 IP 管理标准。通过采用 DHCP 协议，DHCP 服务器为 DHCP 客户端进行动态 IP 地址分配。同时 DHCP 客户端在配置时不必指明 DHCP 服务器的 IP 地址就能获得 DHCP 服务。当同一子网内有多台 DHCP 服务器

时，在默认情况下，客户机采用最先到达的 DHCP 服务器分配的 IP 地址。

1. DHCP 基本知识

当需要跨越多个网段提供 DHCP 服务时必须使用 **DHCP 中继代理**，就是在 DHCP 客户和服务器之间转发 DHCP 消息的主机或路由器。

DHCP 服务端使用 **UDP 的 67 号端口**来监听和接收客户请求消息，保留 **UDP 的 68 号端口**用于接收来自 DHCP 服务器的消息回复。

在 Windows 系统中，在 DHCP 客户端无法找到对应的服务器时、获取合法 IP 地址失败前提下，获取的 IP 地址值为 **169.254.X.X**。

**注意**：Windows 2000 以前的系统在获取合法 IP 地址失败前提下，获取的 IP 地址值为 **0.0.0.0**。

2. DHCP 工作过程

DHCP 的工作过程如图 6-5 所示。

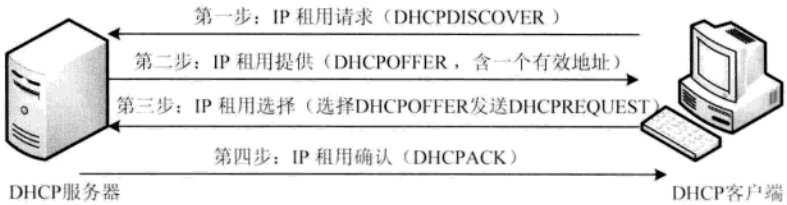



图 6-5　DHCP 工作过程

（1）DHCP 客户端发送 IP 租用请求。

DHCP 客户机启动后发出一个 DHCPDISCOVER 消息，其封包的源地址为 0.0.0.0，目标地址为 255.255.255.255。

（2）DHCP 服务器提供 IP 租用服务。

当 DHCP 服务器收到 DHCPDISCOVER 数据包后，通过 UDP 的 68 号端口给客户机回应一个 DHCPOFFER 信息，其中包含一个还没有被分配的有效 IP 地址。

（3）DHCP 客户端 IP 租用选择。

客户机可能从不止一台 DHCP 服务器收到 DHCPOFFER 信息。客户机选择最先到达的 DHCPOFFER 并发送 DHCPREQUEST 消息包。

（4）DHCP 客户端 IP 租用确认。

DHCP 服务器向客户机发送一个确认（DHCPACK）信息，信息中包括 IP 地址、子网掩码、默认网关、DNS 服务器地址以及 IP 地址的租约（默认为 8 天）。

（5）DHCP 客户端重新登录。

获取 IP 地址后的 DHCP 客户端在每次重新联网，不再发送 DHCPDISCOVER，直接发送包含前次分配地址信息的 DHCPREQUEST 请求。DHCP 服务器收到请求后，如果该地址可用，则返回 DHCPACK 确认；否则发送 DHCPNACK 信息否认。收到 DHCPNACK 的客户端需要从第一步开始

重新申请 IP 地址。

（6）更新租约。

DHCP 服务器向 DHCP 客户机出租的 IP 地址一般都有一个租借期限，期满后，DHCP 服务器便会收回出租的 IP 地址。如果 DHCP 客户机要延长其 IP 租约，则必须更新其 IP 租约。DHCP 客户机启动时和 IP 租约期限过一半时，DHCP 客户机都会自动向 DHCP 服务器发送更新其 IP 租约的信息。

3. DHCP 管理

由于用户不同，需要租约的 IP 地址时间就会不同。因此，分配的 IP 地址需要区别对待。如频繁变化的、出差的、使用远程访问的笔记本、移动设备就只需要提供较短的租约时间。解决办法是：把所有使用 DHCP 协议获取 IP 地址的主机划分为不同的类别进行管理。

## 6.3 WWW 与 HTTP

### 6.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：WWW、HTTP。

### 6.3.2 知识点精讲

1. WWW

万维网（World Wide Web，WWW），是一个规模巨大、可以互联的资料空间。该资料空间的资源依靠 URL 进行定位，通过 HTTP 协议传送给使用者，又由 HTML 来进行文档的展现。由定义可以知道 WWW 的核心由三个主要标准构成：URL、HTTP、HTML。

（1）URL。

统一资源标识符（Uniform Resource Locator，URL）是一个全世界通用的、负责给万维网上资源定位的系统。URL 由四个部分组成：

<协议>://<主机>:<端口>/<路径>

- <协议>：表示使用什么协议来获取文档，之后的“://”不能省略。常用协议有 HTTP、HTTPS、FTP。
- <主机>：表示资源主机的域名。
- <端口>：表示主机服务端口，有时可以省略。
- <路径>：表示最终资源在主机中的具体位置，有时可以省略。

（2）HTTP。

超文本传送协议（HyperText Transport Protocol，HTTP）负责规定浏览器和服务器怎样进行互相交流。

（3）HTML。

超文本标记语言（Hypertext Markup Language，HTML）是用于描述网页文档的一种标记语言。

WWW 采用客户机/服务器的工作模式，工作流程具体如下：

（1）用户使用浏览器或其他程序建立客户机与服务器连接并发送浏览请求。

（2）Web 服务器接收到请求后返回信息到客户机。

（3）通信完成后关闭连接。

2. HTTP

HTTP 是互联网上应用最为广泛的一种网络协议，该协议由万维网协会（World Wide Web Consortium，W3C）和 Internet 工作小组（Internet Engineering Task Force，IETF）共同提出。该协议使用 TCP 的 80 号端口提供服务。

（1）HTTP 工作过程。

HTTP 是工作在客户/服务器（C/S）模式下、基于 TCP 的协议。客户端是终端用户，服务器端是网站服务器。

客户端通过使用 Web 浏览器、网络爬虫或其他的工具，发起一个到服务器上指定端口（默认端口为 80）的 HTTP 请求。一旦收到请求，服务器向客户端发回响应消息，消息的内容可能是请求的文件、错误消息或其他一些信息。

如图 6-6 所示给出了客户端单击 http：//www.itct.com.cn/net/index.html 所发生的事件。

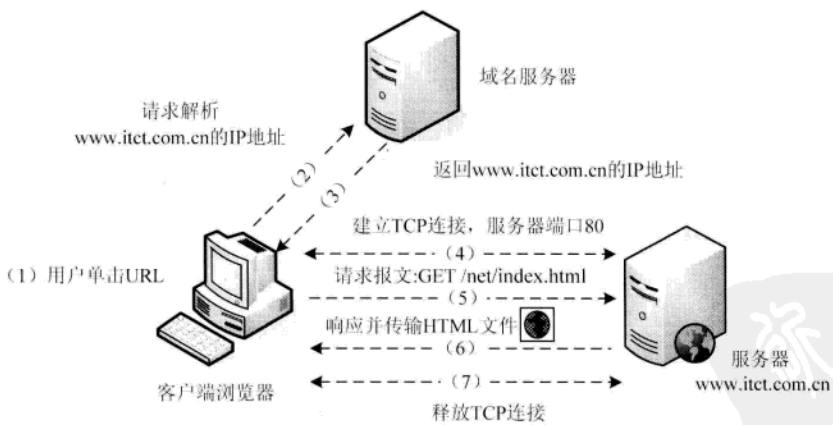



图 6-6　单击 URL 的过程

HTTP 使用 TCP 而不是 UDP 的原因在于打开一个网页必须传送很多数据，而 TCP 协议提供传输控制，可以按顺序组织数据，并且期间可以对错序数据进行纠正。

（2）HTTP 报文。

HTTP 报文分为请求报文和响应报文。

- 请求报文：客户端向服务器发送的报文。
- 响应报文：服务器应答客户端的报文。

常见的请求报文方法如表 6-5 所示。

表 6-5 常见 HTTP 请求报文方法

| 方法 | 意义 |
| --- | --- |
| GET | 请求读取 URL 标识的信息 |
| HEAD | 请求读取 URL 标识的信息的首部 |
| POST | 把消息（如注释）加载到指定网页上，没有 Read 方法 |
| PUT | 指明 URL 创建或修改资源，俗称的上传资源 |
| DELETE | 删除 URL 所指定的资源 |
| OPTION | 请求一些参数信息 |
| TRACE | 进行环回测试 |
| CONNECT | 用于代理服务器 |

## 6.4 Email

### 6.4.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：常见的电子邮件协议、邮件安全、邮件客户端。

### 6.4.2 知识点精讲



电子邮件（electronic mail，E-mail）又称电子信箱，昵称“伊妹儿”，是一种用网络提供信息交换的通信方式。通过网络，电子邮件系统可以用非常低廉的价格、以非常快速的方式与世界上任何一个角落的网络用户联系，邮件形式可以是文字、图象、声音等。

电邮地址的格式是：用户名@域名。

其中，@是英文 at 的意思。选择@的理由比较有意思，电子邮件的发明者汤姆林森给出得解释是：“它在键盘上那么显眼的位置，我一眼就看中了它”。

电子邮件地址是表示在某部主机上的一个使用者账号。

1. 常见的电子邮件协议

常见的电子邮件协议有：简单邮件传输协议、邮局协议和 Internet 邮件访问协议。

（1）简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）。

SMTP 主要负责底层的邮件系统如何将邮件从一台机器发送至另外一台机器。该协议工作在 TCP 协议的 25 号端口。

（2）邮局协议（Post Office Protocol，POP）。

目前的版本为 POP3，POP3 是把邮件从邮件服务器中传输到本地计算机的协议。该协议工作在 TCP 协议的 110 号端口。

（3）Internet 邮件访问协议（Internet Message Access Protocol，IMAP）。

目前的版本为 IMAP4，是 POP3 的一种替代协议，提供了邮件检索和邮件处理的新功能。用户可以完全不必下载邮件正文就可以看到邮件的标题和摘要，使用邮件客户端软件就可以对服务器上的邮件和文件夹目录等进行操作。IMAP 协议增强了电子邮件的灵活性，同时也减少了垃圾邮件对本地系统的直接危害，同时相对节省了用户查看电子邮件的时间。除此之外，IMAP 协议可以记忆用户在脱机状态下对邮件的操作（如移动邮件、删除邮件等），在下一次打开网络连接时会自动执行。该协议工作在 TCP 协议的 143 号端口。

2. 邮件安全

电子邮件在传输中使用的是 SMTP 协议，它不提供加密服务，攻击者可以在邮件传输中截获数据。其中的文本格式和非文本格式的二进制数据（如.exe 文件）都可轻松地还原。同时还存在发送的邮件很可能是冒充的邮件、邮件误发送等问题。因此安全电子邮件的需求越来越强烈，安全电子邮件可以解决邮件的加密传输问题、验证发送者的身份验证问题、错发用户的收件无效问题。

PGP（Pretty Good Privacy）是一款邮件加密软件，可以用它对邮件保密以防止非授权者阅读，它还能为邮件加上数字签名，从而使收信人可以确认邮件的发送者，并能确信邮件没有被篡改。PGP 采用了**RSA 和传统加密的杂合算法、数字签名的邮件文摘算法**和加密前压缩等手段，功能强大、加解密快且开源。

3. 邮件客户端

常见的电子邮件客户端有 Foxmail、Outlook 等。在阅读邮件时，使用网页、程序、会话方式都有可能运行恶意代码。为了防止电子邮件中的恶意代码，应该用纯文本方式阅读电子邮件。



## 6.5 FTP

### 6.5.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：FTP、TFTP。

### 6.5.2 知识点精讲

1. FTP

文件传输协议（File Transfer Protocol，FTP）简称为“文传协议”，用于在 Internet 上控制文件的双向传输。FTP 客户上传文件时，通过服务器**20 号端口**建立的连接是建立在 TCP 之上的**数据连**

**接**，通过服务器 **21 号端口**建立的连接是建立在 TCP 之上的**控制连接**。

FTP 协议有两种工作方式：主动式（PORT）和被动式（PASV）。**主动与被动是相对于服务器是否首先发起数据连接而言的。**

（1）主动式（PORT）。

主动式（PORT）的连接过程：

1）当需要传输数据时，客户端从一个任意的非系统端口 N（N≥1024）连接到 FTP 服务器的 21 号端口（控制连接端口）。

2）客户端开始监听端口 N+1 并发送 FTP 命令“Port N+1”到 FTP 服务器。

3）服务器会从 20 号数据端口向客户端指定的 N+1 号端口发送连接请求并建立一条数据链路来传送数据。

具体流程如图 6-7 所示。

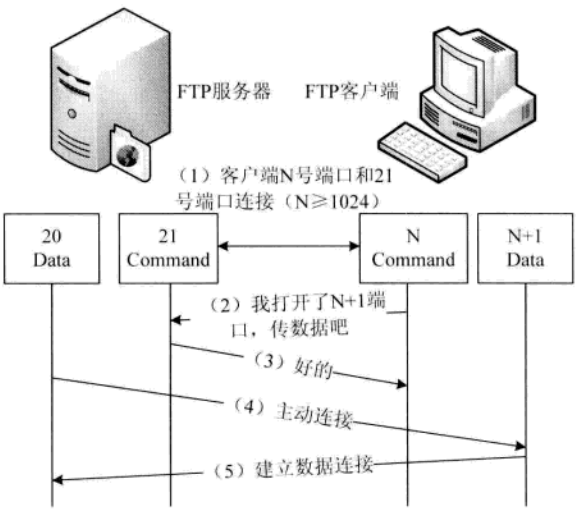



图 6-7 主动式 FTP 模式

（2）被动式（PASV）。

在被动方式 FTP 中，命令连接和数据连接都由客户端发起，这样就可以解决从服务器到客户端的数据端口的入方向连接被客户端所在网络防火墙过滤掉的问题。

被动式（PASV）的连接过程：

1）当需要传输数据时，客户端从一个任意的非系统端口 N（N≥1024）连接到 FTP 服务器的 21 号端口（控制连接端口）。

2）客户端发送 PASV 命令，且服务器响应。

3）服务器开启一个任意的非系统端口 Y（Y≥1024）。

4）客户端从端口 N+1 连接到 FTP 服务器的 Y 号端口。

具体流程如图 6-8 所示。

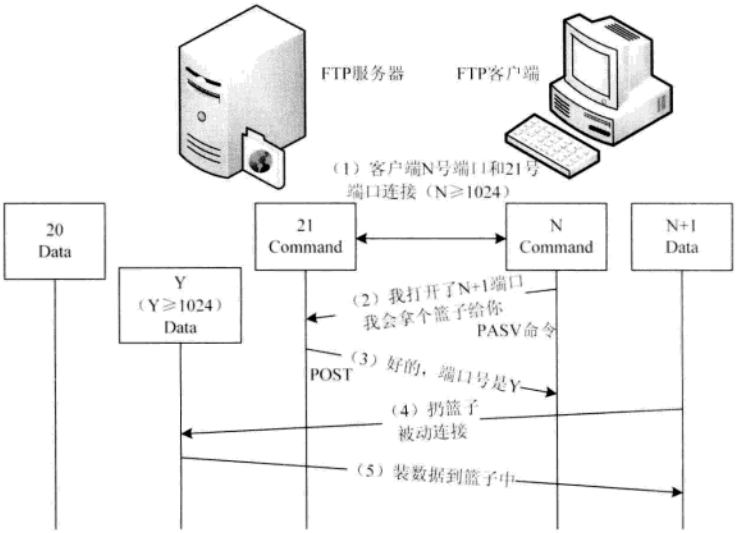



图 6-8　被动式 FTP 模式

2. TFTP

简单文件传送协议（Trivial File Transfer Protocol，TFTP）的功能与 FTP 类似，是一个小而简单的文件传输协议。该协议基于 UDP 协议。一般用于路由器、交换机、防火墙配置文件、IOS 的备份和替换。



## 6.6　SNMP

### 6.6.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：OSI 定义的网络管理、CMIS/CMIP、网络管理系统组成、SNMP、管理信息库、管理信息结构。

### 6.6.2　知识点精讲

网络管理是对网络进行有效而安全的监控、检查。网络管理的任务就是：检测和控制。

1. OSI 定义的网络管理

OSI 定义的网络管理功能有以下 5 大类。

（1）性能管理（Performance Management）。

在最少的网络资源和最小时延的前提下，网络能提供可靠、连续的通信能力。性能管理的功能

有性能检测、性能分析、性能管理、性能控制。

（2）配置管理（Configuration Management）。

用来定义、识别、初始化、监控网络中的被管对象，改变被管对象的操作特性，报告被管对象状态的变化。配置管理的功能有配置信息收集（信息包含设备地理位置、命名、记录，维护设备的参数表、及时更新，维护网络拓扑）和利用软件设置参数并配置硬件设备（设备初始化、启动、关闭、自动备份硬件配置文件）。

（3）故障管理（Fault Management）。

对网络中被管对象故障的检测、定位和排除。故障管理的功能有故障检测、故障告警、故障分析与定位、故障恢复与排除、故障预防。

（4）安全管理（Security Management）。

保证网络不被非法使用。安全管理的功能有管理员身份认证、管理信息加密与完整性、管理用户访问控制、风险分析、安全告警、系统日志记录与分析、漏洞检测。

（5）计费管理（Accounting Management）。

记录用户使用网络资源的情况并核收费用，同时也统计网络的利用率。计费管理的功能有账单记录、账单验证、计费策略管理。

2. CMIS/CMIP

公共管理信息服务/协议（Common Management Information Service/Protocol，CMIS/CMIP）是OSI 提供的网络管理协议簇。CMIS 定义了每个网络组成部件提供的网络管理服务，CMIP 则是实现 CIMS 服务的协议。

3. 网络管理系统组成

网络管理系统由以下 4 个要素组成：

（1）管理站（Network Manager）。

管理站是位于网络系统主干或者靠近主干的工作站，是网络管理系统的核心，负责管理代理和管理信息库，定期查询代理信息，确定独立的网络设备和网络状态是否正常。

（2）代理（Agent）。

代理又称为管理代理，位于被管理设备内部。负责收集被管理设备的各种信息和响应管理站的命令或请求，并将其传输到 MIB 数据库中。代理所在地设备可以是网管交换机、服务器、网桥、路由器、网关及任何合法节点的计算机。

（3）管理信息库（Management Information Base，MIB）。

相当于一个虚拟数据库，提供有关被管理网络各类系统和设备的信息，属于分布式数据库。

（4）网络管理协议。

用于管理站和代理之间传递、交互信息。常见的网管协议有 SNMP 和 CMIS/CMIP。

网管站通过 SNMP 向被管设备的网络管理代理发出各种请求报文，代理则接收这些请求后完成相应的操作，可以把自身信息主动通知给网管站。

网络管理各要素的组成结构如图 6-9 所示。

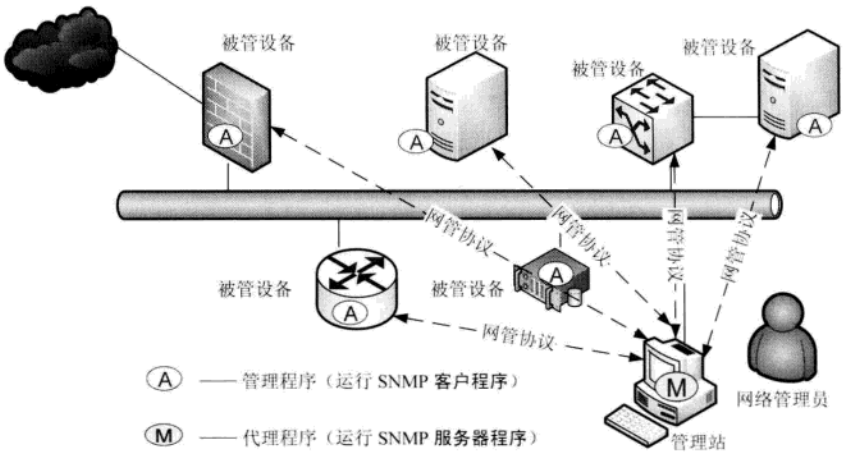



图 6-9　网络管理各要素的组成结构

在 SNMPv3 中把管理站和代理统一叫做 SNMP 实体。SNMP 实体由一个 SNMP 引擎和一个或多个 SNMP 应用程序组成。

4. SNMP

简单网络管理协议（Simple Network Management Protocol，SNMP）是在应用层上进行网络设备间通信的管理协议，可以进行网络状态监视、网络参数设定、网络流量统计与分析、发现网络故障等。SNMP 基于 UDP 协议，**是一组标准，由 SNMP 协议、管理信息库（MIB）和管理信息结构（SMI）组成。**

（1）SNMP PDU。

SNMP 规定了 5 个重要的协议数据单元 PDU，也称为 SNMP 报文。SNMP 报文可以分为从管理站到代理的 SNMP 报文和从代理到管理站的 SNMP 报文（SNMP 报文建议不超过 484 个字节）。常见的 SNMP 报文如表 6-6 所示。

表 6-6　常见的 SNMP 报文

| 从管理站到代理的 SNMP 报文 | | 从代理到管理站的 SNMP 报文 |
|---|---|---|
| 从一个数据项取数据 | 把值存储到一个数据项 | |
| **Get-Request**<br>（从代理进程处提取一个或多个数据项） | **Set-Request**<br>（设置代理进程的一个或多个数据项） | **Get-Response**<br>（这个操作是代理进程作为对 **Get-Request**、**Get-Next-Request**、**Set-Request** 的响应） |
| **Get-Next-Request**<br>（从代理进程处提取一个或多个数据项的下一个数据项） | | **Trap**<br>（代理进程主动发出的报文，通知管理进程有某些事件发生） |

SNMP 协议实体发送请求和应答报文的默认端口号是 161，SNMP 代理发送陷阱报文（Trap）

的默认端口号是 162。

目前 SNMP 有 SNMPv1、SNMPv2、SNMPv3 三个版本。各版本的不同如表 6-7 所示。

表 6-7 各版本 SNMP 的不同

| 版本 | 特点 |
| --- | --- |
| SNMPv1 | 易于实现、**使用团体名认证**（属于同一团体的管理站和被管理站才能互相作用） |
| SNMPv2 | 可以实现**分布和集中**两种方式的管理；增加管理站之间的信息交换；改进管理信息机构（可以一次性取大量数据）；增加多协议支持；引入了信息模块的概念（**模块有 MIB 模块、MIB 的依从性声明模块、代理能力说明模块**） |
| SNMPv3 | 模块化设计，提供安全的支持，**基于用户的安全模型** |

（2）SNMPv2 接收报文和发送报文。

在 SNMPv2 中，一个实体接收到一个报文一般经过以下四个步骤：

1）对报文进行语法检查，丢弃出错的报文。

2）把 SNMP 报文部分、源端口号和目标端口号交给认证服务。如果认证失败，发送一个陷阱，丢弃报文。

3）如果认证通过，则把 SNMP 报文转换成 ASN.1 的形式。

4）协议实体对 SNMP 报文做语法检查。如果通过检查，则根据团体名和适当的访问策略作相应的处理。

在 SNMPv2 中，一个实体发送一个报文一般经过以下四个步骤：

1）根据要实现的协议操作构造 SNMP 报文。

2）把 SNMP 报文、源端口地址、和目标端口地址及要加入的团体名传送给认证服务，认证服务产生认证码或对数据进行加密，返回结果。

3）加入版本号和团体名构造报文。

4）进行 BER 编码，产生 0/1 比特串并发送出去。

（3）SNMPv3 安全分类。

在 SNMPv3 中共有两类安全威胁是一定要提供防护的：主要安全威胁和次要安全威胁。

1）主要安全威胁。

主要安全威胁有两种：修改信息和假冒。修改信息是指擅自修改 SNMP 报文，篡改管理操作，伪造管理对象；假冒就是冒充用户标识。

2）次要安全威胁。

次要安全威胁有两种：修改报文流和消息泄露。修改报文流可能出现乱序、延长、重放的威胁；消息泄露则可能造成 SNMP 之间的信息被窃听。

另外有两种服务不被保护或者无法保护：拒绝服务和通信分析。

（4）SNMP 轮询监控。

SNMP 采用轮询监控方式，管理者按一定时间间隔向代理获取管理信息，并根据管理信息判断

是否有异常事件发生。当管理对象发生紧急情况时，可以使用名为 Trap 信息的报文主动报告。轮询监控的主要优点是对代理资源要求不高，缺点是管理通信开销大。SNMP 的基本功能包括网络性能监控、网络差错检测和网络配置。

假定在 SNMP 网络管理中，轮询周期为 N，单个设备轮询时间为 T，网络没有拥塞，则

$$\text{支持的设备数 } X=\frac{\text{轮询周期N}}{\text{单个设备轮询时间T}} \tag{6-1}$$

例如，某局域网采用 SNMP 进行网络管理，所有被管设备在每 15 分钟内轮询一次，网络没有明显拥塞，单个轮询时间为 0.4s，则该管理站最多可支持 X=N/T=(15×60)÷0.4=2250 个设备。

5. 管理信息库（Management Information Base，MIB）

MIB 指定主机和路由器等被管设备需要保存的数据项和可以对这些数据项进行的操作。换句话说，就是只有在 MIB 中的对象才能被 SNMP 管理。目前使用的是 MIB-2，常见的 MIB-2 信息如表 6-8 所示。

表 6-8 常见的 MIB-2 对象组信息

| 类别（标号） | 描述 |
| --- | --- |
| system（1） | 主机、路由器操作系统 |
| interface（2） | 网络接口信息 |
| Address translation（3） | 地址转换（已经废弃多年） |
| ip（4） | IP 信息 |
| icmp（5） | ICMP 信息 |
| tcp（6） | TCP 信息 |
| udp（7） | UDP 信息 |
| egp（8） | EGP 信息 |
| cmot（9） | CMOT 信息（废弃多年） |

每个 MIB-2 信息下面包含若干个 MIB 变量，如 system 组下的 sysuptime 表示距上次启动的时间，ip 组下的 ipDefaultTTL 表示 IP 在生存时间字段的值。SNMP MIB 中被管对象的访问方式有**只读、读写、只写和不可访问**四种，不包括可执行。

6. 管理信息结构（Structure of Management Information，SMI）

SMI 定义了命名管理对象和定义对象类型（包括范围和长度）的通用规则，以及把对象和对象的值进行编码的规则。SMI 的功能：命名被管理对象、存储被管对象的数据类型、编码管理数据。

SMI 规定，所有被管对象必须在对象命名树（Object Naming Tree）上，如图 6-10 所示为对象命名树的一部分。图中节点 IP 下名为 ipInReceives 的 MIB 变量名字全称为 iso.org.dod.internet.mgmt.mib. ip.ipInReceives，对应数值为 1.3.6.1.2.1.4.3。

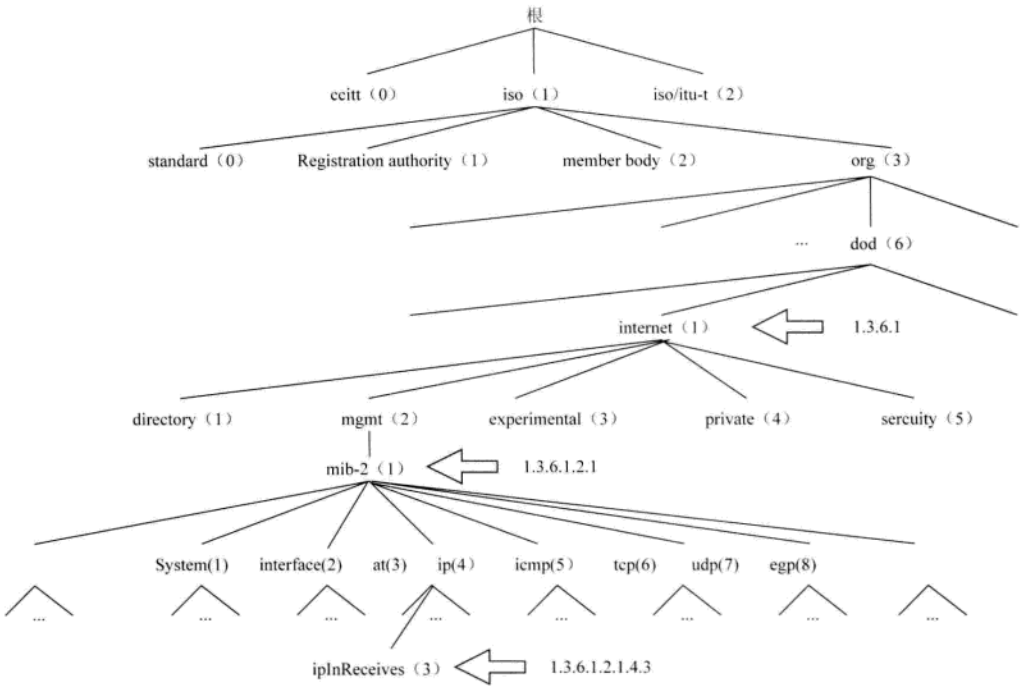



图 6-10 对象命名树

## 6.7 其他应用协议

### 6.7.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：Telnet、代理服务器、SSH、VOIP。

### 6.7.2 知识点精讲

1. Telnet

TCP/IP 终端仿真协议（TCP/IP Terminal Emulation Protocol，Telnet）是一种基于 TCP 的虚拟终端通讯协议，端口号为 23。Telnet 采用客户端/服务器的工作方式，采用网络虚拟终端（Net Virtual Terminal，NVT）实现客户端和服务器的数据传输，可以实现远程登录、远程管理交换机和路由器。

2. 代理服务器

代理服务器（Proxy Server）处于客户端和需要访问网络之间，客户向网络发送信息和接收信息均通过代理服务器转发而实现。代理服务器的优点有：共享 IP 地址、缓存功能提高访问速度、信息转发、过滤和禁止某些通信，提升上网效率、隐藏内部网络细节以提高安全性、监控用户行为、

避免来自 Internet 上病毒的入侵、提高访问某些网站的速度、突破对某些网站的访问限制。

3. SSH

传统的网络服务程序（如 FTP、POP 和 Telnet）其本质上都是不安全的，因为它们在网络上用明文传送数据、用户账号和用户口令，很容易受到中间人（man-in-the-middle）攻击方式的攻击，即存在另一个人或一台机器冒充真正的服务器接收用户传给服务器的数据，然后再冒充用户把数据传给真正的服务器。

安全外壳协议（Secure Shell，SSH）是目前较可靠、专为远程登录会话和其他网络服务提供安全性的协议。由 IETF 的网络工作小组（Network Working Group）所制定，是创建在应用层和传输层基础上的安全协议。

利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。通过 SSH 可以对所有传输的数据进行加密，也能够防止 DNS 欺骗和 IP 欺骗。

SSH 的另一个优点是其传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，既可以代替 Telnet，又可以为 FTP、POP 甚至 PPP 提供一个安全的“通道”。

4. VoIP

VoIP（Voice over Internet Protocol）就是将模拟声音信号数字化，通过数据报在 IP 数据网络上做实时传递。VoIP 最大的优势是能广泛地采用 Internet 和全球 IP 互连的环境，提供比传统业务更多、更好的服务。VoIP 可以在 IP 网络上便宜地传送语音、传真、视频和数据等业务，如统一消息、虚拟电话、虚拟语音/传真邮箱、查号业务、Internet 呼叫中心、Internet 呼叫管理、电视会议、电子商务、传真存储转发和各种信息的存储转发等。

# 第 2 天

## 夯实基础，再学理论

通过第 1 天的学习，您应当对网络工程师考试的体系结构和基础知识脉络有了一个整体上的把握，而且应当也找出了自己的弱点在哪里。学习了 7 层模型各层上重要知识点和关键知识之后，第 2 天就该学习有一定难度的理论知识了。您应当掌握这些基础知识点并学会分析解题，在各个分知识点中还会涉及到一些计算题和综合理解题。

第 2 天学习的知识点包括网络安全、无线基础知识、存储技术基础、网络规划与设计、计算机硬件知识、计算机软件知识。

### 第 1 学时　网络安全

第 2 天的第 1 学时主要学习安全相关的重要知识点。安全是历年考试的重点。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 2～6 分之间。网络安全知识的考察主要集中在上午的考试中。而下午的考试则是这些知识点的应用配置，这将在后面的章节中介绍。本章考点知识结构图如图 7-1 所示。

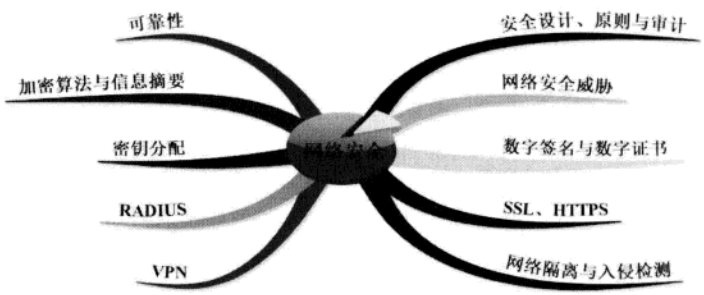



图 7-1　考点知识结构图

# 7.1 安全设计、原则与审计

## 7.1.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：网络安全设计原则、网络安全体系设计、安全审计、信息安全的五要素。

## 7.1.2 知识点精讲

1. 网络安全设计原则

网络安全设计是保证网络安全运行的基础，网络安全设计有以下基本设计原则：

（1）充分、全面、完整地对系统的安全漏洞和安全威胁等各类因素进行分析、评估和检测是设计网络安全系统的必要前提条件。

（2）强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽快恢复网络信息中心的服务，减少损失。

（3）网络安全的“木桶原则”强调对信息均衡、全面地进行保护。木桶的最大容积取决于最短的一块木板，**因此系统安全性取决于最薄弱模块的安全性**。

（4）良好的等级划分是实现网络安全的保障。

（5）网络安全应以不影响系统的正常运行和合法用户的操作活动为前提。

（6）考虑安全问题应考虑安全与保密系统的设计要与网络设计相结合，同时要兼顾性能价格的平衡。

网络安全设计原则还有易操作性原则、动态发展原则、技术与管理相结合原则。

2. 网络安全体系设计

网络安全体系设计可按层次分为物理环境安全、操作系统安全、网络安全、应用安全、管理安全等多个方面，各类涉及的内容如表7-1所示。

表7-1 网络安全体系设计内容

| 分类 | 层次 | 手段 |
| --- | --- | --- |
| 物理环境安全 | 物理层安全 | 线路安全（备份、管理）、设备安全（备份、备件、抗干扰）、机房安全（温度、湿度、电源、烟监控、除尘设施、防盗、防雷） |
| 操作系统安全 | 系统层安全 | 网络操作系统自身安全（系统漏洞补丁、访问控制、身份认证）、系统安全正确配置、防范病毒、防范木马、数据库容灾 |
| 网络安全 | 网络层安全 | 基于网络层的资源访问控制、基于网络层的身份验证、路由安全性 |
| 应用安全 | 应用层安全 | 各类应用软件和数据的安全（如数据库容灾） |
| 管理安全 | 网络管理层安全 | 建立安全管理制度、加强人员管理 |

3. 安全审计

安全审计是一个新概念，指由专业审计人员根据有关的法律法规、财产所有者的委托和管理当局的授权对计算机网络环境下的有关活动或行为进行系统的、独立的检查验证，并作出相应评价。

安全审计分为四个基本要素：

（1）控制目标：企业根据具体的计算机应用、结合单位实际制定出的安全控制要求。

（2）安全漏洞：系统的安全薄弱环节，容易被干扰或破坏的地方。

（3）控制措施：企业为实现其安全控制目标所制定的安全控制技术、配置方法及各种规范制度。

（4）控制测试：将企业的各种安全控制措施与预定的安全标准进行一致性比较，确定各项控制措施是否存在、是否得到执行、对漏洞的防范是否有效，评价企业安全措施的可依赖程度。

4. 信息安全的五要素

信息安全的基本要素主要包括 5 个方面：

（1）机密性：保证信息不泄露给未经授权的进程或实体，只供授权者使用。

（2）完整性：信息只能被得到允许的人修改，并且能够被判别该信息是否已被篡改过。同时一个系统也应该按其原来规定的功能运行，不被非授权者操纵。

（3）可用性：只有授权者才可以在需要时访问该数据，而非授权者应被拒绝访问数据。

（4）可控性：可控制数据流向和行为。

（5）可审查性：出现问题有据可循。

另外，有人将五要素进行了扩展，增加了可鉴别性和不可抵赖性。

（6）可鉴别性：网络应对用户、进程、系统和信息等实体进行身份鉴别。

（7）不可抵赖性：数据的发送方与接收方都无法对数据传输的事实进行抵赖。

## 7.2 可靠性

### 7.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：系统可靠性涉及的概念、系统可靠性。

### 7.2.2 知识点精讲

系统可靠性是系统在规定的时间、环境下，持续完成规定功能的能力，就是系统无故障运行的概率。

1. 系统可靠性涉及的概念

（1）平均无故障时间（Mean Time To Failure，MTTF）。

MTTF 指系统无故障运行的平均时间，取所有从系统开始正常运行到发生故障之间的时间段的

平均值。

（2）平均修复时间（Mean Time To Repair，MTTR）。

MTTR 指系统从发生故障到维修结束之间的时间段的平均值。

（3）平均失效间隔（Mean Time Between Failure，MTBF）。

MTBF 指系统两次故障发生时间之间的时间段的平均值。

三者关系如图 7-2 所示。

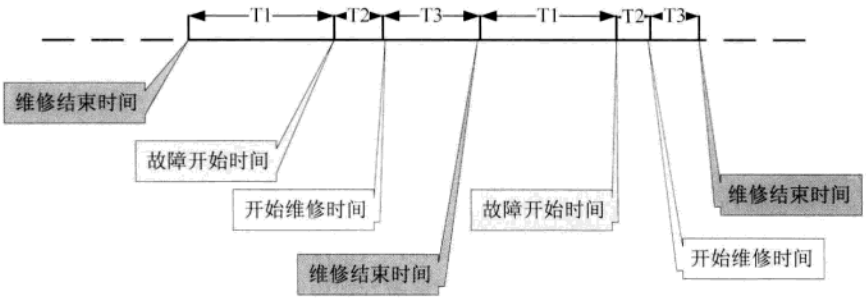



图 7-2　MTTF、MFBF 和 MTTR 关系图

平均失效间隔：MTBF=∑(T2+T3+T1)/N

平均无故障时间：MTTF=∑T1/N

平均修复时间：MTTR =∑(T2+T3)/N

三者之间的关系：MTBF= MTTF+ MTTR　　（7-1）

（4）失效率。单位时间内失效元件和元件总数的比率，用 λ 表示。

$$MTBF=1/\lambda \qquad (7\text{-}2)$$

2. 系统可靠性

系统可靠性是系统正常运行的概率，通常用 R 表示，可靠性和失效率的关系如下：

$$R=e^{-\lambda} \qquad (7\text{-}3)$$

系统可以分为串联系统、并联系统和模冗余系统。

（1）串联系统：由 n 个子系统串联而成，一个子系统失效，则整个系统失效。具体结构如图 7-3（a）所示。

（2）并联系统：由 n 个子系统并联而成，n 个系统互为冗余，只要有一个系统正常，则整个系统正常。具体结构如图 7-3（b）所示。

（3）模冗余系统：由 n 个系统和一个表决器组成，通常表决器是视为永远不会坏的，超过 n+1 个系统多数相同结果的输出作为系统输出。具体结构如图 7-3（c）所示。

系统可靠性和失效率如表 7-2 所示。

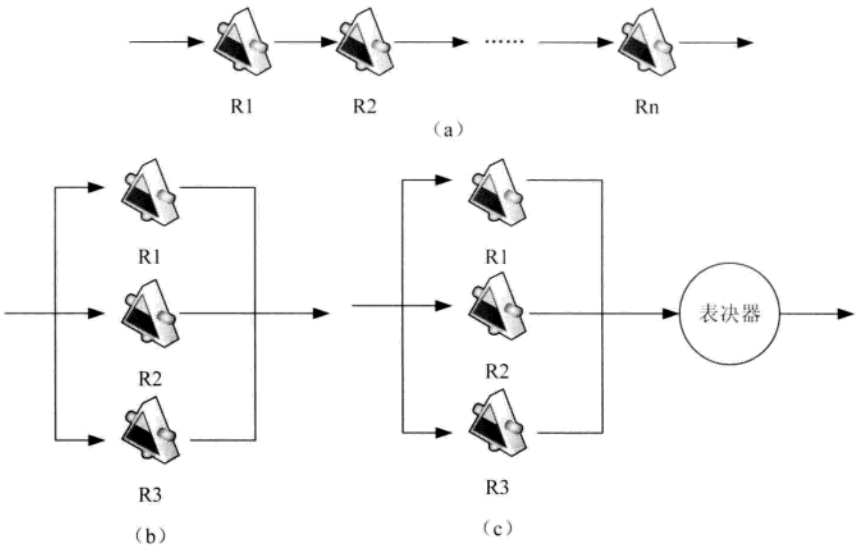



图 7-3 系统可靠性模型

表 7-2 可靠性和失效率计算

| | 可靠性 | 失效率 |
|---|---|---|
| 串联系统 | $\prod_{i=1}^{n} R_i$ | $\sum_{i=1}^{n} \lambda_i$ |
| 并联系统 | $R = 1 - \prod_{i=1}^{n} (1 - R_i)$ | $\frac{1}{\frac{1}{\lambda} \sum_{j=1}^{n} \frac{1}{j}}$ |
| 模冗余系统 | $R = \sum_{i=n+1}^{m} C_m^i \times R^i \times (1-R)^{m-i}$ | |

## 7.3 网络安全威胁

### 7.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：安全攻击类型、病毒、蠕虫、木马、僵尸网络、DOS、DDOS、垃圾邮件。

### 7.3.2 知识点精讲

1. 安全攻击类型

网络攻击是以网络为手段窃取网络上其他计算机的资源或特权、对其安全性或可用性进行破坏的行为。安全攻击依据攻击特征可以分为四类，具体如表 7-3 所示。

表 7-3 安全攻击类型

| 类型 | 定义 | 攻击的安全要素 |
| --- | --- | --- |
| 中断 | 攻击计算机或网络系统，使得其资源变得不可用或不能用 | 可用性 |
| 窃取 | 访问未授权的资源 | 机密性 |
| 篡改 | 截获并修改资源内容 | 完整性 |
| 伪造 | 伪造信息 | 真实性 |

常见的网络攻击有很多，如连续不停 Ping 某台主机、发送带病毒和木马的电子邮件、暴力破解服务器密码等，也有类似有危害但不是网络攻击的（如向多个邮箱群发一封电子邮件）。

2. 病毒、蠕虫、木马、僵尸网络、DOS、DDOS、垃圾邮件

（1）定义。

计算机病毒：是一段附着在其他程序上的、可以自我繁殖的、有一定的破坏能力的程序代码。复制后的程序仍然具有感染和破坏的功能。

蠕虫：是一段可以借助程序自行传播的程序或代码。

木马：是利用计算机程序漏洞侵入后窃取信息的程序，这个程序往往伪装成善意的、无危害的程序。

僵尸网络（Botnet）：是指采用一种或多种传播手段使大量主机感染 bot 程序（僵尸程序），从而在控制者和被感染主机之间所形成的一个可以一对多控制的网络。

拒绝服务（Denial of Service，DOS）：利用大量合法的请求占用大量网络资源，以达到瘫痪网络的目的。例如，驻留在多个网络设备上的程序在短时间内同时产生大量的请求消息冲击某 Web 服务器，导致该服务器不堪重负，无法正常响应其他合法用户的请求，这类形式的攻击就称为 DOS 攻击。又例如，TCP SYN Flooding 建立大量处于半连接状态的 TCP 连接就是一种使用 SYN 分组的 DOS 攻击。

分布式拒绝服务攻击（Distributed Denial of Service，DDOS）：很多 DOS 攻击源一起攻击某台服务器就形成了 DDOS 攻击。常见防范 DOS 和 DDOS 的方式有：根据 IP 地址对数据包进行过滤、为系统访问提供更高级别的身份认证、使用工具软件检测不正常的高流量，由于这种攻击并不在被攻击端植入病毒，因此安装防病毒软件无效。

垃圾邮件：未经用户许可就强行发送到用户邮箱中的任何电子邮件。

（2）各类恶意代码的命名规则。

恶意代码的一般命名格式为：恶意代码前缀.恶意代码名称.恶意代码后缀。

恶意代码前缀是根据恶意代码特征起的名字，具有相同前缀的恶意代码通常具有相同或相似的特征。常见的前缀名如表 7-4 所示。

表 7-4 常见的前缀名

| 前缀 | 含义 | 解释 | 例子 |
| --- | --- | --- | --- |
| Boot | 引导区病毒 | 通过感染磁盘引导扇区进行传播的病毒 | Boot.WYX |
| DOSCom | DOS 病毒 | 只通过 DOS 操作系统进行复制和传播的病毒 | DosCom.Virus.Dir2.2048 （DirII 病毒） |
| Worm | 蠕虫病毒 | 通过网络或漏洞进行自主传播，向外发送带毒邮件或通过即时通讯工具（QQ、MSN）发送带毒文件 | Worm.Sasser（震荡波） |
| Trojan | 木马 | 木马通常伪装成有用的程序诱骗用户主动激活，或利用系统漏洞侵入用户电脑。计算机感染特洛伊木马后的典型现象是有未知程序试图建立网络连接 | Trojan.Win32.PGPCoder.a（文件加密机）、Trojan.QQPSW |
| Backdoor | 后门 | 通过网络或者系统漏洞入侵电脑并隐藏起来，方便黑客远程控制 | Backdoor.Huigezi.ik（灰鸽子变种 IK）、Backdoor.IRCBot |
| Win32、PE、Win95、W32、W95 | 文件型病毒或系统病毒 | 感染可执行文件（如.exe、.com）、.dll 文件的病毒。<br>若与其他前缀连用，则表示病毒的运行平台 | Win32.CIH<br>Backdoor.Win32.PcClient.al，表示运行在 32 位 Windows 平台上的后门 |
| Macro | 宏病毒 | 宏语言编写，感染办公软件（如 Word、Excel），并且能通过宏自我复制的程序 | Macro.Melissa、Macro.Word、Macro.Word.Apr30 |
| Script、VBS、JS | 脚本病毒 | 使用脚本语言编写，通过网页传播、感染、破坏或调用特殊指令下载并运行病毒、木马文件 | Script.RedLof（红色结束符）、Vbs.valentin （情人节） |
| Harm | 恶意程序 | 直接对被攻击主机进行破坏 | Harm.Delfile（删除文件）、Harm.formatC.f（格式化 C 盘） |
| Joke | 恶作剧程序 | 不会对计算机和文件产生破坏，但可能会给用户带来恐慌和麻烦，如做控制鼠标 | Joke.CrayMourse （疯狂鼠标） |

## 7.4 加密算法与信息摘要

### 7.4.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：对称加密算法、非对称加密算法、信息完整性验证算法。

### 7.4.2 知识点精讲

1. 对称加密算法

加密密钥和解密密钥相同的算法，称为对称加密算法，对称加密算法相对非对称加密算法加密的效率高，适合大量数据加密。常见的对称加密算法有DES、3DES、RC5、IDEA，具体特性如表7-5所示。

表7-5 常见的对称加密算法

| 加密算法名称 | 特点 |
| --- | --- |
| DES | 明文分为64位一组，密钥64位（实际位是56位的密钥和8位奇偶校验）。注意：考试中填实际密钥位即56位 |
| 3DES | 3DES是DES的扩展，是执行了三次的DES。其中，第一、三次加密使用同一密钥的方式下，密钥长度扩展到128位（112位有效）；三次加密使用不同密钥，密钥长度扩展到192位（168位有效） |
| RC5 | RC5由RSA中的Ronald L. Rivest发明，是参数可变的分组密码算法，三个可变的参数是：分组大小、密钥长度和加密轮数 |
| IDEA | 明文、密文均为64位，密钥长度128位 |
| RC4 | 常用流密码，密钥长度可变，用于SSL协议。曾经用于802.11 WEP协议中。这也是Ronald L. Rivest发明 |

2. 非对称加密算法

加密密钥和解密密钥不相同的算法，称为非对称加密算法，这种方式又称为公钥密码体制，解决了对称密钥算法的密钥分配与发送的问题。在非对称加密算法中，私钥用于解密和签名，公钥用于加密和认证。

（1）加密、解密的表示方法。

公式7-4表示了明文通过加密算法变成密文的方法，其中K1表示密钥。

$$Y=E_{K1}(X) \tag{7-4}$$

明文X通过加密算法E，使用密钥K1变为密文Y。

公式7-5表示了密文通过解密算法还原成明文的方法，其中K2表示密钥。

$$X=D_{K2}(Y) \tag{7-5}$$

密文Y通过解密算法D，使用密钥K2还原为明文X。

（2）RSA。

RSA（Rivest Shamir Adleman）是典型的非对称加密算法，该算法基于大素数分解。RSA适合进行数字签名和密钥交换运算。

RSA密钥生成过程如表7-6所示。

表 7-6 RSA 密钥生成过程

| |
|---|
| 选出两个大质数 p 和 q，使得 p≠q |
| p×q=n |
| (p-1)×(q-1) |
| 选择 e，使得 1<e<z，并且和(p-1)×(q-1)互为质数 |
| 计算解密密钥，使得 ed=1mod (p-1)×(q-1) |
| 公钥=(n,e) |
| 私钥=d |
| 消除原始质数 p 和 q |

**注意**：质数就是真正因子，只有 1 和本身两个因数，属于正整数。

RSA 加密、解密过程如图 7-4 所示。


图 7-4 RSA 加密和解密

【例 7-1】按照 RSA 算法，若选两个奇数 p=5，q=3，公钥 e=7，则私钥 d 为（ ）。

A．6 B．7 C．8 D．9

【解析】

按 RSA 算法求公钥和密钥：

（1）选两奇数 p=5，q=3；

（2）n=p×q=5×3=15；

（3）(p-1)×(q-1)=8；

（4）公钥 e=7，则依据 ed=1mod(p-1)×(q-1)，即 7d=1mod8。

结合四个选项，得到 d=7，即 49 mod 8=1。

3. 信息完整性验证算法

报文摘要算法（Message Digest Algorithms）使用特定算法对明文进行摘要，生成固定长度的密文。这类算法重点在于“摘要”，即对原始数据依据某种规则提取；摘要和原文具有联系性，即被“摘要”数据与原始数据一一对应，只要原始数据稍有改动，“摘要”的结果就不同。因此，这种方式可以验证原文是否被修改。

消息摘要算法采用“单向函数”，即只能从输入数据得到输出数据，无法从输出数据得到输入数据。常见报文摘要算法有安全散列标准 SHA-1、MD5 系列标准。

（1）MD5。

消息摘要算法 5（MD5），把信息分为 512 比特的分组，并且创建一个 128 比特的摘要。

（2）SHA-1。

安全 hash 算法（SHA-1），也是基于 MD5 的，使用一个标准把信息分为 512 比特的分组，并且创建一个 160 比特的摘要。

## 7.5 数字签名与数字证书

### 7.5.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：数字签名、数字证书。

### 7.5.2 知识点精讲

1. 数字签名

数字签名的作用就是确保 A 发送给 B 的信息就是 A 本人发送的，并且没有改动。数字签名和验证的过程如图 7-5 所示。

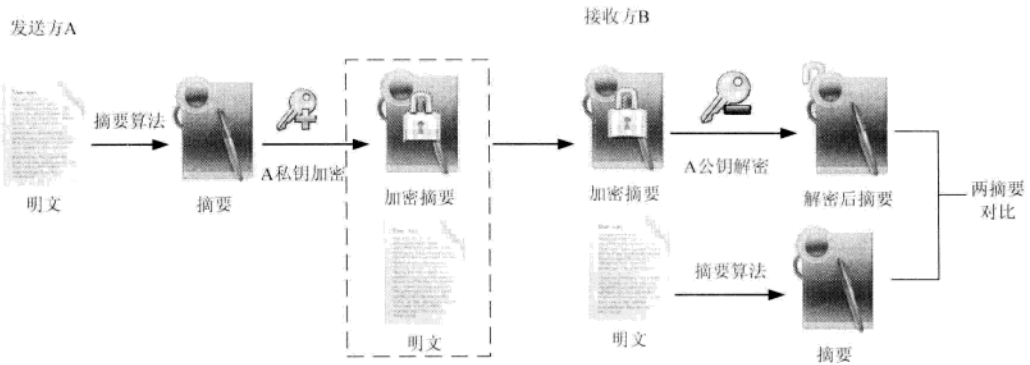



图 7-5 数字签名和验证的过程

数字签名的基本过程：

（1）A 使用“摘要”算法（如 SHA-1、MD5 等）对发送信息进行摘要。

（2）使用 A 的私钥对消息摘要进行加密运算，将加密摘要和原文一并发给 B。

验证签名的基本过程：

（1）B 接收到加密摘要和原文后，使用和 A 同样的“摘要”算法对原文再次摘要，生成新摘要。

（2）使用 A 公钥对加密摘要解密，还原成原摘要。

（3）两个摘要对比，一致则说明由 A 发出且没有经过任何篡改。

由此可见，数字签名功能有信息身份认证、信息完整性检查、信息发送不可否认性，但不提供

原文信息加密，不能保证对方能收到消息，也不对接收方身份进行验证。

2. 数字证书

场景：A 声明自己是某银行办事员向客户索要账户和密码，客户验证了 A 的签名，确认索要密码的信息是 A 发过来的，那么客户就愿意告诉 A 用户名和密码么？

显然不会。因为客户仅仅证明信息确实是 A 发过来的没有经过篡改的信息，但不能确认 A 就是银行职员、做的事情是否合法。这时需要有一个权威中间部门 M（如政府、银监会等），该部门向 A 颁发了一份证书，确认其银行职员身份。这份证书里有这个权威机构 M 的数字签名，以保证这份证书确实是 M 所发。

数字证书采用公钥体制进行加密和解密。每个用户有一个私钥来解密和签名；同时每个用户还有一个公钥来加密和验证。

【例 7-1】说明了数字证书、CA 签名、证书公钥的作用。

某网站向证书颁发机构（Certification Authority，CA）申请了数字证书，用户通过 CA 的签名来验证网站的真伪。在用户与网站进行安全通信时，用户可以通过证书中的公钥进行加密和验证，该网站通过网站的私钥进行解密和签名。

（1）X.509 格式。

目前数字证书的格式大都是 X.509 格式，X.509 是由国际电信联盟（ITU-T）制定的数字证书标准。

在 X.509 标准中，包含在数字证书中的数据域有证书、版本号、序列号（唯一标识每一个 CA 下发的证书）、算法标识、颁发者、有效期、有效起始日期、有效终止日期、使用者、使用者公钥信息、公钥算法、公钥 、颁发者唯一标识、使用者唯一标识、扩展、证书签名算法、证书签名（发证机构，即 CA 对用户证书的签名）。

（2）证书发放。

证书由 CA 中心发放，无需特别措施。

由于网络存在多个 CA 中心，因此提出了证书链。证书链服务是一个 CA 扩展其信任范围的机制，实现不同认证中心发放的证书的信息交换。如果用户 UA 从 A 地的发证机构取得了证书，用户 UB 从 B 地的发证机构取得了证书，那么 UA 通过证书链交换了证书信息，则可以与 UB 进行安全通信。

（3）证书吊销。

当用户个人身份信息发生变化或私钥丢失、泄露、疑似泄露时，证书用户应及时地向 CA 提出证书的撤销请求，CA 也应及时地把此证书放入公开发布的证书撤销列表（Certification Revocation List，CRL）。

证书撤销的流程如下：

1）用户或其上级单位向注册机构（Registration Authority，RA）提出撤销请求。

2）RA 审查撤销请求。

3）审查通过后，RA 将撤销请求发送给 CA 或 CRL 签发机构。

4）CA 或 CRL 签发机构修改证书状态并签发新的 CRL。

当该数字证书被放入 CRL 后，数字证书则被认为失效，而失效并不意味着无法被使用。如果窃取到甲的私钥的乙用甲的私钥签名了一份文件发送给丙，并附上甲的证书，而丙忽视了对 CRL 的查看，丙就依然会用甲的证书成功验证这份非法的签名，并会认为甲对这份文件签过名而接收该文件。

## 7.6 密钥分配

### 7.6.1 考点分析

历年的网络工程师考试试题涉及本部分的相关知识点有：对称密钥分配、公钥分配、SET 协议。

### 7.6.2 知识点精讲

密钥分配分为对称密钥分配和公钥分配体制。

1. 对称密钥分配

Kerberos 这一名词来源于希腊神话“三个头的狗—地狱之门守护者”。Kerberos 协议主要用于计算机网络的身份鉴别（Authentication），鉴别验证对方是合法的，而不是冒充的。同时，Kerberos 协议也是密钥分配中心（Key Distribution Center，KDC）的核心。Kerberos 进行密钥分配时使用 AES 加密。

使用 Kerberos 时，用户只需输入一次身份验证信息就可以凭借此验证获得的票据（ticket-granting ticket）访问多个服务，即单点登录（Single Sign On，SSO）。由于在每个 Client 和 Service 之间建立了共享密钥，使得该协议具有相当的安全性。

（1）Kerberos 组成。

Kerberos 使用两个服务器：鉴别服务器（Authentication Server，AS）和票据授予服务器（Ticket-Granting Server，TGS）。

1）验证服务器。AS 就是一个密钥分配中心（KDC）。同时负责用户的 AS 注册、分配账号和密码，负责确认用户并发布用户和 TGS 之间的会话密钥。

2）票据授予服务器。TGS 是发行服务器方的票据，提供用户和服务器之间的会话密钥。Kerberos 把用户验证和票据发行分开了。虽然 AS 只用对用户本身的 ID 验证一次，但为了获得不同的真实服务器票据，用户需要多次联系 TGS。

（2）Kerberos 流程。

Kerberos 流程原理如图 7-6 所示。

第 1 步：用户 A 使用明文向 AS 验证身份。认证成功后，用户 A 和 TGS 联系。

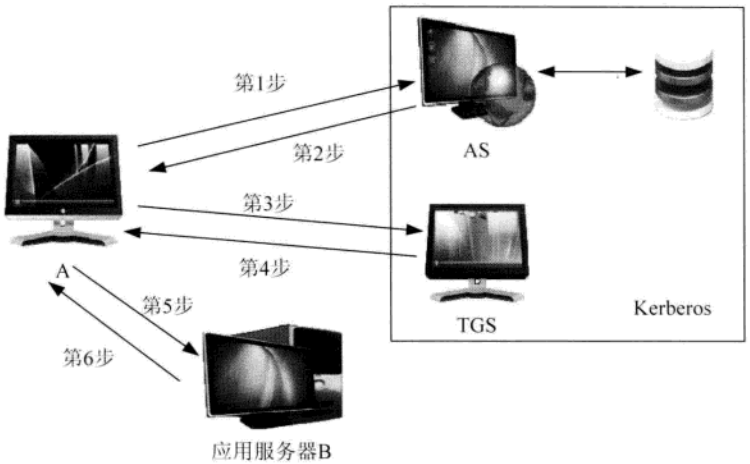



图 7-6 Kerberos 的工作原理

第 2 步：AS 向 A 发送用 A 的对称密钥 $K_A$ 加密的报文，该报文包含 A 和 TGS 通信的会话密钥 $K_s$ 及 AS 发送到 TGS 的票据（该票据使用 TGS 的对称密钥 $K_{TGS}$ 加密）。报文到达 A 时，输入口令则得到数据。

**注意：** *票据包含发送人身份和会话密钥。*

第 3 步：转发 AS 获得的票据、要访问的应用服务器 B 名称，以及用会话密钥 $K_s$ 加密的时间戳（防止重发攻击）发送给 TGS。

第 4 步：TGS 返回两个票据，第一个票据包含 B 名称和会话密钥 $K_{AB}$，使用 $K_s$ 加密；第二个票据包含 A 和会话密钥 $K_{AB}$，使用 $K_B$ 加密。

第 5 步：A 将 TGS 收到的第二个票据（包含 A 名称和会话密钥 $K_{AB}$，使用 $K_B$ 加密）使用 $K_{AB}$ 加密的时间戳（防止重发攻击）发送给应用服务器 B。

第 6 步：服务器 B 进行应答，完成认证过程。

最后，A 和 B 就使用 TGS 发的密钥 $K_{AB}$ 加密。

2. 公钥分配

公钥基础设施（Public Key Infrastructure，PKI）是一种遵循既定标准的密钥管理平台，它能为所有网络应用提供加密和数字签名等密码服务及必需的密钥和证书管理体系。简单来说，PKI 是一组规则、过程、人员、设施、软件和硬件的集合，可以用来进行公钥证书的发放、分发和管理。

典型的 PKI 系统由 5 个基本部分组成：证书申请者、注册机构、CA 认证中心、证书库和证书信任方。

国际电信联盟 ITU X.509 协议是 PKI 技术体系中应用最广泛、最基础的一个国际标准，它定义了一个规范的数字证书的格式。

3. SET 协议

电子商务在提供机遇和便利的同时，也面临着一个最大的挑战，即交易的安全问题。在网上购物环境中，持卡人希望在交易中保密自己的账户信息，使之不被人盗用；商家则希望客户的定单不可抵赖，并且在交易过程中，交易双方都希望验明其他方的身份，以防止被欺骗。针对这种情况，由美国 Visa 和 MasterCard 两大信用卡组织联合国际上多家科技机构，共同制定了应用于 Internet 上的以信用卡为基础进行在线交易的安全标准，这就是安全电子交易（Secure Electronic Transaction，SET）。它采用公钥密码体制和 X.509 数字证书标准，主要用于保障网上购物信息的安全性。

由于 SET 提供了消费者、商家和银行之间的认证，确保了交易数据的安全性、完整可靠性和交易的不可否认性，特别是保证不将消费者的银行卡号暴露给商家等优点，因此成为了目前公认的信用卡/借记卡网上交易的国际安全标准。

SET 协议本身比较复杂，设计比较严格，安全性高，它能保证信息传输的机密性、真实性、完整性和不可否认性。SET 协议是 PKI 框架下的一个典型实现。

## 7.7 SSL、HTTPS

### 7.7.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：SSL、SSL 协议的工作流程、HTTPS、S-HTTP。

### 7.7.2 知识点精讲

1. SSL

安全套接层（Secure Sockets Layer，SSL）协议是一个安全传输、保证数据完整的安全协议，之后的传输层安全（Transport Layer Security，TLS）是 SSL 的非专有版本。SSL 处于应用层和传输层之间。

SSL 主要包括 SSL 记录协议、SSL 握手协议、SSL 告警协议、SSL 修改密文协议等，协议栈如图 7-7 所示。


图 7-7 SSL 协议栈

2. SSL 协议的工作流程

（1）浏览器向服务器发送请求信息（包含协商 SSL 版本号、询问选择何种对称密钥算法），

开始新会话连接。

（2）服务器返回浏览器请求信息，附加生成主密钥所需的信息，确定 SSL 版本号和对称密钥算法，发送服务器证书（包含了 RSA 公钥），并使用某 CA 中心私钥加密。

（3）浏览器对照自己的可信 CA 表判断服务器证书是否在可信 CA 表中。不在，则通信中止；如果在，则使用 CA 表中对应的公钥解密，得到服务器的公钥。

（4）浏览器随机产生一个对称密钥，使用服务器公钥加密并发送给服务器。

（5）浏览器和服务器相互发一个报文，确定使用此对称密钥加密；再相互发一个报文，确定浏览器端和服务器端握手过程完成。

（6）握手完成，双方使用该对称密钥对发送的报文加密。

3. HTTPS

安全超文本传输协议（Hypertext Transfer Protocol over Secure Socket Layer，HTTPS），是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。它使用 SSL 来对信息内容进行加密，使用 TCP 的 443 端口发送和接收报文。其使用语法与 HTTP 类似，使用“HTTPS:// + URL”形式。

4. S-HTTP

安全超文本传输协议（Secure Hypertext Transfer Protocol，S-HTTP）是一种面向安全信息通信的协议，是 EIT 公司结合 HTTP 而设计的一种消息安全通信协议。S-HTTP 可提供通信保密、身份识别、可信赖的信息传输服务及数字签名等。

S-HTTP 和 SSL 的异同如表 7-7 所示。

表 7-7 S-HTTP 和 SSL 的异同

| | SSL | S-HTTP |
|---|---|---|
| 工作层次 | 传输层和应用层之间 | 应用层 |
| 处理对象 | 数据流 | 应用数据 |
| 基于消息的抗抵赖性证明 | 不可以 | 可以 |
| 加密算法 | RC4 | 可以协商加密算法（如 RSA、DSA、DES） |

## 7.8 RADIUS

### 7.8.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：RADIUS。

### 7.8.2 知识点精讲

远程用户拨号认证系统（Remote Authentication Dial In User Service，RADIUS）是目前应用最广泛的授权、计费和认证协议。

RADIUS 基本交互步骤如图 7-8 所示。

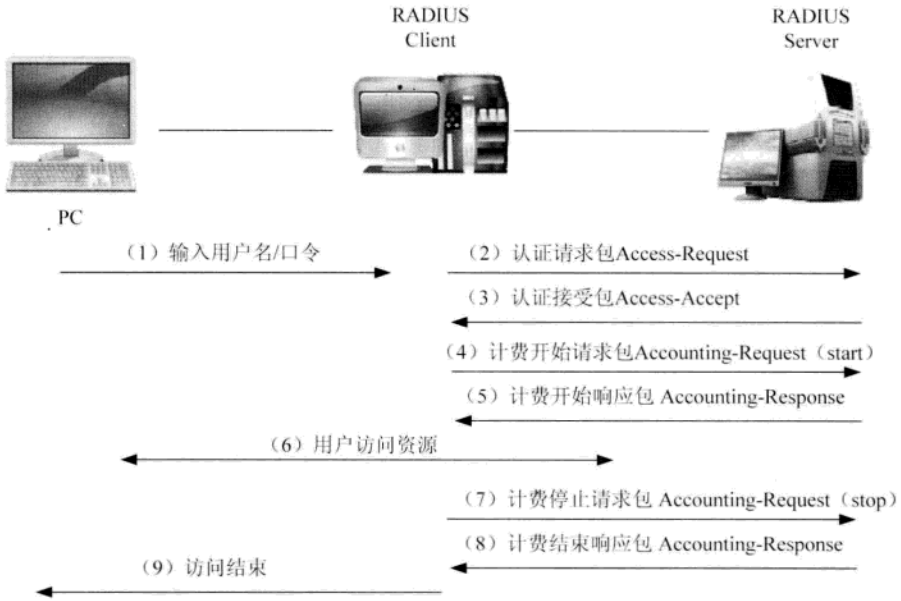



图 7-8　RADIUS 认证过程

（1）用户输入用户名和口令。

（2）客户端根据获取的用户名和口令向 RADIUS 服务器发送认证请求包（Access-Request）。

（3）RADIUS 服务器将该用户信息与 users 数据库信息进行对比分析，如果认证成功，则将用户的权限信息以认证响应包（Access-Accept）发送给 RADIUS 客户端；如果认证失败，则返回 Access-Reject 响应包。

（4）RADIUS 客户端根据接收到的认证结果接入/拒绝用户。如果可以接入用户，则 RADIUS 客户端向 RADIUS 服务器发送计费开始请求包（Accounting-Request），status-type 取值为 start。

（5）RADIUS 服务器返回计费开始响应包（Accounting-Response）。

（6）此时用户可以访问资源。

（7）RADIUS 客户端向 RADIUS 服务器发送计费停止请求包（Accounting-Request），status-type 取值为 stop。

（8）RADIUS 服务器返回计费结束响应包（Accounting-Response）。

（9）通知访问结束。

## 7.9 VPN

### 7.9.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：VPN 基础知识、VPN 隧道技术、IPSec、MPLS。

### 7.9.2 知识点精讲

1. VPN 基础知识

虚拟专用网络（Virtual Private Network，VPN）是在公用网络上建立专用网络的技术。由于整个 VPN 网络中的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路，而是架构在公用网络服务商所提供的网络平台，所以称之为虚拟网。实现 VPN 的关键技术主要有隧道技术、加/解密技术、密钥管理技术和身份认证技术。

2. VPN 隧道技术

实现 VPN 的最关键部分是在公网上建立虚信道，而建立虚信道是利用隧道技术实现的，IP 隧道的建立可以在链路层和网络层。

VPN 主要隧道协议有 PPTP、L2TP、IPsec、SSL VPN、TLS VPN。

（1）PPTP（点到点隧道协议）。

PPTP 是一种用于让远程用户拨号连接到本地的 ISP，是通过因特网安全访问内网资源的技术。它能将 PPP 帧封装成 IP 数据包，以便能够在基于 IP 的互联网上进行传输。PPTP 使用 TCP 连接创建、维护、终止隧道，并使用 GRE（通用路由封装）将 PPP 帧封装成隧道数据。被封装后的 PPP 帧的有效载荷可以被加密、压缩或同时被加密与压缩。该协议是第 2 层隧道协议。

（2）L2TP 协议。

L2TP 是 PPTP 与 L2F（第二层转发）的一种综合，是由思科公司推出的一种技术。该协议是第 2 层隧道协议。

（3）IPSec 协议。

IPSec 协议在隧道外面再封装，保证了隧道在传输过程中的安全。该协议是第 3 层隧道协议。

（4）SSL VPN、TLS VPN。

两类 VPN 使用了 SSL 和 TLS 技术，在传输层实现 VPN 的技术。该协议是第 4 层隧道协议。由于 SSL 需要对传输数据加密，因此 SSL VPN 的速度比 IPSec VPN 慢。SSL VPN 的配置和使用又比其他 VPN 简单。

3. IPSec

Internet 协议安全性（Internet Protocol Security，IPSec）是通过对 IP 协议的分组进行加密和认证来保护 IP 协议的网络传输协议族（一些相互关联的协议的集合）。IPSec 工作在 TCP/IP

协议栈的网络层，为 TCP/IP 通信提供访问控制机密性、数据源验证、抗重放、数据完整性等多种安全服务。

IPsec 是一个协议体系，由建立安全分组流的密钥交换协议和保护分组流的协议两个部分构成，前者即为 IKE 协议，后者则包含 AH、ESP 协议。

（1）IKE 协议。

Internet 密钥交换协议（Internet Key Exchange Protocol，IKE）属于一种混合型协议，由 Internet 安全关联和密钥管理协议（Internet Security Association and Key Management Protocol，ISAKMP）与两种密钥交换协议（OAKLEY 与 SKEME）组成，即 IKE 由 ISAKMP 框架、OAKLEY 密钥交换模式以及 SKEME 的共享和密钥更新技术组成。IKE 定义了自己的密钥交换方式（**手工密钥交换和自动 IKE**）。

**注意**：ISAKMP 只对认证和密钥交换提出了结构框架，但没有具体定义，因此支持多种不同的密钥交换。

IKE 使用了两个阶段的 ISAKMP：①协商创建一个通信信道（IKE SA）并对该信道进行验证，为双方进一步的 IKE 通信提供机密性、消息完整性及消息源验证服务；②使用已建立的 IKE SA 建立 IPsec SA。

（2）AH。

认证头（Authentication Header，AH）是 IPSec 体系结构中的一种主要协议，它为 IP 数据报提供完整性检查与数据源认证，并防止重放攻击。AH 不支持数据加密。AH 常用摘要算法（单向 Hash 函数）MD5 和 SHA1 实现摘要和认证，确保数据完整。

（3）ESP。

封装安全载荷（Encapsulating Security Payload，ESP）可以同时提供数据完整性确认和数据加密等服务。ESP 通常使用 DES、3DES、AES 等加密算法实现数据加密，使用 MD5 或 SHA-1 来实现摘要和认证，确保数据完整。

（4）IPSec VPN 应用场景。

IPSec VPN 应用场景分为站点到站点、端到端、端到站点三种模式。

1）站点到站（Site-to-Site）。

站点到站点又称为网关到网关，多个异地机构利用运营商网络建立 IPSec 隧道，将各自的内部网络联系起来。

2）端到端（End-to-End）。

端到端又称为 PC 到 PC，即两个 PC 之间的通信由 IPSec 完成。

3）端到站点（End-to-Site）。

端到站点，两个 PC 之间的通信由网关和异地 PC 之间的 IPSec 会话完成。

（5）IPSec 工作模式。

IPSec 的两种工作模式分别是**传输模式**和**隧道模式**，具体如图 7-9 所示。

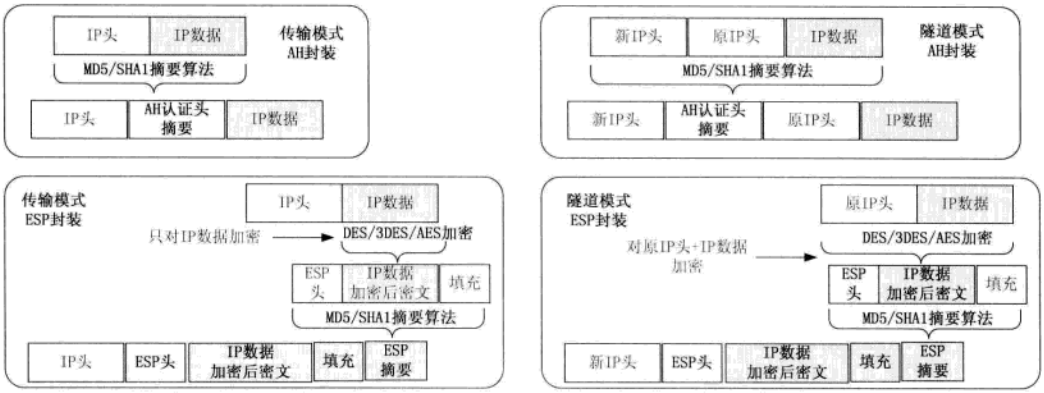



图 7-9　IPSec 工作模式

由图 7-10 可知，传输模式下的 AH 和 ESP 处理后的 IP 头部不变，而隧道模式下的 AH 和 ESP 处理后需要新封装一个新的 IP 头。AH 只作摘要，因此只能验证数据完整性和合法性；而 ESP 既做摘要，也做加密，因此除了验证数据完整性和合法性之外，还能进行数据加密。

4. MPLS

多协议标记交换（Multi-Protocol Label Switching，MPLS）是核心路由器利用含有边缘路由器在 IP 分组内提供的前向信息的标签（Label）或标记（Tag）实现网络层交换的一种交换方式。

MPLS 技术主要是为了提高路由器转发速率而提出的，其核心思想是利用标签交换取代复杂的路由运算和路由交换。该技术实现的核心就是把 **IP 数据报**封装在 **MPLS** 数据包中。MPLS 将 IP 地址映射为简单、固定长度的标签，这和 IP 中的包转发、包交换不同。

MPLS 根据标记对分组进行交换。以以太网为例，MPLS 包头的位置应插入在以太帧头与 IP 头之间，是属于二层和三层之间的协议，也称为 2.5 层协议。

**注意**：*考试中应填 2.5 层。*

MPLS 标签结构与具体承载结构如图 7-10 所示。

（1）MPLS 流程。

当分组进入 MPLS 网络时，由边缘路由器（Label Edge Router，LER）划分为不同的转发等价类（FEC）并打上不同标记，该标记定长且包含了目标地址、源地址、传输层端口号、服务质量、带宽、延长等信息。分类建立，分组被转发到标记交换通路（Label Switch Path，LSP）中，由标签交换路由器（Label Switch Router，LSR）根据标记作转发。在出口 LER 上去除标记，使用 IP 路由机制将分组向目的地转发。

（2）MPLS VPN。

MPLS VPN 承载平台由 **P 路由器、PE 路由器和 CE 路由器**组成。

1）P（Provider）路由器。

P 路由器是 MPLS 核心网中的路由器，在运营商网络中，这种路由器只负责**依据 MPLS 标签**

**完成数据包的高速转发**，P路由器只维护到PE路由器的路由信息，而不维护VPN相关的路由信息。P路由器是不连接任何CE路由器的骨干网路由设备，相当于标签交换路由器（LSR）。

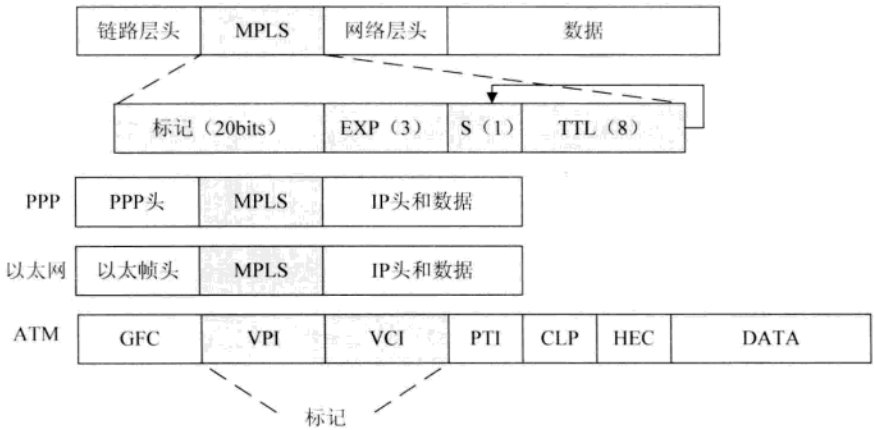



图 7-10　MPLS 标签结构与承载结构

2）PE（Provider Edge）路由器。

PE路由器是MPLS边缘路由器，负责待传送数据包的**MPLS标签的生成和去除**，还负责发起根据路由**建立交换标签的动作**，相当于标签边缘路由器（LER）。PE路由器连接CE路由器和P路由器，是最重要的网络节点。用户的流量通过PE路由器流入用户网络，或者通过PE路由器流到MPLS骨干网。

3）CE（Customer Edge）路由器。

CE路由器是用户边缘设备，是直接与电信运营商相连的用户端路由器，该设备上不存在任何带有标签的数据包。CE路由器通过连接一个或多个PE路由器为用户提供服务接入。CE路由器通常是一台IP路由器，它与连接的PE路由器建立邻接关系。



## 7.10　网络隔离与入侵检测

### 7.10.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：网络隔离、入侵检测。

### 7.10.2　知识点精讲

1. 网络隔离

网络隔离技术的目标是确保把有害的攻击隔离，在保证可信网络内部信息不外泄的前提下，完成网络间数据的安全交换。

Mark Joseph Edwards 对协议隔离进行了归类，他将现有的隔离技术从理论上分为了五类。

（1）第一代隔离技术——完全的隔离。

此方法使得网络处于信息孤岛状态，做到了完全的物理隔离。这种方式需要至少两套网络和系统，更重要的是信息交流的不便和成本的提高，给维护和使用带来了极大的不便。

（2）第二代隔离技术——硬件卡隔离。

在客户端增加一块硬件卡，客户端硬盘或其他存储设备首先连接到该卡，然后再转接到主板上，通过该卡能控制客户端硬盘或其他存储设备。而在选择不同的硬盘时，同时选择了该卡上不同的网络接口以连接到不同的网络。但是，这种隔离产品在大多数情况下仍然需要网络布线为双网线结构，产品存在着较大的安全隐患。

（3）第三代隔离技术——数据转播隔离。

利用转播系统分时复制文件的途径来实现隔离，切换时间非常久，甚至需要手工完成，不仅明显地减缓了访问速度，更不支持常见的网络应用，失去了网络存在的意义。

（4）第四代隔离技术——空气开关隔离。

它是通过使用单刀双掷开关，使得内外部网络分时访问临时缓存器来完成数据交换的，但在安全和性能上存在许多问题。

（5）第五代隔离技术——安全通道隔离。

此技术通过专用通信硬件和专有安全协议等安全机制来实现内外部网络的隔离和数据交换，不仅解决了以前隔离技术存在的问题，并有效地把内外部网络隔离开来，而且高效地实现了内外网数据的安全交换，透明地支持多种网络应用，成为当前隔离技术的发展方向。

常考的网络隔离技术有以下 4 种：

（1）防火墙。

通过 ACL 进行网络数据包的隔离是最常用的隔离方法。控制局限于传输层以下的攻击，对于病毒、木马、蠕虫等应用层的攻击毫无办法。适合小网络隔离，不合适大型、双向访问业务网络隔离。

（2）多重安全网关。

多重安全网关称为统一威胁管理（Unified Threat Management，UTM）被称为新一代防火墙，能做到从网络层到应用层的全面检测。UTM 的功能有 ACL、防入侵、防病毒、内容过滤、流量整形、防 DOS。

（3）VLAN 划分。

VLAN 划分技术避免了广播风暴，解决了有效数据传递问题，通过划分 VLAN 隔离各类安全性部门。

（4）人工策略。

断开网络物理连接，使用人工方式交换数据，这种方式安全性最好。

2. 入侵检测

入侵检测技术是近 20 年来出现的一种主动保护自己免受黑客攻击的新型网络安全技术。入侵检测（Intrusion Detection）就是从系统运行过程中产生的或系统所处理的各种数据中查找出威胁系

统安全的因素，并对威胁做出相应的处理。入侵检测的软件或硬件称为入侵检测系统（Intrusion Detection System，IDS）。入侵检测被认为是防火墙之后的第二道安全闸门，它在不影响网络性能的情况下对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

入侵检测包括两个步骤：**信息收集和数据分析**。入侵检测就是分析攻击者留下的痕迹，而这些痕迹会与正常数据混合。入侵检测就是收集这些数据并分析数据找到痕迹。

入侵检测设备可以部署在DMZ中，这样可以查看受保护区域主机被攻击的状态，可以检测防火墙系统的策略配置是否合理和DMZ中被黑客攻击的重点。部署在路由器和边界防火墙之间可以审计来自Internet上对受保护网络的攻击类型。

# 第2学时　无线基础知识

第2天的第2学时主要学习无线基础知识。无线是每次考试的重点。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在3～18分之间。无线知识点的考察在上、下午考试中均有涉及，而且案例题分值比重也较大。本章考点知识结构图如图8-1所示。


图8-1　考点知识结构图

## 8.1　无线局域网



### 8.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：IEEE 802.11基础知识概述与物理层知识、IEEE 802.11系列标准、IEEE 802.11MAC层协议。

### 8.1.2　知识点精讲

1. IEEE 802.11 基础知识概述与物理层知识

IEEE 802.11定义了无线局域网的两种工作模式：**基础设施网络（Infrastructure Networking）**和**自主网络（Ad Hoc Networking）**。基础设施网络是预先建立起来的，具有一系列能覆盖一定地理范围的固定基站。构建自主网络时，网络组建不需要使用固定的基础设施，仅靠自身就可以临时构建网络。自主网络就是一种不需要有线网络和接入点支持的点对点网络。

（1）服务集。

802.11规定无线局域网最小构件是**基本服务集**（Basic Service Set，BSS），一个基本服务集覆

盖的区域为**基本服务区**（Basic Service Area，BSA）。一个接入 AP 可以成为基本服务集中的**基站**（Base Station）。一个服务集通过接入 AP 连接到**分配系统**（Distribution System，DS），然后再连接一个基本服务集，这样就构成了**扩展服务集**（Extended Service Set，ESS）。安装 AP 需要给 AP 分配一个不超过 32 字节的**服务集标识符**（Service Set Identifier，SSID）和一个信道。

（2）ISM。

工业、科学和医疗频段（Industrial Scientific Medical Band，**ISM Band**）是国际通信联盟无线电通信局的无线电通信部门（ITU Radio communication Sector，ITU-R）定义的。此频段主要是开放给工业、科学和医学三个主要机构使用，属于 Free License，无需授权许可，只需要遵守一定的发射功率（一般低于 1W），只要不对其他频段造成干扰即可。其中，重要的 **2.4GHz 频段**为各国共同的 ISM 频段，因此无线局域网、蓝牙、ZigBee 等无线网络均可以工作在 2.4GHz 频段上。

（3）802.11 物理层。

802.11 物理层比较复杂，最初使用了三种物理层技术。

1）跳频（Frequency-Hopping Spread Spectrum，FHSS）。

扩频技术的基本特征是使用比发送的信息数据速率高很多倍的伪随机码将载有信息数据的基带信号的频谱进行扩展，形成宽带的低功率频谱密度的信号来发射。简而言之，就是用伪随机序列对代表数据的模拟信号进行调制。它的特点是对无线噪声不敏感、产生的干扰小、安全性较高，但是占用带宽较高。**增加带宽可以在低信噪比、等速率的情况下，提高数据传输的可靠性。**而扩频技术属于跳频技术的一种。

FHSS 系统的基本运作过程：发送端首先把信息数据调制成基带信号，然后进入载波频率调制阶段。此时载波频率受伪随机码发生器控制，在给定的某带宽远大于基带信号的频带内随机跳变，使基带信号带宽扩展到发射信号使用的带宽，然后跳频信号便由天线发送出去。接收端接收到跳频信号后，首先从中提取出同步信息，使本机伪随机序列控制的频率跳变与接收到的频率跳变同步，这样才能得到数据载波，将载波解调（即扩频解调）后得到发射机发出的信息。

传统无线通信为了节约宝贵频率资源，在保证通信质量前提下采用最窄带宽；FHSS 则相反，因此安全性较高、带宽消耗较大，占用了比传输信息带宽高许多倍的频率带宽。伪随机序列好比音乐家的指挥棒，而各种乐器好比各种频率，只有在指挥棒指挥各种乐器前提下才能演奏和谐的交响曲。只不过 FHSS 接收方和发送方的指挥棒一定是相同的。

2）红外技术（IR，InfraRed）。

红外线是波长在 750nm 至 1mm 之间的电磁波，它的频率高于微波而低于可见光，是一种人的眼睛看不到的光线。由于红外线的波长较短，对障碍物的衍射能力差，所以更适合应用在需要短距离无线通讯的场合，进行点对点的直线数据传输。红外数据协会将红外数据通讯所采用的光波波长的范围限定在 850nm 至 900nm 之内。

3）直接序列扩频（Direct Sequence Spread Spectrum，DSSS）。

DSSS 的扩频方式是：首先用高速率的伪噪声（PN）码序列与信息码序列作**模二加（波形相乘）运算**，得到一个复合码序列；然后用这个复合码序列去控制载波的相位，从而获得 DSSS 信号。

DSSS 又称为噪声调制扩展，利用了通信中的“废物”噪声，窄带信号通过噪声扩展到相当宽的频道上，数据流比特和噪声比特结合成了更宽的信号，接收双方只有知道承载的噪声特性才能分析出有效信号。

1999 年，人们又引入了 OFDM 和 HR-DSSS 两种新的扩频技术。

**1）正交频分复用技术（Orthogonal Frequency Division Multiplexing，OFDM）。**

OFDM 是一种无线环境下的高速传输技术。OFDM 技术的主要思想就是在频域内将给定信道分成许多正交子信道，在每个子信道上使用一个子载波进行调制，且各子载波并行传输。通俗地讲就是 OFDM 使用了多个频率，在 52 个频率中，48 个用于数据，4 个用于同步。由于在 OFDM 的传输过程中可能会同时使用多个不同的频率，这类工作特性说明 OFDM 也是一种扩频技术。

**2）高速直接序列扩频（High Rate Direct Sequence Spread Spectrum，HR-DSSS）。**

高速直接序列扩频是另一种扩频技术，使得在 2.4GHz 频段内达到了 11Mb/s 的速率。HR-DSSS 采用了补码键控（CCK）等调制技术。

2. IEEE 802.11 系列标准

IEEE 802.11 由 IEEE 802.11 工作组制定，该工作组成立于 1990 年，是一个专门研究无线 LAN 技术、开发无线局域网物理层协议和 MAC 层协议的组织。IEEE 在 1997 年推出了 802.11 无线局域网（Wireless LAN）标准，经过多年的补充和完善形成了一个系列（即 802.11 系列）标准。目前，该系列标准已经成为无线局域网的主流标准。

802.11 系列标准主要有 4 个子标准，具体如表 8-1 所示。

表 8-1　802.11 系列标准

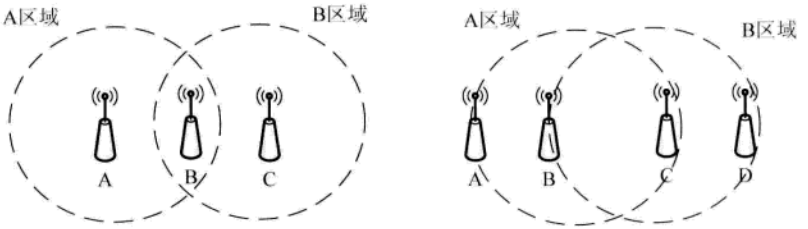
| 标准 | 运行频段 | 主要技术 | 数据速率 |
| --- | --- | --- | --- |
| 802.11 | 2.400～2.483GHz | DBPSK、DQPSK | 1Mb/s 和 2Mb/s |
| 802.11a | 5.150～5.350GHz、5.725～5.850GHz，与 802.11b/g 互不兼容 | OFDM 调制技术 | 54Mb/s |
| 802.11b | 2.400～2.483GHz，与 802.11a 互不兼容 | CCK 技术 | 11Mb/s |
| 802.11g | 2.400～2.483GHz | OFDM 调制技术 | 54Mb/s |
| 802.11n | 支持双频段，兼容 802.11b 与 802.11a 两种标准 | MIMO（多进多出）与 OFDM 技术 | 300～600Mb/s |

- 多进多出（Multiple Input Multiple Output，MIMO）技术

发射端和接收端都采用多个天线（或阵列天线）和多个通道。只要其发射端和接收端都采用了多个天线（或天线阵列）就构成了一个无线 MIMO 系统。MIMO 无线通信技术采用空时处理技术进行信号处理，在多路径环境下，无线 MIMO 系统可以极大地提高频谱利用率，增加系统的数据传输速率。MIMO 技术非常适用于室内环境下的无线局域网系统使用。采用 MIMO 技术的无线局域网系统在室内环境下的频谱效率可以达到 20～40b/s/Hz，而使用传统无线通信技术在移动蜂窝中的频谱效率仅为 1～5b/s/Hz，在点到点的固定微波系统中也只有 10～12b/s/Hz。

3. IEEE 802.11MAC 层协议

IEEE 802.11 采用了类似于 802.3 CSMA/CD 协议的载波侦听多路访问/冲突避免协议（Carrier Sense Multiple Access/Collision Avoidance，CSMA/CA），之所以不采用 CSMA/CD 协议的原因有两点：①无线网络中，接收信号的强度往往远小于发送信号，因此要实现碰撞的花费过大；②隐蔽站（隐蔽终端问题），并非所有站都能听到对方，如图 8-2（a）所示。而暴露站的问题是检测信道忙碌但未必影响数据发送，如图 8-2（b）所示。




（a）A、C同时向B发送信号，发送碰撞　　（b）B向A发送信号，避免碰撞，阻止C向D发送数据

图 8-2　隐蔽站和暴露站问题

因此，CSMA/CA 就是减少碰撞，而不是检测碰撞。

CSMA/CA 的 MAC 层分为 DCF 和 PCF 两层。

（1）分布协调功能（Distributed Coordination Function，DCF）。DCF 没有中心控制，通过争用信道获取信道信息发送权，用于支持突发式通信。

（2）点协调功能（Point Coordination Function，PCF）。PCF 选择接入 AP 集中控制 BSS，支持多媒体应用。

为了避免碰撞，802.11 提出帧间隔（InterFrame Space，IFS）。帧间隔的长短取决于发送帧的类型。优先级高的 IFS 时间短，反之则长。802.11 规定了三种常用 IFS，如表 8-2 所示。

表 8-2　802.11 的各类帧间隔

| 类别 | 定义 | 长度 | 优先级 | 适用范围 |
|---|---|---|---|---|
| SIFS | 短帧间间隔 | 最短 | 最高 | 适用 ACK、CTS 帧、过长 MAC 帧后分片数据帧 |
| PIFS | 点协调帧间间隔 | 适中（SIFS+1 个时隙时间） | 中 | 使用点协调 PCF 方式时 |
| DIFS | 分布协调功能帧间间隔 | 最长（SIFS+2 个时隙时间） | 低 | 使用分布式协调 DCP 方式时 |

CSMA/CA 算法如下：

（1）若站点最初有数据需要发送，并且检测发现传输信道处于空闲状态，则等待时间 DIFS 后发送数据帧。

（2）否则，站点就执行 CSMA/CA 协议的退避算法。期间如果检测到信道忙，就暂停运行退避计时算法。只要信道空闲，退避计时器就继续运行退避计时算法。

（3）当退避计算机时间减少到零时，站点不管信号是否忙都送整个数据帧并等待确认。

（4）发送站收到确认就知道已发送的帧完成。这时如果要发送第二帧，就要从步骤 2 开始，执行 CSMA/CA 退避算法，随机选定一段退避时间。

若发送站在规定时间内没有收到确认帧 ACK 就必须重传，再次使用 CSMA/CA 协议争用接入信道，直到收到确认，或者经过若干次失败放弃传送。

**注意**：发送第一个数据帧时可以不使用退避算法，其余情况都需要使用退避算法。

## 8.2 无线局域网安全

### 8.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：WEP、IEEE 802.11i、WLAN 用户通过 RADIUS 服务器登录的过程。

### 8.2.2 知识点精讲

1. WEP

802.11b 定义了无线网的安全协议（Wired Equivalent Privacy，WEP）。有线等效保密（WEP）协议是对在两台设备间无线传输的数据进行加密的方式，用以防止非法用户窃听或侵入无线网络。WEP 加密和解密使用同样的算法和密钥。WEP 采用的是 RC4 算法，使用 40 位或 64 位密钥，有些厂商将密钥位数扩展到 128 位（WEP2）。由于科学家找到了 WEP 的多个弱点，于是在 2003 年被淘汰。

2. IEEE 802.11i

Wi-Fi 保护接入（Wi-Fi Protected Access，WPA）是新一代的 WLAN 安全标准，该协议采用新的加密协议并结合 802.1x 实现访问控制。在数据保密方面定义了三种加密机制，具体如表 8-3 所示。

表 8-3 WPA 的三种加密机制

| 简写 | 全称 | 特点 |
| --- | --- | --- |
| TKIP | Temporal Key Integrity Protocol | 使用 WEP 机制的 RC4 加密，可通过升级硬件或驱动方式来实现 |
| CCMP | Counter-Mode/CBC-MAC Protocol | 使用 AES（Advanced Encryption Standard）加密和 CCM（Counter-Mode/CBC-MAC）认证，该算法对硬件要求较高，需要更换硬件 |
| WRAP | Wireless Robust Authenticated Protocol | 使用 AES 加密和 OCB 加密 |

3. WLAN 用户通过 RADIUS 服务器登录的过程

WLAN 用户通过 RADIUS 服务器登录的过程：

（1）由无线工作站上的认证客户端发出认证请求。

（2）AP 上的认证系统接收之后交给 RADIUS 服务器进行认证。

（3）通过认证之后对该用户进行授权，并且返回认证成功信息给认证系统。

（4）认证系统打开该用户的数据通道并允许其进行数据传输。

## 8.3 无线局域网配置

### 8.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：家庭无线路由器中的设置。

### 8.3.2 知识点精讲

无线路由器是具有无线接入功能的路由器，是 AP 和路由器的结合。无线路由器具有 AP 所具有的 DHCP 分配、VPN、WPA 加密功能，还具有路由器的路由、NAT、ADSL 接入、802.1x 认证、PPPOE 等功能。目前，无线路由器还包括了多个端口交换机，可以连接有线网卡的计算机。

建立一个家庭无线局域网使得计算机不但能够连接因特网，而且 WLAN 内部还可以直接通信，合适的组网方案是“无线路由器+无线网卡”方式。这里以某无线路由器为例，介绍无线路由器的简单设置。

（1）安全协议选择。

在无线路由设备中可以看到各种安全模式的选择（如图 8-3 所示）和各类加密规则（如图 8-4 所示）。

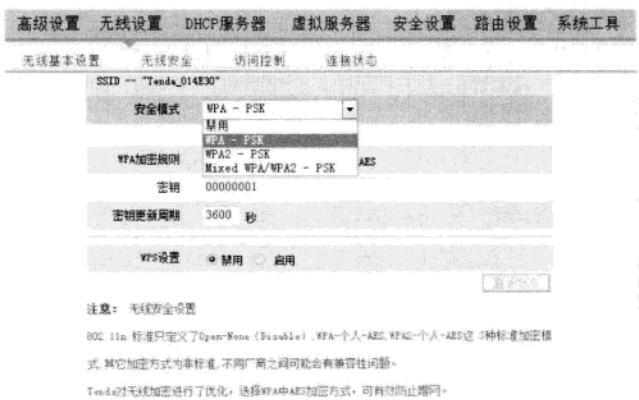



图 8-3 无线路由器中各类安全模式的选择

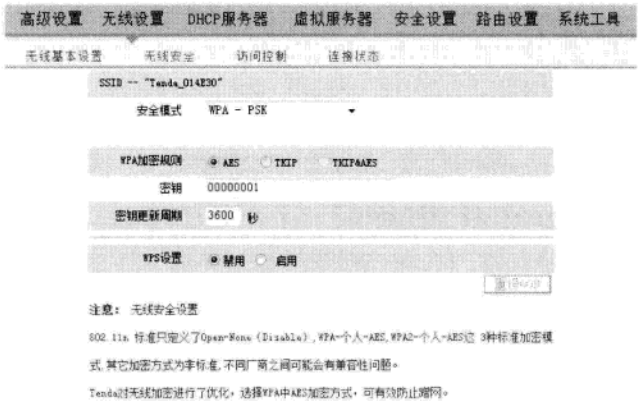



图 8-4　无线路由器中各类加密规则

这里可以发现，由于该路由器较新，已经没有 WEP 的选项了。同时给出，如果采用 802.11n 标准，只能选择禁用、WPA-个人-AES、WPA2-个人-AES 这 3 种标准加密模式。

WPA-PSK 后面的 PSK 表示用于家庭和小型办公室网络，每个用户都有同样的密码口令。WPA-PSK 也叫做 WPA-Personal（WPA 个人）。WPA-PSK 使用 TKIP 或 AES 加密方法将无线设备和接入点联系起来，WPA2-PSK 使用 AES 加密方法将无线设备和接入点联系起来。PSK 方式是预先共享密钥，长度大于 8 且小于 63。

（2）基本设置。

无线路由器的基本设置界面如图 8-5 所示。

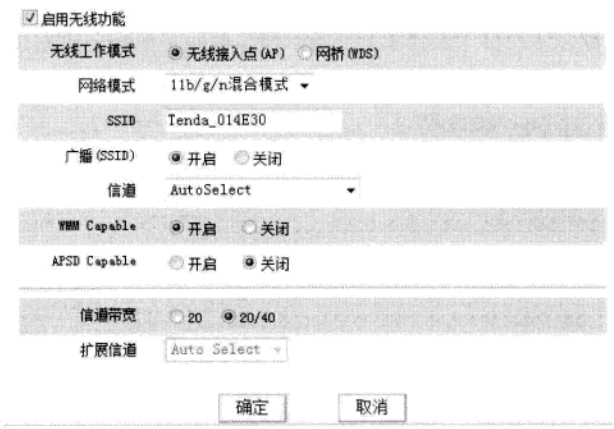



图 8-5　无线路由器的基本配置界面

- 网络模式：选择 802.11 协议族。
- SSID：无线网络中所有设备共享的网络名称。

- 广播（SSID）：当无线客户端在本地区域调查要关联的无线网络时，它们将通过路由器检测 SSID 广播。如果选中，路由器将向所有的无线主机广播自己的 SSID 号。
- 信道：可以选择 1～13 任何一个信道或是自动模式，尽可能选择当前区域使用比较少的信道以避免干扰。
- WMM Capable：802.11e 标准的一个子集。WMM 允许无线通信根据数据类型定义一个优先级范围。时间敏感的数据（如视频/音频数据）将比普通数据有更高的优先级。为了使 WMM 功能工作，无线客户端必须也支持 WMM。开启时可以提高无线多媒体数据的传输性能。
- APSD Capable：自动省电模式功能。
- 扩展信道：用于确定 11n 模式时本网络工作的频率段。

（3）客户端过滤。

路由器可以设置简单的客户端过滤，客户端过滤是基于 IP 地址的，具体如图 8-6 所示。

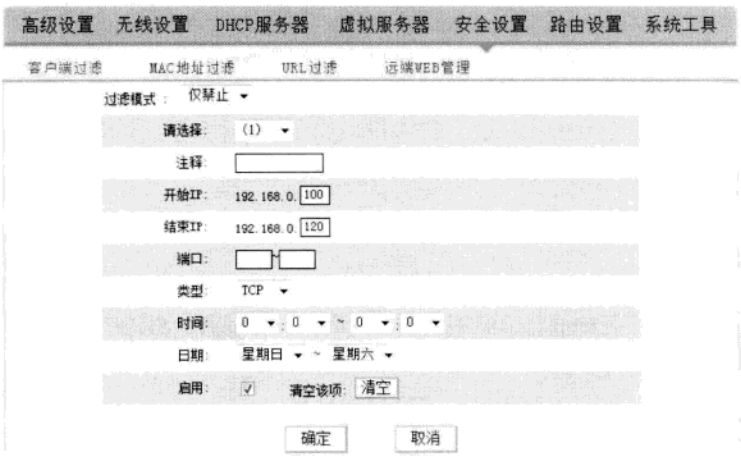



图 8-6　基于客户端的过滤

过滤模式可以选择：禁用、仅禁止、仅允许。其中，“禁用”表示不开启过滤；“仅禁止”表示仅禁止条目内的 IP 或 IP 段访问网络；“仅允许”表示仅允许条目内的 IP 或 IP 段访问网络。时间设置为 0:0～0:0 表示全部时间段。本例表示只有 IP 地址为 192.168.0.100～192.168.0.120 的主机不能访问本路由器和外网。

（4）MAC 地址过滤。

路由器可以设置基于 MAC 地址的过滤，具体如图 8-7 所示。

过滤模式可以选择：禁用、仅禁止、仅允许。其中，“禁用”表示不开启过滤；“仅禁止”表示仅禁止条目内的 MAC 访问网络；“仅允许”表示仅允许条目内的 MAC 访问网络。时间设置为 0:0～0:0 表示全部时间段。本例表示只有 MAC 地址为 00:11:22:33:44:55 的主机不能访问本路由器和外网。

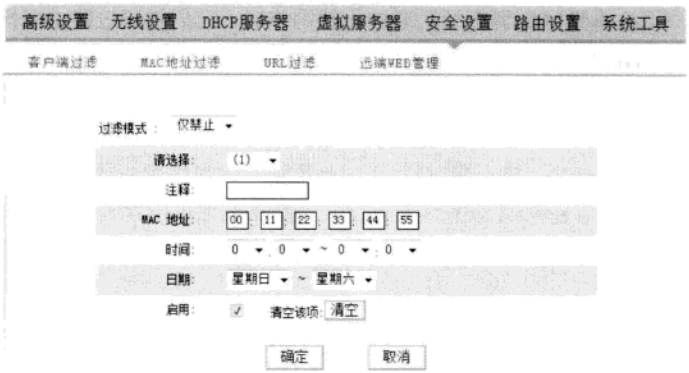



图 8-7　基于 MAC 地址的过滤

## 8.4　3G

### 8.4.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：3G 技术、4G 技术。

### 8.4.2　知识点精讲

码分多址（Code-Division Multiple Access，CDMA）技术是近年来在数字移动通信进程中出现的一种先进的无线扩频通信技术，其具有频谱利用率高、话音质量好、容量大、覆盖广等特点。CDMA 系统中使用的多路复用技术是码分多址。

目前，世界三大 3G 标准是 CDMA 2000、WCDMA、TD-SCDMA。

（1）CDMA 2000。

CDMA 2000 就是第三代 CDMA，适用于 3G CDMA 的 TIA 规范称为 IS-2000，也就是 CDMA 2000。目前被广为接纳与使用的 CDMA 2000 1x EV-DO Rev.A 系统理论上能提供下载和上行峰值速率分别为 3.1Mbit/s 和 1.8Mbit/s 的无线数据带宽，但在实际应用中，运营商一般不会提供全部的带宽。国内主导运营商是中国电信。

（2）WCDMA。

宽带码分多址存取（Wideband CDMA，WCDMA）可支持 384kb/s～2Mb/s 的数据传输速率。国内主导运营商是中国联通。

（3）TD-SCDMA。

时分同步的码分多址技术（Time Division-Synchronous Code Division Multiple Access，TD-SCDMA）是中国提出与自主主导的 3G 标准，TD-SCDMA 的实际网络速度可达 384kb/s。国内主导运营商是中国移动。

3GPP 长期演进技术（3GPP Long Term Evolution，3GPP LTE）为第三代合作伙伴计划（3GPP）标准，使用 OFDM 的射频接收技术，以及 2×2 和 4×4 MIMO 的分集天线技术规格。LTE 是 GSM 超越 3G 和 HSDPA 阶段、迈向 4G 的进阶版本。LTE 也被俗称为 3.9G。2010 年 12 月 6 日，国际电信联盟把 LTE 正式称为 4G。

# 第 3 学时　存储技术基础

第 2 天的第 3 学时主要学习存储相关知识。如今，数据变得越来越重要，数据量变得越来越巨大，因此存储海量数据、安全保护数据、出现问题及时恢复数据是网工和网管必备的技能。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 0～3 分之间。存储知识的考察主要集中在上午的考试中。本章考点知识结构图如图 9-1 所示。


图 9-1　考点知识结构图

## 9.1　RAID

### 9.1.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：RAID 技术。

### 9.1.2　知识点精讲

独立磁盘冗余阵列（Redundant Array of Independent Disk，RAID）是由美国加利福尼亚大学伯克莱分校于 1987 年提出的，利用一个磁盘阵列控制器和一组磁盘组成一个可靠、高速的大容量的逻辑硬盘。

RAID 分为很多级别，常见的 RAID 如下：

（1）RAID0。

无容错设计的条带磁盘阵列（Striped Disk Array without Fault Tolerance）。数据并不是保存在一个硬盘上，而是分成数据块保存在不同驱动器上。因为将数据分布在不同驱动器上，所以数据吞吐率大大提高。如果是 **n 块硬盘，则读取相同数据时间减少为 1/n**。由于**不具备冗余技术**，如果坏了一块盘，则阵列数据全部丢失。实现 RAID0 至少需要 2 块硬盘。

（2）RAID1。

磁盘镜像，可并行读数据，由于在不同的两块磁盘写入相同数据，写入数据比 RAID0 慢点。安全性最好，但空间利用率为 50%，利用率最低。实现 RAID1 至少需要 2 块硬盘。

（3）RAID2。

使用了海明码校验和纠错。将数据条块化分布于不同硬盘上，现在几乎不再使用。实现 RAID2 至少需要 2 块硬盘。

（4）RAID3。

使用单独的一块校验盘进行奇偶校验。**磁盘利用率=n-1/n**，其中 n 为 RAID3 中的磁盘总数。实现 RAID3 至少需要 2 块硬盘。

（5）RAID5。

具有独立的数据磁盘和分布校验块的磁盘阵列，无专门的校验盘。RAID5 常用于 I/O 较频繁的事务处理上。RAID5 可以为系统提供数据安全保障，虽然可靠性比 RAID1 低，但是磁盘空间利用率要比 RAID1 高。RAID5 具有和 RAID0 近似的数据读取速度，只是多了一个奇偶校验信息，写入数据的速度比对单个磁盘进行写入操作的速度稍慢。**磁盘利用率=n-1/n**，其中 n 为 RAID3 中的磁盘总数。实现 RAID5 至少需要 3 块硬盘。

（6）RAID6。

具有独立的数据硬盘与两个独立的分布校验方案，即存储两套奇偶校验码。因此安全性更高，但构造更复杂。磁盘**利用率=n-2/n**，其中 n 为 RAID3 中磁盘总数。实现 RAID6 至少需要 4 块硬盘。

（7）RAID10。

高可靠性与高性能的组合。RAID10 是建立在 RAID0 和 RAID1 基础上的，即为一个条带结构加一个镜像结构，这样即利用了 RAID0 极高的读写效率，又利用了 RAID1 的高可靠性。磁盘利用率为 50%。实现 RAID10 至少需要 4 块硬盘。

## 9.2 NAS 和 SAN



### 9.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：NAS、SAN。

### 9.2.2 知识点精讲

1. 网络附属存储（Network Attached Storage，NAS）

NAS 采用独立的服务器，单独为网络数据存储而开发的一种文件服务器来连接所有的存储设备。数据存储至此不再是服务器的附属设备，而成为网络的一个组成部分。

2. 存储区域网络及其协议（Storage Area Network and SAN Protocols，SAN）

SAN 是一种专用的存储网络，用于将多个系统连接到存储设备和子系统。SAN 可以被看作是负责存储传输的后端网络，而前端的数据网络负责正常的 TCP/IP 传输。作为一种新的存储连接拓扑结构，光纤通道为数据访问提供了高速的访问能力，它被设计用来代替现有的系统和存储之间的 SCSI I/O 连接。SAN 可以分为 FC SAN 和 IP SAN。

# 第 4 学时　网络规划与设计

第 2 天的第 4 学时主要学习网络规划与设计相关知识。作为网络工程师，在实际项目中需要从宏观角度去设计网络，能知道交换机、路由器、防火墙等设备应处于什么位置，什么时候能排上用场，网络设计的流程如何。根据历年考试的情况来看，网络规划与设计知识的考查主要集中在上午考试中，下午考试偶尔考到，一旦出现就是一道 15 分的大题。每次考试涉及相关知识点的分值一般在 0～3 分之间，偶尔会出现 15 分大题。本章考点知识结构图如图 10-1 所示。


图 10-1　考点知识结构图

## 10.1　网络生命周期

### 10.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：五阶段周期模型。

### 10.1.2　知识点精讲

网络生命周期就是网络系统从思考、调查、分析、建设到最后淘汰的总过程。常见的网络生命周期是五阶段周期，该模型分为 5 个阶段：需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段，如图 10-2 所示。

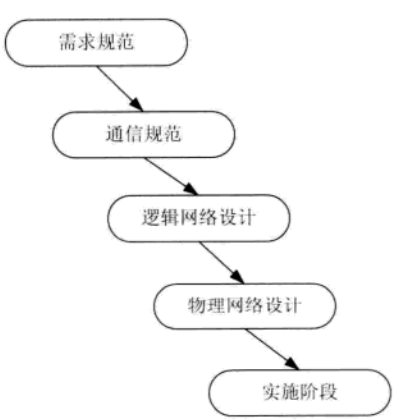



图 10-2　五阶段周期模型

（1）需求规范阶段的任务就是进行网络需求分析。

（2）通信规范阶段的任务就是进行网络体系分析。

（3）逻辑网络设计阶段的任务就是确定逻辑的网络结构

（4）物理网络设计阶段的任务就是确定物理的网络结构。

（5）实施阶段的任务就是进网络设备安装、调试及网络运行时的维护工作。

## 10.2 网络需求分析

### 10.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：需求分析的内容、网络工程文档的编制。

### 10.2.2 知识点精讲

需求分析阶段就是分析现有网络，与用户从多个角度做深度交流，最后得到比较全面的需求。需求分析阶段的主要工作内容（即了解的各类需求）如下：

功能需求：用户和用户业务具体需要的功能。

应用需求：用户需要的应用类型、地点和网络带宽的需求；对延迟的需求；吞吐量需求。

计算机设备需求：主要是了解各类PC机、服务器、工作站、存储等设备以及运行操作系统的需求。

网络需求：网络拓扑结构需求、网络管理需求、资源管理需求、网络可扩展的需求。

安全需求：可靠性需求、可用性需求、完整性需求、一致性需求。

需求分析几点注意事项：任何网络都不可能是一张能够满足各项功能需求的万能网；采用合适的、而不是最先进的网络设备，获得合适的、而不是最高的网络性能；网络需求分析不能脱离用户、应用系统等现实因素；考虑网络的扩展性，极大地保护投资。

需求分析完毕后需要编制需求说明书，这是一类网络工程文档。实际上，网络工程的每个阶段完成后都需要生成相关的项目文档。网络工程文档的编制在网络项目开发工作中占有突出的地位，是设计人员在一定阶段的工作成果和结束标识，有助于提高网络规划人员的设计效率。按照规范要求生成一套文档的过程就是按照网络分析与设计规范完成网络项目分析与设计的过程。

## 10.3 通信规范

### 10.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：通信规范分析任务、80/20规则、20/80规则。

### 10.3.2 知识点精讲

1. 通信规范分析任务

通信规范分析就是通过分析网络通信模式和网络的流量特点，发现网络的关键点和瓶颈，为逻辑网络设计工作提供有意义的参考和模型依据，从而避免了设计的盲目性。

通信规范分析任务包含：

（1）通信模式分析。

对通信模式进行分析，确定现有网络中的网络通信模式。通信模式有对等通信模式、客户机/服务器（C/S）通信模式、浏览器/服务器通信模式、分布式计算通信模式四种。

（2）通信边界分析。

确定局域网通信边界（广播域、冲突域），确定广域网通信边界（自治区域、路由算法区域和局域网交界），虚拟专用网络通信边界。

（3）通信流分布分析。

通信流分布分析有时需要汇总所有单个信息流量的大小。

【例 10-1】假设生产管理网络系统采用 B/S 工作方式，经常上网的用户数为 300 个，每个用户每分钟产生 2 个事务处理任务，平均事务量大小为 0.1MB，则这个系统需要的信息传输速率为多少？

需要的传输速率=用户数×每单位时间产生事务的数量×事务量大小　　（10-1）

$$需要的传输速率=300\times\frac{2}{60}\times0.1\times8=8Mb/s$$

计算单个信息流量的方式比较复杂，汇总就更加麻烦，因此可以引入一些简单规则，如 80/20 规则、20/80 规则等。

2. 80/20 规则

对于一个网段内部总的通信流量，80%的流量流转在网段内部，而剩下的 20%则是网段外部流量。这个规则适用于内部交流较多而外部访问较少的网络。

3. 20/80 规则

对于一个网段内部总的通信流量，20%的流量流转在网段内部，而剩下的 80%则是网段外部流量。这个规则适用于外部联系较多而内部联系较小的网络，可以较大限度地满足用户的远程联网需求，这个规则适用的网络允许存在具有特殊外部应用的网段。

通信规范分析完毕的同时，网络规划人员需要完成通信规范说明书的编写。

## 10.4 逻辑网络设计

### 10.4.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：分层化网络设计模型、网络设计原则。

### 10.4.2 知识点精讲

逻辑网络设计就是根据需求分析，依据用户分布、特点、数量和应用需求等形成符合的逻辑网络结构，大致得出网络互联特性及设备分布，但不涉及具体设备和信息点的确定。简而言之，逻辑网络设计阶段的任务是根据需求规范和通信规范实施资源分配和安全规划。

逻辑网络设计工作主要包括网络结构的设计、物理层技术选择、局域网技术选择与应用、广域网技术选择与应用、地址设计和命名模型、路由选择协议、网络管理和网络安全等。

逻辑网络设计的一个重要概念是分层化网络设计模型。

1. 分层化网络设计模型

分层化网络设计模型可以帮助设计者按层次设计网络结构，并对不同层次赋予特定的功能，为不同层次选择正确的设备和系统。三层网络模型是最常见的分层化网络设计模型，通常划分为接入层、汇聚层和核心层。

（1）接入层。

网络中直接面向用户连接或访问网络的部分称为接入层，接入层的作用是允许终端用户连接到网络，因此接入层交换机具有低成本和高端口密度特性。接入层的其他功能有用户接入与认证、二三层交换、QOS、MAC 地址过滤。

（2）汇聚层。

位于接入层和核心层之间的部分称为汇聚层，汇聚层是多台接入层交换机的汇聚点，它必须能够处理来自接入层设备的所有通信流量，并提供到核心层的上行链路，因此汇聚层交换机与接入层交换机比较需要更高的性能、更少的接口和更高的交换速率。汇聚层的其他功能有访问列表控制、VLAN 间的路由选择执行、分组过滤、组播管理、QOS、负载均衡、快速收敛等。

（3）核心层。

核心层的功能主要是实现骨干网络之间的优化传输，骨干层设计任务的重点通常是冗余能力、可靠性和高速的传输。网络核心层将数据分组从一个区域高速地转发到另一个区域，快速转发和收敛是其主要功能。网络的控制功能最好尽量少在骨干层上实施。核心层一直被认为是所有流量的最终承受者和汇聚者，所以对核心层的设计及网络设备的要求十分严格。核心层的其他功能有链路聚合、IP 路由配置管理、IP 组播、静态 VLAN、生成树、设置陷阱和报警、服务器群的高速连接等。

2. 网络设计原则

网络设计原则有：

（1）考虑设备先进性，但不一定必须采用最先进的设备，需要考虑合理性。

（2）网络系统设计应该采用开放的标准和技术。

（3）网络设计考虑近期目标和远期目标，要考虑其扩展性，为将来扩展考虑。

（4）结合实际情况进行设计考虑。例如在进行金融业务系统的网络设计时，应该优先考虑高可用性原则；在进行小型企业的网络设计时，应该优先考虑经济性原则。

逻辑网络设计完成时需要生成逻辑设计文档。

## 10.5 物理网络设计

### 10.5.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：设备选择原则、综合布线。

### 10.5.2 知识点精讲

在网络系统设计过程中，物理网络设计阶段的任务是依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境。

1. 设备选择原则

物理网络阶段的设备选择比较关键。下面介绍分层模型下的设备选择原则，具体如表 10-1 所示。

表 10-1 分层模型下设备选择原则

| 层次 | 设备选用原则 |
| --- | --- |
| 接入层 | 提供多种固定端口数量搭配供组网选择，可堆叠、易扩展；在满足技术性能要求的基础上，最好价格便宜、使用方便、即插即用、配置简单；支持二层交换和高带宽链路；支持 ACL 和安全接入；具备一定的网络服务质量、控制能力及端到端的 QOS 可选；支持三层交换、远程管理和 SNMP |
| 汇聚层 | 提供多种固定端口数量搭配供组网选择，可堆叠、易扩展；在满足技术性能要求的基础上，最好价格便宜、使用方便、即插即用、配置简单；支持 IP 路由，提供高带宽链路，保证高速数据转发；具备一定的网络服务质量、控制能力及端到端的 QOS；提供负载均衡的自动冗余链路、远程管理和 SNMP |
| 核心层 | 数据的高速交换、高稳定性；保证设备的正常运行和管理；支持提供数据负载均衡和自动冗余链路、VLAN 定义与下发、生成树 |

网络设备选型原则还要考虑以下几点：

- 所有网络设备尽可能选取同一厂家的产品，这样在设备可互连性、协议互操作性、技术支持、价格等方面都更有优势。
- 尽可能保留并延长用户对原有网络设备的投资，减少在资金投入上的浪费。
- 选择性能价格比高、质量过硬的产品，使资金的投入产出达到最大值。
- 根据实际需要进行选择。选择稍好的设备，尽力保留现有设备，或降级使用现有设备。
- 网络设备选择要充分考虑其可靠性。
- 厂商技术支持，即定期巡检、咨询、故障报修、备件响应等服务是否及时。
- 产品备件库，设备故障时是否能及时更换。

2. 综合布线

综合布线能支持话音、数据、图形图像应用的布线技术。综合布线支持 UTP、光纤、STP、同轴电缆等各种传输载体，能支持话音、图形、图像、数据多媒体、安全监控、传感等各种信息的传输。

综合布线系统由工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统、建筑群子系统 6 个部分组成，具体组成如图 10-3 所示。

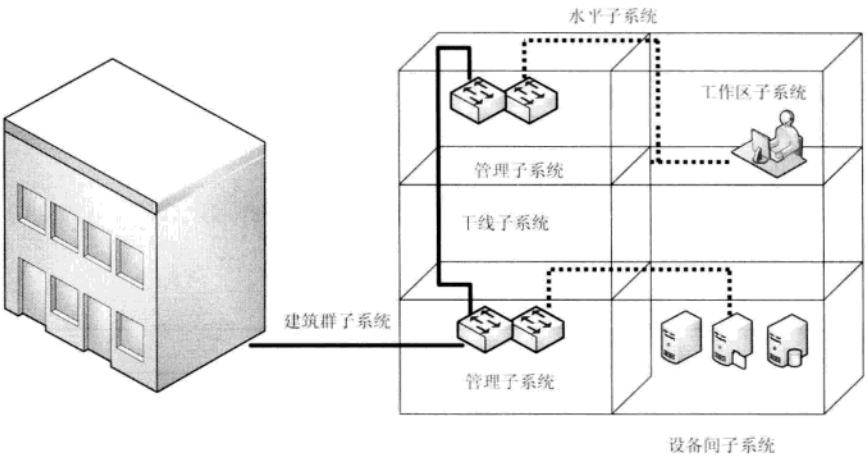



图 10-3　综合布线系统图

（1）干线子系统：是各水平子系统（各楼层）设备之间的互联系统。

（2）水平子系统：是各个楼层配线间中的配线架到工作区信息插座之间所安装的线缆。

（3）工作区子系统：是由终端设备连接到信息插座的连线组成的，包括连接线和适配器。工作区子系统中信息插座的安装位置距离地面的高度为 30～50cm；如果信息插座到网卡之间使用无屏蔽双绞线，布线距离最大为 10m。

（4）设备间子系统：位置处于设备间，并且集中安装了许多大型设备（主要是服务器、管理终端）的子系统。

（5）管理子系统：该系统由互相连接、交叉连接和配线架、信息插座式配线架及相关跳线组成。

（6）建筑群子系统：将一个建筑物中的电缆、光缆和无线延伸到建筑群的另外一些建筑物中的通信设备和装置上。建筑群之间往往采用单模光纤进行连接。

最后一个阶段是实施阶段，该阶段的作用是测试（线路测试、设备测试）、运行和维护，如布线实施后需要进行测试。

在测试线路的主要指标中，近端串扰是指一对相邻的另一对线通过电磁感应所产生的偶合信号，衰减是由于集肤效应、绝缘损耗、阻抗不匹配、连接电阻等因素造成信号沿链路传输时的损失。

# 第 5 学时　计算机硬件知识

第 2 天的第 5 学时主要学习计算机硬件的相关知识点。计算机硬件知识涉及的面比较广，内容比较多。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 4～7 分之间。这部分知识点的考察主要集中在上午的考试中。本章考点知识结构图如图 11-1 所示。

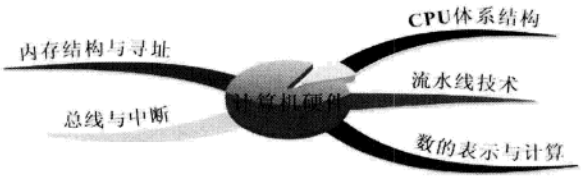



图 11-1　考点知识结构图

## 11.1　CPU 体系结构

### 11.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：CPU 体系结构、指令集、各种主要寄存器的作用等。历年考试中基本寄存器的作用考查得比较多。

### 11.1.2　知识点精讲

CPU 是中央处理单元（Central Processing Unit）的缩写，也称为微处理器（Microprocessor）。CPU 是计算机中最核心的部件，主要由运算器、控制器等构成。

控制器由程序计数器 PC、指令寄存器 IR、地址寄存器 AR、数据寄存器 DR、指令译码器等组成。

（1）程序计数器 PC：用于指出下条指令在主存中的存放地址，CPU 根据 PC 的内容去主存处取得指令。由于程序中的指令是按顺序执行的，所以 PC 必须有自动增加的功能，也就是指向下一条指令的地址。

（2）指令寄存器 IR：用于保存当前正在执行的这条指令的代码。

（3）地址寄存器 AR：用于存放 CPU 当前访问的内存单元地址。

（4）数据寄存器 DR：用于暂存从内存储器中读出或写入的指令或数据。

（5）指令译码器：用于对获取的指令进行译码，产生该指令操作所需要的一系列微操作信号，以控制计算机各部件完成该指令。

运算器由算术逻辑单元 ALU、通用寄存器、数据暂存器等组成、程序状态字寄存器，它接收

从控制器送来的命令并执行相应的动作，主要负责对数据的加工和处理。

（1）算术逻辑单元 ALU：用于进行各种算术逻辑运算。

（2）通用寄存器：用来存放操作数、中间结果和各种地址信息的一系列存储单元。

（3）数据暂存器：用来暂存从主存储器读出的数据，这个数据不能存放在通用寄存器中，否则会破坏其原有的内容。

（4）程序状态字寄存器 PSW：用于保留与算术逻辑运算指令或测试指令的结果对应的各种状态信息。移位器在 ALU 输出端用暂存器来存放运算结果，具有对运算结果进行移位运算的功能。

1. CPU 指令的执行

计算机中的一条指令就是机器语言的一个语句，由一组二进制代码来表示。一条指令由两部分构成：操作码和地址码，如图 11-2 所示。


图 11-2　计算机指令结构

其中操作码用于说明指令的操作性质及功能；地址码用于说明操作数的地址。一条指令必须有一个操作码，但有可能包含几个地址码。CPU 为了执行任何给定的指令必须用指令译码器对操作码进行测试，以便识别所要求的操作。指令寄存器中操作码字段的输出就是指令译码器的输入。操作码经过译码后即可向操作控制器发出具体操作的对应信号。

CPU 中指令的执行过程分为以下 3 个步骤：

（1）取指令。

根据程序计数器 PC 提供的指令地址从主存储器中读取指令，送到主存数据缓冲器中。然后再送往 CPU 内的指令寄存器 IR 中，同时改变程序计数器的内容，使其指向下一条指令地址或紧跟当前指令的立即数或地址码。

（2）取操作数。

如果是无操作数指令，则可以直接进入下一个过程；如果需要操作数，则根据寻址方式计算地址，然后到存储器中去取操作数；如果是双操作数指令，则需要两个取数周期来取操作数。

（3）执行操作。

根据操作码完成相应的操作，并根据目的操作数的寻址方式保存结果。

其中与操作紧密相关的是指令执行的周期，在指令执行过程中要清楚各个周期中机器所完成的工作。

- 取指周期：地址由 PC 给出，取出指令后，PC 内容自动递增。当出现转移情况时，指令地址在执行周期被修改。取操作数周期期间要解决的是计算操作数地址并取出操作数。
- 执行周期：执行周期的主要任务是完成由指令操作码规定的动作，包括传送结果及记录状态信息。执行过程中要保留状态信息，尤其是条件码要保存在 PSW 中。若程序出现转移，则在执行周期内还要决定转移地址的问题。因此，执行周期的操作对不同指令也不相同。
- 指令周期：将一条指令从取出到执行完成所需要的时间称为指令周期。

指令周期与机器周期和时钟周期的关系如下：指令周期是完成一条指令所需的时间，包括取指

令、分析指令和执行指令所需的全部时间。指令周期划分为几个不同的阶段，每个阶段所需的时间称为机器周期，又称为 CPU 工作周期或基本周期，一般来说与取指时间或访存时间是一致的。时钟周期是时钟频率的倒数，也可称为节拍脉冲，是处理操作的最基本单位。一个指令周期由若干个机器周期组成，每个机器周期又由若干个时钟周期组成。一个机器周期内包含的时钟周期个数决定于该机器周期内完成的动作所需的时间。一个指令周期包含的机器周期个数也与指令所要求的动作有关，如单操作数指令只需要一个取操作数周期，而双操作数指令需要两个取操作数周期。

2. CPU 指令系统

CPU 根据所使用的指令集可以分为 CISC 指令集和 RISC 指令集两种。

（1）复杂指令集（Complex Instruction Set Computer，CISC）处理器中，不仅程序的各条指令是顺序串行执行的，而且每条指令中的各个操作也是顺序串行执行的。顺序执行的优势是控制简单，但计算机各部分的利用率低，执行速度相对较慢。为了能兼容以前开发的各类应用程序，现在还在继续使用这种结构。

（2）精简指令集（Reduced Instruction Set Computer，RISC）技术是在 CISC 指令系统基础上发展起来的，实际上 CPU 执行程序时，各种指令的使用频率非常悬殊，使用频率最高的指令往往是一些非常简单的指令。因此 RISC 型 CPU 不仅精简了指令系统，而且还采用了超标量和超流水线结构，大大增强了并行处理能力。RISC 的特点是指令格式统一、种类比较少、寻址方式简单，因此处理速度大大提高。但是 RISC 与 CISC 在软件和硬件上都不兼容，当前中高档服务器中普遍采用 RISC 指令系统的 CPU 和 UNIX 操作系统。

这两种不同指令系统的主要区别在于以下几个方面：

（1）指令系统的指令数目。

通常 CISC 的 CPU 指令系统的指令数目要比同样功能的 RISC 的 CPU 指令数目多得多。

（2）编程的便利性。

CISC 系统的编程相对要容易一些，因为其可用的指令多，编程方式灵活。而 RISC 因为指令较少，要实现与 RISC 相同功能的程序代码一般编程量更大，源程序更长。

（3）寻址方式。

RISC 使用尽可能少的寻址方式以简化实现逻辑，提高效率；CISC 则使用较丰富的寻址方式来为用户编程提供灵活性。

（4）指令长度。

RISC 指令格式非常规整，绝大部分使用等长的指令，而 CISC 则使用可变长的指令。

（5）控制器复杂性。

正是因为 RISC 指令格式整齐划一，指令在执行时间和效率上相对一致，因此控制器可以设计得比较简单。

3. CPU 的主要性能指标

（1）主频。

主频也叫时钟频率，单位是 MHz（或 GHz），用来表示 CPU 的运算和处理数据的速度。主频

仅仅是 CPU 性能的一个方面，不能代表 CPU 的整体运算能力，但人们还是习惯于用主频来衡量 CPU 的运算速度。

（2）位和字长。

位：计算机中采用二进制代码来表示数据，代码只有 0 和 1 两种，无论是 0 还是 1，在 CPU 中都是 1“位”。

字长：计算机对 CPU 在单位时间内能一次处理的二进制数的位数称为字长。通常能一次处理 16bit 数据的 CPU 就叫 16 位的 CPU。

（3）缓存。

缓存是位于 CPU 与内存之间的高速存储器，通常其容量比内存小，但速度却比内存快，甚至接近 CPU 的工作速度。缓存主要是为了解决 CPU 运行速度与内存读写速度之间不匹配的问题。缓存容量的大小是 CPU 性能的重要指标之一。缓存的结构和大小对 CPU 速度的影响非常大。

通常 CPU 有三级缓存：一级缓存、二级缓存和三级缓存。

一级缓存（L1 Cache）是 CPU 的第一层高速缓存，分为数据缓存和指令缓存。受制于 CPU 的面积，L1 通常很小。

二级缓存（L2 Cache）是 CPU 的第二层高速缓存，按芯片所处的位置分为内部和外部两种。内部的芯片二级缓存运行速度与主频接近，而外部芯片的二级缓存运行速度则只有主频的 50%左右。L2 高速缓存容量也会影响 CPU 的性能，理论上芯片的容量是越大越好，但实际上会综合考虑成本与性能等各种因素，CPU 的 L2 高速缓存一般是 2～4MB。

三级缓存（L3 Cache）的作用是进一步降低内存延迟，提升大数据量计算时处理器的性能。因此在数值计算领域的服务器 CPU 上增加 L3 缓存可以在性能方面获得显著的效果。

## 11.2 流水线技术



### 11.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：流水线技术，流水线的效率，加速比等计算。

### 11.2.2 知识点精讲

流水线（Pipeline）是一种将指令分解为多个小的步骤，并让几条不同指令的各个操作步骤重叠，从而实现几条指令并行处理以加速程序运行速度的技术。因为计算机中的一个指令可以分解成多个小步骤，如取指令、译码、执行等。在 CPU 内部，取指令、译码和执行都是由不同的部件来完成的。因此在理想的运行状态下，尽管单条指令的执行时间没有减少，但是由多个不同部件同时工作，同一时间执行指令的不同步骤，从而使总执行时间极大地降低，甚至可以低至这个过程中最慢的那个步骤的处理时间。如果各个步骤的处理时间相同，则指令分解成多少个步骤，处理速度就

能提高到标准执行速度的多少倍。具体执行过程如下：

假设执行一条指令需要执行以下 3 个步骤：

（1）取指令：从内存中读取出指令。

（2）译码：将指令翻译出来，指出具体要执行什么动作。

（3）执行：将指令交给运算器运行出结果。

这 3 个步骤在 CPU 内部对应地需要 3 个执行部件，假设每个部件执行的时间均为 T。

若不采用流水线，则执行一条指令需要依次进行这 3 个步骤，总的执行时间为 3T，依此类推，要顺序执行 N 条指令，所需要的总时间就是 3T*N。这里可以看到，3 个部件在这个 3T 时间内总是只有一个部件在运行，其余三个部件处于闲置状态，显然这不是一种好的方法。

如图 11-3 所示可以看到，采用流水线执行方式，在第 1 个 T 时间内，第一条指令在取指令，其余两个部件空闲。在第 2 个 T 时间内，第 1 条指令已经完成取指令，直接交给第 2 个部件进行分析，同时取指令部件可以去取第 2 条指令。此时同时有两条指令在运行，其中只有执行部件空闲。在第 3 个 T 时间内，第 1 条指令可以直接进入执行部件执行，第 2 条指令直接进入分析部件分析，取指令部件可以去取第 3 条指令。此时 3 个部件都在工作，同时有 3 条指令在运行。

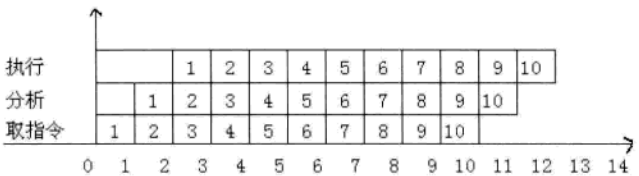



图 11-3 流水线时空图

依此类推，可以看到，每经过一个 T 时间，就会有一条指令执行完毕，因此执行 N 条指令的总时间是 3T+(n-1)×T，也就是第一条指令从开始执行到执行完毕的总时间是 3T，以后每隔一个 T 时间就会多完成一条指令。因此只要再过(n-1)×T 时间后，余下的 n-1 条指令都会执行完毕。从上面的分析还可以看出，在线性流水线中，流水线各段执行时间最长的那段变成了整个流水线的瓶颈。一般地，将其执行时间称为流水线的周期。所以执行的总时间主要取决于流水操作步骤中最长时间的那个操作。

可以据此得出：设流水线由 N 段组成，每段所需时间分别为 $\Delta t_i (1 \leqslant i \leqslant N)$，完成 M 个任务的实际时间可计算如下：$\sum_{i=1}^{n} \Delta t_i + (M-1)\Delta t_j$，其中 $\Delta t_j$ 为时间最长的那一段的执行时间。

【例 11-1】若指令流水线把一条指令分为取指、分析和执行三部分，且三部分的时间分别是 $t_{取指}=2ns$，$t_{分析}=2ns$，$t_{执行}=1ns$，则 100 条指令全部执行完毕所需的时间是多少？

从题中可以看出，三个操作中，执行时间最长的操作时间的是 T=2ns，因此总时间为(2+2+1)+(100-1)×2=5+198=203ns。

1. 流水线的性能指标

一种流水线处理方式的性能高低主要由吞吐率、效率和加速比这三个参数来决定。

（1）吞吐率。

吞吐率指的是计算机中的流水线在单位时间内可以处理的任务或执行指令的个数。

例 11-1 中执行 100 条指令的吞吐率可以表示为 $TP=\frac{N}{T}=\frac{100}{203\times10^{-9}}$，其中 N 表示指令的条数，T 表示执行完 N 条指令的时间。

（2）加速比。

加速比是指某一流水线采用串行模式的工作速度与采用流水线模式的工作速度的比值。加速比数值越大，说明这条流水线的工作安排方式越好。

例 11-1 中若串行执行 100 条指令的时间是 T1=5×100=500ns，采用流水线工作方式的时间 T2=203ns，因此加速比 R=T1/T2=500/203=2.463。

（3）效率。

效率是指流水线中各个部件的利用率。由于流水线在开始工作时存在建立时间，在结束时存在排空时间，各个部件不可能一直在工作，总有某个部件在某一个时间处于闲置状态。用处于工作状态的部件和总部件的比值来说明这条流水线的工作效率。

## 11.3 内存结构与寻址

### 11.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：存储器类型、内存容量计算、命中率的计算等。

### 11.3.2 知识点精讲



计算机中的存储器按用途大致可分为两类：主存储器和辅助存储器。主存储器也称为内存储器，辅助存储器也称外存储器。外存通常是磁性介质或光盘，能长期保存信息（如硬盘、磁带等），其速度相对内存而言要慢很多。近几年的网络工程师考试中，对外部的辅助存储器的相关概念和计算题已经很少考查，因此本节主要讨论内存储器。

1. 内存储器类型

在计算机中，存储器按照数据的存取方式可以分为五类。

（1）随机存取存储器（Random Access Memory，RAM）。

随机存取是指 CPU 可以对存储器中的数据随机地存取，与信息所处的物理位置无关。RAM 具有读写方便、灵活的特点，但断电后信息全部丢失，因此常用于主存和高速缓存中。

RAM 又可分为 DRAM 和 SRAM 两种。其中 DRAM 的信息会随时间的延长而逐渐消失，因此需要定时对其进行刷新来维持信息不丢失；SRAM 在不断电的情况下，信息能够一直保持而不丢失，也不需要刷新。

（2）只读存储器（Read Only Memory，ROM）。

ROM 也是随机存取方式的存储器，但 ROM 中的信息是固定在存储器内的，只可读出，不能修改，其读取的速度通常比 RAM 要慢一些。

（3）顺序存取存储器（Sequential Access Memory，SAM）。

SAM 只能按某种顺序存取，存取时间的长短与信息在存储体上的物理位置相关，所以只能用平均存取时间作为存取速度的指标。磁带机就是 SAM 的一种。

（4）直接存取存储器（Direct Access Memory，DAM）。

DAM 采用直接存取方式对信息进行存取，当需要存取信息时，直接指向整个存储器中的某个范围（如某个磁道）；然后在这个范围内顺序检索，找到目的地后再进行读写操作。DAM 的存取时间与信息所在的物理位置有关，相对 SAM 来说，DAM 的存取时间要更短。

（5）相联存储器（Content Addressable Memory，CAM）。

CAM 是一种基于数据内容进行访问的存储设备。当写入数据时，CAM 能够自动选择一个未使用的空单元进行存储；当读出数据时，并不直接使用存储单元的地址，而是使用该数据或该数据的一部分内容来检索地址。CAM 能对所有存储单元中的数据同时进行比较，并标记符合条件的数据以供读取。因为比较是并行进行的，所以 CAM 的速度非常快。

2. 高速缓存

在计算机存储系统的层次结构中，介于中央处理器和主存储器之间的高速小容量存储器和主存储器一起构成一级的存储器。高速缓冲存储器和主存储器之间信息的调度和传送是由硬件自动完成的。当 CPU 存取主存储器时，硬件首先自动对存取地址进行译码，以便检查主存中的数据是否在高速缓存中：若要存取的主存储器单元的数据已在高速存储器中，则称为命中，硬件就将存取主存储器的地址映射为高速存储器的地址并执行存取操作；若该单元不在高速存储器中，则称为脱靶，硬件将执行存取主存储器操作，并自动将该单元所在的主存储器单元调入高速存储器中的空闲存储单元中。

3. 命中率

高速缓存中，若直接访问主存的时间为 M 秒，访问高速缓存的时间为 N 秒，CPU 访问内存的平均时间为 L 秒，设命中率为 H，则满足下列公式：$L=M\times(1-H)+N\times H$。

【例 11-2】若主存读写时间为 30ns，高速缓存的读写时间为 3ns，平均读写时间为 3.27ns，则该高速缓存的命中率可以代入公式 $3.27=30\times(1-h)+3\times h$，解方程可知 H=0.99，即命中率为 99%。

4. 内存地址编址

编址也就是给“内存单元”编号，通常用十六进制数字表示，按照从小到大的顺序连续编排成为内存的地址。每个内存单元的大小通常是 8bit，也就是 1 个字节。内存容量与地址之间有如下关系：

内存容量=最高地址–最低地址+1

【例 11-3】若某系统的内存按双字节编址（每个字节 16bit），地址从 B5000H 到 DCFFFH 共有多少双字节？若用存储容量为 16K×8bit 的存储芯片构成该内存，至少需要多少片芯片？

这种题实际上是考察考生对内存地址表示的理解，属于套用公式的计算型题目。内存容量=DCFFF–B5000+1 就可以得出具体的容量大小，再除以 1024 化为 K，共有 160K×16bit。因为芯片是按照双字节编址的，而芯片的容量是 16K×8bit，所以只要 160×16/32×8=10 片才能实现。

## 11.4 数的表示与计算

### 11.4.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：原码、反码、补码等的基本概念及各种码的相关计算。

### 11.4.2 知识点精讲

如今在计算机中为了方便计算，数值并不是完全以真值形式的二进制码来表示。计算机中的数大致可以分为定点数和浮点数两类。所谓定点，就是指机器数中的小数点的位置是固定的。根据小数点固定的位置不同可以分为定点整数和定点小数。

- 定点整数：指机器数的小数点位置固定在机器数的最低位之后。
- 定点小数：指机器数的小数点位置固定在符号位之后，有效数值部分在最高位之前。

所谓的浮点数就是把一个数的有效数字和数的范围分别用存储单元存放，用这种数的范围和精度分别表示的方法表示的数的小数点位置是在一定范围内自由浮动的，因此将用这种表示方法表示的数称为浮点数。定点数在计算机中的主要表示方式有 3 种：原码、补码和反码，另外为了方便阶码的运算还定义了移码。

（1）原码。

用真实的二进制值直接表示数值的编码就叫原码。原码表示法在数值前面增加了一位符号位，通常用 0 表示正数，1 表示负数。8 位原码的表示范围是（-127～-0 +0～127）共 256 个。

定点整数的原码表示：

$$[X]_{原}=\begin{cases}X & 0\leqslant X<2^n\\ 2^n-X & -2^n<X\leqslant 0\end{cases}$$

定点小数的原码表示：

$$[X]_{原}=\begin{cases}X & 0\leqslant X<1\\ 1-X & -1<X\leqslant 0\end{cases}$$

【例 11-4】定点整数

$X_1=+1001$，则 $[X_1]_{原}=01001$

$X_2=-1001$，则 $[X_2]_{原}=11001$

【例 11-5】定点小数

$X_1$=+0.1001，则$[X_1]_{原}$= 01001

$X_2$ =-0.1001，则$[X_2]_{原}$= 11001

**注意**：用带符号位的原码表示的数在加减运算时可能会出现问题，如例 11-6。

【例 11-6】

$(1)_{10}-(1)_{10}=(1)_{10}+(-1)_{10}=(0)_{10}$ 可以转化为$(00000001)_{原}+(10000001)_{原}=(10000010)_{原}=(-2)$，显然这是不正确的。因此计算机通常不使用原码来表示数据。

（2）反码。

正整数的反码就是其本身，而负整数的反码则通过对其绝对值按位求反来取得。基本规律是：除符号位外的其余各位逐位取反就得到反码。反码表示的数和原码相同且一一对应。

定点整数的反码表示：

$$[X]_{反}=\begin{cases}X & 0\leqslant X<2^n\\ 2^{n+1}-1+X & -2^n<X\leqslant 0\end{cases}$$

定点小数的反码表示：

$$[X]_{反}=\begin{cases}X & 0\leqslant X<1\\ 2-2^{n-1}-X & -1<X\leqslant 0\end{cases}$$

【例 11-7】定点整数

$X_1$ = + 1001，则 $[X_1]_{反}$ = 01001

$X_2$ = -1001，则 $[X_2]_{反}$ = 10110

【例 11-8】定点小数

$X_1$=+0.1001，则$[X_1]_{反}$= 01001

$X_2$ =-0.1001，则$[X_2]_{原}$= 10110

**注意**：带符号位的负数在运算上也会出现问题，如例 11-9。

【例 11-9】

$(1)_{10}-(1)_{10}=(1)_{10}+(-1)_{10}=(0)_{10}$ 可以转化为$(00000001)_{反}+(11111110)_{反}=(11111111)_{反}=(-0)$，则结果是-0，也就是 0，但这样反码中就出现了两个 0：$+0(00000000)_{反}$与$-0(11111111)_{反}$。

（3）补码。

正数的补码与原码一样；负数的补码是对其原码（除符号位外）按各位取反，并在末位补加 1 而得到的。

定点整数的补码表示：

$$[X]_{补}=\begin{cases}X & 0\leqslant X<2^n\\ 2^{n+1}+X & -2^n\leqslant X<0\end{cases}$$

定点小数的补码表示：

$$[X]_{补}=\begin{cases}X & 0\leqslant X<1\\ 2+X & -1\leqslant X<0\end{cases}$$

【例 11-10】定点整数

$X_1=+1001$，则 $[X_1]_{补}=01001$

$X_2=-1001$，则 $[X_2]_{补}=10111$

【例 11-11】定点小数

$X_1=+0.1001$，则$[X_1]_{补}=01001$

$X_2=-0.1001$，则$[X_2]_{补}=10111$

上面反码的问题出现在(+0)和(-0)上，在现实计算中零是不区分正负的。因此计算机中引入了补码概念。负数的补码就是对反码加一，而正数不变。因此正数的原码、反码和补码都是一样的。在 8 位补码中，用(-128)代替了(-0)，所以 8 位补码的表示范围为(-128～0～127)共 256 个。因此(-128)没有相对应的原码和反码，这个要尤其注意，网络工程师考试往往就考这些特殊的数字。补码运算的例子如例 11-12。

【例 11-12】

$(1)_{10}-(1)_{10}=(1)_{10}+(-1)_{10}=(0)_{10}$

$(00000001)_{补}+(11111111)_{补}=(00000000)_{补}=(0)$

$(1)_{10}-(2)_{10}=(1)_{10}+(-2)_{10}=(-1)_{10}$

$(01)_{补}+(11111110)_{补}=(11111111)_{补}=(-1)$

可以看到，这两个结果都是正确的。

（4）移码。

又叫增码，是符号位取反的补码，一般用做浮点数的阶码表示，因此只用于整数。目的是保证浮点数的机器零为全零。移码和补码仅仅是符号位相反，如例 11-13 所示。

【例 11-13】

$X=+1001$，则$[X]_{补}=010011$，移码 $[X]_{移}=11001$

$X=-1001$，则$[X]_{补}=10111$，移码$[X]_{移}=00111$

## 11.5 总线与中断

### 11.5.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：总线的类型、中断的原理等。

### 11.5.2 知识点精讲

总线（Bus）是连接计算机有关部件的一组信号线，是计算机中用来传送信息的公共通道。通过总线，计算机内的各部件之间可以相互通信，而不是任意两个部件之间直连，从而大大提

高系统的可扩展性。总线可以分为两类：一类是内部总线，也就是 CPU 内部连接各寄存器的总线；另一类是系统总线，即通常意义上所说的总线，是 CPU 与主存储器及外部设备接口相连的总线。按传输信号的种类可分为数据总线 DB（Data Bus）、地址总线 AB（Address Bus）和控制总线 CB（Control Bus）。

（1）数据总线：一般情况下是双向总线，用于各个部件之间的数据传输。

（2）地址总线：单向总线，是微处理器或其他主设备发出的地址信号线。

（3）控制总线：微处理器与存储器或接口等之间控制信号。

CPU 向地址总线提供访问主存单元或 I/O 接口的地址；CPU 向数据总线发送或接收数据，以完成与主存单元或 I/O 接口之间的数据传送，主存和 I/O 设备之间也可以通过数据总线传送数据；CPU 通过控制总线向主存或 I/O 设备发送或接收相关的控制信号，I/O 设备也可以向控制总线发出控制信号。

尤其要注意在存储器的地址总线中，地址线的根数与存储器的容量大小之间有密切的关系，若设地址线的根数为 N，则此地址总线可以访问的最大存储容量为 $M=2^N$ 字节，根据需要可以进一步换算成 KB 和 MB 等。

计算机中，主机与外设间进行数据传输的控制方法主要有程序控制方式、中断方式、DMA 等。

程序控制方式是通过 CPU 执行相应的程序代码控制数据的输入输出，此过程依赖程序代码和 CPU 运算，是效率比较低的一种方式。

中断的控制方式是在系统运行过程中有紧急事件发生时，CPU 暂停当前正在执行的程序，先转去处理紧急事件的子程序，此时需要保存 CPU 中各种寄存器的值，称为保存现场；紧急事件处理结束后恢复原来的状态，再继续执行原来的程序。这种对紧急事件的处理方式称为程序中断控制方式，简称中断。中断方式提供了一种让 CPU 处理紧急事件的手段，但是每一次中断的处理都要进行现场的保存和中断的恢复，需要额外占用一定的 CPU 周期，因此效率不会非常高。

在 DMA 控制方式下，若 CPU 处理 I/O 事件时有大量数据需要处理时，通常不使用中断，而采用 DMA 方式，所谓的 DMA 方式，是指在传输数据时将从一个地址空间复制到另一个地址空间的过程中，只要 CPU 初始化这个传输动作，传输动作的具体操作由 DMA 控制器来实行和完成，这个过程中不需要 CPU 参与，数据传送完毕后再把信息反馈给 CPU，这样就极大地减轻了 CPU 的负担，节省系统资源，提高 I/O 系统处理数据的能力，并减少 CPU 的周期浪费。



## 第 6 学时　计算机软件知识

第 2 天的第 6 学时主要学习计算机软件的相关知识点。计算机软件知识涉及的面比较广，内容非常多。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 4～8 分之间。这部分知识点的考察主要集中在上午的考试中。本章考点知识结构图如图 12-1 所示。


图 12-1　知识体系结构图

## 12.1　操作系统概念

### 12.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：操作系统概念、进程、线程等。

### 12.1.2　知识点精讲

1. 操作系统

操作系统是用户与计算机硬件之间的桥梁，用户通过操作系统管理和使用计算机的硬件来完成各种运算和任务。目前计算机上流行的操作系统有 Windows、UNIX 和 Linux 三类，最常见的是 Windows 系统。现在流行的 Windows 服务器的版本是由 Windows NT 发展而来的。

UNIX 系统具有多用户分时、多任务处理的特点，以及良好的安全性和强大的网络功能成为了互联网的主流服务器操作系统。

Linux 是在 UNIX 的基础之上发展而来的一种完全免费的操作系统，其程序源代码完全向用户免费公开，因此也得到广泛的应用。

2. 应用软件

应用软件是指用户利用计算机的软硬件资源为某一专门的应用目的而开发的软件，通常通过程序设计语言来开发。通过程序设计语言编制程序后，由计算机运行该程序，按设计者的意图对数据进行处理。计算机系统中各种软件的对应关系如图 12-2 所示。

操作系统是计算机系统中的核心系统软件，负责管理和监控系统中的所有硬件和软件资源，其他系统软件主要是一些编译程序和数据库管理系统等。应用软件包含常见的办公软件、管理软件和某些行业应用的软件等。

3. 进程的状态转换

进程简单来说就是操作系统中正在运行的程序以及与之相关的资源的集合。操作系统中进程的运行有三种基本状态：就绪态、运行态和阻塞态。这三种基本状态在进程的生命周期中是不断变换的，如图 12-3 所示表明了进程各种状态转换的情况。

从图 12-3 中可以看出，由于调度程序的调度可以将就绪状态的进程转入运行状态；当运行的进程由于分配的时间片用完了，也可以转入就绪状态；阻塞状态的进程由于 I/O 操作完成，将该进程从阻塞队列中唤醒，使其进入就绪状态；还有一种情况就是运行状态的进程可能由于 I/O 请求的

资源得不到满足而进入阻塞状态。网络工程师考试中，对进程的基本状态和变化条件是出题较多的知识点，因此掌握这个知识点是非常必要的。


图 12-2　计算机系统软件层次示意图

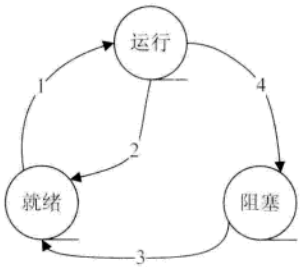



图 12-3　进程的状态转换

4. 进程的同步和互斥

进程是操作系统的核心，引进进程的目的就是让程序能并发执行，提高资源利用率和系统的吞吐量。考生需要注意并发和并行是两个完全不同的概念。

（1）所谓的并发是指：在一定时间内，物理机器上有两个或两个以上的程序同时处于开始运行却尚未结束的状态，并且次序并不是事先确定的。在单处理机系统中同时存在多个并发程序，从宏观上看，这些程序是同时执行的；从微观上看，任何时刻都只有一个程序在执行，这些程序按照分配的时间片在 CPU 上轮流执行。

（2）所谓的并行是指：严格意义上的同时执行在多处理机系统中才可能实现。并发进程间的关系可以是无关的，也可以是相互影响的。

并发进程间无关是指它们是各自独立的，即一个进程的执行不影响其他进程的执行，且与其他进程的运行情况无关，就不需要特别的控制。并发进程间的相互影响是指一个进程的执行可能影响其他进程的执行，即一个进程的执行依赖其他进程的运行情况。相互影响的并发进程之间一定会共享某些资源。

进程之间互相竞争某一个资源，这种关系称为进程的互斥，也就是说对于某个系统资源，如果一个进程正在使用，其他的进程就必须等待其用完才能供自己使用，而不能同时供两个以上的进程使用。例如，A 和 B 两个进程共享一台打印机，如果系统已经将打印机分配给了 A 进程，当 B 进程需要打印时，因得不到打印机而等待，只有 A 进程将打印机释放后，系统才将 B 进程唤醒，B 进程才有可能获得打印机。

并发进程使用共享资源时，除了竞争资源之外也有协作，要利用互通消息的办法来控制执行速度，使相互协作的进程正确工作。进程之间相互协作来完成某一任务，这种关系称为进程的同步。例如，A 和 B 两个进程通过一个数据缓冲区合作完成一项任务，A 进程将数据送入缓冲区后通知 B 进程缓冲区中有数据，B 进程从缓冲区中取走数据再通知 A 进程缓冲区已经为空。当缓冲区为空时，B 进程因得不到数据而阻塞，只有当 A 进程将数据送入缓冲区时才将 B 进程唤醒；反之，当缓冲区满时，A 进程因不能继续送数据而阻塞，只有当 B 进程取走数据时才唤醒 A 进程。相互影响的并

发进程可能会同时使用共享资源，如果对这种情况不加以控制，在使用共享资源时就会出错。

对于进程之间的互斥和同步，操作系统必须采取某种控制手段才可以保证进程安全可靠地执行。对于进程互斥，要保证在临界区内不能交替执行；对于进程同步，则要保证合作进程必须相互配合、共同推进，并严格按照一定的先后顺序。因此，操作系统必须使用信号量机制来保证进程的同步和互斥。

5. 用 PV 原语实现进程的互斥

为了解决进程之间的互斥，操作系统设置一个互斥的信号量 S，这个信号量与所有的并发进程都有关，因此称为公有信号量。只要把临界区置于 P(S)和 V(S)之间即可实现进程间的互斥。这种情况下，任何想访问临界资源的进程在进入临界区之前，要先对信号量 S 执行 P 操作，若该资源未被访问，则本次 P 操作成功，该进程便可以进入临界区，这时若再有其他的进程想进入临界区，在其对信号量 S 执行 P 操作后一定会失败而阻塞，从而保证了临界资源被互斥的访问。当访问临界资源的进程退出临界区后，应该再对其执行 V 操作，释放该临界资源。

类似于广场上只有一个公共电话机，广场上的所有人都可以去使用这个电话机，但是在任何时刻都只允许一个人使用这个电话机。为了让打电话的人能知道电话机的状态，在电话亭上安装一个工作指示灯（相当于信号量 S），在有用户使用电话机时，只要一拿起话筒（相当于执行 P(S)操作），指示灯亮，其他人不可以再使用该电话机。当通话完毕，放下话筒（相当于执行 V(S)操作），指示灯灭，其他人可以使用该电话机。

6. 用 PV 原语实现进程的同步

与进程互斥不同的是，进程同步时的信号量只与制约进程和被制约进程有关，而不会与其他的并发进程有关，所以称同步的信号量为私有信号量。

利用 PV 原语实现进程同步的方法是：首先判断进程间的关系是否为同步，若是，则为各并发进程设置各自的私有信号量，并为私有信号量赋初值，然后利用 PV 原语和私有信号量来规定各个进程的执行顺序。可以通过消费者和生产者进程之间的同步来说明。

假设可以通过一个缓冲区把生产者和消费者联系起来。生产者把产品生产出来后送入仓库，并给消费者发信号，消费者得到信号后到仓库取产品，取走产品后给生产者发信号。并且假设仓库中一次只能放一个产品。当仓库满时，生产者不能放产品；当仓库空的时候，消费者不能取产品。

生产者只关心仓库是否为空，消费者只关心仓库是否为满。可设置信号量 empty 和 full，其初值分别为 1 和 0。full 表示仓库中是否满，empty 表示仓库是否为空。

生产进程和消费者进程是并发执行的进程，假定生产进程先执行且执行 P(empty)成功，把生产产品放入缓冲区并执行 V(full)操作，使 full=1，表示在缓冲区中已有可供消费者使用的产品，然后执行 P(empty)操作将自己阻塞起来，等待消费进程将缓冲区中的产品取走。当调度程序调度到消费进程执行时，由于 full =1，所以 P(full)成功，可以从缓冲区中取走产品消费并执行 V(empty)操作，将生产进程唤醒，然后又返回到进程的开始去执行 P(full)操作，将自己阻塞起来，等待生产进程送来下一个产品，接下去又是生产进程执行。这样不断地重复，保证了生产进程和消费进程依次轮流执行，从而实现了两个进程之间的同步操作。

为了便于考生理解这两个概念，这里可以简单总结一下：进程之间的互斥是进程间竞争共享资源的使用权，这种竞争没有固定的先后顺序关系；而进程同步涉及共享资源的并发进程之间有一种必然的依赖关系。

在网络工程师考试中考查较多的是系统中进程资源的分配问题。在进程的互斥资源分配过程中，只要能在极端情况下保证各个进程都能获得其等待的资源，而不至于死锁，这就是系统不死锁的基本条件。所谓的死锁，是指多个进程之间相互等待对方的资源，而在得到对方资源之前又不会释放自己的资源，因此造成相互等待的一种现象。在操作系统中，往往一个进程的死锁会造成系统死锁。

## 12.2 软件开发

### 12.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：结构化程序设计、面向对象的基本概念、软件开发模型、软件测试等。

### 12.2.2 知识点精讲

1. 结构化程序设计

结构化程序设计是以模块功能和详细处理过程设计为主的一种传统的程序设计思想，通常采用自顶向下、逐步求精的方式进行。在结构化程序设计中，任何程序都可以由顺序、选择、循环三种基本结构构成。结构化程序往往采用模块化设计的思想来实现，其基本思路是：任何复杂问题都是由若干相对简单的问题构成的。从这个角度来看，模块化是把程序要解决的总目标分解为若干个相对简单的小目标来处理，甚至可以再进一步分解为具体的任务项来实现。每一个小目标就称为一个模块。由于模块相互独立，因此在模块化的程序设计中，应尽量做到模块之间的高内聚低耦合。也就是说，功能的实现尽可能在模块内部完成，以降低模块之间的联系，减少彼此之间的相互影响。

2. 面向对象的基本概念

（1）对象。

对象简单来说就是要研究的任何事物，可以是自然界的任何事物，如一本书、一条流水生产线等都可以看作是对象，它不仅能表示有形的实体，也能表示抽象的规则、计划或事件等。对象由数据和作用于数据的操作构成一个独立整体。从程序设计者来看，对象是一个程序模块；从用户来看，对象可以提供用户所希望的行为。

（2）类。

类可以看作是对象的模板。类是对一组有相同数据和相同操作的对象的定义，一个类所包含的方法和数据描述是一组对象的共同属性和行为。类是在对象之上的抽象，对象则是类的具体化，是类的实例。面向对象的程序设计语言通过类库来代替传统的函数库，程序设计语言的类库越丰富，则该程序设计语言越成熟。面向对象的软件工程可以把多个相关的类构成一个组件。

（3）消息和方法。

对象之间进行通信的机制叫做消息。在对象的操作中，当一个消息发送给某个对象时，消息包含接收对象去执行某种操作的信息。发送一条消息至少要包括接收消息的对象名、发送给该对象的消息名等基本信息，通常还要对参数加以说明，参数一般是认识该消息的对象所知道的变量名。类中操作的实现过程叫做方法，一个方法有方法名、参数等信息。

3. 面向对象的主要特征

（1）继承性。

继承性是子类自动共享父类的数据结构和方法的一种机制。在定义和实现一个类时，可以在一个已经存在的类的基础上来进行，把这个已经存在的类所定义的内容作为自己的内容，并加入若干新的内容。继承性是面向对象程序设计语言不同于其他语言的最重要的特点。在类层次中，子类若只继承一个父类的数据结构和方法，则称为单重继承；若是子类继承了多个父类的数据结构和方法，则称为多重继承。在软件开发中，类的继承性使所建立的软件具有开放性和可扩充性。它简化了对象和类的创建工作量，增加了代码的可重用性。

（2）多态性。

多态性是指相同的操作、函数或过程可作用于多种不同类型的对象上，并获得不同的结果。不同的对象收到同一个消息可以产生不同的结果，这种现象称为多态性。多态性允许每个对象以适合自身的方式去响应共同的消息，也增强了软件的灵活性和重用性。

（3）封装性。

封装是一种信息隐蔽技术，它体现在类的说明，是对象的一种重要特性。封装使数据和加工该数据的方法变为一个整体以实现独立性很强的模块，使得用户只能见到对象的外部特性，而对象的内部特性对用户是隐蔽的。封装的目的在于把对象的设计者和使用者分开，使用者不必知道行为实现的细节，只须用设计者提供的消息来访问该对象即可。

4. 面向对象的方法

面向对象开发方法主要有 Booch 方法、Coad 方法和 OMT 方法等。

（1）Booch 方法。

Booch 方法最先探讨面向对象的软件开发方法中的基础问题，认为面向对象开发是一种根本不同于传统的功能分解的设计方法，软件分解应该最接近人对客观事务的理解。Booch 方法可分为逻辑设计和物理设计，其中逻辑设计包含类图文件和对象图文件；物理设计包含模块图文件和进程图文件，用以描述软件系统结构。Booch 方法中的基本概念有：

1）类图：描述类与类之间的关系。

2）对象图：描述实例和对象间传递消息。

3）模块图：描述构件。

4）进程图：描述进程分配处理器的情况。

Booch 方法也可划分为静态模型和动态模型，其中静态模型表示系统的构成和结构；动态模型表示系统执行的行为。动态模型又包含时序图和状态转换图。

1）时序图：描述对象图中不同对象之间的动态交互关系。

2）状态图：描述一个类的状态变化。

（2）Coad 方法。

该方法是多年来开发大系统的经验与面向对象概念的有机结合，在对象、结构、属性和操作的认定方面提出了一套系统的原则。Coad 方法可分为面向对象分析（OOA）和面向对象设计（OOD）两部分。在 OOA 中建立了概念模型，由类与对象、属性、服务、结构和主题等 5 个分析层次组成。

1）类与对象：从问题域和文字出发，寻找并标识类与对象。

2）属性：确定对象信息及其之间的关系。可分为原子概念层的单个数据和类结构中的公有属性与特定属性。

3）服务：标识消息连接和所有服务说明。

4）结构：标识类层次结构，确定类之间的整体部分结构与通用特定结构。

5）主题：主题是比结构更高层次的模块，与相关类一起控制着系统的复杂度。

面向对象设计（OOD）就是根据已建立的分析模型，运用面向对象技术进行系统软件设计，它将 OOA 模型直接变成 OOD 模型。

（3）OMT 方法。

该方法认为开发工作的基础是对真实世界的对象建模，然后围绕这些对象使用分析模型来进行独立于语言的设计，面向对象的建模和设计促进了对需求的理解，有利于开发更清晰、更容易维护的软件系统。

5. 软件规模度量

准确的软件规模度量是科学进行项目工作量估算、计划进度编制和成本预算的前提。软件规模度量有助于开发人员把握开发时间、费用等。常用的方法有以下几种：

（1）代码行。

代码行（line of code）指所有可执行的源代码行数。此方法的问题是只能等软件开发完毕之后才能准确地计算，而且越是高级的语言，实现同样的功能其代码行越多，因此现在已经很不准确了，在现代软件工程中不再使用此方法。

（2）功能点分析法。

功能点分析法（Function Point Analysis，FPA）是在软件需求分析阶段依据系统功能的一种规模估算方法，由 IBM 的研究人员提出的，随后被国际功能点用户协会（The International Function Point Users' Group，IFPUG）提出的 IFPUG 方法继承。从系统的复杂性和特性两个角度来度量软件的规模，根据具体方法和编程语言的不同，功能点可以转换为代码行。

（3）德尔菲法。

德尔菲法（Delphi Technique）是最流行的一种专家评估技术，这种方式适用于评定过去与将来、新技术与特定程序之间的差别，这个结果会受专家的影响，利用德尔菲技术可以尽量减少这种影响。

（4）构造性成本模型。

构造性成本模型（Constructive Cost Model，COCOMO）是一种精确的、易于使用的基于模型的成本估算方法。该模型按其详细程度分为三种：基本模型、中间模型和详细模型。基本模型是一个静态模型；中间模则在基本模型的基础上，再参考产品、硬件、人员等因素的影响来调整工作量的估算；详细模型在中间模型的基础上，还要考虑对软件工程过程中的分析和设计等的影响。

6. UML

UML 最早由著名的 Jim Rumbaugh、Ivar Jacobson 和 Grady Booch 创造，因为他们各自的建模方法（分别是 OMT、OOSE 和 Booch）彼此之间存在竞争。最终，他们一起创造了一种开放的标准。UML 成为标准建模语言主要是因为它与程序设计语言无关。而且，UML 符号集只是一种语言，而不是一种方法学。因为是一种语言，所以可以在不做任何更改的情况下很容易地适应各种业务运作方式。

UML 提供了多种类型的模型描述图（Diagram），当使用这些图时，UML 使得开发中的应用程序更易理解。这些最常用的 UML 图包括用例图、类图、序列图、状态图、活动图、组件图和部署图。

（1）用例图。

用例图描述了系统提供的一个功能单元，帮助开发人员以一种可视化的方式理解系统的功能需求。

（2）类图。

类图表示不同的实体如何彼此相关，换句话说，它显示了系统的静态结构。类图可用于表示逻辑类（通常就是业务人员所谈及的事物种类）和实现类（程序员处理的实体）。

（3）序列图。

序列图显示具体用例的详细流程。它几乎是自描述的，并且显示了流程中不同对象之间的调用关系，同时还可以很详细地显示对不同对象的不同调用。

（4）状态图。

状态图表示某个类所处的不同状态和该类的状态转换信息。

（5）活动图。

活动图表示在处理某个活动时，两个或多个类对象之间的过程控制流。活动图可用于在业务单元的级别上对更高级别的业务过程进行建模，或者对低级别的内部类操作进行建模。

（6）组件图。

组件图提供系统的物理视图，显示系统中的软件对其他软件的依赖关系。

（7）部署图。

部署图表示该软件系统如何部署到硬件环境中。用于显示该系统不同的组件将在何处运行，以及将如何彼此通信。

7. 软件开发模型

软件开发模型（Software Development Model）是指软件开发的全部过程、活动和任务的结构框架。其主要过程包括需求、设计、编码、测试及维护阶段等环节。软件开发模型使开发人员能清晰、直观地表达软件开发的全过程，明确了解要完成的主要活动和任务。对于不同的软件，通常会采用不同的开发方法和不同的程序设计语言，并运用不同的管理方法和手段。现在软件开发过程中，常用的软件开发模型可以概括成以下六类：

（1）瀑布模型。

瀑布模型是最早出现的软件开发模型，它将软件生命周期分为制定计划、需求分析、软件设计、程序编写、软件测试和运行维护六个基本活动，并且规定了它们自上而下、相互衔接的固定次序，如同瀑布流水，逐级落下，因此形象地称为瀑布模型。在瀑布模型中，软件开发的各项活动严格按照线性方式组织，当前活动依据上一项活动的工作成果完成所需的工作内容。当前活动的工作成果需要进行验证，若验证通过，则该成果作为下一项活动的输入继续进行下一项活动；否则返回修改。尤其要注意的是瀑布模型强调文档的作用，并在每个阶段都进行仔细验证。由于这种模型的线性过程太过理想化，已不适合现代的软件开发模式。

（2）快速原型模型。

快速原型模型首先建立一个快速原型，以实现客户与系统的交互，用户通过对原型进行评价，进一步细化软件的开发需求，从而开发出令客户满意的软件产品。因此快速原型法可以克服瀑布模型的缺点，减少由于软件需求不明确带来的风险。因此快速原型的关键在于尽可能快速地建造出软件原型，并能迅速修改原型以反映客户的需求。

（3）增量模型。

增量模型又称演化模型，增量模型认为软件开发是通过一系列的增量构件来设计、实现、集成和测试的，每一个构件由多种相互作用的模块构成。增量模型在各个阶段并不交付一个完整的产品，而仅交付满足客户需求子集的一个可运行产品即可。整个产品被分解成若干个构件，开发人员逐个构件地交付产品以便适应需求的变化，用户可以不断地看到新开发的软件，从而降低风险。但是需求的变化会使软件过程的控制失去整体性。

（4）螺旋模型。

结合了瀑布模型和快速原型模型的特点，尤其强调了风险分析，特别适合于大型复杂的系统。螺旋模型沿着螺线进行若干次迭代以实现系统的开发，是由风险驱动的，强调可选方案和约束条件，从而支持软件的重用，因此尤其注重软件质量。

（5）喷泉模型。

喷泉模型也称为面向对象的生存期模型，相对传统的结构化生存期而言其增量和迭代更多。生存期的各个阶段可以相互重叠和多次反复，而且在项目的整个生存期中还可以嵌入子生存期。就像喷泉水喷上去又可以落下来，可以落在中间，也可以落在最底部一样。

（6）混合模型。

混合模型也称为过程开发模型或元模型（Meta-Model），把几种不同模型组合成一种混合模型，

它允许一个项目能沿着最有效的路径发展，这就是过程开发模型。

在实际的软件开发模型的选择上，通常开发企业为了确保开发都是使用由几种不同的开发方法组成的混合模型。

8. CMM 模型

能力成熟度模型（Capability Maturity Model for Software，CMM）是对软件组织在定义、实施、度量、控制和改善其软件过程的实践中各个发展阶段的描述。最早是在美国国防部的指导下，由软件开发团体和软件工程学院（SEI）等共同开发的。CMM 的核心是把软件开发视为一个过程，并根据这一原则对软件开发和维护进行过程监控和研究，以使其更加科学化、标准化，使企业能够更好地实现商业目标。CMM 是一种用于评价软件承包能力并帮助其改善软件质量的方法，侧重于软件开发过程的管理及工程能力的提高与评估。CMM 分为五个等级：一级为初始级；二级为可重复级；三级为已定义级；四级为已管理级；五级为优化级。

（1）初始级：这个级别的特点是无秩序，甚至是混乱。整个软件开发过程中没有一个标准的规范或步骤可以遵循的一种状态，所开发的软件产品能否取得成功往往取决于个别人的努力或机遇。初始级的软件过程是一种无定义的随性过程，项目的执行也很随意。

（2）可重复级：这个级别已经建立了最基本的项目管理过程，可以对成本、进度等进行跟踪管理。对类似的软件项目，可以借鉴之前的成功经验来获职成功。也就是说，在软件管理过程中，一个可以借鉴的成功的过程是一个可重复的过程，并且这个重复能逐渐完善和成熟。

（3）可定义级：这个级别已经用于管理和工程的软件过程标准化，并形成相应的文档进行管理。各种项目都可以采用结合实际情况修改后的标准软件过程来进行操作。此级别中的过程管理可以遵照形成了标准的文档执行，各种开发的项目都需要根据这个标准进行操作。

（4）可管理级：这个级别通过详细的度量标准来衡量软件过程和产品质量，实现了质量的和管理的量化。

（5）优化级：这个级别通过将新方法、新技术等各种有用信息进行定量分析，从而持续地对软件过程和管理进行改进。



9. 软件测试

软件测试是软件开发过程中的一个重要环节，其主要目的是检验软件是否符合需求，尽可能多地发现软件中潜在的错误并加以改正。测试的对象不仅有程序部分，还有整个软件开发过程中各个阶段产生的文档，如需求规格说明、概要设计文档等。根据软件开发过程中阶段的不同，可以分为单元测试、集成测试、系统测试、验收测试和回归测试。

根据动态测试在软件开发过程中所处的阶段和作用，动态测试可分为：单元测试、集成测试、系统测试、验收测试和回归测试。

（1）单元测试。

单元测试是对软件中的基本组成单位进行的测试，如一个模块、一个过程等，是最微小规模的测试。它是软件动态测试最基本的部分，也是最重要的部分之一，其目的是检验软件基本组成单位的正确性。一个软件单元的正确性是相对于该单元的规约而言的，因此单元测试以被

测试单位的规约为基准。典型的由程序员而非测试员来做，因为它需要工作人员知道内部程序设计和编码的细节知识。

（2）集成测试。

集成测试是指一个应用系统的各个部件的联合测试，以决定其能否在一起共同工作而没有冲突。部件可以是代码块、独立的应用、网络上的客户端或服务器端程序。这种类型的测试尤其与客户服务器和分布式系统有关。一般在集成测试前单元测试已经完成。集成测试是单元测试的逻辑扩展。其最简单的形式是：两个已经测试过的单元组合成一个组件，并且测试它们之间的接口。从这一层意义上讲，组件是指多个单元的集成聚合。

在现实方案中，许多单元组合成组件，而这些组件又聚合成程序的更大部分。方法是测试片段的组合并最终扩展进程，将模块与其他组的模块一起测试。最后，将构成进程的所有模块一起测试。此外，如果程序由多个进程组成，应该对其进行成对测试，而不是同时测试所有进程。集成测试识别组合单元时出现的问题。通过使用要求在组合单元前测试每个单元，并确保每个单元的生存能力的测试计划，可以知道在组合单元时所发现的任何错误很可能与单元之间的接口有关。这种方法将可能发生的情况数量减少到更简单的分析级别系统测试。

（3）系统测试。

系统测试的对象不仅包括需要测试的产品系统的软件，还包括软件所依赖的硬件、外设甚至某些数据、某些支持软件及其接口等。因此，必须将系统中的软件与各种依赖的资源结合起来，在系统实际运行环境下进行测试。

（4）验收测试。

验收测试是指系统开发生命周期方法的一个重要阶段，也是部署软件之前的最后一个测试操作。测试目的就是确保软件准备就绪，并且可以让最终用户能执行该软件的实现既定功能和任务。测试中，相关的用户或独立测试人员根据测试计划和结果对系统进行测试和接收，让系统用户决定是否接收系统。它是一项确定产品是否能够满足合同或用户所规定的需求的测试。验收测试一般有三种策略：正式验收、非正式验收、α 测试、β 测试。

1）正式验收。

正式验收测试是一项管理严格的过程，它通常是系统测试的延续。计划和设计这些测试的周密和详细程度甚至超过系统测试。正式验收测试一般是开发组织与最终用户组织的代表一起执行的。也有一些完全由最终用户组织执行。

2）非正式验收

在非正式验收测试中，执行测试过程的限制不如正式验收测试中那样严格。测试过程中，主要是确定并记录要研究的功能和业务任务，但没有可以遵循的特定测试用例。测试内容由各测试员决定。这种验收测试方法不像正式验收测试那样组织有序，并且主观性比较大。

3）α 测试（Alpha Testing）。

又称 Alpha 测试，是由一个用户在开发环境下进行的测试，也可以是公司内部的用户在模拟实际操作环境下进行的受控测试，Alpha 测试不能由该系统的程序员或测试员完成。在系统开发接近

完成时对应用系统进行的测试；测试后仍然会有少量的设计变更。这种测试一般由最终用户或其他人员来完成，不能由程序员或测试员完成。

4）β测试（Beta Testing）。

又称Beta测试、用户验收测试（UAT）。β测试是软件的多个用户在一个或多个用户的实际使用环境下进行的测试。开发者通常不在测试现场，Beta 测试不能由程序员或测试员完成。当开发和测试基本完成时所做的测试，而最终的错误和问题需要在发行前找到。这种测试一般由最终用户或其他人员完成，不能由程序员或测试员完成。

（5）回归测试。

回归测试是指在发生修改之后重新测试之前的测试以保证修改的正确性。理论上，软件产生新版本都需要进行回归测试，验证之前发现和修复的错误是否在新软件版本上再次出现。根据修复好了的缺陷再重新进行测试。回归测试的目的在于验证之前出现过但已经修复好的缺陷不再重新出现。一般指对某已知修正的缺陷再次围绕它原来出现时的步骤重新测试。通常确定所需的再测试范围时是比较困难的，特别当临近产品发布日期时。因为为了修正某缺陷必须更改源代码，因而就有可能影响这部分源代码所控制的功能。所以在验证修好的缺陷时不仅要服从缺陷原来出现时的步骤重新测试，而且还要测试有可能受影响的所有功能。因此应当对所有回归测试用例进行自动化测试。

此外，考生还需要掌握白盒测试和黑盒测试的概念。

- 白盒测试（White Box Testing）。

又称结构测试或逻辑驱动测试。它是把测试对象看作一个能打开、可以看见内部结构的盒子。利用白盒测试法对软件进行动态测试时，主要是测试软件产品的内部结构和处理过程，而不关注软件产品的功能。白盒测试法中对测试的覆盖标准主要有：逻辑覆盖、循环覆盖和基本路径测试。由于知道产品内部的工作过程，因此白盒测试可以检测产品内部动作是否按照规格说明书的规定正常进行，按照程序内部的结构测试程序，检验程序中的每条通路是否都有能按预定要求正确工作而不顾它的功能，白盒测试的主要方法有逻辑驱动、基路测试等，通常用于软件验证。

- 黑盒测试（Black Box Testing）。

又称功能测试或数据驱动测试。是根据软件的规格进行的测试，这类测试把软件看作一个不能打开的盒子，因此不考虑软件内部的运作原理。软件测试人员以用户的角度，通过各种输入和对应的输出结果来发现软件存在的缺陷，而不关心程序具体是如何实现的。

## 12.3 项目管理基础

### 12.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：CPM 的概念及相关计算、甘特图的特点等。

### 12.3.2 知识点精讲

网络工程师考试关于项目管理的主要内容就是考察 PERT 图和甘特图的基本特点，尤其是 PERT 图中的关键路径及计算。

计划评审技术（Program Evaluation and Review Technique，PERT）是由美国海军提出的利用网络分析制定计划及对计划予以评价的技术。它能协调整个计划的各个任务，合理安排人力、物力、时间、资金，加速计划地完成，在现代计划的编制和分析中广泛应用。PERT 网络是一种类似流程图的箭线图，它描绘出项目包含的各种活动的先后次序，标明每项活动的时间或相关的成本。对于 PERT 网络，考生最主要的是要知道计算关键路径。

1. 关键路径

关键路径法（Critical Path Method，CPM），在一个项目中，只有项目网络中最长的或耗时最多的活动完成之后，项目才能结束，这条最长的活动路线就叫关键路径，组成关键路径的活动称为关键活动。CPM 是通过寻找项目过程中活动序列的进度安排的最少总时差来预测项目工期的一种网络分析方法。用网络图表示各项工作之间的相互关系，找出控制工期的关键路线，在一定工期和资源条件下获得最佳的计划安排，以达到缩短工期、降低成本的目的。

关键路径法是确定网络图中每一条路线从起始到结束找出工期最长的线路的方法，也就是说，整个项目工期是由最长的线路来决定的。基本工作原理是：给每个最小任务单元计算工期、定义最早开始和结束日期、最迟开始和结束日期、按照活动的关系形成顺序的网络逻辑图，找出其中最长的路径，即为关键路径。

2. 关键路径法的时间计算

关键路径法的时间计算一般采用正推法或逆推法进行。

（1）正推法。正推法用于计算活动的最早时间，其算法如下：

1）选择一个开始于第一个节点的活动开始进行计算，第一个节点的时间如没有设置，则将其设置为 1。活动最早开始时间就是开始节点的最早时间。

2）在选择的活动最早开始时间上加上其工期，就是其最早结束时间。

3）比较此活动的最早结束时间和结束节点的最早开始时间。如果结束节点还没有设置时间，则此活动的最早结束时间就是该结束节点的最早开始时间；如果活动的结束时间比结束节点的最早开始时间大，则取此活动的最早结束时间作为结束节点的最早开始时间；如果此活动的最早结束时间小于其结束节点的最早开始时间，则保留此节点的时间作为其最早开始时间。

4）检查是否还有其他活动开始于此节点，如果有，则回到步骤 2）进行计算；如果没有，则进入下一个节点的计算，并回到步骤 2）开始，直到最后一个节点。

（2）逆推法。逆推法用于计算活动的最迟时间的计算，一般从项目的最后一个活动开始计算，直到计算到第一个节点的时间为止，在逆推法的计算中，首先令最后一个节点的最迟时间等于其最早时间，然后开始计算，具体的计算步骤如下：

1）设置最后一个节点的最迟时间，令其等于正推法计算出的最早时间。

2）选择一个以此节点为结束节点的活动进行计算。

3）令此活动的最迟结束时间等于此节点的最迟时间。

4）从此活动的最迟结束时间中减去其工期，得到其最迟开始时间。

5）比较此活动的最迟开始时间和开始节点的最迟时间，如果开始节点还没有设置最迟时间，则将活动的最迟开始时间设置为此节点的最迟时间；如果活动的最迟开始时间早于节点的最迟时间，则将此活动的最迟开始时间设置为节点的最迟时间；如果活动的最迟开始时间迟于节点的最迟时间，则保留原节点的时间作为最迟时间。

6）检查是否还有其他活动以此节点为结束节点，如果有，则进入第二步计算；如果没有，则进入下一个节点，然后进入第二步计算，直至最后一个节点。

7）第一个节点的最迟时间是本项目必须要开始的时间，假设取最后一个节点的最迟时间和最早时间相等，则其值应该等于 1。

【例 12-1】某网络工程使用如图 12-4 所示的 PERT 图进行进度安排，则该工程的关键路径是（　　）；整个项目的最短工期为（　　）；在不延误项目总工期的情况下，任务 F 最多可以推迟开始的时间是（　　）天。

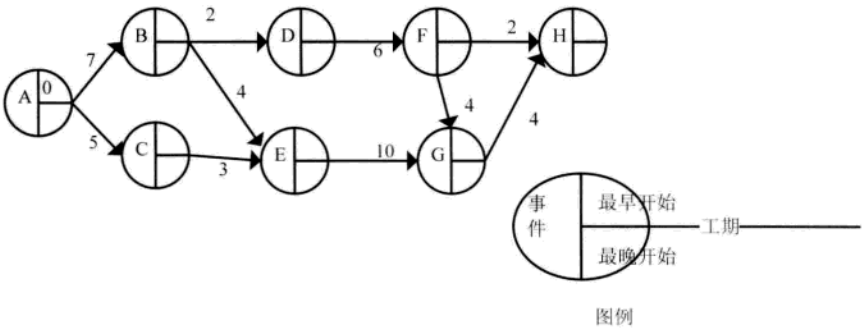



图 12-4　某工程的 PERT 图

可选答案：A．ACEGH　　B．ABEGH　　C．ABDFH　　D．ABDFGH

根据关键路径的定义可知，最长的路径就是关键路径，因此图中任务流 ACEGH 的持续时间是 5+3+10+4=22，其余的路径依此类推，可分别得到任务流 ABEGH 的持续时间是 25，ABDFGH 的持续时间是 23，ABDFH 的持续时间是 17。所以项目关键路径长度为 25，也就是整个项目的最短工期了，关键路径就是 ABEGH。路径 ABDFH 的持续时间是 17 天，路径 ABDFGH 的持续时间是 23 天，而总工期是 25 天，因此可以推迟 25-23=2 天。也就是找经过的事件 F 到完成的整个项目的所有路径中最长的那个时间，然后用总工期减去此时间即为可以提前的时间；也可以使用反推法，H 的最迟完成时间是 25 天，则 F 的最迟完成时间是 25-8=17 天，F 的最早完成时间是 15 天，因此最多可以推迟 17-15=2 天。

3. 甘特图

甘特图内在思想简单，基本是一条线条图，横轴表示时间，纵轴表示活动，线条表示在整个期间上计划和实际的活动完成情况。它直观地表明任务计划在什么时候进行，及实际进展与计划要求的对比；也可以表示子任务之间的并行和串行关系。管理者由此极为便利地弄清一项任务还剩下哪些工作要做，并可以评估工作进度。但是甘特图不能清晰地描述任务之间的依赖关系，也不能清晰地指出关键任务在哪里。

在甘特图的表示中，往往用水平线表示任务的工作阶段，其起点和终点分别对应任务的开始时间和完成时间，水平线的长度表示完成任务的时间。

【例 12-2】网络工程师小张制定的某项目的开发计划中有 X、Y、Z 三个任务，任务之间的关系满足下列条件：任务 X 必须最先开始，其完成时间为 4 周；任务 Y 必须在任务 X 启动 2 周后才能开始，且需要 3 周完成；任务 Z 必须在任务 X 全部完成后才能开始，且需要 2 周完成。则此项目的甘特图如图 12-5 所示表示。

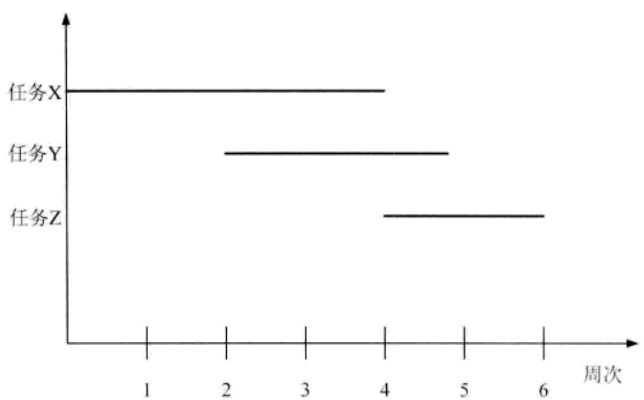



图 12-5　甘特图

## 12.4　软件知识产权

### 12.4.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：软件著作权主题，著作权的基本权力，权力的保护期限，如何判断侵权等，通常的考试分值是 1～2 分。近几年关于标准化方面的知识点出题的可能性越来越小，本书不再讨论。

### 12.4.2 知识点精讲

著作权法是为了保护文学、艺术和科学作品作者的著作权及与著作权有关的权益。著作权法中涉及到的作品的概念是文学、艺术和自然科学、社会科学、工程技术等作品，具体来说，这些作品包括以下九类：

（1）文字作品：包括小说、散文、诗词和论文等表现形式的作品。

（2）口述作品：如演说、辩论等以口头形式表现的作品。

（3）音乐、戏剧、曲艺、舞蹈、杂技艺术作品。

（4）美术、建筑作品、摄影作品。

（5）电影作品和以类似摄制电影的方法创作的作品。

（6）工程设计图、产品设计图、地图、示意图等图形作品和模型作品。

（7）地图、示意图等图形作品。

（8）计算机软件。

（9）法律、行政法规规定的其他作品。

计算机软件著作权是指软件的开发者或其他权利人依据有关著作权法律的规定，对软件作品所享有的各项专有权利。就权利的性质而言是一种民事权利，具备民事权利的基本特征。著作权是知识产权中的一种特殊情况，因为著作权的取得无须经过别人确认，这就是所谓的“自动保护”原则。软件经过登记后，软件著作权人即享有发表权、开发者身份权、使用权、使用许可权和获得报酬权。

1. 著作权人及其权利

著作权法中的著作权人包括作者或能合法取得著作权的公民、法人或组织。著作权的人身权和财产权就是所谓的版权，包括以下具体权力：

（1）发表权：决定是否公之于众的权利。

（2）署名权：表明作者身份，在作品上署名的权利。

（3）修改权：修改或者授权他人修改作品的权利。

（4）保护作品完整权：保护作品不受篡改的权利。

（5）复制权：以印刷、复印、录音、录像、翻拍等方式将作品制作一份或多份的权利。

（6）发行权：以出售或者赠与方式向公众提供作品的原件或复制件的权利。

（7）出租权：有偿许可他人临时使用电影作品或以类似摄制电影的方法创作的作品的权利。

（8）展览权：公开陈列美术作品、摄影作品的原件或复制件的权利。

（9）表演权：公开表演作品，以及用各种手段公开播送作品的表演的权利。

（10）放映权：通过放映机、幻灯机等技术设备公开再现美术、摄影、电影和以类似摄制电影的方法创作的作品等权利。

（11）广播权：以无线方式公开广播，以有线传播或转播的方式向公众传播广播的作品的权利。

（12）信息网络传播权：以有线或无线方式向公众提供作品，使公众可以在其个人选定的时间和地点获得作品的权利。

（13）摄制权：以摄制电影或者以类似摄制电影的方法将作品固定在载体上的权利。

（14）改编权：改变作品，创作出具有独创性的新作品的权利。

（15）翻译权：将作品从一种语言文字转换成另一种语言文字的权利。

（16）汇编权：将作品或作品的片段通过选择或者编排汇集成新作品的权利。

创作作品的公民是作者。由法人或其他组织主持，代表法人或其他组织意志创作，并由法人或其他组织承担责任的作品，法人或其他组织视为作者。通常在作品上署名的公民、法人或其他组织为作者。

2. 权利的保护期限

著作权利中作者的署名权、修改权、保护作品完整权的保护期不受限制。公民的作品，其发表权及其他相关权利的保护期为作者终生及其死亡后五十年，截止于作者死亡后第五十年的12月31日；若是合作作品，则截止于最后死亡的作者死亡后第五十年的12月31日。

法人或者其他组织的作品、著作权（署名权除外）由法人或者其他组织享有的职务作品，其发表权及其他相关权利的保护期为五十年，截止于作品首次发表后第五十年的12月31日，但作品自创作完成后五十年内未发表的不再保护。

电影作品和以类似摄制电影的方法创作的作品、摄影作品，其发表权及其他相关权利的保护期为五十年，截止于作品首次发表后第五十年的12月31日，但作品自创作完成后五十年内未发表的，不再保护。

3. 权利的限制

在下列情况下使用作品可以不经著作权人许可，不向其支付报酬，但应当指明作者姓名和作品名称，并且不得侵犯著作权人依照本法享有的其他权利：

（1）为个人学习、研究或者欣赏，使用他人已经发表的作品。

（2）介绍、评论某一作品或者说明某一问题，在作品中适当引用他人已经发表的作品。

（3）报道时事新闻，在报纸、期刊、电台等媒体中不可避免地再现或者引用已经发表的作品。

（4）报纸、期刊、广播电台、电视台等媒体刊登或者播放其他报纸、期刊、广播电台、电视台等媒体已经发表的关于政治、经济、宗教问题的时事性文章，但作者声明不许刊登、播放的除外。

（5）报纸、期刊、广播电台、电视台等媒体刊登或者播放在公众集会上发表的讲话，但作者声明不许刊登、播放的除外。

（6）为学校课堂教学或科学研究翻译或者少量复制已经发表的作品，供教学或科研人员使用，但不得出版发行。

（7）国家机关为执行公务在合理范围内使用已经发表的作品。

（8）图书馆、档案馆、纪念馆、博物馆、美术馆等为陈列或者保存版本的需要，复制本馆收藏的作品。

（9）免费表演已经发表的作品，该表演未向公众收取费用，也未向表演者支付报酬。

（10）对设置或陈列在室外公共场所的艺术作品进行临摹、绘画、摄影、录像。

（11）将中国公民、法人或其他组织已经发表的以汉语言文字创作的作品翻译成少数民族语言文字作品在国内出版发行。

（11）将已经发表的作品改成盲文出版。

以上规定适用于对出版者、表演者、录音录像制作者、广播电台、电视台的权利的限制。为实施九年制义务教育和国家教育规划而编写出版教科书，除作者事先声明不许使用的外，可以不经著作权人许可，在教科书中汇编已经发表的作品片段，短小的文字作品、音乐作品或单幅的美术作品、摄影作品，但应当按照规定支付报酬，指明作者姓名和作品名称，并且不得侵犯著作权人的其他权利。

4. 侵权的判断

网络工程师考试中对著作权的考查，往往是以案例的形式考查考生是否掌握了如何判断侵权行为。因此这一节中提到的侵权行为必须要充分掌握。对计算机软件侵权行为的认定，实际是指对发生争议的某一个计算机程序与具有明确权利的正版程序的对比和鉴别。

凡是侵权人主观上具有故意或过失对著作权法和计算机软件保护条例保护的软件人身权和财产权实施侵害行为的，都构成计算机软件的侵权行为。对著作权侵权行为的判断主要基于以下几个方面：

（1）未经软件著作权人的同意而发表其软件作品。软件著作人享有对软件作品的公开发表权，未经允许，著作权人以外的任何人都无权擅自发表特定的软件作品。这种行为侵犯著作权人的发表权。

（2）将他人开发的软件当作自己的作品发表。这种行为的构成主要是行为人欺世盗名，剽窃软件开发者的劳动成果，将他人开发的软件作品假冒为自己的作品而署名发表。只要行为人实施了这种行为，不管其发表该作品是否经过软件著作人的同意都构成侵权。这种行为侵犯了身份权和署名权。

（3）未经合作者的同意将与他人合作开发的软件当作自己独立完成的作品发表。这种侵权行为发生在软件作品的合作开发者之间。作为合作开发的软件，软件作品的开发者身份为全体开发者，软件作品的发表权也应由全体开发者共同行使。如果未经其他开发者同意，将合作开发的软件当作自己的独创作品发表即构成侵权。

（4）在他人开发的软件上署名或者涂改他人开发的软件上的署名。这种行为是在他人开发的软件作品上添加自己的署名，替代软件开发者署名或者将软件作品上开发者的署名进行涂改的行为。这种行为侵犯身份权和署名权。

（5）未经软件著作权人的同意修改、翻译、注释其软件作品。这种行为侵犯了著作权人的使用权中的修改权、翻译权与注释权。对不同版本的计算机软件，新版本往往是旧版本的提高和改善。这种提高和改善应认定为是对原软件作品的修改和演绎。这种行为应征求原版本著作权人的同意，否则构成侵权。如果征得软件作品著作人的同意，因修改和改善新增加的部分，创作者应享有著作

权。对是职务作品的计算机软件，参与开发的人员离开原单位后，如其对原单位享有著作权的软件进行修改、提高，应经过原单位许可，否则构成侵权。软件程序员接受第一个单位委托开发完成一个软件，又接受第二个单位委托开发功能类似的软件，仅将受第一个单位委托开发的软件略作改动即算完成提交给第二个单位，这种行为也构成侵权。

（6）未经软件著作权人的同意，复制或部分复制其软件作品。这种行为侵犯了著作权人的使用权中的复制权。计算机软件的复制权是计算机软件最重要的著作财产权，也是通常计算机软件侵权行为的对象。这是由于软件载体价格相对低廉，复制软件简单易行、效率极高，而销售非法复制的软件即可获得高额利润。因此，复制是最为常见的侵权行为，是防止和打击的主要对象。当软件著作权经当事人的约定合法转让给转让者后，软件开发者未经允许不得复制该软件，否则也构成侵权。

（7）未经软件著作权人同意，向公众发行、展示其软件的复制品。这种行为侵犯了发行权与展示权。

（8）未经软件著作权人同意，向任何第三方办理软件权利许可或转让事宜。这种行为侵犯了许可权和转让权。

# 第 3 天

# 动手操作，案例配置

经过第 2 天的学习，我们应当已经掌握了网络工程师考试所涉及的大部分基础知识了，也还学习了计算机软件、计算机硬件这 2 个核心知识领域的知识。那么在第 3 天的学习中，将重点讲述 Windows 的管理与配置和 Linux 的管理与配置。

## 第 1 学时　必考题 1——Windows 管理

第 3 天的第 1 学时主要学习 Windows 管理。Windows 管理是计算机网络应用中的基础知识点。根据历年考试的情况来看，每次考试涉及相关知识点的分值在 1～3 分之间，大部分是在上午考试中出现，近几年来看，在下午的考题中也逐渐出现 Windows 管理方面的试题，但是数量少，多以选择题的形式出现，与上午考的题大同小异。本章考点知识结构图如图 13-1 所示。


图 13-1　Windows 管理知识结构图

## 13.1　域与活动目录

### 13.1.1　考点分析

历年网络工程师考试涉及本部分的相关知识点有：域的概念、域控制器的概念、活动目录的概

念以及活动目录的安装等基本知识。

### 13.1.2 知识点精讲

本书采用 Windows Server 2003 做为蓝本来阐述 Windows 相关的知识点，而目前网络工程师考试中 Windows 部分的试题也是以 Windows Server 2003 为蓝本的。这部分内容中概念性的知识较多，因此先要掌握本节所涉及的基本概念。

1. 域

域（Domain）是 Windows 网络中共享公共账号数据库和数据安全策略的一组计算机的逻辑集合，其中有一台服务器可以为集合内的计算机提供登录验证服务，并且这个逻辑集合拥有唯一的域名与其他的域区别。这个逻辑集合可以看作一个资源的集合体，通过服务器控制网络上的其他计算机能否加入这个组合。

在没有使用域的工作组上，所有计算机的相关设置都是存储在本机上的，不涉及网络中的其他计算机。而在域模式下，至少有一台服务器为域中的每一台计算机或用户提供验证，这台服务器就是本域的域控制器（Domain Controller，DC）。

域控制器上包含了这个域的所有账号、密码以及属于本域的计算机信息的数据库。一旦某台计算机要加入到域中，其访问网络的各种策略都是由域控制器统一设置，其用户名和密码等都要发送到网络中的域控制器上进行验证。这是域模式与工作组的一个最大区别。Windows 网络中常见的域模式有单域模型、主域模型、多主域模型和完全信任模型等。

（1）单域模型。

网络中只有一个域，适用于用户较少的网络。

（2）主域模型。

由于某种原因需要将网络分成多个域，仅在一个称为主域的域中创建网络中的所有用户和全局组，而其他的域都信任主域，并且可以使用在主域中定义的用户和全局组的一种模式。在这种模型下，主域通常是账户域，负责管理用户账户；网络中的其他域是资源域，负责提供各种资源给网络中的用户使用，适用于网络中用户和组的数量不太多的情况。

（3）多主域模型。

网络中有多个主域和多个资源域，其中主域作为账户域，所有的用户账户和组都创建在主域中，各个主域之间相互信任，其他的所有资源域都信任主域。这种模型的缺点是：如果一个全局组需要保存来自两个或两个以上域的用户，则每个主域都要创建一个全局组，而在其他域模型中只使用一个全局组。这种模型适用于网络中用户非常多，且有专门的管理部门的情况。

（4）完全信任模型。

网络中具有多个主域，每个域中都有自己的用户和全局组，且这些域都相互信任。这种模型适用于网络中用户众多且没有专门的管理部门的情况。

在企业网络中，管理员通常会根据实际情况选择合适的域模型实现高效的管理。尤其要注意的是，如果要在不同的域间相互访问，则需要通过建立域间的信任关系来实现，当一个域与其他域建

立了信任关系后，这两个域之间的计算机就可以进行资源共享。但是，每个域管理员只能管理本域的内部资源，除非其他的域明确赋予本域相应的管理权限，才能够管理其他的域。

2. 活动目录

活动目录（Active Directory）是 Windows 2000 及之后版本的服务器中提供的一种目录服务。活动目录中使用了一种结构化的数据存储方式存储有关网络对象的信息，并且让管理员和用户能够轻松地查找和使用这些信息，同时也能对目录信息进行灵活的逻辑分层组织。

目录数据都存储在被称为域控制器的服务器上，并且可以被网络应用程序或服务所访问。一个域可能拥有一台以上的域控制器，但是只能有一台主域控制器，其他的都是备份域控制器。每一台域控制器都拥有它所在域的目录的一个副本。

Windows Server 2003 中的活动目录数据复制有以下两种方式：

（1）单主机复制模式。对目录的任何修改都是从主域控制器复制到域中的其他域控制器上的。

（2）多主机复制模式。多个域控制器没有主次之分。域中每个域控制器都能接收其他域控制器对目录的改变信息，也可以把自己改变的信息复制到其他域控制器上。

由于目录可以被复制，而且所有的域控制器都拥有目录的一个可写副本，所以用户和管理员便可以非常方便地在域的任何位置获得所需的目录信息。在各台域控制器之间进行复制的有三种类型的目录数据：域数据、配置数据和架构数据。

（1）域数据：域数据包含了与域中对象有关的信息，如用户、计算机账户属性等信息。

（2）配置数据：配置数据描述了目录的拓扑结构，包括所有域及域控制器的位置等信息。

（3）架构数据：架构是对目录中存储的所有对象和属性数据的正式定义。定义了多种对象类型，如用户和计算机账户、组、域及安全策略等。

考试中与活动目录相关的概念如下：

（1）名字空间。

简单来说就是任何给定名字的解析边界，所谓边界就是指这个名字所关联或者映射的所有信息范围。Windows 中的活动目录就是一个名字空间。要在活动目录中查找一个名字为“张三”的用户，如果服务器上已经给这个用户定义了用户名、密码、权限级别、联系方式等，则服务器上所定义的这些信息的综合就是“张三”这个名字的名字空间。

（2）对象。

对象是活动目录中具体的信息实体。通过属性描述实体的基本特征，如一个用户账号。

（3）容器。

容器是活动目录名字空间的一部分，与活动目录一样都是有属性的，但是它不表示任何具体的实体，而是表示存放对象的空间，是名字空间的子集。例如，名字空间例中的用户“张三”，它的容器就只有用户名和密码，而其他的信息就不属于张三的容器范围。

（4）目录树。

在任何一个名字空间中，由容器和对象构成的树形层次结构就称为目录树，树的叶子节点就是对象，树的非叶子节点是容器。目录树描述了对象的连接方式，也显示了从一个对象到另一个对象

的路径。

（5）域。

域是 Windows 网络系统的安全性边界。每个域都有自己的安全策略和与其他域的信任关系。当多个域通过信任关系连接起来之后，活动目录可以被多个信任域共享。

（6）组织单元。

包含在域中的目录对象类型就是组织单元。组织单元可以将用户、组、计算机等放入活动目录的容器中，组织单元不能包括来自其他域的对象。组织单元是可以指派组策略设置或委派管理权限的最小作用单位，类似于 Windows 网络中的工作组的概念。

（7）域树。

域树由多个域组成，这些域共享一个配置，形成一个连续的名字空间。树中的域是通过信任关系建立连接的，活动目录中包含一个或多个域树。域树表示方式采用标准域名，其中的域层次越深级别越低，通常用“.”表示一个层次，如域 lib.hunau.net 就比 hunau.net 的域级别低。域树中的域是通过双向可传递信任关系连接在一起的。由于这些信任关系是双向且可传递的，因此在域树中新创建的新域可以立即与域树中其他的域建立信任关系。

（8）域林。

指由一个或多个没有形成连续名字空间的域树组成。域林中的所有域树共享同一个配置和全局目录。所有的域树都通过 Kerberos 建立信任关系，不同的域树可以交叉引用其他域树中的对象。根域是域林中创建的第一个域。

（9）域控制器。

域控制器是使用活动目录安装向导配置的 Windows Server 的计算机。域控制器存储着目录数据并管理用户域的交互关系。一个域可有一个或多个域控制器。

复习过程中，只要能区分这些概念即可。

3. 活动目录的安装

安装域控制器时，必须是具有本地管理员权限的用户在服务器上安装活动目录（AD），并且要保证本地磁盘上有一个 NTFS 文件系统的分区。

活动目录的安装步骤如下：

（1）执行域控制器上的“开始”菜单→“运行”→输入 dcpromo 命令。

（2）进入创建新域的向导。DC 有两种类型可以选择：新域的域控制器和现有域的额外域控制器。一般选择新域的域控制器。

（3）新域的 DNS 全名。

（4）新域的 NetBIOS 名。

（5）数据库和日志文件夹。

为了优化性能，可以将数据库和日志放在不同的硬盘上，该文件夹不一定在 NTFS 分区。若本计算机是域中的第一台域控制器，则 SAM 数据库会自动升级到 C:\windows\ntds\ntds.dit，原来的本地用户账号自动变成域用户账号。

（6）还原模式密码。

目录服务还原模式的管理员密码是在目录服务还原模式下登录系统时使用的。由于在目录服务还原模式下，所有的域账号用户都不能使用，只能使用这个还原模式管理员账号登录。

（7）安装完成后需重启计算机。

将其他计算机加入域中，基本操作步骤如下：

必须具有管理权限的用户才能将计算机加入到域中，同时会在域中自动创建计算机账号。在确保网络正常的前提下，在客户计算机系统属性中的“计算机名”选项卡里单击“更改”按钮，可以打开“计算机加入域”对话框，选中域后输入正确的域名，然后再根据提示输入具有加入域权限的用户名和密码即可。

## 13.2 用户与组

### 13.2.1 考点分析

历年网络工程师考试涉及本部分的相关知识点有：用户与组的概念、常见用户的权限、常见组的权限等基本知识。

### 13.2.2 知识点精讲

1. 用户账号

在 Windows Server 2003 中，系统安装完之后会自动创建一些默认用户账号，常用的是 Administrator、Guest 及其他一些基本的账号。为了便于管理，系统管理员可以通过对不同的用户账号和组账号设置不同的权限，从而大大提高系统的访问安全性和管理的效率。

（1）Administrator 账户。

Administrator 账号是服务器上 Administrators 组的成员，具有对服务器的完全控制权限，可以根据需要向用户分配权限。不可以将 Administrator 账户从 Administrators 组中删除，但可以重命名或禁用该账号。若此计算机加入到域中，则域中 domain admins 组的成员会自动加入到本机的 Administrators 组中。因此域中 domain admins 组的成员也具备本机 Administrators 的权限。

（2）Guest 账号。

Guest 账号是 Guests 组的成员，一般是在这台计算机上没有实际账号的人使用。如果已禁用但还未删除某个用户的账号，该用户也可以使用 Guest 账号。Guest 账号默认是禁用的，可以手动启用。

（3）IUSR_机器名、IWAM_机器名。

IUSR_机器名、IWAM_机器名这两个账号是安装了 IIS 之后的系统自动生成的账号，IUSR_机器名通常称为“Web 匿名用户”账号或“Internet 来宾”账号。当匿名用户访问 IIS 时，实际上系统是以“IUSR_机器名”账号在访问。IWAM_机器名是应用程序所使用的账号，在 IIS 中，ASP 默

认执行的用户账号就是 IWAM_机器名。

2. 组账号

组账号是具有相同权限的用户账号的集合。组账号可以对组内的所有用户赋予相同的权利和权限。在安装运行 Windows Server 2003 操作系统时会自动创建一些内置的组，即默认本地组。具体的默认本地组如下：

（1）Administrators 组。

Administrators 组的成员对服务器有完全控制权限，可以为用户指派用户权利和访问控制权限。

（2）Guests 组。

Guests 组的成员拥有一个在登录时创建的临时配置文件，注销时将删除该配置文件。“来宾账号”（默认为禁用）也是 Guests 组的默认成员。

（3）Power Users 组。

Power Users 组的成员可以创建本地组，并在已创建的本地组中添加或删除用户，还可以在 Power Users 组、Users 组和 Guests 组中添加或删除用户。

（4）Users 组。

Users 组的成员可以运行应用程序，但是不能修改操作系统的设置。

（5）Backup Operators 组。

该组成员不管是否具有访问该计算机文件的权限，都可以运行系统的备份工具，对这些文件和文件夹进行备份和还原。

（6） Network Configuration Operators 组。

该组成员可以在客户端执行一般的网络设置任务（如更改 IP 地址），但是不能设置网络服务器。

（7）Everyone 组。

任何用户都属于这个组，因此当 GUEST 被启用时，改组的权限设置必须严格限制。

（8）Interactive 组。

任何本地登录的用户都属于这个组。

（9）System 组。

该组拥有系统中最高的权限，系统和系统级服务的运行都是依靠 System 赋予的权限，从任务管理器中可以看到很多进程是由 System 开启的。System 组只有一个用户（即 System），它不允许其他用户加入，在查看用户组的时候也不显示出来。默认情况下，只有系统管理员组用户（Administrator）和系统组用户（System）拥有访问和完全控制终端服务器的权限。

## 13.3 文件系统与分区管理

### 13.3.1 考点分析

历年网络工程师考试涉及本部分的相关知识点有：文件系统概念、分区概念、NTFS 分区特点

等基本知识。

### 13.3.2 知识点精讲

1. 文件管理

Windows 的文件系统采用树型目录结构。在树型目录结构中，根结点就是文件系统的根目录，所有的文件作为叶子节点，其他所有目录均作为树型结构上的节点。任何数据文件都可以找到唯一的一条从根目录到自己的通路，从树根开始，将全部目录名与文件名用“/”连接起来构成该文件的绝对路径名，且每个文件的路径名都是唯一的，因此可以解决文件重名问题。但是在多级的文件系统中使用绝对路径比较麻烦，通常使用相对路径名。当系统访问当前目录下的文件时，就可以使用相对路径名以减少访问目录的次数，提高效率。

系统中常见的目录结构有三种：一级目录结构、二级目录结构和多级目录结构。

（1）一级目录的整个目录组织成线性结构，整个系统中只建立一张目录表，系统为每个文件分配一个目录项表示即可。尽管一级目录结构简单，但是查找速度过慢，且不允许出现重名，因此较少使用。

（2）二级目录结构是由主文件目录 MFD（Master File Directory）和用户目录 UFD（User File Directory）组成的层次结构，可以有效地将多个用户隔离开，但是不便于多用户共享文件。

（3）多级目录结构，允许不同用户的文件可以具有相同的文件名，因此适合共享。

2. Windows 分区文件系统

Windows 系列操作系统中主要有以下几种最常用的文件系统：FAT16、FAT32、NTFS。其中的 FAT16 和 FAT32 均是文件配置表（FAT，File Allocation Table）方式的文件系统。

（1）FAT16。

FAT16 是使用较久的一种文件系统，其主要问题是：大容量磁盘利用率低。因为在 Windows 中，磁盘文件的分配以簇为单位，而且一个簇只分配给一个文件使用，因此不管多么小的文件也要占用一个簇，剩余的簇空间就浪费了。

（2）FAT32。

由于分区表容量的限制，FAT16 分区被淘汰，微软在 Windows 95 及以后的版本中推出了一种新分区格式 FAT32，采用 32 位的文件分配表，突破了 FAT16 分区 2GB 容量的限制。它的每个簇都固定为 4KB，与 FAT16 相比大大提高了磁盘的利用率。但是 FAT32 不能保持向下兼容。

（3）NTFS。

随着 Windows NT 操作系统推出了新的 NTFS 文件系统，使文件系统的安全性和稳定性大大提高，成为了 Windows 系统中的主要文件系统。Windows 的很多服务和特性都依赖于 NTFS 文件系统，如活动目录就必须安装在 NTFS 中。NTFS 文件系统的主要优势是能通过 NTFS 许可权限保护网络资源。在 Windows Server 2003 下，网络资源的本地安全性就是通过 NTFS 许可权限实现的，它可以为每个文件或文件夹单独分配一个许可，从而提高访问的安全性。另一个显著特点是使用 NTFS 对单个文件和文件夹进行压缩，从而提高磁盘的利用率。

# 第 2 学时　上、下午考试共同考点 1——Windows 命令

第 3 天的第 2 学时主要学习 Windows 命令这一部分，作为最为常见的网络操作系统，Windows 系统中提供了非常多的命令，可以分为 IP 网络有关的命令、系统服务及管理有关的命令、与故障诊断和系统监控相关的命令。根据历年考试的情况来看，每次考试主要涉及到的是 IP 网络命令和故障诊断命令，这两个相关知识点的分值约在 3～5 分之间。本章考点知识结构图如图 14-1 所示。


图 14-1　考点知识结构图

## 14.1　IP 配置网络命令

### 14.1.1　考点分析

本节主要讲解网络工程师考试中最常考查的 Windows 系统中与配置 IP 网络相关的命令，这部分出题的频率比较高。**注意本书中涉及的各类配置命令参数太多，因此只讲重要的、常考的参数。**

### 14.1.2　知识点精讲

1. ipconfig

ipconfig 是 Windows 网络中最常使用的命令，用于显示计算机中网络适配器的 IP 地址、子网掩码及默认网关等信息。这仅是 ipconfig 不带参数的用法，在网络工程师的考试中考察的主要是它带参数用法的题，尤其是下面讨论到的基本参数，必须得要熟练掌握。

命令基本格式：

**ipconfig** [ **/all** | **/renew** [*adapter*] | **/release** [*adapter*] | **/flushdns** | **/displaydns** | **/registerdns** |]

具体参数解释如表 14-1 所示。

表 14-1　ipconfig 基本参数表

| 参数 | 参数作用 | 备注 |
| --- | --- | --- |
| /all | 显示所有网络适配器的完整 TCP/IP 配置信息 | 尤其是查看 MAC 地址信息，DNS 服务器等配置 |
| /release adapter | 释放全部（或指定）适配器的、由 DHCP 分配的动态 IP 地址，仅用于 DHCP 环境 | DHCP 环境中的释放 IP 地址 |

续表

| 参数 | 参数作用 | 备注 |
| --- | --- | --- |
| /renew adapter | 为全部（或指定）适配器重新分配 IP 地址。常用 release 结合使用 | DHCP 环境中的续借 IP 地址 |
| /flushdns | 清除本机的 DNS 解析缓存 | |
| /registerdns | 刷新所有 DHCP 的租期和重注册 DNS 名 | DHCP 环境中的注册 DNS |
| /displaydns | 显示本机的 DNS 解析缓存 | |

在 Windows 中可以选择“开始菜单”→“运行”命令并输入 CMD 进入 Windows 的命令解释器，然后再输入各种 Windows 提供的命令，也可以执行“开始菜单”→“运行”命令直接输入相关命令。在实际应用中，为了完成一项工作，往往会连续输入多个命令，最好是直接进入命令解释器界面。

常见的命令显示效果如图 14-2 所示。

```
Ethernet adapter 无线网络连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) Wireless WiFi Link
4965AG
        Physical Address. . . . . . . . . : 00-1F-3B-CD-29-DD
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.0.235
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DHCP Server . . . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 202.103.96.112
                                            211.136.17.108
        Lease Obtained. . . . . . . . . . : 20xx年10月6日 10:59:50
        Lease Expires . . . . . . . . . . : 20xx年10月6日 11:29:50
```

图 14-2　ipconfig/all 显示效果图

从此命令中不仅可以知道本机的 IP 地址、子网掩码和默认网关，还可以看到系统提供的 DHCP 服务器地址和 DNS 服务器地址。从图中最后两项还可以看到 DHCP 服务器设置的租期是半个小时。

2. tracert

tracert 是 Windows 网络中 Trace Route 功能的缩写。基本工作原理是：通过向目标发送不同 IP 生存时间（TTL）值的 ICMP ECHO 报文，在路径上的每个路由器转发数据包之前将数据包上的 TTL 减 1。当数据包上的 TTL 减为 0 时，路由器返回给发送方一个超时信息。

在 tracert 工作时，先发送 TTL 为 1 的回应报文，并在随后的每次发送过程中将 TTL 增加 1，直到目标响应或 TTL 达到最大值为止，通过检查中间路由器超时信息确定路由。

以下命令是网络工程师在实际中最常使用的检查数据包路由路径的命令，其基本格式如下：

**tracert** [-d] [-h *maximumhops*] [-w *timeout*] [-R] [-S *srcAddr*] [-4][-6] *targetname*

其中各参数的含义如下：

- -d：禁止 tracert 将中间路由器的 IP 地址解析为名称，这样可加速显示 tracert 的结果。
- -h maximum hops：指定搜索目标的路径中存在节点数的最大数（默认为 30 个节点）。

- -w timeout：指定等待“ICMP 已超时”或“回显答复”消息的时间。如果超时的时间内未收到消息，则显示一个星号（*）（默认的超时时间为 4000 毫秒）。
- -R：指定 IPv6 路由扩展标头用来将“回显请求”消息发送到本地计算机，使用目标作为中间目标并测试反向路由。
- -S：指定在“回显请求”消息中使用的源地址，仅当跟踪 IPv6 地址时才使用该参数。
- -4：指定 IPv4 协议。
- -6：指定 IPv6 协议。
- targetname：指定目标，可以是 IP 地址或计算机名。

【例 14-1】tracert 应用实例。为了提高其回显的速度，可以使用-d 选项，tracert 不会对每个 IP 地址都查询 DNS。命令显示如下：

```
C：\Documents and Settings\Administrator>tracert  -d  61.187.55.33
Tracing route to 61.187.55.33 over a maximum of 30 hops
  1    <1 ms    <1 ms    <1 ms  172.28.27.254
  2     1 ms    <1 ms    <1 ms  10.0.1.1
  3     3 ms     3 ms     3 ms  61.187.55.33
Trace complete.
```

从命令返回的结果可以看到数据包必须通过两个路由器 172.28.27.254 和 10.0.1.1 才能到达目标计算机 61.187.55.33，同时也可以知道本计算机的默认网关是 172.28.27.254。另外，若是内部的网络地址使用了地址转换，则地址转换之后的地址范围一般就是 61.187.55.33 同一网络的地址。

如果要查找从本地出发，经过 3 个跳步到达名字为 www.hunau.net 的目标主机的路径，则其命名显示如下：

```
C：\Documents and Settings\Administrator>tracert -h 3 www.hunau.net
Tracing route to www.hunau.net [61.187.55.40]
over a maximum of 3 hops：
  1     3 ms     4 ms     4 ms  10.1.0.1
  2    16 ms    39 ms     3 ms  222.240.45.188
  3     5 ms     4 ms     4 ms  61.187.55.40
Trace complete.
```

3. pathping

要跟踪路径并为路径中的每个路由器和链路提供网络延迟和数据包丢失等相关信息，此时应该使用 pathping 命令。其工作原理类似于 tracert，并且会在一段指定的时间内定期将 ping 命令发送到所有的路由器，并根据每个路由器的返回数值生成统计结果。命令行下返回的结果有两部分内容，第一部分显示到达目的地经过了哪些路由；第二部分显示了路径中源和目标之间的中间节点处的滞后和网络丢失的信息。pathping 在一段时间内将多个回应请求消息发送到源和目标之间的路由器，然后根据各个路由器返回的数据包计算结果。因为 pathping 显示在任何特定路由器或链接处的数据包的丢失程度，因此用户可据此确定存在故障的路由器或子网。

命令基本格式：

**pathping**[**-g** *host-list*] [**-h** *maximum_hops*] [**-i** *address*] [**-n**] [**-p** *period*] [**-q** *num_queries*] [**-w** *timeout*] [**-4**] [**-6**] *target_name*

其中各参数的含义如下：

- -g host-list：与主机列表一起的松散源路由。
- -h maximum_hops：指定搜索目标路径中的节点最大数（默认值为 30 个节点）。
- -i address：使用指定的源地址。
- -n：禁止将中间路由器的 IP 地址解析为名字，可以提高 pathping 显示速度。
- -p period：两次 ping 之间等待的时间（单位为毫秒，默认值为 250 毫秒）。
- -q num_queries：指定发送到路径中每个路由器的回响请求消息数。默认值为 100 查询。
- -w timeout：指定等待每个应答的时间（单位为毫秒，默认值为 3000 毫秒）。
- -4：强制使用 IPv4。
- -6：强制使用 IPv6。

targetname 指定目的端，它既可以是 IP 地址，也可以是计算机名。pathping 参数要区分大小写。实际使用中要注意：为了避免网络拥塞，影响正在运行的网络业务，应以足够慢的速度发送 ping 信号。

【例 14-2】pathping 应用实例。

```
C：\Documents and Settings\Administrator>pathping 61.187.55.33
Tracing route to 61.187.55.33 over a maximum of 30 hops
  0   1be2f61eecdb4fc [172.28.27.249]
  1   172.28.27.254
  2   10.0.1.1
  3      *        *        *
Computing statistics for 75 seconds...
 Source to Here    This Node/Link      Hop      RTT      Lost/Sent = Pct      Lost/Sent = Pct Address
  0    1be2f61eecdb4fc   [172.28.27.249]                0/ 100 =   0%   |
  1    0ms    0/ 100 =   0%      0/ 100 =   0%     172.28.27.254        0/ 100 =   0%   |
  2    0ms    0/ 100 =   0%      0/ 100 =   0%     10.0.1.1             100/ 100 =100%   |
  3   ---   100/ 100 =100%      0/ 100 =   0%    1be2f61eecdb4fc [0.0.0.0]
Trace complete.
```

若带有-n 参数，则上例中的“0 1be2f61eecdb4fc [172.28.27.249]”位置不会解析 172.28.27.249 对应的机器名，也可以提高命令回显的速度。当运行 pathping 时，将首先显示路径信息。此路径与 tracert 命令所显示的路径相同。接着，将显示约 75 秒的繁忙消息，这个时间随着中间节点数的变化而变化。在此期间，命令会从先前列出的所有路由器及其链接之间收集信息，结束时将显示测试结果。

在【例 14-2】中，This Node/Link、Lost/Sent = Pct 和 Address 列显示出 172.28.27254 与 10.0.1.1 之间的链接丢失了 0%的数据包。在 Address 列中所显示的链接丢失速率表明造成路径上转发数据包丢失的链路拥挤状态；路由器所显示的丢失速率表明这些路由器已经超载。

4. ARP

在以太网中规定，同一局域网中的一台计算机要与另一台计算机进行直接通信，必须要知道目标计算机的 MAC 地址。而在 TCP/IP 协议中，网络层和传输层只考虑目标计算机的 IP 地址。因此

在以太网中使用 TCP/IP 协议时，必须要能根据目的计算机的 IP 地址获得对应的 MAC 地址，这就是 ARP 协议。另一种情况是，当发送计算机和目的计算机不在同一个局域网中时，必须经过路由器才可以通信。因此，发送计算机通过 ARP 协议获得的就不是目的计算机的 MAC 地址，而是作为网关路由器接口的 MAC 地址。所有发送给目的计算机的帧都将先发给该路由器，然后通过它发给目标计算机，这就是 ARP 代理（ARP Proxy）。

由于 ARP 在工作过程中无法 ARP 响应数据的来源和真实性进行验证，导致了很多基于 ARP 的攻击的出现，解决的基本办法是绑定 IP 和 MAC 或者使用专门的 ARP 防护软件。具体做法就是在网内把客户计算机和网关都由管理员用静态命令对 IP 和 MAC 绑定。

命令基本格式：

（1）**ARP -s** inet_addr　eth_addr　[if_addr]

（2）**ARP -d** inet_addr [if_addr]

（3）**ARP -a** [inet_addr] [**-N** if_addr]

参数说明：

-s：静态指定 IP 地址与 MAC 地址的对应关系。

-a：显示所有的 IP 地址与 MAC 地址的对应，使用-g 的参数与-a 是一样的，尤其注意一下这个参数。

-d：删除指定的 IP 与 MAC 的对应关系。

-N if_addr：只显示 if_addr 这个接口的 ARP 信息。

【例 14-3】arp 应用示例。

命令“arp　-s 172.28.27.249　AA-BB-AA-BB-AA-BB”。在主机上设置此命令后，通过执行 arp -a 可以看到相关的提示：

```
Internet Address          Physical Address          Type
172.28.27.249             AA-BB-AA-BB-AA-BB         static
```

而在 arp 默认的动态解析情况下看到的是：

```
Internet Address Physical      Address                Type
172.28.27.249                  AA-BB-AA-BB-AA-BB      dynamic
```

这种方式对于计算机数量比较大的网络而言是非常不便的，因为每次重启之后均要重新设置，因此网络中通常使用防护软件来自动设置。

5. route

route 命令主要用于手动配置静态路由并显示路由信息表。

基本命令格式：

**route** [**-f**] [**-p**] *command* [*destination*] [**mask** *netmask*] [*gateway*] [**metric** metric ] [**if interface**]

参数说明：

（1）-f：清除所有不是主路由（子网掩码为 255.255.255.255 的路由）、环回网络路由（目标为 127.0.0.0 的路由）或多播路由（目标为 224.0.0.0，子网掩码为 240.0.0.0 的路由）的条目路由表。如果它与命令 Add、Change 或 Delete 等结合使用，路由表会在运行命令之前清除。

（2）-p：与 add 命令共同使用时，指定路由被添加到注册表并在启动 TCP/IP 协议的时候初始化 IP 路由表。默认情况下，启动 TCP/IP 协议时不会保存添加的路由，与 Print 命令一起使用时，则显示永久路由列表。

（3）command：该选项下可用以下几个命令：

1）print：用于显示路由表中的当前项目，由于用 IP 地址配置了网卡，因此所有这些项目都是自动添加的。

【例 14-4】route print 应用示例。

```
C:\ route print   172.*
显示 IP 路由表中以 172.开始的所有路由。
```

2）add：用于向系统当前的路由表中添加一条新的路由表条目。

【例 14-5】route add 应用示例。

```
C:\ route add 210.43.230.33 mask 255.255.255.224 202.103.123.7 metric 5
设定一个到目的网络 210.43.230.33 的路由，中间要经过 5 个路由器网段，首先要经过本地网络上的一个路由器，其 IP 为 202.103.123.7，子网掩码为 255.255.255.224。
```

3）delete：从当前路由表中删除指定的路由表条目。

【例 14-6】route delete 应用示例。

```
C:\ route delete 10.41.0.0 mask 255.255.0.0
删除到目标子网 10.41.0.0，掩码为 255.255.0.0 的路由
C:\ route delete 10.*
删除所有的以 10.起始的目标子网的 IP 路由表
```

4）change：修改当前路由表中已经存在的一个路由条目，但不能改变数据的目的地。

【例 14-7】route change 应用示例。

```
C:\ route change 210.43.230.33 mask 255.255.255.224 202.103.123.250 metric 3
命令将数据的路由改到另一个路由器，它采用一条包含 3 个网段的更近的路径。
```

（4）Destination：指定路由的网络目标地址。目标地址对于计算机路由是 IP 地址，对于默认路由是 0.0.0.0。

（5）mask subnetmask：指定与网络目标地址的子网掩码。子网掩码对于 IP 网络地址可以是一适当的子网掩码，对于计算机路由是 255.255.255.255，对于默认路由是 0.0.0.0。如果将其忽略，则使用子网掩码 255.255.255.255。

（6）gateway：指定超过由网络目标和子网掩码定义的可达到的地址集的前一个或下一个节点 IP 地址。对于本地连接的子网路由，网关地址是分配给连子网接口的 IP 地址。

（7）Metric：为路由指定所需节点数的整数值（范围是 1～9999），用来在路由表里的多个路由中选择与转发包中的目标地址最为匹配的路由。所选的路由具有最少的节点数。

（8）if interface：指定目标可以到达的接口索引。

6. netstat

netstat 是一个监控 TCP/IP 网络的工具，它可以显示路由表、实际的网络连接、每一个网络接口设备的状态信息，以及与 IP、TCP、UDP 和 ICMP 等协议相关的统计数据。一般用于检验本机各端口的网络连接情况。

若计算机有时接收到的数据报导致出现出错数据或故障，TCP/IP 可以容许这些类型的错误，并能够自动重发数据报。

Netstat 基本命令格式：

**netstat** [**-a**] [**-e**] [**-n**] [**-o**] [**-p** *proto*] [**-r**] [**-s**] [**-v**] [**interval**]

-a：显示所有连接和监听端口。

-e：用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。这些统计数据既有发送的数据报数量，也有接收的数据报数量。此选项可以与 -s 选项组合使用。

-n：以数字形式显示地址和端口号。

-o：显示与每个连接相关的所属进程 ID。

-p proto：显示 proto 指定协议的连接；proto 可以是下列协议之一：TCP、UDP、TCPv6 或 UDPv6。如果与 -s 选项一起使用则显示按协议统计信息。

-r：显示路由表，与 route print 显示效果一样。

-s：显示按协议统计信息。默认显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息。

-v：与-b 选项一起使用时，将显示包含为所有可执行组件创建连接或监听端口的组件。

interval：重新显示选定统计信息，每次显示之间暂停的时间间隔（以秒计）。按 Ctrl+C 键停止重新显示统计信息。如果将其省略，则 netstat 只显示一次当前配置信息。

【例 14-8】netstat 示例 1。

以数字方式显示系统所有的连接和端口，显示结果如下：

```
C：\Documents and Settings\Administrator>netstat -an
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0：135           0.0.0.0：0             LISTENING
  TCP    0.0.0.0：445           0.0.0.0：0             LISTENING
  TCP    127.0.0.1：1028        127.0.0.1：1029        ESTABLISHED
  TCP    127.0.0.1：1029        127.0.0.1：1028        ESTABLISHED
```

【例 14-9】netstat 示例 2。

显示以太网统计信息，显示结果如下：

```
C：\Documents and Settings\Administrator>netstat -e
Interface Statistics
                           Received            Sent
Bytes                      243559830           37675026
Unicast packets            360118              341200
Non-unicast packets        178339252           39836
Discards                   0                   0
Errors                     0                   75
Unknown protocols          33074
```

【例 14-10】netstat 示例 3。

显示系统的路由表，功能同 route print，显示结果如下：

```
C：\Documents and Settings\Administrator>netstat -r
Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x20006 ...00 19 21 d3 3b 05 ...... Realtek RTL8139 Family PCI Fast Ethernet NIC

Active Routes：
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    172.28.27.254   172.28.27.249      20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
       172.28.27.0  255.255.255.0   172.28.27.249   172.28.27.249      20
     172.28.27.249  255.255.255.255      127.0.0.1       127.0.0.1      20
     172.28.255.255 255.255.255.255   172.28.27.249   172.28.27.249      20
          224.0.0.0        240.0.0.0   172.28.27.249   172.28.27.249      20
    255.255.255.255  255.255.255.255   172.28.27.249   172.28.27.249       1
Default Gateway：      172.28.27.254
===========================================================================
Persistent Routes：
  None
```

7. nslookup

nslookup（name server lookup）是一个用于查询 Internet 域名信息或诊断 DNS 服务器问题的工具。Windows 下的 nslookup 命令格式比较丰富，可以直接使用带参数的形式，也可以使用交互式命令设置参数。

（1）非交互式查询。

简单查询时可以使用非交互式查询，基本命令格式：

**nslookup** [- *option*] [{*name*| [-*server*]}]

参数说明：

-option：在非交互式中可以使用选项直接指定要查询的参数，具体如下：

- -timeout=x：指明系统查询的超时时间，如“-timeout=10”表示超时时间是 10 秒。
- -retry=x：指明系统查询失败时重试的次数。
- -querytype=x：指明查询的的资源记录的类型，x 可以是 A、PTR、MX、NS 等。
- name：要查询的目标域名或 IP 地址。若 name 是 IP 地址，并且查询类型为 A 或 PTR 资源记录类型，则返回计算机的名称。
- -server：使用指定的 DNS 服务器解析，而非默认的 DNS 服务器。

【例 14-11】nslookup 应用示例。

```
C: >nslookup   -querytype=mx   hunau.net
Server:   ns1.hn.chinamobile.com
Address:   211.142.210.98
Non-authoritative answer:
hunau.net        MX preference = 5, mail exchanger = mail.hunau.net
hunau.net        nameserver = ns.timeson.com.cn
hunau.net        nameserver = db.timeson.com.cn
```

```
mail.hunau.net    internet address = 61.187.55.38
db.timeson.com.cn          internet address = 202.103.64.139
ns.timeson.com.cn          internet address = 202.103.64.138
```

由此可以看出，本机的默认 dns 服务器是 211.142.210.98，查询 hunau.net 的 mx 记录可以知道，邮件服务器的名字是 mail.hunau.net，其优先级是 5。hunau.net 注册的名字服务器是 ns.timeson.com.cn 和 db.timeson.com.cn，这两台 DNS 服务器的 IP 地址分别是 202.103.64.139 和 202.103.64.138。

（2）交互式查询。

使用交互式时，命令基本格式：**nslookup**。

直接使用 nslookup 命令且不带任何参数即进入 nslookup 的交互式模式查询界面。可以使用的交互命令如下：

- NAME：显示域名为 NAME 的域的相关信息。
- server NAME：设置查询的默认服务器为 NAME 所指定的服务器。
- exit：退出 nslookup。
- set option：设置 nslookup 的选项，nslookup 有很多选项，用于查找 DNS 服务器上相关的设置信息。下面对这些选项进行仔细讲解。

all：显示当前服务器或主机的所有选项。

domain=NAME：设置默认的域名为 NAME。

root=NAME：设置根服务器的 NAME。

retry=X：设置重试次数为 X。

timeout=X：设置超时时间为 X 秒。

type=X：设置查询的类型，类型可以是 A、ANY、CNAME、MX、NS、PTR、SOA、SRV 等。

querytype=X：与 type 命令的设置一样。

【例 14-12】查询 hunau.net 域名信息，此时查询 PC 的 DNS 服务器是 211.142.210.98。

```
C：>nslookup
Default Server：    ns1.hn.chinamobile.com
Address：    211.142.210.98
#当前的 DNS 服务器 ，可用 server 命令改变。设置查选条件为所有类型记录（A、MX 等）查询域名
> set querytype=ns
> hunau.net
#交互式命令，先输入查询的类型，再输入要查询的域名
Non-authoritative answer：
#非权威回答，出现此提示表明该域名的注册主 DNS 非提交查询的 DNS 服务器
hunau.net          nameserver = db.timeson.com.cn
hunau.net          nameserver = ns.timeson.com.cn
#查询域名的名字服务器
> set querytype=soa
> hunau.net
Server:   ns1.hn.chinamobile.com
Address:   211.142.210.98
Non-authoritative answer:
hunau.net   #返回 hunau.net 的信息。
```

```
primary name server = ns.timeson.com.cn
##主要名字服务器
responsible mail addr = admin. hunau.net
#联系人邮件地址 admin@hunau.net
serial = 2001082925
#区域传递序号，又叫文件版本，当发生区域复制时，该域用来指示区域信息的更新情况
refresh = 3600（1 hours）
#重刷新时间，当区域复制发生时，指定区域复制的更新时间间隔
retry = 900  (15 mins)
#重试时间，区域复制失败时，重新尝试的时间
expire = 1209600  （14 days）
#有效时间，区域复制在有效时间内不能完成，则终止更新
default TTL =43200  （12 hour）
#TTL 设置
hunau.net          nameserver = ns.timeson.com.cn
hunau.net          nameserver = db.timeson.com.cn
db.timeson.com.cn          internet address = 202.103.64.139
ns.timeson.com.cn          internet address = 202.103.64.138
#域名注册的 DNS 服务器的
```

关于 DNS 服务器，网络工程师考试中需要注意以下情况：任何合法有效的域名都必须有至少一个主名字服务器。当主 DNS 服务器失效时才会使用辅助名字服务器。

DNS 中的记录类型有很多，分别起到不同的作用，常见的有 A、MX、CNAME、SOA 和 PTR 等。一个有效的 DNS 服务器必须在注册机构注册，这样才可以进行区域复制。所谓区域复制，就是把自己的记录定期同步到其他服务器上。当 DNS 接收到非法 DNS 发送的区域复制信息后，会将信息丢弃。

8. FTP 客户端命令

FTP 是一个 Windows 机器常使用的命令。

（1）FTP 命令基本格式为：

**FTP** [**-v**] [**-n**][**-s:***filename*] [**-a**] [**-A**] [**-x:***sendbuffer*] [**-r:***recvbuffer*] [**-b:***asyncbuffers*] [**-w:***windowsize*] [**host**]

参数说明：

- -v：显示远程服务器的所有响应信息。
- -n：禁止在初始连接时自动登录。
- -s:filename：指定一个包含 FTP 命令的文本文件，这些命令会在 FTP 开始之后自动运行。
- -a：可以使用任意的本地接口绑定数据连接。
- -A：以匿名用户（Anonymous）身份登录。
- -x:send sockbuf：覆盖默认的 SO_SNDBUF 大小 8192。
- -r:recv sockbuf：覆盖默认的 SO_RCVBUF 大小 8192。
- -b:async count：覆盖默认的异步计数 3。
- -w:windowsize：覆盖默认的传输缓冲区大小 65535。
- host：FTP 服务器的 IP 地址或主机名。

（2）使用 FTP 命令连接主机之后，还可以使用内部命令进行操作，常见方法如下：

- ![cmd[args]]：在本地主机中执行交互 shell 命令，exit 回到 ftp 环境，如：!dir *.zip。

- ascii：数据传输使用 ascii 类型传输方式。
- bin：数据传输使用二进制文件传输方式。
- bye：退出 ftp 会话过程。
- cd remote-dir：进入远程主机目录。
- close：中断与远程服务器的 ftp 会话（与 open 对应）。
- delete remote-file：删除远程主机文件。
- dir[remote-dir][local-file]：显示远程主机目录，并将结果存入本地文件 local-file 中。
- get remote-file[local-file]：将远程主机的文件 remote-file 传至本地硬盘的 local-file 中。
- lcd[dir]：将本地工作目录切换至 dir。
- mdelete[remote-file]：删除远程主机文件。
- mget remote-files：传输多个远程文件。
- mkdir dir-name：在远程主机中建一个目录。
- mput local-file：将多个文件传输至远程主机。
- open host[port]：建立指定 ftp 服务器连接，可指定连接端口。
- passive：进入被动传输方式。
- put local-file[remote-file]：将本地文件 local-file 传送至远程主机。
- pwd：显示远程主机的当前工作目录。
- rmdir dir-name：删除远程主机目录。
- user user-name [password]：向远程主机表明自己的身份，需要口令时必须输入口令，如 user anonymous xp@hunau.net。

## 14.2 系统管理命令

### 14.2.1 考点分析

本节主要讲解网络工程师考试中最常考查的 Windows 系统管理相关的命令。这部分出题的频率不高，**只要掌握命令的基本作用即可。**

### 14.2.2 知识点精讲

1. MMC

微软从 Windows 2000 开始使用了管理控制台（Microsoft Management Console，MMC）的思想来管理计算机中的系统设置。在 MMC 中，用户可以添加不同的控制台组件，利用这些组件就可以对系统进行设置。通过 MMC 组件，所有的设置都可以在统一的界面中完成，降低了设置的难度。启动 MMC 可以在运行中输入 MMC 并按回车键，第一次运行的控制台是空白的，用户可以按照自己的需要添加各种管理单元进去，方法是执行“文件”→“添加/删除管理单元”命令。系统本身

已经带有很多可以添加的管理单元，并且在你安装了某些具有管理功能的第三方软件之后，只要软件支持，也可以把该软件添加到控制台中。

2. regedit

regedit 是 Windows 系统的注册表编辑器，其操作界面与 Windows 资源管理器很像。注册表将系统中每一种信息都分门别类地保存在不同的目录下面，每一个目录分支下保存有相关的配置信息，如 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 就保存了系统启动时需要自动执行的一系列程序的名字。

# 第 3 学时　案例难点 1——Windows 配置

第 3 天的第 6 学时主要学习 Windows Server 相关的服务器配置，此知识点不管是上午试题还是下午试题，均占较大的比例。从历年的考试情况来看，上午主要考查基本概念，下午主要考查 Windows Server 提供的主要应用服务器的配置以及与实际结合的应用配置。这部分所占的分值约 10～15 分。本章考点知识结构图如图 15-1 所示。


图 15-1　考点知识结构图

## 15.1　DNS 服务器配置



本部分主要讲解 DNS 服务器的配置、测试和基本应用。

### 15.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：DNS 服务器配置、测试、与实际的应用环节结合、在 DNS 中该如何设置满足实际的应用需求。

### 15.1.2　知识点精讲

DNS 服务器是 Internet 最基本的服务，所有基于域名的 Internet 服务都必然使用到 DNS 服务，Windows Server 2003 中内置了 DNS 服务器，可以实现各种 DNS 功能。本节主要以 DNS 服务器的配置为例详细讲解。在 Windows 中，DNS 服务器的安装过程比较简单，与 IIS、DHCP 等安装过程是一样的，在“Web 服务器的配置”这一节中有详细讲解，此处不在赘述。下面先了解 DNS 服务

器的基本配置。

启动 DNS 的配置界面如图 15-2 所示，执行“开始”→“所有程序”→“管理工具”→DNS 命令启动 DNS 服务管理器，管理器界面如图 15-3 所示。

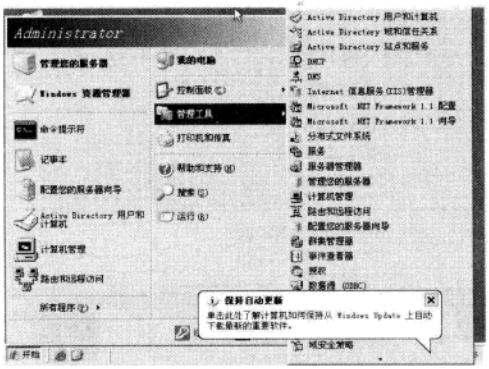



图 15-2 启动 DNS 服务器管理界面

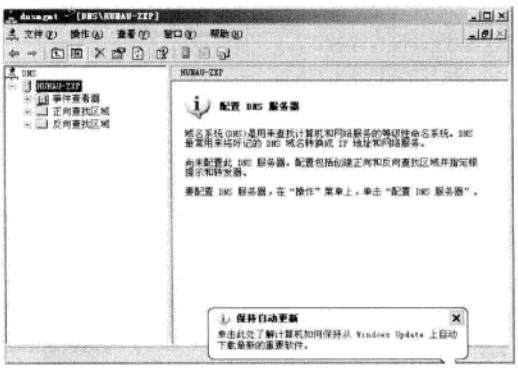



图 15-3 DNS 服务管理器

在图 15-3 的 DNS 服务管理器中，右击“正向查找区域”选项，在弹出的快捷菜单中选择“新建区域”选项，弹出如图 15-4 所示的对话框。此时系统会启动新建区域向导程序。

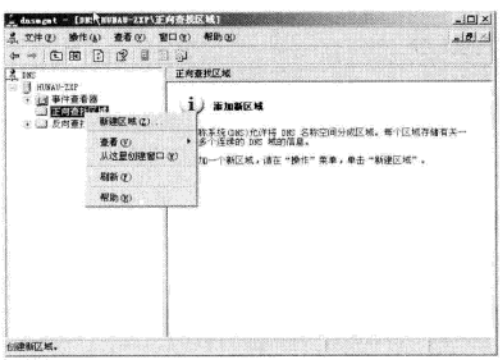



图 15-4 新建区域

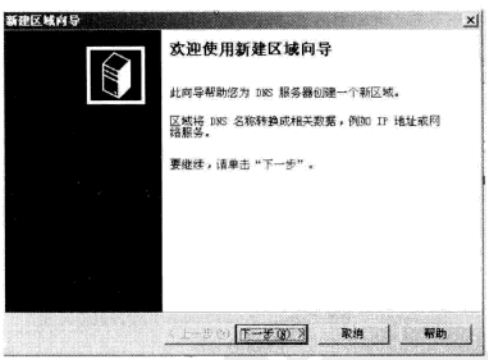



图 15-5 新建区域向导

在图 15-5 的向导欢迎界面中单击“下一步”按钮进入区域类型选择界面，如图 15-6 所示。DNS 服务器中通常创建主要区域，若是为了确保 DNS 系统的可靠性，可以再在另外一台 DNS 服务器上创建辅助区域，以实现容错；若是简单地提供域名查询，则可以建立存根区域。

本例中的服务器由于配置了活动目录，所以会出现“活动目录的区域复制作用域”选项，这里使用默认选择即可。在如图 15-7 所示的界面中，单击“下一步”按钮出现区域名称设定的界面，如图 15-8 所示，可以直接输入该区域的名称即可。单击“下一步”按钮出现动态更新选择，如图 15-9 所示。由于很多系统获得的是动态 IP 地址，因此服务器的域名必须要能动态解析到新的 IP 地址，此时就要用到动态更新。根据需要选择动态更新后，单击“下一步”按钮，DNS 的区域创建完成。

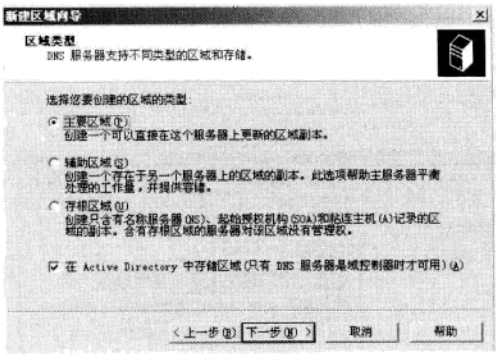



图 15-6　区域类型

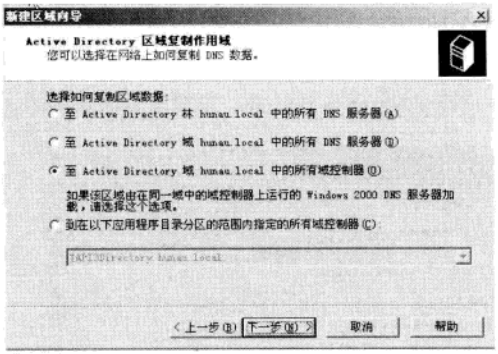



图 15-7　活动目录区域复制域

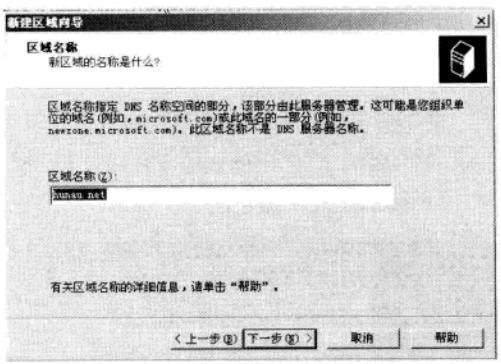



图 15-8　区域名称

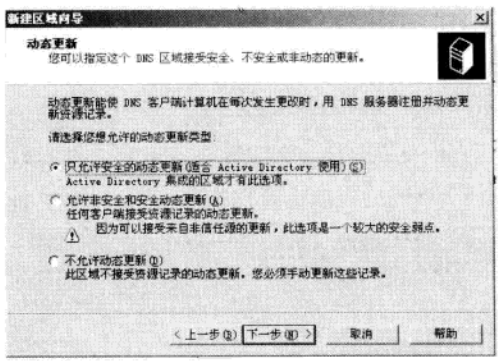



图 15-9　动态更新

在图 15-10 中单击“确定”按钮返回 DNS 服务管理器，可以看到新的区域已经创建完毕，如图 15-11 所示。



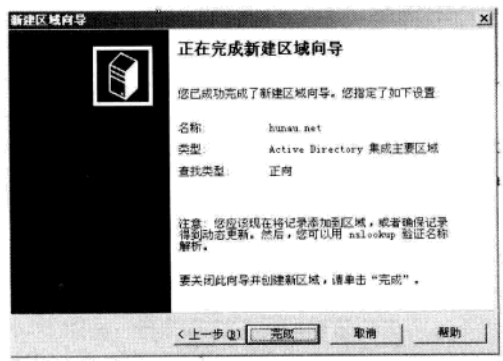



图 15-10　向导完成

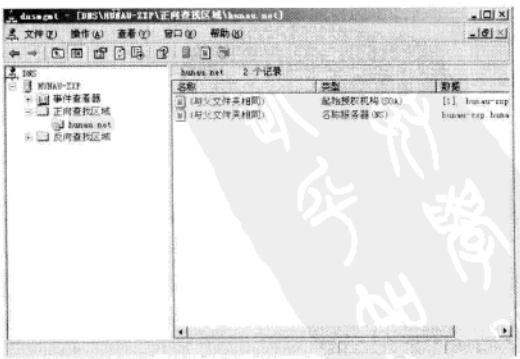



图 15-11　创建域之后的 DNS 服务器管理器

创建好区域之后，只要在区域内新建主机即可实现域名解析。在图 15-12 的界面中，在左侧窗格中右击新建的区域“hunau.net”，在右侧窗格的空白处右击，弹出快捷菜单，选择“新建主机”选项，弹出“新建主机”对话框。按照如图 15-13 所示界面中的要求输入新建主机的参数即可。

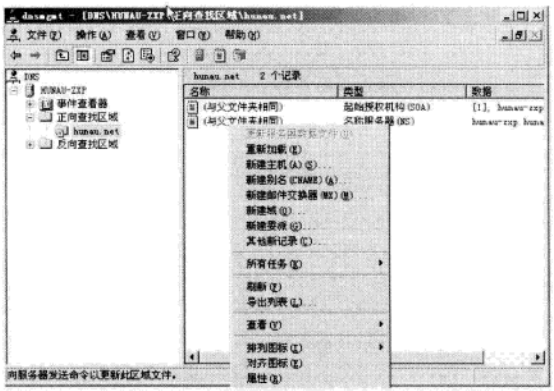



图 15-12 新建主机

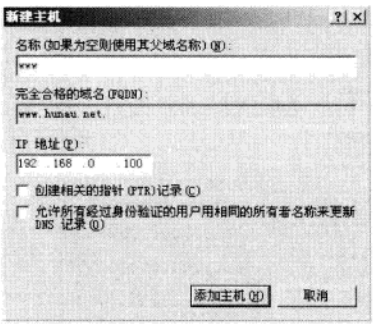



图 15-13 “新建主机”对话框

若系统已经创建了该主机 IP 地址对应的反向区域，则可以选中“创建相关的指针（PTR）记录”复选框，再单击“添加主机”按钮即可添加新主机的正向解析和反向解析，如图 15-14 所示。若反向解析区域没有创建，则不能创建反向的 PTR 记录并要报错。但正向的可以正常创建。主机记录可以创建多条，为了便于管理主机名字，DNS 运行为每个主机创建一个别名。在“新建主机”快捷菜单选中“新建别名”选项即可创建别名记录，如图 15-15 所示。在做 DNS 负载均衡时，可以给几台要分担负载的服务器取一个相同的别名。

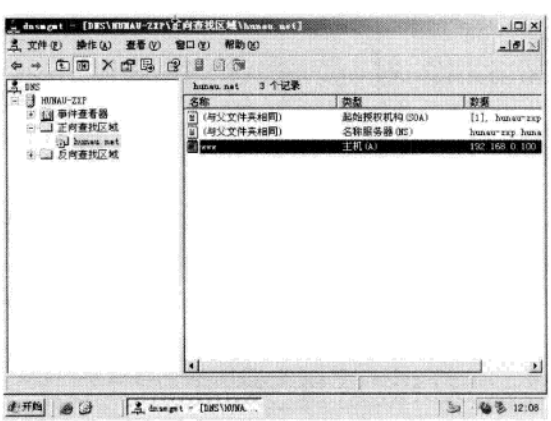



图 15-14 新建 www 主机

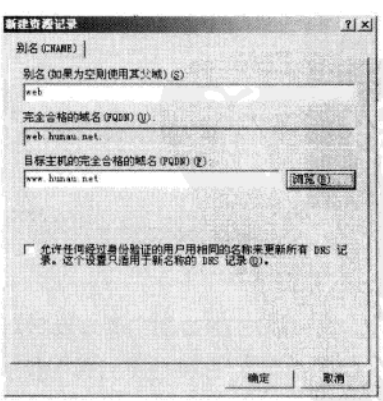



图 15-15 新建别名

要实现 DNS 的高级功能，可以在 DNS 管理器中右击区域名，在弹出的快捷菜单中选择“属性”

选项。再选择“高级”选项卡，可以对 DNS 服务器的高级功能进行设置，如图 15-16 所示。DNS 服务器也可以实现反向域名解析，可以参照创建正向解析的方式创建反向查找区域，如图 15-17 所示。

**注意**：这里的网络 ID 必须是域名对应的 IP 地址的部分。

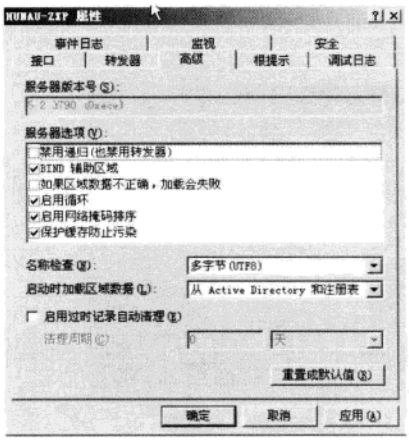



图 15-16　DNS 服务器高级属性

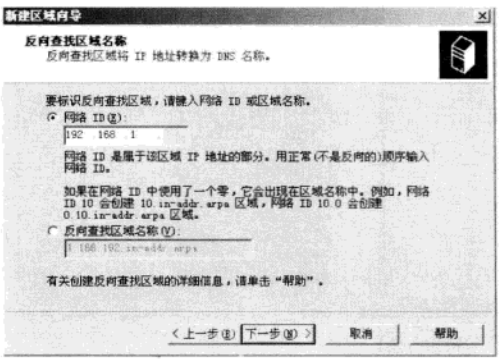



图 15-17　新建反向查找区域

按照向导提示输入 IP 地址信息即可。创建完成之后的效果如图 15-18 和图 15-19 所示。

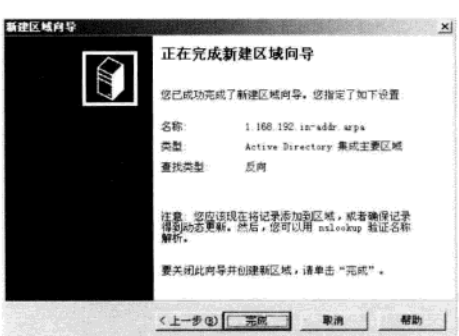



图 15-18　反向区域完成


图 15-19　DNS 服务器管理器

创建别名可以在 DNS 服务管理器的左窗格中点中区域并右击，在弹出的快捷菜单中选择“新建别名”选项，如图 15-20 所示。输入对应的别名和目标主机名后，按“确定”按钮即可看到如图 15-21 所示的界面。

DNS 服务器的其他特性都可以在域名的属性中选择，如要让 DNS 服务器在指定的网卡上接受用户请求，则可以在如图 15-22 所示的“接口”选项卡中设定地址。若要实现转发器的功能，则可

以在如图 15-23 所示的“转发器”选项卡中输入转发器的 IP 地址。

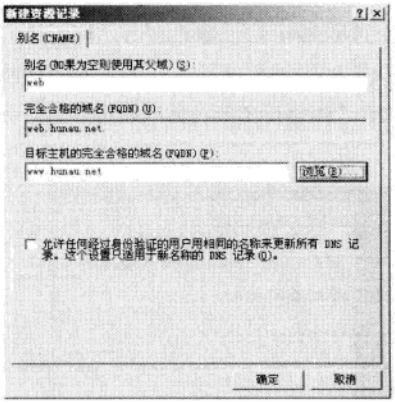



图 15-20 添加别名界面

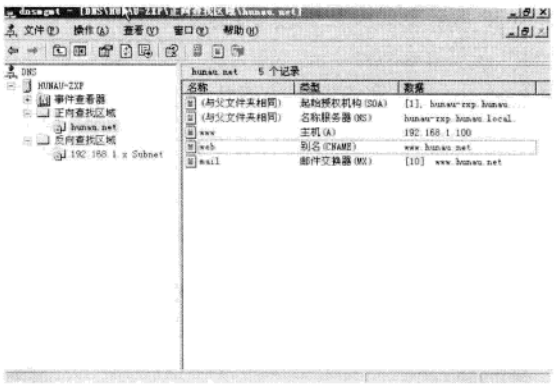



图 15-21 添加别名后的服务器管理器

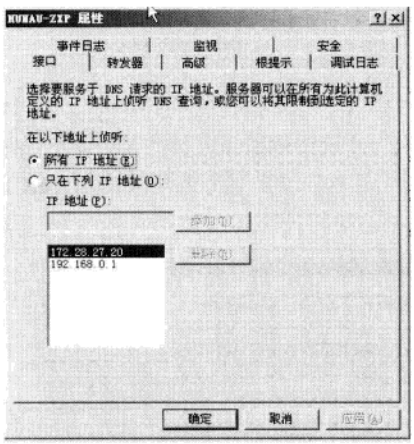



图 15-22 “接口”选项卡

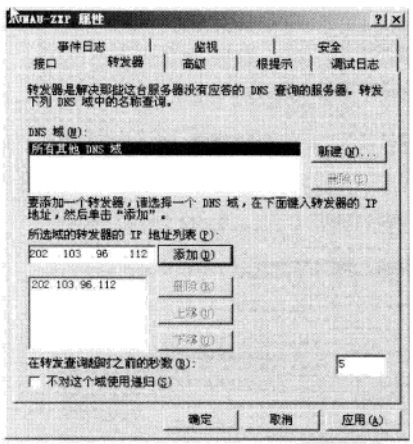



图 15-23 “转发器”选项卡

至此 Windows 中的 DNS 服务器配置完毕。

## 15.2 DHCP 服务器配置

本部分主要讲解 DHCP 服务器的安装、配置、测试和基本应用。

### 15.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：DHCP 基本配置、IP 地址池配置、DHCP 选项配置、租期配置、DHCP 服务器的测试等。

### 15.2.2 知识点精讲

DHCP 服务器的安装过程与 DNS 服务器的安装类似，在此不再赘述。安装完之后，可以执行“开始”→“所有程序”→“管理工具”→DHCP 命令启动 DHCP 服务管理器，管理器界面如图 15-24 所示。右击左窗格中的计算机名，从弹出的快捷菜单中选择“新建作用域”选项即可打开“新建作用域向导”对话框，如图 15-25 所示。

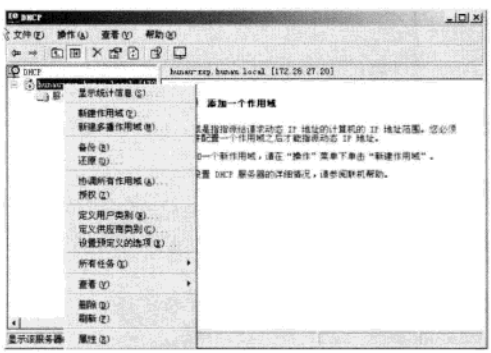



图 15-24 DHCP 服务管理器

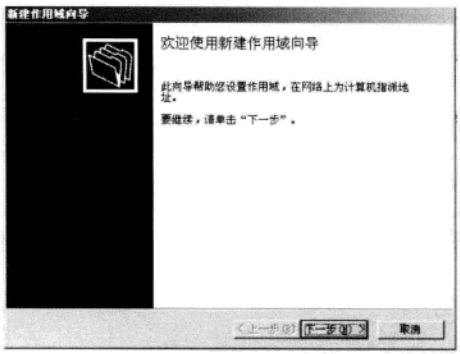



图 15-25 “新建作用域向导”对话框

按照向导的提示，在接下来的“作用域名”对话框中输入一个用于标识作用域的名字即可，如图 15-26 所示。单击“下一步”按钮，弹出“IP 地址范围”对话框，按照规划的要求输入 DHCP 服务器要分配的地址范围，如图 15-27 所示。

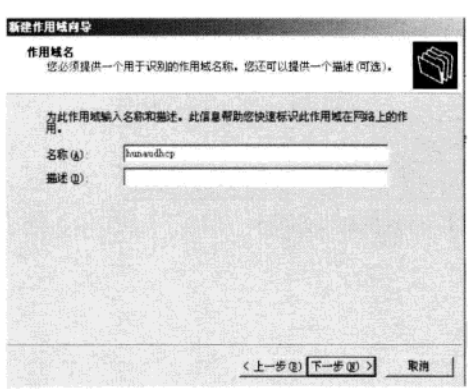



图 15-26 “作用域名”对话框

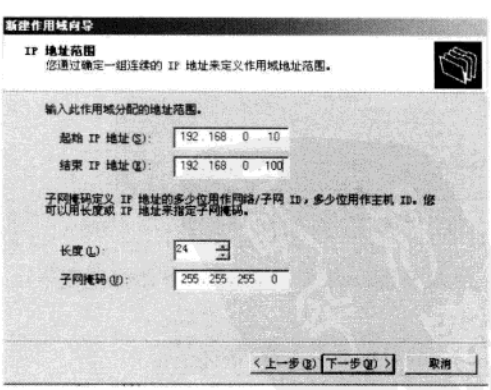



图 15- 27 “IP 地址范围”对话框

单击“下一步”按钮会出现如图 15-28 所示的“添加排除”对话框，用于使 IP 地址范围中输入的 IP 地址中的某些页数地址不参与分配。如通常可以设置一个较大的地址范围，但是某些服务器或路由器的接口地址必须使用静态地址，因此可以将这一部分地址排除。单击“下一步”按钮，可以看到如图 15-29 所示的“租约期限”对话框，注意 Windows 中 DHCP 的默认租期是 8 天。

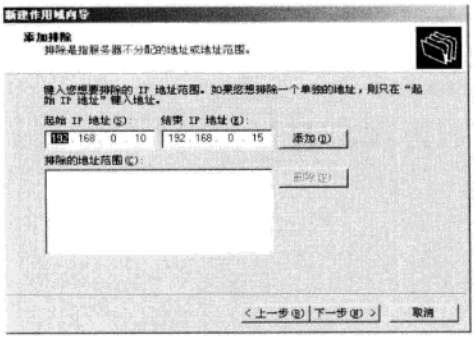



图 15-28 “添加排除”对话框

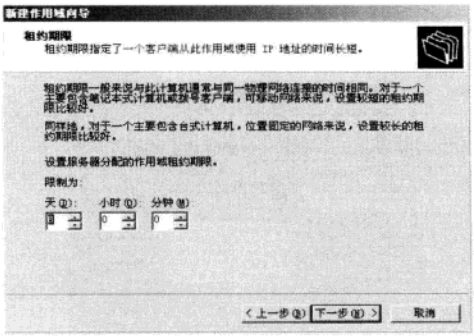



图 15-29 “租约期限”对话框

DHCP 主要用于给客户机器分配 IP 地址和子网掩码等最基本的信息，但是作为在实际 IP 网络中使用的计算机，必须还要有相关的 IP 设置，如默认网关地址、DNS 服务器地址等，这些设置也可以通过 DHCP 服务分配。实现这些设置可以在如图 15-30 所示的“配置 DHCP 选项”对话框中选择“是，我现在想配置这些选项”单选项继续按照向导程序提供的配置界面配置即可，也可以选择“否，我想稍后配置这些选项”单选项，返回 DHCP 服务管理器界面配置。如果选择“是，我现在想配置这些选项”单选项，将弹出图 15-31 所示的“路由器（默认网关）”对话框，根据规划输入这个地址范围所要使用的网关的 IP 地址。

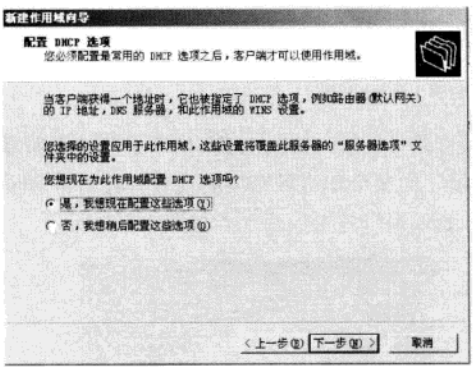



图 15-30 “配置 DHCP 选项”对话框

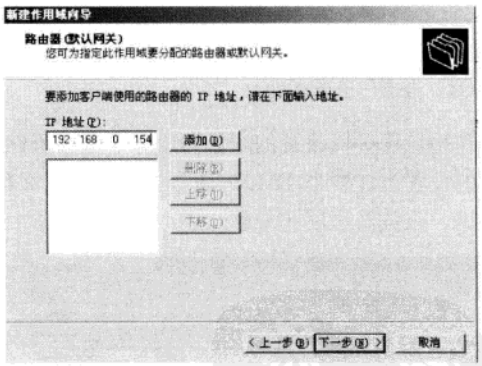



图 15-31 “路由器（默认网关）”对话框

单击“下一步”按钮，进入如图 15-32 所示的“域名称与 DNS 服务器”对话框，输入客户计算机要使用的 DNS 服务器的地址。单击“下一步”按钮后，弹出如图 15-33 所示的“激活作用域”对话框，通常选择“是，我想现在激活此作用域”单选项，否则 DHCP 服务器不会分配此区域内的 IP 地址。

当然也可以在如图 15-34 所示的 DHCP 管理器界面右击区域名，在弹出的快捷菜单中选择“激活”选项。至此，简单的 DHCP 服务器配置完成，出现如图 15-35 所示的界面。DHCP 服务器配置完成。

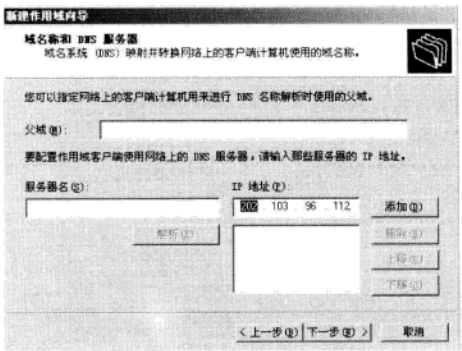



图 15-32 “域名称和 DNS 服务器”对话框

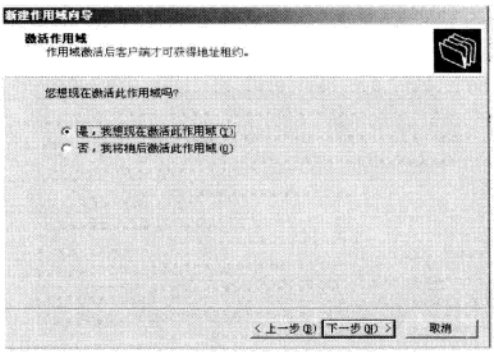



图 15-33 “激活作用域”对话框

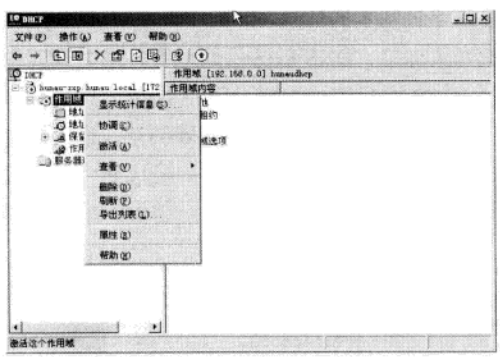



图 15-34 激活作用域菜单

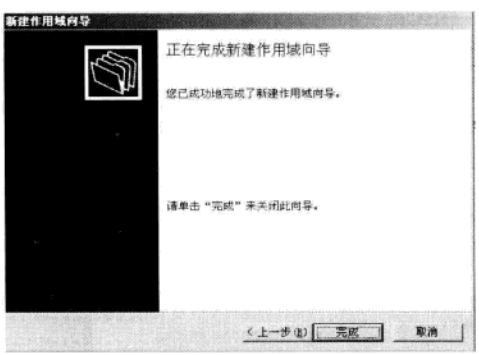



图 15-35 安装完成

作用域选项所设置的项目与服务器选项所设置的项目是一样的，如图 15-36 所示。但是服务器选项的设置会对整个 DHCP 服务器的所有区域都起作用，而某个作用域选项的设置只会对本区域起作用。服务器选项非常多，还可以自定义添加选项来处理系统内置的选项，如图 15-37 所示。

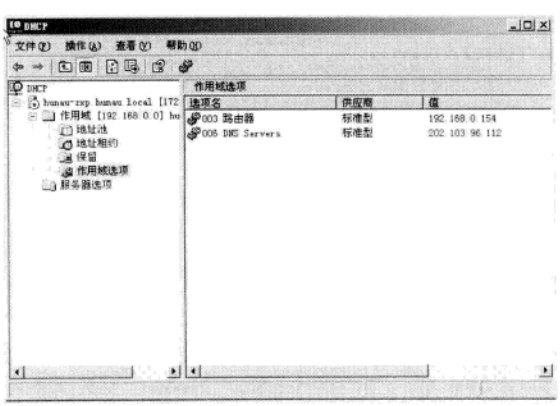



图 15-36 已配置的作用域选项

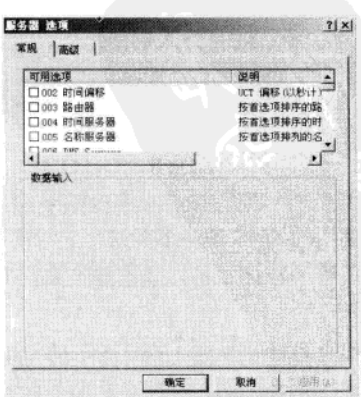



图 15-37 可配置的作用域选项

通过 DHCP 服务管理器可以方便、直观地看到此服务器上的设置。在如图 15-38 所示的界面中单击左边窗格中的地址，可以看到该作用域的地址池信息。

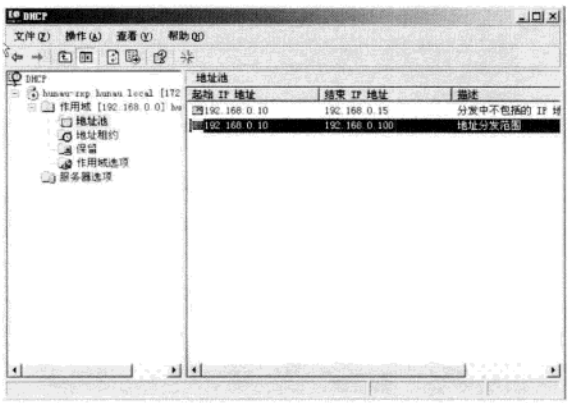



图 15-38 DHCP 地址池

## 15.3 Web 服务器配置

本部分主要讲解 Web 服务器的安装、配置、测试等。

### 15.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：Web 服务器的配置、目录权限、SSL 配置等。

### 15.3.2 知识点精讲

Web 服务是 Internet/Intranet 中最为常见的服务，在 Windows Server 2003 中集成的 IIS 包含了 Web 服器、FTP 服务器及虚拟的 SMTP 服务器等，网络工程师考试主要的考点是 Windows 的 Web 服务器和 FTP 服务器。

下面就 Windows Server 2003 上 Web 服务器的配置细节进行阐述，并详细讲解网络工程师考试中可能考到的内容。

1. Web 服务器安装于配置

要安装 Web 服务器，可以执行“开始”→“所有程序”→“管理工具”→“管理您的服务器”命令进入 Web 配置界面，也可以执行“控制面板”→“管理工具”→“添加删除程序”→“Windows 组件”命令选择 IIS 组件进行安装，安装向导提供了便利的安装步骤，只需要按照 Web 服务器的实际情况输入相关的参数接口即可。首先从开始菜单打开“管理您的服务器“界面，如图 15-39 所示。

在打开的“应用程序服务器”窗口中（如图 15-40 所示）可以看到“Internet 信息服务（IIS）管理器”选项，单击后可以展开列表，找到其中的默认网站项，右击后弹出快捷菜单，选择“新建”选项可以看到新建网站或虚拟目录两大类，如图 15-41 所示。

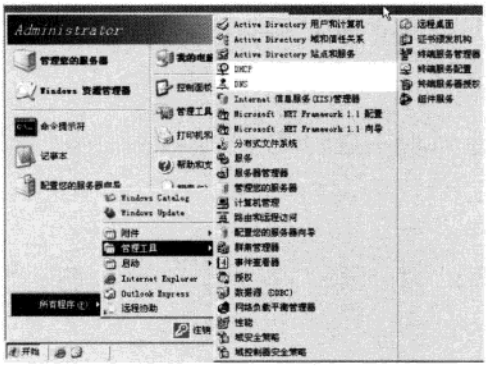



图 15-39　管理您的服务器

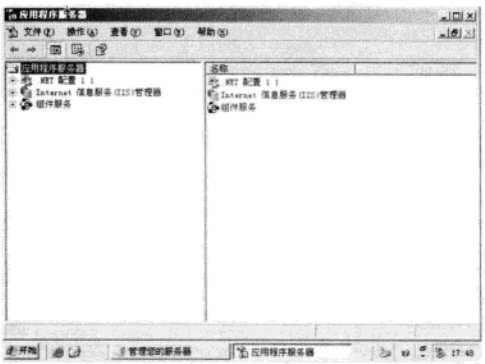


图 15-40　IIS 配置主界面

单击“新建网站”选项将出现网站创建向导，如图 15-42 所示。

图 15-41　“新建网站”选项

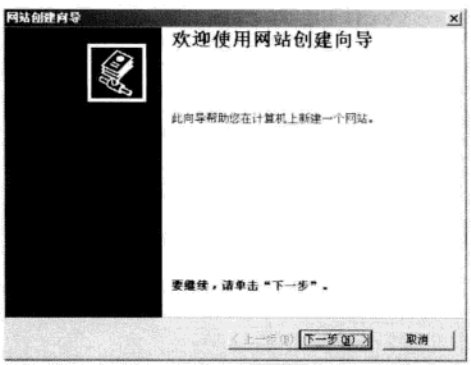



图 15-42　网站创建向导

在向导中输入网站的描述，便于在 IIS 管理器中区分，如图 15-43 所示。在 IP 地址与端口设置界面中要注意网站 IP 的选择，默认的是“全部未分配”，意味着通过 Web 服务器上任何一个 IP 地址都可以访问该网站。在一台 Web 服务器上可以同时创建多个网站，具体以下有三种实现方式：

（1）通过不同的 TCP 端口对应不同的网站。

（2）通过不同的 IP 地址对应多个不同的网站，但这种方式需要消耗多个 IP 地址，所以较少使用。

（3）通过不同的主机头区分不同的网站，这些网站可以有相同的端口和 IP 地址。

因此在如图 15-44 所示的对话框中配合不同的 IP 地址、端口和主机头的配置方式，可以在一台服务器上组建多个网站。若是指定某个具体的 IP 地址，则只能在该 IP 地址上访问网站，其他的

接口 IP 是不可以访问的；若要在一台服务器上实现通过 IP 地址区分多个不同的网站，则可以在不同的网站配置向导中将网站分别绑定到不同的接口地址上。默认端口是 80，可以不修改，若服务器的端口改变了，则客户端在访问网站时，URL 地址中必须增加端口号；若要在一台服务器上通过端口区分多个不同的网站，则可以在网站的配置向导中，对不同的网站配置不同的端口即可。此网站的主机头默认设置为空，若需要设置主机头区分网站，可以在 DNS 上注册多个域名对应同一个 IP 地址，然后在每个网站的主机头设置成对应的 DNS 中注册的域名即可。

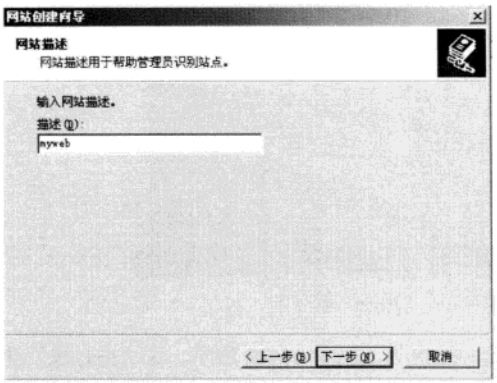



图 15-43 “网站描述”对话框

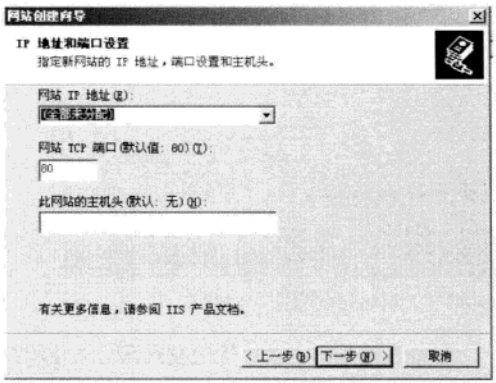



图 15-44 “IP 地址与端口设置”对话框

单击“下一步”按钮后将打开“网站主目录”对话框，默认的主目录在 systemroot\inetpub\wwwroot 文件夹下。可以通过“浏览文件夹”对话框选择自定义的文件夹，如图 15-45 所示。若选中了“允许匿名访问网站”复选框，则所有用户都可以访问该网站，如图 15-46 所示。

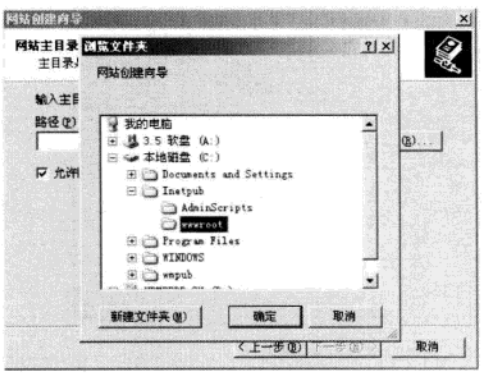



图 15-45 “浏览文件夹”对话框

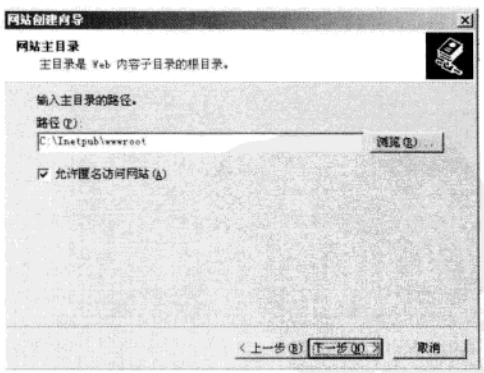



图 15-46 “网站主目录”对话框

单击“下一步”按钮后打开“网站访问权限”对话框，如图 15-47 所示，若是静态页面网站，则只要选中“读取”复选框即可；若是网站运行有 ASP 程序，则要选中“运行脚本”复选框；若是网站还有 CGI 程序或 ISAPI 的动态网站程序，则必须选中“执行”复选框。根据网站是否需要

写入数据确定写入权限。最后的“浏览”复选项通常不能选择，否则客户端可以看到网站的目录结构，造成安全隐患。

至此，网站基本设置完成。若需要进一步设置网站，可以在IIS管理器中单击“myweb属性”选项，有八大项可以详细设置，如图15-48所示，其中网站部分上面已经讲解过了。

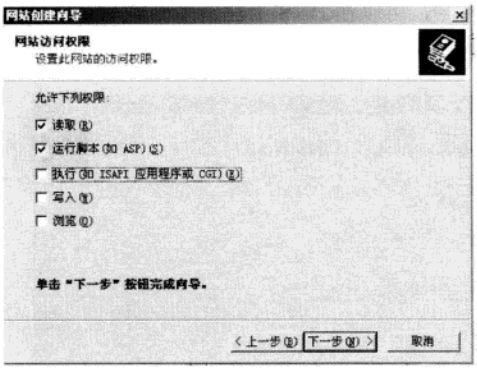



图15-47 “网站访问权限”对话框

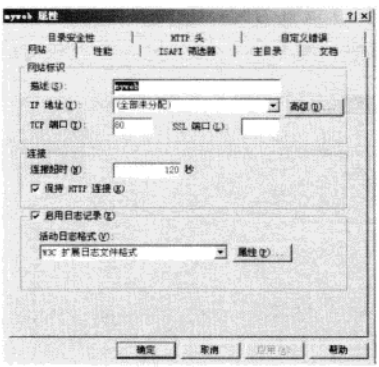



图15-48 “网站”选项卡

“性能”选项卡主要用于限制网站可以使用的带宽和连接数，如图15-49所示。在“主目录”选项卡中可以设置网站的资源来源，大部分网站的资源都是放在Web服务器上的，也可以来自另外一台计算机上的共享文件夹，当然也可以通过重定向直接将访问指向固定的URL，如图15-50所示。

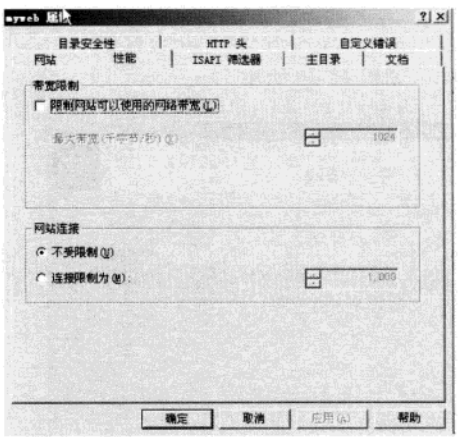



图15-49 Web性能设置

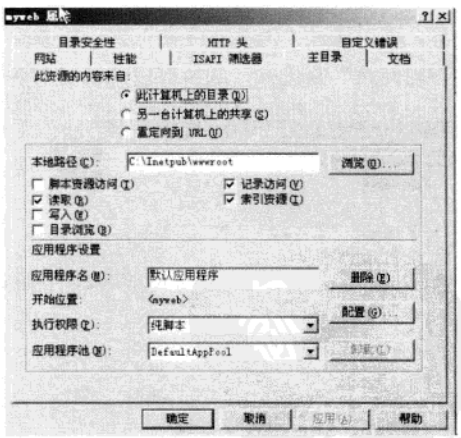



图15-50 Web主目录设置

“文档”选项卡主要用于指定网站的默认文档的名字，在设定默认文档后，用户只要输入域名或IP地址，网站会自动寻找默认文档名对应的文档并传给客户端，如图15-51所示。启用文档页脚的功能是在网站设计过程中获得统一的网站页脚效果，具体的网页不设计页脚，而是设计一个页脚文档，存放到服务器上，然后设置启用文档页脚，则网站的每一个页面都自动附加页脚文档的内

容，形成同样的风格。在“HTTP 头”选项卡中可以添加自定义的 MIME 类型和扩展名，如图 15-52 所示，MIME 格式的内容广泛用于网页文档中，通常可以将 MPEG 视频文件连接到一个网页上播放。当用户浏览这个网页并单击这个 MPEG 文件连接时，IIS 会将这个文件及注册的 MIME 类型和子类型（video/mpeg）发送到这个浏览器。客户浏览器如果对 MPEG MIME 格式支持，则浏览器就会显示这个文件；若浏览器不支持这个 MIME 格式，则根据其文件名和扩展名去查找助手应用程序列表，再选择相应的应用程序显示这个文件或者返回一个错误信息。因此需要根据网站的需要注册常用的 MIME 类型和扩展名。

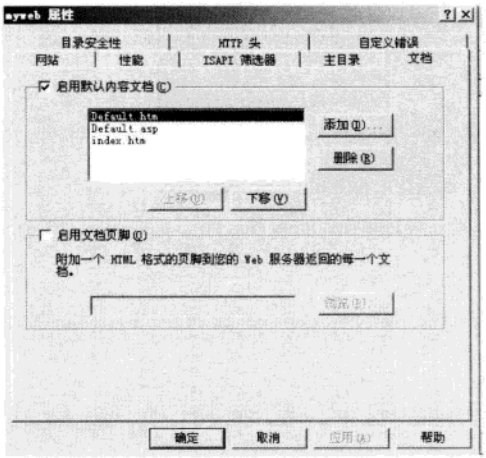



图 15-51 Web 默认文档设置

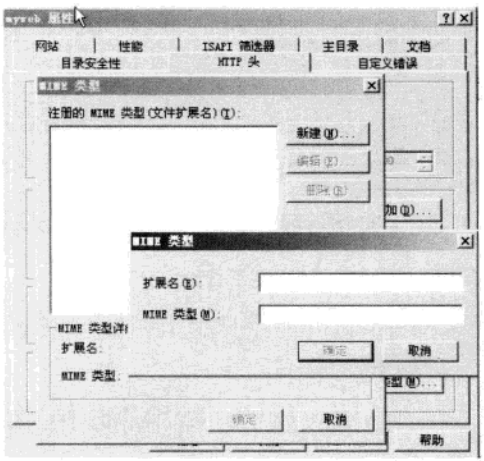



图 15-52 MIME 类型设置

在“目录安全性”选项卡中，主要体现在身份验证和访问控制、IP 地址和域名限制、安全通信三方面。在身份验证方式中，通常 Web 站点都允许匿名访问，此时 IIS 会自动使用 IUSR_computername 的用户作为匿名访问的用户，如图 15-53 所示。

只有在禁用匿名访问并使用 NTFS 访问控制列表限制了权限才可以使用验证身份的方式访问网站，IIS 提供了以下几种不同的身份验证方式，如图 15-54 所示。

（1）集成的 Windows 身份验证。该验证要求用户在与受限的内容建立连接前提供 Windows 用户名和密码，并且用户名和密码是以哈希值的形式通过网络传输的，是一种安全的身份验证形式。

（2）Windows 域服务器的摘要式身份验证。该验证可以使用 Active Directory（R）并在网络上发送哈希值，而不是明文密码。

（3）基本身份验证（以明文形式发送密码）。该验证以明文方式通过网络发送密码，由于用户名和密码没有加密，因此可能存在安全风险，但是基本身份验证是 HTTP 规范的一部分并受大多数浏览器支持。

还可以通过对 IP 地址和域名的限制来约束用户的访问，如图 15-55 所示。若需要使用安全通信，则需要先申请服务器证书，导入证书后才可以在 Web 上建立安全通信，此时可以使用的 SSL

协议端口是443。用户访问网站必须以HTTPS://IP地址的形式访问。

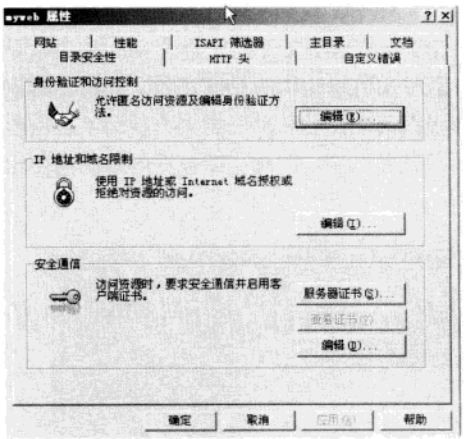



图15-53　目录安全性设置

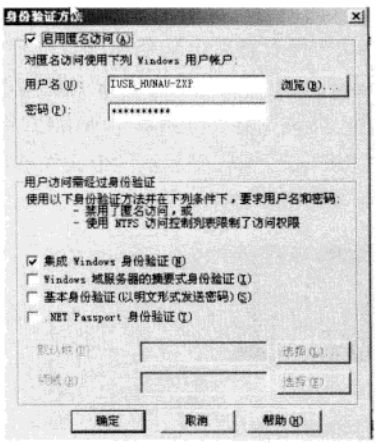



图15-54　身份验证方式设置

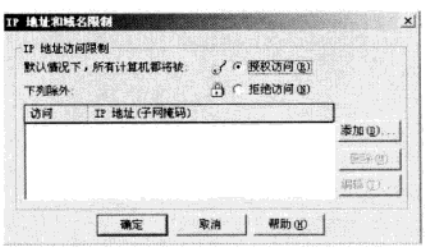



图15-55　IP地址域名限制

## 15.4　FTP服务器配置



本部分主要讲解FTP服务器的安装、配置、测试和基本应用。

### 15.4.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：FTP服务器基本配置、FTP用户、FTP访问权限、用户隔离等。

### 15.4.2　知识点精讲

1. FTP服务器的安装

因为FTP服务器是IIS中的另一个服务，因此其安装过程类似于Web服务器的安装。本节介绍从控制面板中的“添加/删除程序”界面入手的安装过程。首先执行“开始”→“控制面板”→“添加/

删除程序”→“添加/删除 Windows 组件”命令，打开“Windows 组件向导”对话框，如图 15-56 所示。

在“Windows 添加/删除组件”界面中拉动滚动条，找到“Internet 信息服务（IIS）”选项，单击“详细信息”按钮，选择“文件传输协议（FTP）服务”选项。依据向导完成 FTP 服务器的安装，如图 15-57～图 15-60 所示。


图 15-56　启动安装界面

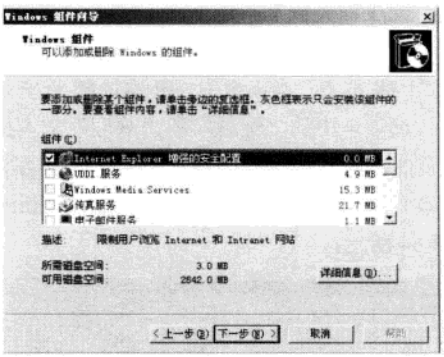



图 15-57　Windows 添加/删除组件

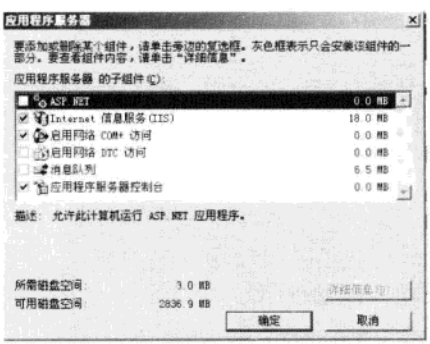



图 15-58　选择应用程序服务器

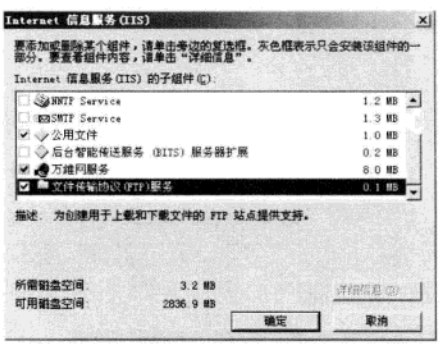



图 15-59　安装 FTP 组件


图 15-60　安装完成

2. FTP服务器的配置

FTP服务器的基本配置相对Web服务器而言要简单一些，但是其FTP用户隔离相对比较复杂，本节先讨论FTP服务器的基本配置。首先通过打开IIS信息服务管理器找到FTP站点，右击默认FTP站点，如图15-61所示，从弹出的快捷菜单中选择“新建FTP站点”选项，启动新建FTP向导程序，此过程类似于新建Web站点，在此不再赘述。FTP站点建立之后，可以通过FTP站点属性进行详细的设置。

在“FTP站点”选项卡中，IP地址和TCP端口的设置与Web中的设置相同，如图15-62所示。“消息”选项卡中的“标题”和“欢迎”文本框用于FTP客户端连接FTP服务器时显示的信息，“退出”文本框用于客户关闭FTP连接时显示的信息，如图15-63所示。“主目录”选项卡主要是设定站点目录的路径，默认的是systemroot\inetpub\ftproot目录下，根据需要设定好访问的权限，如图15-64所示。

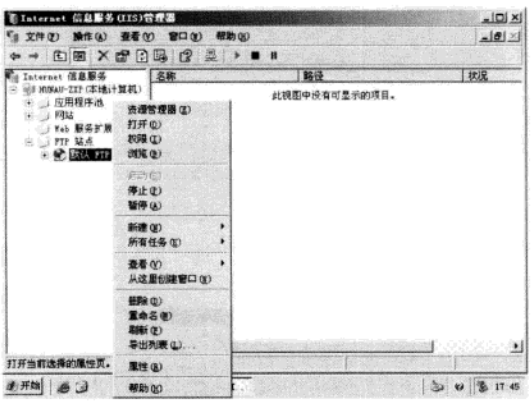



图15-61 FTP管理界面

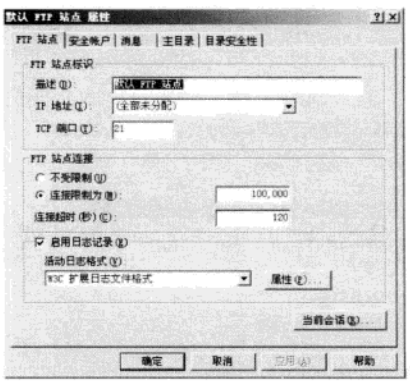



图15-62 FTP站点属性

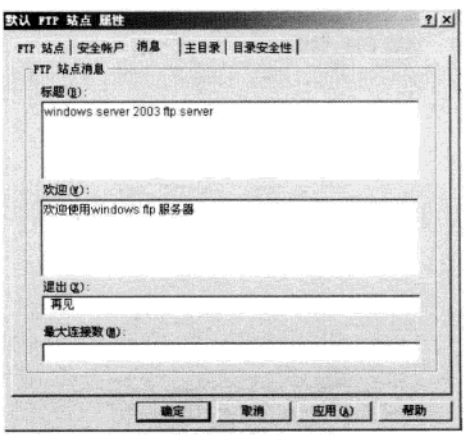



图15-63 FTP消息配置

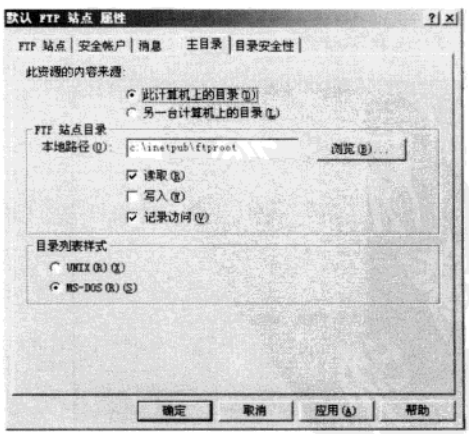



图15-64 FTP主目录设置

在“目录安全性”选项卡中也可以设置 IP 地址或 IP 地址段的访问限制，如图 15-65 所示。

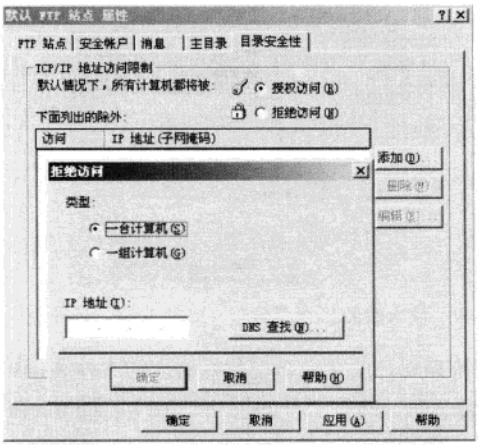



图 15-65　目录安全性配置

3. FTP 用户隔离操作

在 FTP 服务器中，最重要的设置是各个用户之间的隔离以及对目录的访问权限。在 Windows Server 2003 中提供了隔离配置。执行“开始”→“所有程序”→“管理工具”→“活动目录用户和计算机”命令（如图 15-66 所示），从中创建需要隔离的用户账号。在“用户和计算机”窗口的左窗格中单击域名 hunau.local 文件夹，使其展开，单击其中的 Users 文件，列出域上的用户名，如图 15-67 所示。

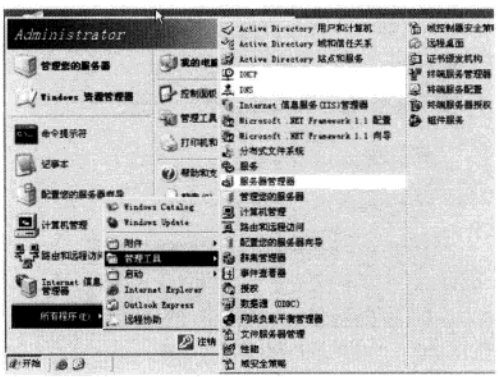



图 15-66　FTP 消息配置

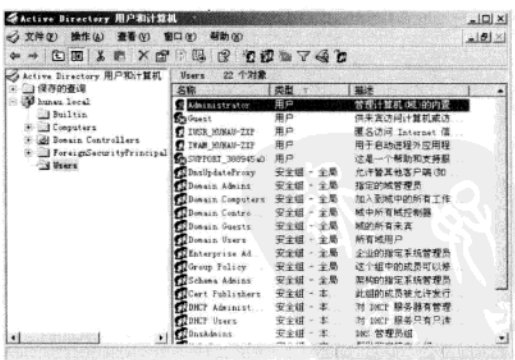



图 15-67　FTP 主目录设置

在域用户列表上右击，选择“新建用户”选项，弹出“新建对象-用户”对话框，如图 15-68 所示，根据向导提示输入用户的姓名和登录名，如图 15-69 所示，单击“下一步”按钮直到完成。不断地重复刚才的步骤，创建好需要的用户账号。

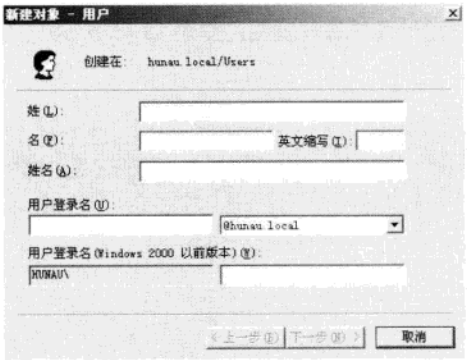



图 15-68 “新建对象-用户”对话框

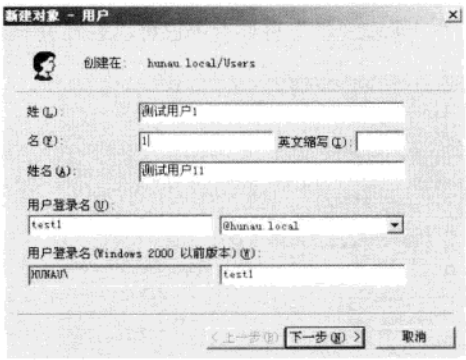



图 15-69 输入姓名和登录名

域用户账号建立好之后，可以在磁盘的用户目录下根据用户的登录名创建好对应的文件夹，以便用户登录 FTP 服务器时能限制在对应的用户名的文件夹内。执行“开始”→“运行”命令，在“运行”对话框中输入 CMD，进入 Windows 的命令行界面，输入 IISftp /setadprop 用户登录名 FTPROOT 根目录和 IISftp /setadprop 用户登录名 FTPdir 用户目录这两条命令，注册用户对应的 FTP 根目录和用户目录。然后再进入 IIS 信息管理界面，右击默认的 FTP 站点，从弹出的快捷菜单中选择“新建 FTP 站点”选项，启动新建 FTP 站点向导。在“FTP 用户隔离”对话框中，根据实际情况选择隔离的类型，如图 15-71 所示。在不隔离的情况下，用户可以互相访问主目录，可能导致存在安全隐患。普通的隔离用户方式必须为每个用户指定 FTP 站点根目录下的 FTP 主目录，而使用活动目录隔离用户可以方便地为每个用户指定 FTP 主目录。

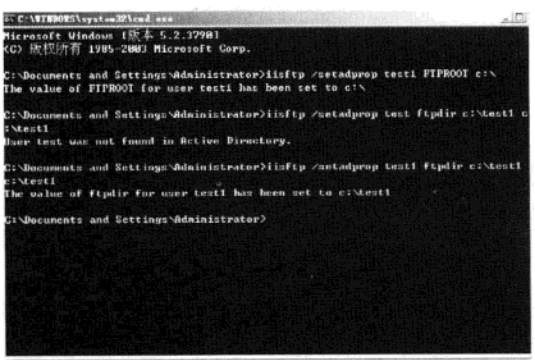



图 15-70 FTP 消息配置

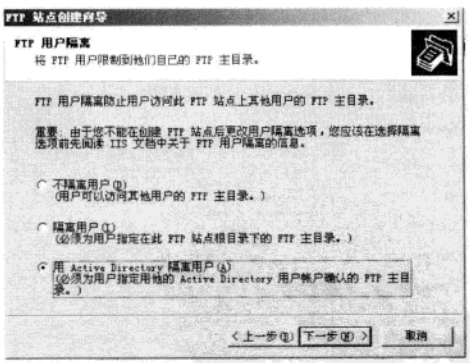



图 15-71 “FTP 用户隔离”对话框

单击“下一步”按钮，选择要隔离的 FTP 用户的用户名和对应的活动目录域，如图 15-72 所示。此时可以在“选择用户”对话框中看到之前创建的用户并单击选择，如图 15-73 和图 15-74 所示。

按“确定”按钮后返回“FTP 用户隔离”对话框，如图 15-75 所示。

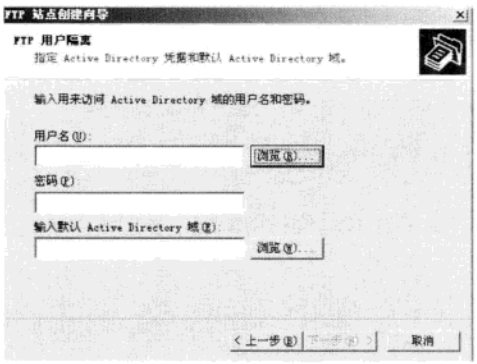



图 15-72 “FTP 用户隔离”对话框

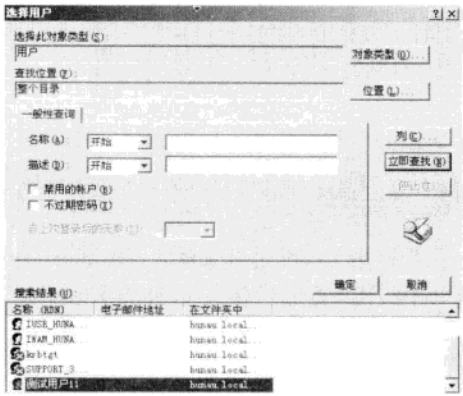



图 15-73 “选择用户”对话框

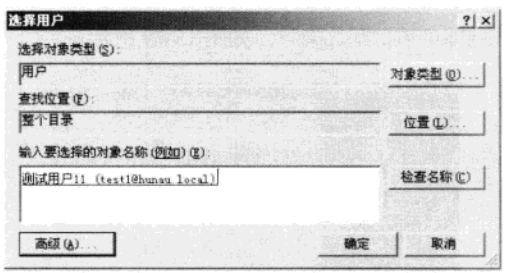



图 15-74 选择创建的用户

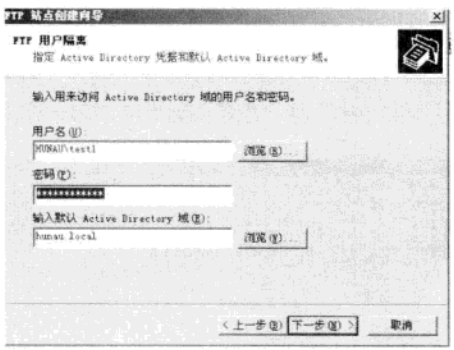



图 15-75 “FTP 用户隔离”对话框

单击“下一步”按钮，弹出“FTP 站点访问权限”对话框，如图 15-76 所示，根据需要设置相应的读取和写入权限即可。

至此，用户隔离的 FTP 站点配置完成，如图 15-77 所示。

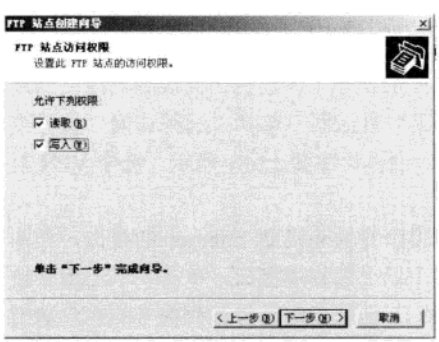



图 15-76 “FTP 站点访问权限”对话框

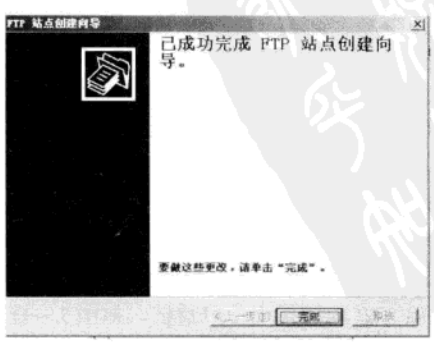



图 15-77 FTP 站点配置完成

## 15.5 远程访问与路由配置

本部分主要讲解 Windows 路由和远程访问配置服务器的安装、配置、测试和基本应用。

### 15.5.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：路由和远程访问配置、静态路由添加、DHCP 中级代理配置、拨号 VPN 服务器配置等。

### 15.5.2 知识点精讲

路由和远程访问是 Windows Server 2003 服务器提供的一个强大的网络路由和访问的功能组件，在实际应用中可以根据不同的需要来设置 Windows Server 2003 成为路由器、远程访问服务器或 VPN 服务器等。要启动路由和远程访问配置，可以执行“开始”→“所有程序”→“管理工具”→“路由和远程访问”命令，如图 15-78 所示。再从“路由和远程访问”窗口中单击找到计算机名并右击，在弹出的快捷菜单中选择“配置并启用路由和远程访问”选项即可启动配置向导，如图 15-79 所示。

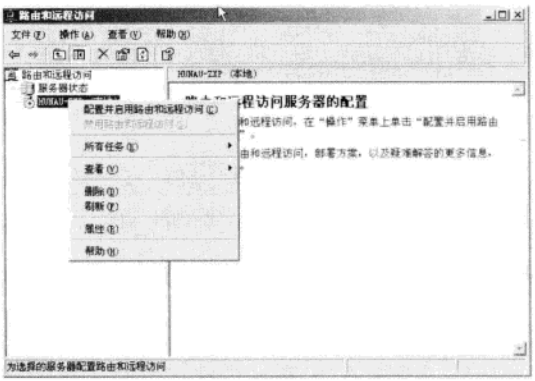



图 15-78 “路由和远程访问”窗口

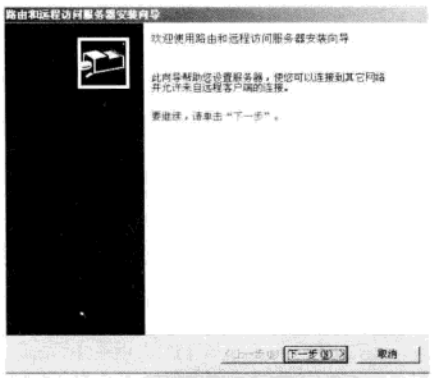



图 15-79 路由和远程访问安装向导

在“配置”对话框中可以选择多种不同的服务，如图 15-80 所示，如远程访问服务器或网络地址转换服务器等。本节先从远程访问服务器开始，在“配置”对话框中选择“远程访问（拨号或 VPN）”单选项，单击“下一步”按钮，弹出“远程访问”对话框，如图 15-81 所示，选中 VPN 复选项，再单击“下一步”按钮即可。

在“VPN 连接”对话框中需要选择一个网络接口作为将服务器连接到 Internet 的接口，如图 15-82 所示。一般做 VPN 远程连接服务器的主机要求有两个以上的物理接口。单击“下一步”按钮，弹出“IP 地址指定”对话框，如图 15-83 所示，此处的 IP 地址指定是为远程拨号的客户端指定 IP 地址。有两种方式可以选择：①通过专用的 DHCP 服务器来指定地址；②指定一个固定的 IP

地址范围。本例中选择“来自一个指定的地址范围”单选项，单击“下一步”按钮。

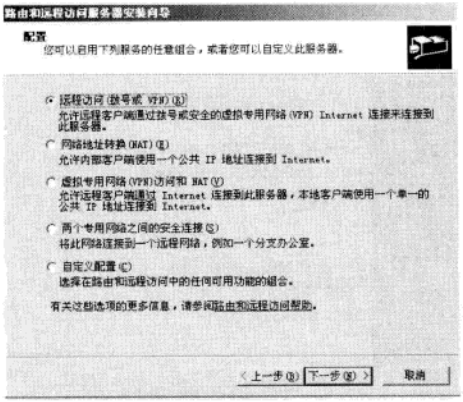



图 15-80 “配置”对话框

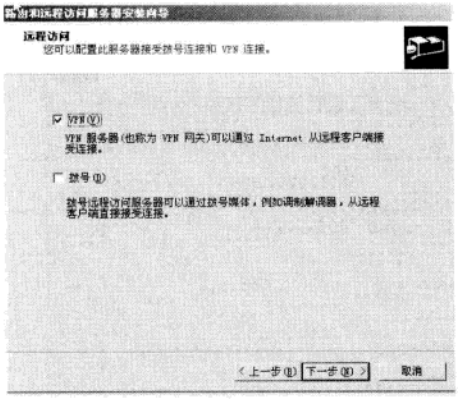



图 15-81 “远程访问”对话框

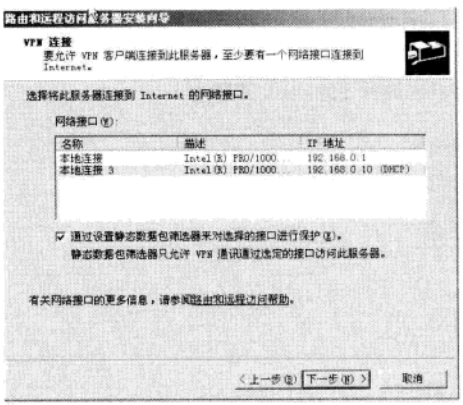



图 15-82 “VPN 连接”对话框

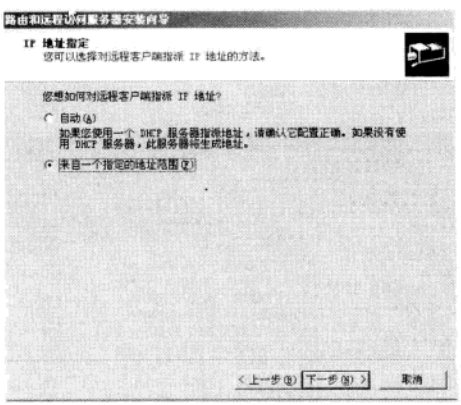



图 15-83 “IP 地址指定”对话框

在弹出的“编辑地址范围”对话框中输入起始和结束的 IP 地址，单击“确定”按钮，如图 15-84 所示。打开“管理多个远程服务器”对话框，指定是否使用独立的 RADIUS 服务器来进行身份验证，如图 15-85 所示。本例中选择“否，使用路由和远程访问来对连接请求进行身份验证”单选项。

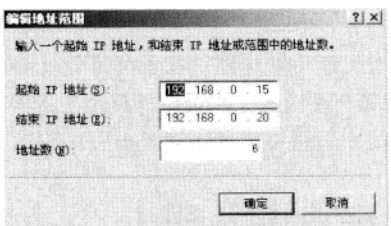



图 15-84 “编辑地址范围”对话框

弹出如图 15-86 所示的对话框，至此，远程拨号服务配置完成。

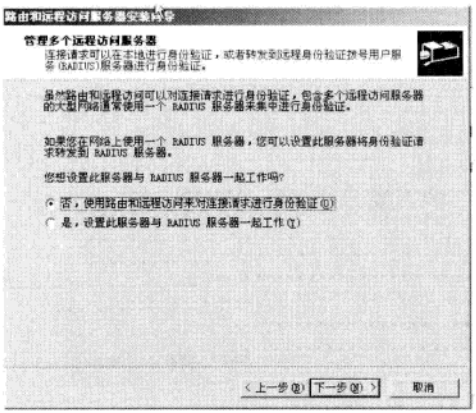



图 15-85　“管理多个远程访问服务器”对话框

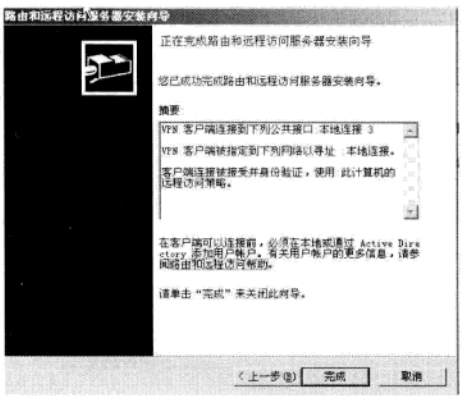



图 15-86　配置完成

要对路由和远程访问进行管理，可以通过如图 15-87 所示的“路由和远程访问”窗口进行，如单击左边窗格中的“端口”选项，可以看到路由和远程访问服务的端口配置情况。

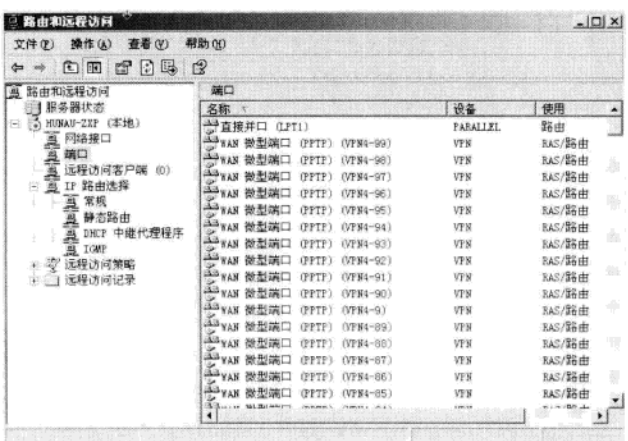



图 15-87　远程访问接口

若要配置成路由器，可以配置静态路由和动态路由以及 DHCP 中继代理。首先在如图 15-88 所示的窗口中，先右击左边窗格中的静态路由，在弹出的快捷菜单中选择“添加静态路由”选项，弹出如图 15-89 所示的“静态路由”对话框。在弹出的“静态路由”对话框中依次选择接口、目标、网络掩码、网关和跃点数，单击“确定”按钮即可。

若需要多条静态路由，则依照上述操作，把所有需要的静态路由都添加上去即可。

若服务器还需要为多个网段提供 DHCP 中继代理服务，则只要在如图 15-88 所示的“DHCP

中继代理程序属性”对话框中右击“DHCP 中继代理程序”选项，在弹出的快捷菜单中选择“属性”选项，打开如图 15-90 所示的“DHCP 中继代理程序属性”对话框，在“服务器地址”文本框中输入指定的 DHCP 服务器的 IP 地址即可。

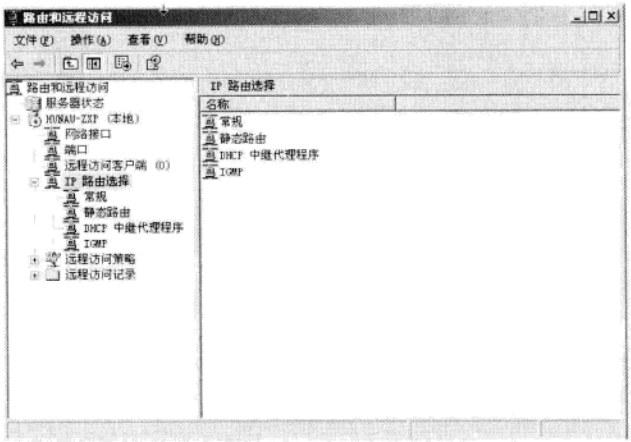



图 15-88 “路由和远程访问”窗口

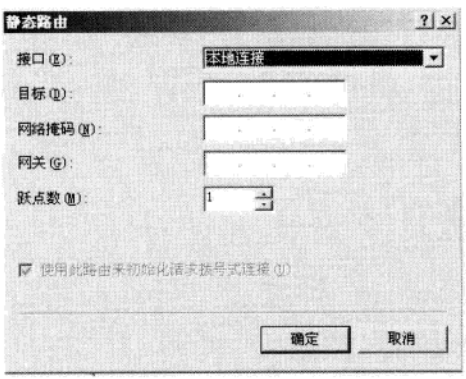



图 15-89 “静态路由”对话框

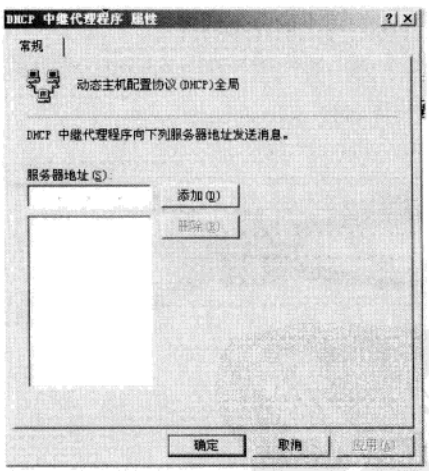



图 15-90 “DHCP 中继代理程序 属性”对话框

若要使用动态路由协议，则需要在如图 15-91 所示的窗口中右击“IP 路由选择”下的“常规”选项，在弹出的快捷菜单中选择“新增路由协议”选项即可打开如图 15-92 所示的“新增路由协议”对话框。根据网络的实际情况选择合适的路由协议。

根据图 15-92，Windows Server 2003 支持 OSPF 和 RIP v2 两种基本的动态路由协议。选择其中的路由协议，单击“确定”按钮即可。

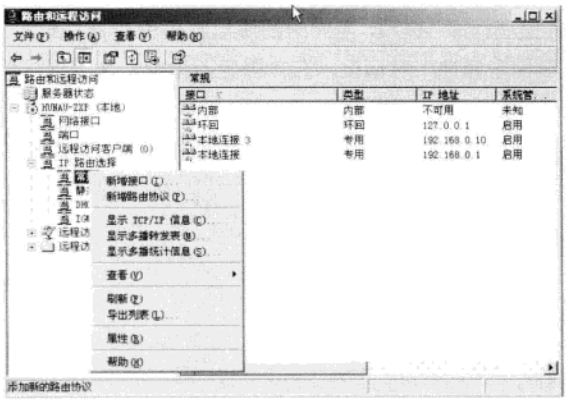



图 15-91　新增路由协议

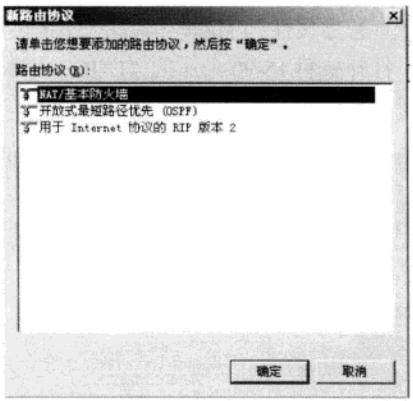



图 15-92　新增路由协议

## 第 4 学时　必考题 2——Linux 管理

第 3 天的第 4 学时主要学习 Linux 管理所涉及的重要知识点。Linux 系统是网络中服务器操作系统的一个重要平台，Linux 的管理是历年考试的核心考点之一。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 3～7 分之间。Linux 管理知识点的考察主要在上午的考试中，下午主要是在 Linux 服务器部分的大题中以小题的形式出现，多是选择题的形式。本章考点知识结构图如图 16-1 所示。

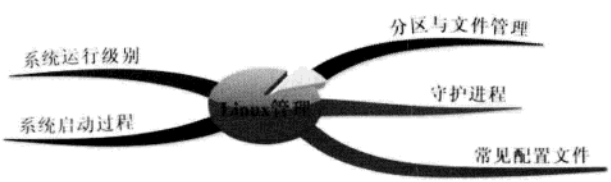



图 16-1　考点知识结构图



## 16.1　分区与文件管理

本部分主要讲解 Linux 的分区格式与文件管理。

### 16.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：Linux 的分区格式、文件管理、设备管理、分区管理等。

### 16.1.2 知识点精讲

Linux 系统相关的管理和配置指令是网络工程师考试中一个比较重要的知识点，对于 Linux，大部分考生并不是特别熟悉，因此我们主要掌握 Linux 系统最基本的知识点，包括系统的安装、分区格式、常用系统管理命令和网络配置命令等。

在安装 Linux 时，也需要像安装 Windows 一样对硬盘进行分区，为了能更好地规划分析，我们必须要对硬盘分区的相关知识有所了解。

1. 分区管理

为了区分每个硬盘上的分区，系统分配了一个 1～16 的序列号码，用于表示硬盘上的分区，如第一个 IDE 硬盘的第一个分区就用 hda1 表示，第二个分区就用 hda2 表示。因为 Linux 规定每一个硬盘设备最多能有 4 个主分区(包含扩展分区)，任何一个扩展分区都要占用一个主分区号码，也就是在一个硬盘中，主分区和扩展分区一共最多有 4 个。主分区的作用就是使计算机可以启动操作系统的分区，因此每一个操作系统启动的引导程序都应该存放在主分区上。

Linux 的分区不同于其他操作系统分区，一般 Linux 至少需要两个专门的分区 Linux Native 和 Linux Swap。通常在 Linux 中安装 Linux Native 硬盘分区。

- Linux SWAP 分区的特点是不用指定“载入点”(Mout Point)，既然作为交换分区并为其指定大小，它至少要等于系统实际内存容量，一般来说取值为系统物理内存的 2 倍比较合适。系统也支持创建和使用一个以上的交换分区，最多支持 16 个。
- Linux Native 分区是存放系统文件的地方，它能用 EXT2 和 EXT3 等分区类型。对 Windows 用户来说，操作系统的文件必须装在同一个分区里。而 Linux 可以把系统文件分几个区来装，也可以装在同一个分区中。

2. Linux 常见分区格式

(1) ext。

ext 是第一个专门为 Linux 设计的文件系统类型，叫做扩展文件系统。

(2) ext2。

ext2 是为解决 ext 文件系统的缺陷而设计的一种高性能的文件系统，又称为二级扩展文件系统。ext2 是目前 Linux 文件系统类型中使用最多的格式，并且在速度和 CPU 利用率上表现突出，是 Linux 系统中标准的文件系统，其特点为存取文件的性能极好。

(3) ext3。

ext3 是由开放资源社区开发的日志文件系统，是 ext2 的升级版本，尽可能地方便用户从 ext2fs 向 ext3fs 迁移。ext3 在 ext2 的基础上加入了记录元数据的日志功能，因此 ext3 是一种日志式文件系统。

(4) iso9660。

iso9660 标准 CDROM 文件系统，允许长文件名。在使用 CD-ROM 时常用。

（5）NFS。

Sun 公司推出的网络文件系统，允许多台计算机之间共享同一个文件系统，易于从所有计算机上存取文件。

（6）HPFS。

HPFS 是高性能文件系统，能访问较大的硬盘驱动器，提供更多的组织特性并改善了文件系统的安全特性，是 Microsoft 的 LAN Manager 中的文件系统，同时也是 IBM 的 LAN Server 和 OS/2 的文件系统。

3. 文件管理

每种操作系统都有自己独特的文件系统，用于对本系统的文件进行管理，文件系统包括了文件的组织结构、处理文件的数据结构、操作文件的方法等。Linux 文件系统采用了多级目录的树型层次结构管理文件。

（1）树型结构的最上层是根目录，用“/”表示。

（2）在根目录之下是各层目录和文件。在每层目录中可以包含多个文件或下一级目录，每个目录和文件都有由多个字符组成的目录名或文件名。

系统所处的目录称为当前目录。这里的目录是一个驻留在磁盘上的文件，称为目录文件。

4. 设备管理

Linux 中只有文件的概念，因此系统中的每一个硬件设备都映射到一个文件。对设备的处理简化为对文件的处理，这类文件称为设备文件，如 Linux 系统对硬盘的处理就是每个 IDE 设备指定一个由 hd 前缀组成的文件，每个 SCSI 设备指定一个由 sd 前缀组成的文件。系统中的第一个 IDE 设备指定为 hda，第二个 SCSI 设备定义为 sdb。

5. Linux 主要目录及其作用

（1）/：根目录。

（2）/boot：包含了操作系统的内核和在启动系统过程中所要用到的文件。

（3）/home：用于存放系统中普通用户的宿主目录，每个用户在该目录下都有一个与用户同名的目录。

（4）/tmp：是系统临时目录，很多命令程序在该目录中存放临时使用的文件。

（5）/usr：用于存放大量的系统应用程序及相关文件，如说明文档、库文件等。

（6）/var：系统专用数据和配置文件，即用于存放系统中经常变化的文件，如日志文件、用户邮件等。

（7）/dev：终端和磁盘等设备的各种设备文件，如光盘驱动器、硬盘等。

（8）/etc：用于存放系统中的配置文件，Linux 中的配置文件都是文本文件，可以使用相应的命令查看。

（9）/bin：用于存放系统提供的一些二进制可执行文件。

（10）/sbin：用于存放标准系统管理文件，通常也是可执行的二进制文件。

（11）/mnt：挂载点，所有的外接设备（如 cdrom、U 盘等）均要挂载在此目录下才可以访问。

在网络工程师考试中，只需要知道常见的目录及其作用即可。

## 16.2 系统启动过程

本部分主要讲解启动过程、启动配置、测试和基本应用。

### 16.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：启动引导程序、配置。

### 16.2.2 知识点精讲

1. Linux 启动过程

Linux 从加电自检后就要从硬盘上开始引导操作系统，具体的过程如下：

（1）引导加载程序 GRUB/LILO。

当机器引导操作系统时，首先读取硬盘主引导记录（MBR）中的信息，找到主引导加载程序，加载操作系统即可。在单一的 MBR 中只能存储一个操作系统的引导记录，因此同时安装多个操作系统时就必须使用引导加载程序。Linux 中的引导加载程序有两个，分别是 GRUB 和 LILO，通过它们的引导，操作系统可以顺利地启动。

GRUB 相对 LILO 而言有更多的优势，如支持网络引导、交互式命令界面等。GRUB 还不需要像 LILO 一样将引导的操作系统位置的信息存储在 MBR 中，因而可以避免由于错误配置 MBR 导致系统无法引导的故障。现在的系统基本倾向于 GRUB 引导。

（2）加载内核。

内核映像不是一个可执行的内核，而是一个经过压缩过的内核映像。通常它是一个 zImage 或 bzImage 文件，将其加载到内存之后，内核就开始执行了。

（3）执行 init 进程。

init 进程作为系统的第一个进程，是所有进程的发起者和控制者。init 的进程 ID（PID）为 1。它完成系统的初始化工作并维护系统的各种运行级别，包括系统的初始化、系统结束、单用户运行模式和多用户运行模式。由于 init 进程是系统所有进程的起点，内核在完成核内引导后就开始加载 init 程序。

init 进程有两个作用：第一个作用是能终结父进程。因为 init 进程绝对不会被终止，所以系统总可以使用 init 并以它为参照。如果某个进程在它衍生出来的全部子进程结束之前被终止，此时就必须以 init 为参照进程，所有失去父进程的子进程就都会以 init 作为父进程；第二个作用是在进入某个特定的运行级别（Runlevel）时运行相应的程序，以此对各种运行级别进行管理。它的这个作用是由/etc/inittab 文件定义的。

（4）通过/etc/inittab 文件进行初始化。

init 的工作是根据/etc/inittab 来执行相应的脚本进行系统初始化。网络工程师考试通常以 Redhat

为蓝本，因此本章主要讨论 Redhat 的执行顺序。Redhat 的基本执行步骤如下：

1）执行/etc/rc.d/rc.sysinit。

这是由 init 执行的第一个脚本，其主要功能是完成各个不同运行级别中相同部分的初始化工作，包括设置初始的$PATH 变量、配置网络等。

2）执行/etc/rc.d/rcX.d/下的脚本。

在系统目录/etc/rc.d/init.d 下有许多服务器脚本程序，一般称为服务（service），在系统初始化启动时会选择性地执行这些脚本程序的一部分。在/etc/rc.d 目录下有 7 个名为 rcx.d 的目录，对应系统的 7 个运行级别，这里的 X 是不同运行级别的级别数，实际中使用相应运行级别的数字代替，如运行级别 3，则执行的是/etc/rc.d/rc3.d/下的脚本。

这些脚本实际上都是一些连接文件，而不是真正的 rc 启动脚本，存放在/etc/rc.d/init.d 子目录中的、被符号连接上的命令脚本程序才是真正的程序，是它们完成了启动或者停止各种服务的操作过程。

这个脚本程序的连接文件命名规则为 K+xx+服务名或 S+xx+服务名的形式，其中 xx 为一个两位数字，K（Kill）表示结束，S（Start）表示启动。

通常这些命令脚本程序的执行顺序很重要，基本规则是先终止 K 开头的服务，然后启动 S 开头的服务，再根据字母 S 或 K 后面这个两位数字的大小来决定执行顺序，数值小比数值大的先执行，如/etc/rc.d/rc3.d/S50inet 就会在 /etc/rc.d/rc3.d/S55named 之前执行。以字母 K 开头的命令脚本程序会传递 Stop 参数；类似地，以字母 S 开头的命令脚本程序会传递 Start 参数，同时也能接收如 Restart、Status 等参数。

root 用户可以用 init x 命令改变当前运行级别，如可以将 init 0 用作关机指令，init 6 用作重启系统的指令。

3）执行/etc/rc.d/rc.local。

Redhat 中的运行模式 2、3、5 都会将/etc/rc.d/rc.local 作为最后一个运行的初始化脚本，所以用户可以在这个文件中添加脚本指令，以实现在系统开机后自动运行某个程序或者执行某项常规操作的功能。如在系统开机启动后要自动执行 pptpd 服务，则可以在/etc/rc.d/rc.local 中增加一行启动 pptpd 的指令即可。

（5）执行 /bin/login。

login 程序检验用户的输入账号和密码，若获得通过，则为使用者进行初始化环境，并将控制权交给 shell，即等待用户登录，启动过程完成。

2. GRUB 和 LILO 的配置

（1）配置 LILO 可以通过编辑/etc/lilo.conf 文件实现，其具体内容如下：

```
[root@localhost etc]# vi   /etc/lilo.conf
prompt
timeout=50
default=linux
boot=/dev/hda
map=/boot/map
```

```
install=/boot/boot.b
message=/boot/message
linear

image=/boot/vmlinuz-2.6.20-8
label=linux
initrd=/boot/initrd-2.6.20-8.img
read-only
append="root=LABEL=/"

other=/dev/hda1
optional
label=DOS
```

启动加载文件配置的说明如下：

```
prompt
timeout=50
default=linux
```

这三行表示系统启动时将会显示一个 LILO 提示信息并等待 5 秒钟，注意，timeout 的单位是 0.1 秒。如果 5 秒钟之内没有输入系统名字，那么将使用默认引导 deafault=Linux，引导标号为 Linux 的系统。

LILO 配置文件解析：

- boot=/dev/hda 表示启动盘使用第一个 ide 硬盘，也就是 hda。
- install=/boot/boot.b 表示要将/boot/boot.b 文件内容写到引导记录中，该文件在安装 Linux 时已经创建。
- image=/boot/vmlinuz-2.6.20-8 表示启动时使用的内核映像是/boot/vmlinuz-2.6.20-8。
- label=Linux 表示这个启动选择项的名称是 Linux，然后是其他的引导系统，这种配置适合同时安装了 Linux 和 Windows 两个系统的计算机。

要使得修改了的 LILO 生效，还需要执行/sbin/lilo 命令。

（2）配置 GRUB 可以通过编辑/boot/grub/grub.conf 文件实现，其具体内容如下：

```
[root@localhost grub]# vi   /boot/grub/grub.conf
default=0
  timeout=10
  splashimage=(hd1,2)/boot/grub/splash.xpm.gz
  title Windows2K3
  rootnoverify (hd0,0)
  chainloader +1

title Ubuntu
  root (hd1,2)
  kernel /boot/vmlinuz-2.6.20-8 ro root=LABEL=/
  initrd /boot/initrd-2.6.20-8.img

title Mandrake10
  kernel (hd1,4)/boot/vmlinuz root=/dev/hdb5 quiet devfs=mount acpi=off vga=788
initrd (hd1,4)/boot/initrd.img
```

GRUB 配置文件解析：

- default=表示默认启动的系统，0 为排在第一个的系统，依此类推。
- timeout=X 为 GRUB 菜单停留的时间，单位为秒。
- title XXX：XXX 为标题，就是要引导的操作系统的名字。
- root(hdX,Y)X 和 Y 都代表一个数值，X 是 Linux 的根分区所在的硬盘。如只有一个硬盘，则就是 hd0。Y 是代表 Linux 安装所在的分区，这个数值有点特别。如配置文件中将 Mandrake 安装到第二块硬盘的第二个分区，也就是 hdb5。则 root(hdX,Y)就应该写为 root(hd1,4)，也就是说 Y=hdaZ 或 hdbZ 中的 Z 减去 1。
- kernel (hdX,Y)/boot/vmlinuz root=/dev/hdaZ 和 initrd (hdX,Y)/boot/initrd.img 就是要引导硬盘分区的映像和 initrd 文件，一定要写正确 X 和 Y 的值，不然无法引导系统。

网络工程师考试要求考生掌握 Linux 启动配置文件的程度是能解释清楚每行的命令所起的作用即可。

## 16.3 系统运行级别

### 16.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：Linux 运行级别、级别之间的切换。

### 16.3.2 知识点精讲

1. 运行级别

**运行级别**，简单地来理解其实就是操作系统当前正在运行的功能级别。Linux 系统的级别是**从 0 到 6**，每个级别都具有不同的功能。这些级别在/etc/initab 文件中有详细的定义。init 程序也是通过寻找 initab 文件来使相应的运行级别有相应的功能，通常每个级别最先运行的服务是放在/etc/rc.d 目录下的文件，Linux 下共有 7 个运行级别，分别是：

- 0：系统停机状态，系统默认运行级别不能设置为 0，否则不能正常启动，导致机器直接关闭。
- 1：单用户工作状态，仅有 root 权限，用于系统维护，不能远程登录，类似 Windows 的安全模式。
- 2：多用户状态，但不支持 NFS，同时也不支持网络功能。
- 3：完整的多用户模式，支持 NFS，登录后可以使用控制台命令行模式。
- 4：系统未使用，该级别一般不用，在一些特殊情况下可以用它来做一些事情。
- 5：X11 控制台，登录后进入图形用户界面 XWindow 模式。
- 6：系统正常关闭并重启，默认运行级别不能设为 6，否则不能正常启动。运行 init 6 时机器会重启。

**标准的 Linux 运行级别为 3 或 5。**

2. etc/inittab 文件格式

/etc/inittab 文件控制系统启动过程中运行哪些程序。文件中的每一行都有以下相同的格式：

id:runlevel:action:process

（1）id 是指入口标识符，它是一个字符串，只要保证唯一即可，但是对于 getty 或 mingetty 等 login 程序项，要求 id 与 tty 后面的编号相同，否则 getty 程序将不能正常工作。

（2）runlevel 是 init 所处运行级别的标识，一般使用 0～6、S 或 s 表示。其中 0、1、6 运行级别被系统保留做特殊用途：0 为 shutdown，1 为重启至单用户模式，6 为重启；S 和 s 意义相同，表示单用户模式，且无需 inittab 文件支持，所以可以不在 inittab 中出现。而实际上，进入单用户模式时，init 直接在控制台（/dev/console）上运行/sbin/sulogin。runlevel 可以是并列的多个值，以匹配多个运行级别，对大多数 action 来说，仅当 runlevel 与当前运行级别匹配成功才会执行。

（3）action 是描述其后 process 的运行方式的。action 可取的值比较多，表 16-1 给出了 action 选项的解释。

表 16-1 action 选项

| | |
|---|---|
| respawn | 表示 init 应该监视这个进程，只要进程一停止，该进程就重新启动 |
| wait | 进程只运行一次，init 将一直等待它结束，再执行下一步操作 |
| once | init 控制这个进程只运行一次 |
| boot | 系统引导进程中，运行该进程时，init 将忽略运行等级这段 |
| bootwait | 系统引导过程中，进程运行，init 将等待进程结束 |
| off | 不采取任何行动，功能相当于将这行注释掉 |
| initdefault | 系统设置默认运行级别。process 字段被忽略。当 init 由核心激活以后，从本项取得 runlevel 并作为当前的运行级别 |
| sysinit | 只要系统引导，该进程便运行，优先于 boot 与 bootwait |
| powerwait | 当 init 接收到 SIGPWR 信号时进程开始运行，一般为电源故障时运行 |
| powerfail | 与 powerwait 相同，但 init 不会等待进程完成 |
| powerokwait | 当电源故障修复时运行 |
| ctrialdel | 当 init 收到 SIGNT 信号时（按下 Ctrl+Alt+Delete），进程运行 |

（4）process 是具体的执行程序，后面可以带参数。该进程采用的格式与在命令行下运行该进程的格式一样，因此 process 字段都以该进程的名字开头，紧跟着的是运行时要传递给该进程的参数。如/sbin/shutdown -t3 -r now，该进程在按下 Ctrl+Alt+Delete 组合键时执行，在命令行下也可以直接按住这三个键来重新启动系统。

下面给出系统实际的 inittab 的配置，并进行详细解释。

```
id:3:initdefault:
# 表示系统默认的运行级别是 3
# System initialization
si::sysinit:/etc/rc.d/rc.sysinit
```

#调用执行了/etc/rc.d/rc.sysinit，而 rc.sysinit 是一个 bash shell 的脚本，它主要是完成一些系统初始化的工作，rc.sysinit 是每一个运行级别都要首先运行的重要脚本。若管理员需要让 Linux 开机之后自动运行某个程序，就可以在 rc.sysinit 中增加相应的指令即可

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
#当运行级别为 5 时，以 5 为参数运行/etc/rc.d/rc 脚本，也就是执行/etc/rc.d/rc5.d ，init 将等待其返回（wait）
l6:6:wait:/etc/rc.d/rc 6
# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
#在启动过程中允许按 CTRL-ALT-DELETE 重启系统
# When our UPS tells us power has failed，assume we have a few minutes
# of power left. Schedule a shutdown for 2 minutes from now.
# This does，of course，assume you have powerd installed and your
# UPS connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in，cancel it.
pr：12345：powerokwait：/sbin/shutdown -c "Power Restored; Shutdown Cancelled"
# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6
#在 2、3、4、5 级别上以 ttyX 为参数执行/sbin/mingetty 程序，打开 ttyX 终端用于用户登录，如果进程退出则再次运行 mingetty 程序（respawn）
# Run xdm in runlevel 5
x:5:once:/etc/X11/prefdm –nodaemon
#在第 5 运行级别上运行 xdm
```



## 16.4 守护进程

本部分主要讲述 Linux 的守护进程。

### 16.4.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：守护进程的概念、特点、常见的守护进程。

### 16.4.2 知识点精讲

1. 守护进程的概念

也就是通常说的 Daemon 进程，Linux 系统中的后台服务多种多样，每个服务都运行一个对应

程序，这些后台服务程序对应的进程就是守护进程。守护进程常常在系统引导时自动启动，在系统关闭时才终止，平时并没有一个程序界面与之对应。系统中可以看到很多如 DHCPD 和 HTTPD 之类的进程，这里的结尾字母 D 就是 Daemon 的意思，表示守护进程。

在早期的 Linux 版本中，有一种称为 inetd 的网络服务管理程序，也叫做“超级服务器”，就是监视一些网络请求的守护进程，它根据网络请求调用相应的服务进程来处理连接请求。inetd.conf 则是 inetd 的配置文件，它告诉 inetd 监听哪些网络端口，为每个端口启动哪个服务。在任何网络环境中使用 Linux 系统，第一件要做的事就是了解服务器到底要提供哪些服务。不需要的服务应该被禁止掉，这样可以提高系统的安全性。用户可以通过打开/etc/inetd.conf 文件，了解 inetd 提供和开放了哪些服务，以根据实际情况进行相应的处理。

而在 7.x 版本中则使用 xinetd（扩展的超级服务器）的概念对 inetd 进行了扩展和替代。xinetd 的默认配置文件是/etc/xinetd.conf，其语法和/etc/inetd.conf 不兼容。

除了 xinetd 这个超级服务器之外，Linux 系统中的每个服务都有一个对应的守护进程。考生必须要了解一些基本守护进程。

2. 常见守护进程

Linux 系统常见的守护进程如下：

- dhcpd：动态主机控制协议（Dynamic Host Control Protocol，DHCP）的服务守护进程。
- crond：crond 是 UNIX 下的一个传统程序，该程序周期性地运行用户调度的任务。比起传统的 UNIX 版本，Linux 版本添加了不少属性，而且更安全，配置更简单。类似于 Windows 中的计划任务。
- httpd：Web 服务器 Apache 守护进程，可用来提供 HTML 文件及 CGI 动态内容服务。
- iptables：iptables 防火墙守护进程。
- named：DNS（BIND）服务器守护进程。
- pppoe：ADSL 连接守护进程。
- sendmail：邮件服务器 sendmail 守护进程。
- smb：Samba 文件共享/打印服务守护进程。
- snmpd：简单网络管理守护进程。
- squid：代理服务器 squid 守护进程。
- sshd：SSH 服务器守护进程。Secure Shell Protocol 可以实现安全地远程管理主机。

## 16.5 常见配置文件

### 16.5.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：配置文件的作用。

### 16.5.2 知识点精讲

本部分主要讲解 Linux 系统中的常见配置文件及基本作用。

1. ifcfg-ethx 配置文件

用于存放系统 eth 接口的 IP 配置信息，类似于 Windows 中“本地连接”的属性界面能修改的参数。文件位于/etc/sysconfig/networking/ifcfg-ethx 中，x 可以是 0 或 1，代表不同的网卡接口。

具体内容如下：

```
DEVICE=eth0
BOOTPROTO=static
BROADCAST=220.169.45.255
HWADDR=4C:00:10:59:6B:20
IPADDR=220.169.45.188
NETMASK=255.255.255.0
NETWORK=220.169.45.0
ONBOOT=yes
TYPE=Ethernet
GATEWAY=220.169.45.254
```

一般情况下，系统默认读取 etc/sysconfig/network 为默认网关。若不生效，则需要首先检查配置文件内容是否正确；其次检查/etc/sysconfig/networking/devices/ifcfg-eth0 里是否设置 GATEWAY=，如果也设置了，就会以 ifcfg-eth0 里的 GATEWAY 为默认网关，network 中的设置失效。

2. /etc/sysconfig/network 配置文件

用于存放系统基本的网络信息，如计算机名、默认网关等，与 ifcfg-ethx 配置文件配合使用。实际的 network 文件配置如下：

```
[root@hunau ~]# vi /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=hunau
GATEWAY=220.169.45.254
#配置文件中 networking=yes，表明启用了网络功能
```

3. /etc/host.conf 配置文件

用于保存系统解析主机名或域名的解析顺序。

```
[root@hunau ~]#   Vi host.conf
order hosts，bind
#用于配置本机的名称解析顺序，本例中是先检查本机 hosts 文件中的名字与 IP 的对应关系，找不到再用 DNS 解析
```

4. /etc/hosts 配置文件

用于存放系统中的 IP 地址和主机对应关系的一个表，在网络环境中使用计算机名或域名时，系统首先会去/etc/host.conf 文件中寻找配置，确定解析主机名的顺序。实际的 hosts 文件配置如下：

```
[root@hunau ~]#   Vi   /etc/hosts
# Do not remove the following line，or various programs
# that require network functionality will fail.
127.0.0.1 hunau.net localhost.localdomain localhost
#配置基本的主机名与 IP 地址的对应关系，在访问主机名时，配合 host.conf 的配置可以直接从本文件获取对应的 IP 地址，也可以到 DNS 服务中去查询
```

5. /etc/resolv.conf 配置文件

用于存放 DNS 客户端设置文件。

```
[root@hunau ~]# vi /etc/resolv.conf
用于存放 DNS 客户端配置文件
[root@hunau ~]# vi /etc/resolv.conf
nameserver      10.8.9.125
#此文件设置本机的 DNS 服务器是 10.8.9.125
```

Linux 系统中与网络工程师考试有关的主要配置文件就是以上这些内容，因此复习过程中要注意全面了解。其他与服务器配置有关的配置文件在“服务器配置”一章有详细介绍，这里就不再赘述了。

# 第 5 学时　上、下午考试共同考点 2——Linux 命令

第 3 天的第 5 学时主要学习 Linux 命令对应的知识点。Linux 命令是 Linux 系统运行中不可缺少的基本辅助工具，对于 Linux 系统而言显得尤其重要，因此这个知识点也就成了历年考试的核心考点之一。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 3～5 分之间。上午考试主要考察基本的命令，如系统管理与维护、网络参数配置等方面。下午考试则偏向网络故障排除、服务器检测等命令。本章考点知识结构图如图 17-1 所示。**注意本书中涉及的各类配置命令参数太多，因此只讲重要的、常考的参数。**


图 17-1　考点知识结构图

## 17.1　系统与文件管理命令

本部分主要讲解 Linux 系统管理命令、文件系统的概念、文件系统的管理与维护等。

### 17.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：文件管理命令、系统管理命令、权限管理命令等。

### 17.1.2　知识点精讲

1. Linux 系统管理命令

（1）ls [list] 命令。

基本命令格式：**ls**　[*OPTION*]　[*FILE*]

这是 Linux 控制台命令中最重要的几个命令之一，其作用相当于 dos 下的 dir，用于查看文件和目录信息的命令。ls 最常用的参数有三个：-a、-l、-F。

- ls -a：Linux 中以“.”开头的文件被系统视为隐藏文件，仅用 ls 命令是看不到的，而用 ls -a 除了显示一般文件名外，连隐藏文件也会显示出来。
- ls -l：可以使用长格式显示文件内容，通常需要察看详细的文件信息时，就可以使用 ls -l 这个指令。

【例 17-1】ls -l 示例 13467691067。

```
[root@hunau ~]# ls -l
文件属性    文件数 拥有者  所属的 group  文件大小   建档日期          文件名
drwx------    2    Guest    users       1024     Nov 11 20：08    book      /
brwx--x--x    1    root     root        69040    Nov 19 23：46    test      *
lrwxrwxrwx    1    root     root        4        Nov 3 17：34     zcat->gzip  @
-rwsr-x---    1    root     bin         3853     Aug 10 5：49     javac     *
```

第一列：表示文件的属性。Linux 的文件分为三个属性：可读（r）、可写（w）、可执行（x）。从上例中可以看到，一共有十个位置可以填。第一个位置是表示类型，可以目录或连结文件，其中 d 表示目录，l 表示连结文件，“-”表示普通文件，b 代表块设备文件，c 代表字符设备文件。剩下的 9 个位置以每 3 个为一组。因为 Linux 是多用户多任务系统，所以一个文件可能同时被多个用户使用，所以管理员一定要设好每个文件的权限。若文件的权限位置排列顺序是：rwx（Owner）r-x（Group）r-x（Other）关于权限的问题在后面会详细讲到。

第二列：表示文件个数。如果是文件，这个数就是 1；如果是目录，则表示该目录中的文件个数。

第三列：表示该文件或目录的拥有者。

第四列：表示所属的组（group）。每一个使用者都可以拥有一个以上的组，但是大部分的使用者应该都只属于一个组。

第五列：表示文件大小。文件大小用 byte 来表示，而空目录一般都是 1024byte。

第六列：表示创建日期。以“月，日，时间”的格式表示。

第七列：表示文件名。

- ls -F：使用这个参数表示在文件的后面多添加表示文件类型的符号，如*表示可执行，/表示目录，@表示连接文件。

（2）“>”输入出重定向和管道命令。

基本命令格式：cmd1 > cmd2

在 Linux 命令行模式中，如果命令所需的输入不是来自键盘，而是来自指定的文件，这就是输入重定向。同理，命令的输出也可以不显示在屏幕上，而是写入到指定文件中，这就是输出重定向。

【例 17-2】输入重定向示例。

```
[root@hunau ~]# wc   xx.txt
```

将文件 xx.txt 作为 wc 命令的输入，统计出 xx.txt 的行数、单词数和字符数。所输入的信息不再是键盘，而是文件 xx.txt。

【例 17-3】输出重定向示例。

```
[root@hunau ~]# ls > xx.txt
```

ls 命令的输出不再显示在屏幕上，而是保存在一个名为 xx.txt 的文件中。如果“>”符号后边的文件已存在，则直接覆盖该文件。

（3）“|”管道命令。

基本命令格式：cmd1 | cmd2 | cmd3

利用 Linux 所提供的管道符“|”将两个命令隔开，管道符左边命令的输出就会作为管道符右边命令的输入。连续使用管道意味着第一个命令的输出会作为第二个命令的输入，第二个命令的输出又会作为第三个命令的输入，依此类推。

【例 17-4】一个管道示例。

```
[root@hunau ~]# rpm -qa|grep gcc
```

这条命令使用一个管道符“|”建立了一个管道。管道将 rpm -qa 命令输出系统中所有安装的 RPM 包作为 grep 命令的输入，从而列出带有 gcc 字符的 RPM 包来。

多个管道示例如下：

```
[root@hunau ~]# cat /etc/passwd | grep /bin/bash | wc -l
```

这条命令使用了两个管道，利用第一个管道使 cat 命令显示 passwd 文件的内容输出送给 grep 命令，grep 命令找出含有“/bin/bash”的所有行；第二个管道将 grep 的输出送给 wc 命令，wc 命令统计出输入中的行数。这个命令的功能在于找出系统中有多少个用户使用 bash。

（4）chmod 命令。

基本命令格式：**chmod** *mode file*

Linux 中文档的存取权限分为三级：文件拥有者、与拥有者同组的用户、其他用户，不管权限位如何设置，root 用户都具有超级访问权限。利用 chmod 可以精确地控制文档的存取权限。默认情况下，系统将创建的普通文件的权限设置为-rw-r-r-。

Mode：权限设定字串，格式如下为[ugoa...][[+-=][rwxX]...][, ...]，其中 u 表示该文档的拥有者，g 表示与该文档的拥有者同一个组（group）者，o 表示其他的人，a 表示所有的用户。

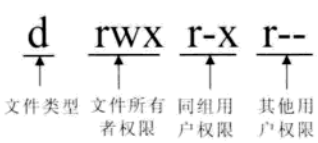



图 17-2 文件权限位示意图

如图 17-2 所示，“+”表示增加权限、“-”表示取消权限、“=”表示直接设定权限。“r”表示可读取，“w”表示可写入，“x”表示可执行，“X”表示只有当该文档是个子目录或者该文档已经被设定过为可执行。此外 chmod 也可以用数字来表示权限。

数字权限基本命令格式：**chmod** *abc file*

其中，a、b、c 各为一个数字，分别表示 User、Group 及 Other 的权限。其中各个权限对应的数字为 r=4，w=2，x=1。因此对应的权限属性如下：

属性为 rwx，则对应的数字为 4+2+1=7；

属性为 rw-，则对应的数字为 4+2=6；

属性为 r-x，则对应的数字为 4+1=7。

命令示例如下：

```
chmod a=rwx file 和 chmod 777 file 效果相同
chmod ug=rwx，o=x file 和 chmod 771 file 效果相同
```

（5）cd 命令。

基本命令格式：**cd** [*change directory*]

其作用是改变当前目录。

**注意**：Linux 的目录对大小写是敏感的。

【例 17-5】cd 命令示例。

```
[root@hunau ~]# cd /
[root@hunau /]#
```

此命令将当前工作目录切换到“/”目录。

（6）mkdir 和 rmdir 命令。

基本命令格式：

●**mkdir** [*directory*]

●**rmdir** [*option*] [*directory*]

mkdir 命令用来建立新的目录，rmdir 用来删除已建立的目录。其中 rmdir 的参数主要是-p，该参数在删除目录时，会删除掉指定目录中的每个目录，包括其中的父目录。如“rmdir -p a/b/c”的作用与“rmdir a/b/c a/b a”的作用类似。

【例 17-6】mkdir 和 rmdir 命令示例。

```
[root@hunau /]# mkdir testdir
```

在当前目录下创建名为 testdir 的目录。

```
[root@hunau /]# rmdir testdir
```

在当前目录下删除名为 testdir 的目录。

（7）cp 命令。

基本命令格式：**cp** -r 源文件（source） 目的文件（target）

主要参数-r 是指连同源文件中的子目录一同拷贝，在复制多级目录时特别有用。

【例 17-7】cp 命令示例。

```
[root@hunau etc]# mkdir /backup/etc
[root@hunau etc]# cp -r /etc /backup/etc
```

该命令的作用是将/etc 下的所有文件和目录复制到/backup/etc 下作为备份。

（8）rm 命令。

基本命令格式：**rm** [*option*] *filename*

作用是删除文件，其常用的参数有-i、-r、-f。“-i”参数系统会加上提示信息，确认才能删除；“-r”操作可以连同这个目录下面的子目录都删除，功能和 rmdir 相似；“-f”操作是进行

强制删除。

【例 17-8】rm 命令示例。

```
[root@hunau etc]## rm -i /backup/etc/etc/mail.rc
rm:  remove regular file `/backup/etc/etc/mail.rc'? n
[root@hunau etc]# rm -f /backup/etc/etc/mail.rc
```

带“-i”参数系统会提示是否删除，而带“-f”参数就直接删除了。

（9）**mv** 命令。

基本命令格式：**mv** [*option*] *source dest*

移动目录或文件，可以用于给目录或文件重命名。当使用该命令来移动目录时，它会连同该目录下面的子目录也一同移动。常用参数“-f”表示强制移动，覆盖之前也不会提示。

【例 17-9】mv 命令示例。

```
[root@hunau etc]# mv -f /etc /test
```

将/etc 下的所有文件和目录全部移动到/test 目录下，若/test 中有同名文件则会被直接覆盖。

（10）cat 命令。

基本命令格式：**cat** [*option*] [*file*]

它的功能是显示或连结一般的 ascii 文本文件。类似于 DOS 下面的 type。Cat 可以结合重定向符号一起使用，如 cat file1 file2>file3，把 file1 和 file2 的内容结合起来，再“重定向（>）”到 file3 文件中。若 file3 不存在，则自动创建；若 file3 是已经存在的文件，则被覆盖。

【例 17-10】cat 命令示例。

```
[root@hunau etc]# cat /etc/hosts
# Do not remove the following line，or various programs
# that require network functionality will fail.
127.0.0.1   hunau localhost.localdomain localhost
```

【例 17-10】输入 cat /etc/hosts 命令，则直接显示/etc/hosts 文件的内容。

（11）pwd 命令。

基本命令格式：**pwd**

pwd 命令用于显示用户的当前工作目录。

【例 17-11】pwd 命令示例。

```
[root@hunau etc]# pwd
/etc
```

【例 17-11】显示目前所在工作目录的绝对路径名称是/etc。

（12）ln [link]。

基本命令格式：**ln** *soure_file* **-s** *des_file*

该命令的作用是为某一个文件在另外一个位置建立一个不同的链接，常用的参数是-s，要注意两个问题：①ln 命令会保持每一处链接文件的同步性，也就是说，不论改动了哪一处，其他的文件都会发生相同的变化；②ln 的链接有软链接和硬链接两种，软链接是 ln -s **，它只会在你选定的位置上生成一个文件的镜像，不会占用磁盘空间；硬链接是 ln ** **，没有参数-s，它会在选定的位置上生成一个和源文件大小相同的文件。无论是软链接还是硬链接，文件都必须保持

同步变化。

【例 17-12】ln 命令示例。

```
[root@hunau ~]# ln   /etc/hosts -s /root/hosts
```

在/root 目录下创建一个名为 hosts 的软连接文件，对应到/etc/hosts 文件。

（13）grep 命令。

基本命令格式：**grep** [*option*] *string*

grep 命令用于查找当前文件夹下的所有文件内容，列出包含 string 中指定的字符串的行并显示行号。

*option* 参数主要有：

- -a：作用是将 binary 文件以 text 文件的方式搜寻数据。
- -c：计算找到 string 的次数。
- -I：忽略大小写的不同，即大小写视为相同。

【例 17-13】命令示例。

```
[root@hunau ~]# grep -a   '127'
```

在当前目录下的所有文件中查找“127”这个字符串。

（14）mount 命令。

基本命令格式：**mount -t** *type dev dir*

用于将分区作为 Linux 的一个“文件”挂载到 Linux 的一个空文件夹下，从而将分区和/mnt 这个目录联系起来，因此我们只要访问这个文件夹就相当于访问该分区了。

**注意：必须将光盘、U 盘等放入驱动器再实施挂载操作，不能在挂载目录下实施挂载操作，至少在上一级不能在同一目录下挂载两个以上的文件系统。**

【例 17-14】命令示例。

```
[root@hunau ~]# mount -t iso9660 /dev/cdrom /mnt/cdrom   #挂载光盘
[root@hunau ~]# umount /mnt/cdrom   #卸载光盘
[root@hunau ~]# mount /dev/sdb1 /mnt/usb#挂载 U 盘
```

（15）rpm 命令。

基本命令格式：**rpm** [*option*] name

RPM 是 RedHat Package Manager 的缩写，最早是 RedHat 开发的，现在已经是公认的行业标准了。用于查询各种 rpm 包的情况。这里的参数不做详细讲解，主要熟悉使用-q 参数实现查询，如常用的查询有以下几项：

```
[root@hunau ~]# rpm -q bind #查询 bind 软件包是否有安装
[root@hunau ~]#rpm –qa   #查询系统安装的所有软件包
[root@hunau ~]#rpm -qa|grep bind #查询系统安装的所有软件包，并从中过滤出 bind
```

（16）ps 命令。

基本命令格式：**ps** [*option*]

用于查看进程，常用选项 *option* 有：

- -aux：用于查看所有静态进程。

- -top：用于查看动态变化的进程。
- -A：用于查看所有的进程。
- -r：表示只显示正在运行的进程。
- -l：表示用长格式显示。

在 ps 查看的进程通常有以下几类状态：

- D：Uninterruptible sleep。
- R：正在运行中。
- S：处于休眠状态。
- T：停止或被追踪。
- W：进入内存交换。
- Z：僵死进程。

【例 17-15】ps 命令示例。

```
[root@hunau ~]# ps -Al
F S   UID   PID  PPID  C PRI  NI ADDR SZ WCHAN  TTY          TIME CMD
4 S     0     1     0  0  76   0 -   436 -      ?        00:00:02 init
1 S     0     2     1  0  94  19 -   0   ksofti ?        00:00:46 ksoftirqd/0
5 S     0     3     1  0 -40   - -   0   -      ?        00:00:00 watchdog/0
1 S     0     4     1  0  70  -5 -   0   worker ?        00:00:00 events/0
1 S     0     5     1  0  71  -5 -   0   worker ?        00:00:00 khelper
4 R     0  2754  1760  0  78   0 -   1110 -     pts/1    00:00:00 ps
```

（17）kill 命令。

基本命令格式：**kill** *signal PID*

其中 PID 是进程号，可以用 ps 命令查出，signal 是发送给进程的信号，TERM（或数字 9）表示“无条件终止”。

【例 17-16】命令示例。

```
[root@hunau ~]# Kill 9 2754
```

表示无条件终止进程号为 2754 的进程。

（18）chkconfig 命令。

基本命令格式：**chkconfig**[**-add**][**-del**][**-list**][*系统服务*]

或 **chkconfig** [**-level**<*等级代号*>][*系统服务*][**on/off/reset**]

chkconfig 命令提供了一种简单的方式来设置一个服务的运行级别，也可以用来检查系统的各种服务。基本参数如下：

- -add：增加所指定的系统服务，在系统启动的配置文件中增加相关配置。
- -del：删除所指定的系统服务，在系统启动的配置文件内删除相关配置。
- -level <等级代号>：指定该系统服务要在哪一个执行等级中开启或关闭。

【例 17-17】chkconfig 命令示例。

```
[root@hunau ~]#chkconfig --list
用于列出所有的系统服务
```

```
[root@hunau ~]#chkconfig --add httpd
增加 httpd 服务
[root@hunau ~]#chkconfig --level httpd 2345 on
把 httpd 在运行级别为 2～5 的情况下都是启用的状态
```

（19）Passwd 命令。

基本命令格式：**passwd** [*option*]　<accountName>

主要参数说明：

- -l：锁定口令，即禁用账号。
- -u：口令解锁。
- -d：使账号无口令。
- -f：强迫用户下次登录时修改口令。

如果默认用户名，则修改当前用户的口令。

Linux 系统中的/etc/passwd 文件是用于存放用户密码的重要文件，这个文件对所有用户都是可读的，系统中的每个用户在/etc/passwd 文件中都有一行对应的记录。/etc/shadow 保存着加密后的用户口令。而/etc/group 是管理用户组的基本文件，在/etc/group 中，每行记录对应一个组，它包括用户组名、加密后的组口令、组 ID 和组成员列表。可以通过 passwd 指令直接修改用户的密码。

【例 17-18】命令示例如下：

```
[root@hunau ~]# passwd
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
直接修改当前登陆用户的口令
```

可以通过 vi /etc/passwd 查看系统中的用户信息，下面列出系统的部分用户信息。

```
[root@hunau ~]# vi /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
```

（20）useradd 命令。

基本命令格式：useradd　[option]　username

此命令的作用是在系统中创建一个新用户账号，创建新账号时要给账号分配用户号、用户组、主目录和登录 Shell 等资源。

参数说明：

- -c comment：指定一段注释性描述。
- -d 目录：指定用户主目录，如果此目录不存在，则同时使用-m 选项可以创建主目录。
- -g 用户组：指定用户所属的用户组。
- -G 用户组：指定用户所属的附加组。
- -s Shell 文件：指定用户的登录 Shell。

- -u 用户号：指定用户的用户号，如果同时有-o 选项，则可以重复使用其他用户的标识号。
- username：指定新账号的登录名，保存在/etc/passwd 文件中，同时更新其他系统文件，如/etc/shadow, /etc/group 等。

【例 17-19】命令示例。

```
[root@hunau ~]# useradd –d   /usrs/sam -m sam
```

创建了一个用户账号 sam，其中-d 和-m 选项用来为登录名 sam 产生一个主目录/usrs/sam，其中/usrs 是默认的用户主目录所在的父目录。

```
[root@hunau ~]# useradd -s /bin/sh -g apache –G admin,root   test
```

此命令新建了一个用户 test，该用户的登录 Shell 是/bin/sh，属于 apache 用户组，同时又属于 admin 和 root 用户组。

类似的命令还有 userdel 和 usermod，分别用于删除和修改用户账号的信息。

（21）groupadd 命令。

基本命令格式：groupadd [option] groupname

主要参数：

- -g gid：用于指定组的 ID，这个 ID 值必须是唯一的且不可以为负数，在使用-o 参数时可以相同。通常 0～499 是保留给系统账号使用的，新建的组 ID 都是从 500 开始往上递增。组账户信息存放在/etc/group 中。
- -r：用于建立系统组号，它会自动选定一个小于 499 的 gid。
- -f：用于在新建一个已经存在的组账号时，系统弹出错误信息，然后强制结束 groupadd。避免对已经存在的组进行修改。
- -o：用于指定创建新组时，gid 不使用唯一值。

【例 17-20】命令示例。

```
[root@hunau ~]#groupadd –r   apachein
```

创建一个名为 apachein 的系统组，其 gid 是系统默认选用的 0～499 之间的数值。

也可以通过 vi /etc/group 看到系统中的组，下面列出系统部分组。

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
```

## 17.2 网络配置命令

本部分主要讲解 Linux 系统基本网络配置命令及其应用。

### 17.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：IP 配置、连通性检查、路由配置等。

### 17.2.2 知识点精讲

Linux 系统中的网络命令与 Windows 系统中的网络命令有一部分是一致的，因此本小节不做详细讨论。这里主要讨论 Linux 系统与 Windows 系统中不同的网络命令。

1. ifconfig 命令

ifconfig 是一个用来查看、配置、启用或禁用网络接口的工具，这个工具极为常用。类似 Windows 中的 ipconfig 指令，但是其功能更为强大，在 Linux 系统中可以用这个工具来配置网卡的 IP 地址、掩码、广播地址、网关等。

常用的方式有查看网络接口状态和配置网络接口信息两种。

（1）ifconfig 查看网络接口状态。

```
[root@hunau ~]# ifconfig
eth0 Link encap:Ethernet HWaddr 00:00:1F:3B:CD:29:DD
inet addr:172.28.27.200 Bcast:172.28.27.255 Mask:255.255.255.0
inet6 addr: fe80::203:dff:fe21:6C45/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:618 errors:0 dropped:0 overruns:0 frame:0
TX packets:676 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:409232 (409.7 KiB) TX bytes:84286 (84.2 KiB)
Interrupt:5 Base address:0x8c00
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:1694 errors:0 dropped:0 overruns:0 frame:0
TX packets:1694 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:3203650 (3.0 MiB) TX bytes:3203650 (3.0 MiB)
```

ifconfig 如果不接任何参数，就会输出当前网络接口的情况。上面命令结果中的具体参数说明：

- eth0：表示第一块网卡，其中 HWaddr 表示网卡的物理地址，可以看到目前这个网卡的物理地址是 00:00:1F:3B:CD:29:DD；
- inet addr：用来表示网卡的 IP 地址，此网卡的 IP 地址是 172.28.27.200，广播地址 Bcast 是 172.28.27.255，掩码地址 Mask 是 255.255.255.0。lo 是表示主机的回环地址，这个一般是用来作测试用途。

若要查看主机所有网络接口的情况，可以使用下面的指令：

```
[root@hunau ~]#ifconfig  -a
```

若要查看某个端口状态，可以使用下面的命令：

```
[root@hunau ~]#ifconfig  eth0
```

这就可以查看 eth0 的状态。

（2）ifconfig 配置网络接口。

ifconfig 可以用来配置网络接口的 IP 地址、掩码、网关、物理地址等。

ifconfig 的基本命令格式：**ifconfig** if_num IPaddres hw MACaddres **netmask** *mask* **broadcast** *broadcast_address* [**up/down**]

【例 17-21】命令示例。

```
[root@hunau ~]#ifconfig eth0 down
```

ifconfig eth0 down 表示如果 eth0 是激活的，就把它 down 掉。此命令等同于 ifdown eth0。

```
[root@hunau ~]#ifconfig eth0 192.168.1.99 broadcast 192.168.1.255 netmask 255.255.255.0
```

用 ifconfig 来配置 eth0 的 IP 地址、广播地址和网络掩码。

```
[root@hunau ~]#ifconfig eth0 up
```

用 ifconfig eth0 up 来激活 eth0。此命令等同于 ifup eth0。

（3）ifconfig 配置虚拟网络接口。

有时为了满足不同的应用需求，Linux 系统可以允许配置虚拟网络接口，如用不同的 IP 地址来运行多个 Web 服务器，就可以用虚拟地址；虚拟网络接口指的是为一个网络接口指定多个 IP 地址，虚拟接口通常是以 eth0:0 、eth0:1、eth0:2、.....、eth0:N 的形式。

【例 17-22】命令示例。

```
[root@hunau ~]#ifconfig eth1:0 172.28.27.199 hw ether 00:19:21:D3:6C:46 netmask 255.255.255.0 broadcast 172.28.27.255 up
```

ifconfig 在网络工程师考试中经常考到，需要认真对待。

2. ifdown 和 ifup 命令

ifdown 和 ifup 命令是 Linux 系统中的两个常用命令，其作用类似于 Windows 中对本地连接的启用和禁用。这两个命令是分别指向/sbin/ifup 和/sbin/ifdown 的符号连接，这是该目录下唯一可以直接调用执行的脚本。这两个符号连接为了一致，所以放在这个目录下，可以用 ls -l 看到。

```
[root@hunau network-scripts]# ls -l
lrwxrwxrwx  1 root root   20  7 月  23 22:34 ifdown -> ../../../sbin/ifdown
lrwxrwxrwx  1 root root   18  7 月  23 22:34 ifup -> ../../../sbin/ifup
```

若要关闭 eth0 接口，可以直接使用下面的命令：

```
[root@hunau network-scripts]# ifdown eth0
```

此时 eth0 关闭，用 ifconfig 查看不到 eth0 的信息。要开启 eth0，只要将 ifdown 改成 ifup 即可。

3. route 命令

Linux 系统中的 route 命令的用法与 Windows 中的用法有一定的区别，因此在学习的过程中要注意区分。

基本命令格式：#route [-add][-net|-host] targetaddress [-netmask mask] [dev] If]

#route [-delete] [-net|-host] targetaddress [gw Gw] [-netmask mask] [dev] If]

基本参数说明：

- -add：用于增加一条路由。
- -delete：用于删除路由。
- -net：表明路由到达的是一个网络，而不是一台主机。
- -host：路由到达的是一台主机，与-net 选项只能选其中的一个使用。
- -netmask mask：指定目标网络的子网掩码。

- gw：指定路由所使用的网关。
- [dev] If：指定路由使用的接口。

【例 17-23】命令示例。

```
[root@hunau ~]# route
Kernel IP routing table
```

| Destination | Gateway | Genmask | Flags | Metric | Ref | Use Iface |
|---|---|---|---|---|---|---|
| 220.169.45.160 | * | 255.255.255.224 | U | 0 | 0 | 0 eth1 |
| 172.28.164.0 | * | 255.255.255.0 | U | 0 | 0 | 0 eth0 |
| 210.43.224.0 | 172.28.164.254 | 255.255.224.0 | UG | 0 | 0 | 0 eth0 |
| 172.16.0.0 | 172.28.164.254 | 255.240.0.0 | UG | 0 | 0 | 0 eth0 |
| default | 220.169.45.163 | 0.0.0.0 | UG | 0 | 0 | 0 eth1 |

直接使用 route 命令且不带任何参数时，则显示系统当前的路由信息。此路由表中各列的意义也是网络工程师考试中常考的知识点，下面对各项进行详细解释。

- Destination：路由表条目中目标网络的范围。如果一个 IP 数据包的目的地址是目标列中的某个网络范围内，这个数据包按照此路由表条目进行路由。
- Gateway：到指定目标网络的数据包必须经过的主机或路由器。通常用星号“*”或是默认网关地址表示；星号表示目标网络就是主机接口所在的网络，因此不需要路由；默认网关将所有去往非本地的流量都发送到的一个指定 IP。
- Flags：是一些单字母的标志位，一共有 9 个，是路由表条目的信息标识。
- U：表明该路由已经启动，是一个有效的路由。
- H：表明该路由的目标是一个主机。
- G：表明该路由到指定目标网络需要使用 Gateway 转发。
- R：表明使用动态路由时，恢复路由的标识。
- D：表明该路由是由服务功能设定的动态路由。
- M：表明该路由已经被修改。
- !：表明这个路由将不会被接收。
- Metric：到达指定网络所需的跳数，在 Linux 内核中没有用。
- Ref：表明对这个路由的引用次数，在 Linux 内核中没有用。
- Use：表明这个路由器被路由软件查寻的次数，可以粗略估计通向指定网络地址的网络流量。
- Iface：表明到指定网络的数据包应该发往哪个网络接口。

若某服务器到达 172.28.27.0/24 的网络可以通过一个地址为 172.28.3.254 的路由器，则可以通过下列命令实现添加静态路由：

```
[root@hnnau ~]# route add –net 172.28.27.0 netmask 255.255.255.0 gw 172.28.3.254
```

若要添加一条默认路由，则可以使用下面的命令：

```
[root@hnnau ~]# route add –net 0.0.0.0   netmask 0.0.0.0 gw 172.28.3.254
```

4. traceroute 命令

此命令的作用与 Windows 中的 tracert 作用类似，用于显示数据包从源主机到达目的主机的中

间路径，帮助管理了解数据包的传输路径。

基本命令格式：traceroute [-dFlnrvx][-f <firstTTL>][-g <gw>][-I <ifname>] [-m <TTL>][-p <port>] [-s<src IP>][-t <tos> ][-w <timeout> ][dst ip] [packetsize]

参数说明：

- -d：使用 Socket 层级的排错功能。
- -f <firstTTL>：设置第一个检测数据包的存活数值 TTL 的大小。
- -g <gw>：设置来源路由网关，最多可设置 8 个。
- -I <ifname>：使用指定的网络接口名发送数据包。
- -I：使用 ICMP 回应取代 UDP 资料信息。
- -m <TTL>：设置检测数据包的最大存活数值 TTL 的大小。
- -n：直接使用 IP 地址，而非主机名称。
- -p <port>：设置 UDP 传输协议的通信端口。
- -r：忽略普通的 Routing Table，直接将数据包送到远端主机上。
- -s<src ip>：设置本地主机送出数据包的 IP 地址。
- -t <tos>：设置检测数据包的 TOS 数值。
- -v：详细显示指令的执行过程。
- -w <timeout>：设置等待远端主机回报的时间。
- -x：开启或关闭数据包的正确性检验。

【例 17-24】命令示例。

```
[root@hunau~]# traceroute -i eth0 61.187.55.33
traceroute to 61.187.55.33 (61.187.55.33), 30 hops max, 38 byte packets
1  172.28.164.254 (172.28.164.254)  0.739 ms  0.637 ms  0.601 ms
2  10.0.1.1 (10.0.1.1)  1.028 ms  0.979 ms  0.956 ms
3  10.0.0.10 (10.0.0.10)  0.328 ms  0.419 ms  0.260 ms
4  61.187.55.33 (61.187.55.33)  0.321 ms  0.912 ms  0.420 ms
```

5. iptables 命令

iptables 是 Linux 系统中常用的一个 IP 包过滤功能，使用比较广泛，作为网络工程师，在实际中可能会比较多地使用到，在网工的考试中也经常出现，因此有必要掌握。鉴于 iptables 的功能和命令参数都非常复杂，本书着重介绍与网络工程师实际使用较频繁和考试经常涉及的知识点。

了解 iptables 的功能之前，先了解 IP 数据包经过 Linux 的 iptables 的路径，当源地址是外部主机地址时，发送的目标地址是本机，也就是安装有 iptables 的 Linux 的数据，在图 17-3 中会按照自上而下经过最左边的路径，由本机产生的包，在图中可以看做是从“本地进程”开始，自上而下经过最左边路径；而当源地址是外部主机，目标地址也是外部主机的数据包时，则自上而下经过图中最右边路径。由于 mangle 规则表不常用，并且 iptables 大部分都是处理从外部来、到外部去的数据，因此流程可以简化为如图 17-4 所示的路径。

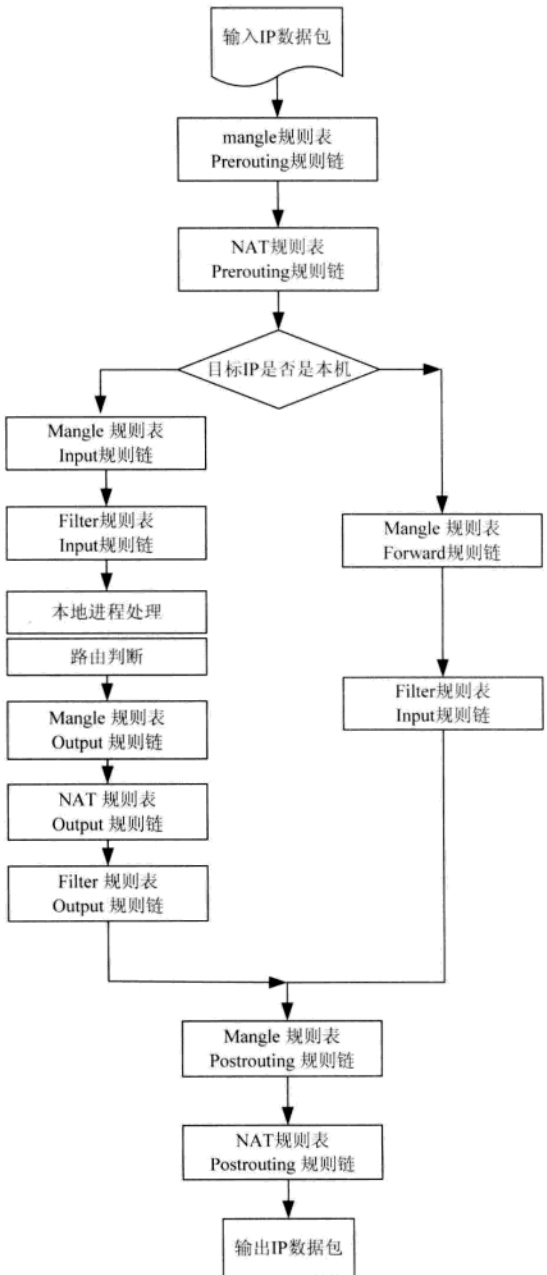



图 17-3　iptabels 中数据包的处理流程

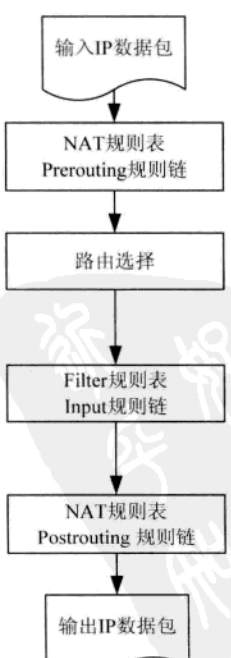



图 17-4　iptabels 简化处理流程

iptables 基本语法如下：

**iptables** [-t table] command [match] [-j target/jump]

其中[-t table] 指定规则表，在 iptables 中内建的规则表有三个：nat、mangle 和 filter，当命令省略[-t table]时，默认的是 filter。这三个规则表的功能如下：

- nat：此规则表拥有 prerouting 和 postrouting 两个规则链，主要功能是进行一对一、一对多、多对多等地址转换工作（snat、dnat），这个规则表在网络工程中使用得非常频繁。
- mangle：此规则表拥有 prerouting、forward 和 postrouting 三个规则链。除了进行网络地址转换外，还在某些特殊应用中改写数据包的 ttl、tos 的值等，这个规则表使用得很少，因此在这里不做讨论。
- filter：这个规则表是默认规则表，拥有 input、forward 和 output 三个规则链，顾名思义，它是用来进行数据包过滤的处理动作（如 drop、accept 或 reject 等），通常的基本规则都建立在此规则表中。

command 常用命令列表（以下命令中的同一行的两个命令作用是同等的，写法上的区别）：

- 命令 -a，-append 用于新增规则到某个规则链中，该规则将会成为规则链中的最后一条规则。
- 命令 -d，-delete 用于从某个规则链中删除一条规则，可以输入完整规则，或直接指定规则编号加以删除。
- 命令 -r，-replace 用于取代现行规则，规则被取代后并不会改变顺序。
- 命令 -i，-insert 用于插入一条规则，原本该位置上的规则将会往后移动一个位置。
- 命令 -l，-list 用于列出某规则链中的所有规则。
- 命令 -f，-flush 用于删除 filter 表中 input 链的所有规则。
- 命令 -z，-zero 用于将数据包计数器归零。数据包计数器是用来计算同一数据包的出现次数，用于过滤阻断式攻击。
- 命令 -n，-new-chain 用于定义新的规则链。
- 命令 -x，-delete-chain 用于删除某个规则链。
- 命令 -p，-policy 用于定义过滤策略，也就是未符合过滤条件的数据包的默认处理方式。

match 常用数据包匹配参数：

- 参数 -p，-protocol 用于匹配通讯协议类型是否相符，可以使用“!”运算符进行反向匹配，如-p !tcp 的意思是指除 TCP 以外的其他类型，如 udp、icmp 等非 TCP 的其他协议。如果要匹配所有类型，则可以使用 all 关键词。
- 参数 -s，-src，-source 用来匹配数据包的来源 IP 地址（单机或网络），匹配网络时用数字来表示子网掩码，如-s 192.168.0.0/24，也可以使用“!”运算符进行反向匹配。
- 参数 -d，-dst，-destination 用来匹配数据包的目的 IP 地址。
- 参数-i，-in-interface 用来匹配数据包是从哪块网卡进入的，可以使用通配字符“+”来做大范围匹配，如-i eth+表示所有的 ethernet 网卡，也可以使用“!”运算符进行反向匹配。

- 参数-o，-out-interface 用来匹配数据包要从哪块网卡送出。
- 参数-sport，-source-port 用来匹配数据包的源端口，可以匹配单一端口或一个范围，如--sport 22:80 表示从 22 到 80 端口之间都算是符合条件，如果要匹配不连续的多个端口，则必须使用--multiport 参数。
- 参数 --dport，--destination-port 用来匹配数据包的目的地端口号。

-j target/jump 常用的处理动作：

- -j 参数用来指定要进行的处理动作，常用的处理动作包括：accept、reject、drop、redirect、masquerade、log、dnat、snat、mirror 等。具体如下：
- accept：将数据包放行，进行完此处理动作后将不再匹配其他规则，直接跳往下一个规则链（nat postrouting）。
- reject：拦阻该数据包并传送数据包通知对方，进行完此处理动作后将不再匹配其他规则，直接中断过滤程序。
- drop：丢弃数据包不予处理，进行完此处理动作后将不再匹配其他规则，直接中断过滤程序。
- redirect：将数据包重新导向到另一个端口（pnat），进行完此处理动作后将会继续匹配其他规则。
- masquerade：改写数据包的源 IP 地址为自身接口的 IP 地址，可以指定 port 对应的范围，进行完此处理动作后直接跳往下一个规则链（mangle postrouting）。这个功能与 snat 不同的是，当进行 IP 伪装时不需指定要伪装成哪个 IP 地址，这个 IP 地址会自动从网卡读取，尤其是当使用 DHCP 方式获得地址时 masquerade 特别有用。
- log：将数据包相关信息纪录在/var/log 中，进行完此处理动作后将会继续匹配其他规则。
- snat：改写数据包的源 IP 为某特定 IP 或 IP 范围，可以指定 port 对应的范围，进行完此处理动作后将直接跳往下一个规则（mangle postrouting）。
- dnat：改写数据包目的 IP 地址为某特定 IP 或 IP 范围，可以指定 port 对应的范围，进行完此处理动作后将会直接跳往下一个规则链（filter:input 或 filter:forward）。



IPtables 的命令参数非常多，在网络工程师的考试中，主要用到的是 IP 地址伪装和数据包过滤的相关参数。如例 17-21 和例 17-22 所示。

【例 17-25】IP 伪装命令示例。

```
[root@hunau sbin]#iptables -t nat -A POSTROUTING -s 172.28.27.0/24 -o eth0 -j SNAT --to 61.187.55.36
```

#将所有来自 172.28.27.0/24 数据包的源 IP 地址改为 61.187.33.36，实现内部私有地址转换为公网地址，能够连接 Internet 上的资源。

```
[root@hunau sbin]#iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

#对于出口 IP 地址是动态获取的情况，适合 IP 伪装的形式。作用是将内部的私有地址伪装成 PPP0 接口动态获取的公网 IP 地址，实现地址转换上网。

在实际的网络工程中，往往需要将一台内部私有地址的服务器映射到公网的 IP 地址上，实现

Internet 的服务，此时就要用到 IP 地址映射。可以使用以下命令实现：

```
[root@hunau sbin]#iptables -A PREROUTING -i eth0 -d 61.187.55.35 -j DNAT --to 172.28.27.100
[root@hunau sbin]#iptables -A POSTROUTING -o eth0 -s 172.28.27.100 -j SNAT --to 61.187.55.35
```

因为通信是双向的，所以 IPtables 先将接收到的目的 IP 为 61.187.55.35 的所有数据包进行目的 nat（dnat），然后对接收到的源 IP 地址为 172.28.27.100 的数据包进行源 nat（snat）。这样，所有目的 IP 为 61.187.55.35 的数据包都将被转发给 172.28.27.100，而所有来自 172.28.27.100 的数据包都将被伪装成 61.187.55.35，从而实现了 IP 映射。

【例 17-26】数据包过滤命令示例。

用 IPtables 建立包过滤防火墙，以实现对内部的 www 和 ftp 服务器进行保护。基本规则如下：

```
[root@hunau sbin]# iptables -f  #先清除 input 链的所有规则
[root@hunau sbin]# iptables -p forward drop  #设置防火墙 forward 链的策略为 drop，也就是防火墙的默认规则是：先禁止转发任何数据包，然后再依据规则允许通过的包
[root@hunau sbin]# iptables -a forward -p tcp -d 172.28.27.100 --dport www -i eth0 -j accept  #开放服务端口为 TCP 协议 80 端口的 WWW 服务
[root@hunau sbin]# iptables -a forward -p tcp -d 172.28.27.100 --dport ftp -i eth0 -j accept  #开放 FTP 服务，其余的服务依此类推即可。这里要特别注意的是，设置服务器的包过滤规则时要保证服务器与客户机之间的通信是双向的，因此不仅要设置数据包流出的规则，还要设置数据包返回的规则。下面是内部数据包流出的规则
[root@hunau sbin]# iptables -a forward -s 172.28.27.0/24 -i eth1 -j accept  #接受来自整个内部网络的数据包并使之通过
```

其他的一些命令（如 nslookup、ping），与 Windows 命令的用法基本相同，有时网络工程师考试中不涉及具体的系统平台，只要会使用即可，因此不再赘述。

## 第 6 学时　案例难点 2——Linux 配置

第 3 天的第 6 学时主要学习 Linux 配置。Linux 服务器是当前互联网上非常流行的一个服务器的操作系统，因此包含相当多的服务器配置和应用技术，是历年考试的核心考点之一。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 3～15 分之间。简单概念性的问题主要在上午的考试中出现，下午考试主要是以服务器配置的一道大题出现，分值高达 15 分，因此要尤其重视这一章的内容。本章考点知识结构图如图 18-1 所示。


图 18-1　考点知识结构图

### 18.1　DNS 服务器配置

本部分主要讲述 DNS 服务器的配置、测试和基本应用。

### 18.1.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：DNS 服务器配置、测试等。

### 18.1.2 知识点精讲

Linux 中域名解析的方法可以通过 HOSTS、NIS 服务器或 DNS 服务器的形式，其中 HOSTS 方式适用于小型网络；NIS 服务器用库文件存放解析记录，适用于中型网络；DNS 服务器用分布式存放和管理目录。在 Linux 下配置 DNS 需要 bind 软件实现。与之相关的文件（包括相关配置文件）如下所示：

/etc/named.conf
这是 bind 的基本配置文件，安装完 bind 之后系统自带，配置的是要修改的主要文件
/etc/rc.d/init.d/named
这是 bind 的启动脚本，用于接收 start、stop、restart 等参数，控制 bind 进程的工作，系统自带
/var/named.ca
存放有系统中顶层根域名服务器的地址信息，用于 bind 去其他 DNS 服务器上查询其他的域名。安装完 bind 之后，系统自带，无须配置
/var/named/localhosts.zone
本机区域文件，此文件通常保存本机的 LOCALHOST 主机对应的 IP 地址信息。也可以使用用户自定义的名字
/etc/resolv.conf
本机的 DNS 服务器地址配置文件。在“Linux 主要配置文件”一节已经介绍过
/etc/host.conf
主机名解析顺序配置文件。在“Linux 主要配置文件”一节已经介绍过

DNS 的主配置文件是/etc 目录下面的 named.boot 或 named.conf，bind 的老版本使用 named.boot 作为配置文件。新版本的 named 使用 named.conf 作为配置文件，必须注意 named.boot 的文件格式与 named.conf 不同，不能混用。而数据文件通常是/var/named 目录下面所有的文件。DNS 服务器可以配置成不同的形式，如主域名服务器、辅助域名服务器、转发域名服务器等，下面介绍网络工程师考试中常见的几种类型服务器的配置。

1. named.conf

首先了解 named.conf 文件的基本配置格式，通过 vi/etc/named.conf 可以看到基本的配置。基本格式如下：

```
（1）option {
        directory   "目录名";
    };
```

这一段中的 option 声明用于定义 DNS 的属性。option 中可以指定 DNS 服务器的部分属性，如区域文件的存放位置、转存文件的存放位置等。实例如下：

```
option{
    directory   "/var/named";   #定义区域文件的存放位置
    dump-file   "/var/named/backup/cache_dump.db"; #系统转存文件的位置
}
```

此配置就是指定 DNS 服务器的区域文件存储在/var/named 下，配置中相关的区域文件都必须保

存此目录下。

（2）zone "区域名" IN {

type: 类型;

file: "区域文件名";

}

- zone：声明是用于定义一个区域，区域名可以自己定义，每个 DNS 服务器都有“.”的区域名，用于指明系统的根域名区域。
- type：声明区域的类型，基本类型有四种：master，表明该区域是主区域，拥有区域数据文件，并对此区域提供管理数据；slave 表明该区域是辅助区域，拥有主 DNS 服务器区域数据文件的副本，辅助 DNS 服务器从主 DNS 服务器同步所有区域数据，因此往往与主区域一起使用；hint 表明该区域是提示区域（或者叫线索区域），它使用根线索来查找全球的根域名服务器；stub 区域和 slave 类似，但只复制主 DNS 服务器上的 NS 记录，而不复制所有区域。
- file“文件名”：指定区域配置文件，该文件中将定义资源记录。在辅助区域服务器的配置文件中，这个文件不需要建立，只要启动 named 服务，辅助区域配置文件的内容会自动从主域服务器上复制过来。
- allow-update：指定动态更新类型，none 表示不允许动态更新。
- include 选项：包含配置文件。

DNS 中的区域文件主要有两种类型：一种正向区域，用于从域名解析 IP 地址；另一种是反向区域，用于从 IP 地址中反向查找域名。这两种区域都是用 zone 建立的，区别在于“区域名”的命名不一样。反向区域的命名一般采用“IP 地址前 3 字节.in-addr.arpa”，而且 IP 地址的前 3 个字节通常写成反的形式，如 61.187.55.0 对应的反向区域名就可以命名为 55.187.61.in-addr.arpa。

正向区域实例如下：

```
zone  "hunau.net"  IN  {
    type master;
    file "hunau.net.db";
}
```

反向区域实例如下：

```
zone  "55.187.61.in-addr.arpa"  IN  {
    type master;
    file "hunau.net.rev";
};
```

2. 正向区域配置文件

根据 named.conf 中的配置，区域 hunau.net 对应的区域文件为 huanu.net.db，这个文件定义了区域 hunau.net 中的各种更新信息和资源记录，使用 vi /var/named/hunau.net.db 即可查看，内容如下：

```
    $TTL 86400
@ IN SOA   hunau.net.   root.hunau.net. (
```

```
        2001082925; Serial
        3600 ; Refresh
        900 ; Retry
        1209600 ; Expire
        43200 ) ; Minimum
@       IN    NS    ns1.hunau.net.
@       IN    NS    ns2.hunau.net.
ns1     IN    A     172.28.27.1
ns2     IN    A     172.28.27.3
www     IN    A     61.187.55.34
mail    IN    A     61.187.55.38
@       IN    MX    5    61.187.55.38
```

参数说明：

- $TTL：DNS 缓存时间，单位为秒。
- SOA：在主域名服务器中，区域的 DNS 服务器管理员的邮件地址中的@用“.”代替。

序列号：区域复制依据，每次主要区域修改完数据后要手动增加其值。

刷新间隔：默认以秒为单位，辅助 DNS 服务器请求与源服务器同步的等待时间。当刷新间隔到期时，辅助 DNS 服务器请求源服务器的 SOA 记录副本。然后，辅助 DNS 服务器将源服务器的 SOA 记录的序列号与其本地 SOA 记录的序列号比较，如果不同，则辅助 DNS 服务器从主要 DNS 服务器请求区域传输。这个域的默认时间是 900 秒。

- 重试时间：默认以秒为单位，辅助 DNS 服务器在请求失败后等待多长时间重试。通常这个应该短于刷新时间。默认为 600 秒。
- 过期时间：默认以秒为单位，当这个时间到期时（如辅助 DNS 服务器还无法与源服务器进行区域传输），则辅助 DNS 服务器会将其本地数据当作不可靠数据。默认值为 86400 秒。
- TTL：默认以秒为单位，区域的默认生存时间和缓存否定应答名称查询的最大间隔，默认值为 3600 秒。

接下来是各种类型的记录，如 NS 记录是表明域名服务器的记录。通常情况下不需要设置 NS 记录，因为此时的域名是通过 ISP 提供的域名服务器解析的，若用户需要自己用 DNS 服务器来解析自己的域名，则要创建 NS 记录，并且将域名服务器的 IP 地址告诉 ISP 登记即可。

A 记录用于指明一个域名对应的 IP 地址。

CNAME 记录（也就是别名记录）可以将多个不同名称指向同一个服务器。在创建别名记录之前必须要先创建 A 记录。

MX 记录用于指明邮件服务器的 IP 地址。

3. 反向域名解析文件

反向域名解析文件格式与正向域名解析文件的配置大致类似，区别在于最后 PTR 记录的写法。用 vi /var/named/hunau.net.rev 看到的文件内容如下：

```
$TTL    86400
@       IN      SOA     hunau.net.   root.hunau.net.  (
                                      2001082926 ; Serial
                                      28800      ; Refresh
```

```
                                    14400       ; Retry
                                    3600000     ; Expire
                                    86400 )     ; Minimum
                    IN      NS      hunau.net
38          IN      PTR     mail.hunau.net
34          IN      PTR     www.hunau.net
```

实际的 DNS 服务器通常配置成主域名服务器、辅助域名服务器和转发域名服务器，下面针对网络工程师考试中常考的三种类型的域名服务器的配置通过举例来介绍。

（1）主域名服务器的配置。

网络中常用 DNS 服务器的类型是主域名服务器，其配置比较简单，通常只要定义一个区域并指定区域的定义文件，在对应的区域定义文件中添加相应的资源记录即可。若需要新建一个 hunau.net 的区域并作为主域名服务器，则只要完成以下两步。

1）在 named.conf 文件中设置域 hunau.net。

建立正向解析域：

```
zone "." IN {                       #指定根域
    type hint;
    file "named.ca";
    };

zone    "hunau.net" {               #定义本地域
    type master;
    file "hunau.net.db";
    };
```

建立反向解析域：

```
zone "27.28.172.in-addr.arpa" {     #定义反向域
    type master;
    file "hunau.net.rev";
    };
```

2）在 hunau.net.db 中配置文件资源记录。

```
$TTL 86400
@ IN SOA   hunau.net.   root.hunau.net. (
      2001082925; Serial
      3600 ; Refresh
      900 ; Retry
      1209600 ; Expire
      43200 ) ; Minimum
@       IN    NS    ns1.hunau.net.
@       IN    NS    ns2.hunau.net.
www     IN    A     61.187.55.34
mail    IN    A     61.187.55.38
```

此时重启 DNS 服务器，则 hunau.net 的主域名服务器建立完成。

（2）辅助域名服务器的配置。

辅助域名服务器作为主域名服务器的辅助和备份服务器，自身不建立区域文件，而是从主域名

服务器中查询，它可以与主域名服务器提供相同的域名解析服务。要为上例中的 hunau.net 配置辅助域名服务器，则只要完成以下步骤即可。

在 named.conf 文件中建立正向解析域：

```
zone "hunau.net" {
    type slave;                #type 设置为 slave，表示当前 DNS 服务器是辅助域名服务器
    file "hunau.net.db"        #辅助域名服务器中的区域文件将从主域名服务器中获取并保存在本机的指定文件内，为了方便管理，尽量使用与主服务器相同的区域文件名称。如果该文件不存在，named 就自动生成一个，并从主域名服务器中获取配置数据，然后将这些数据写入新创建的文件中。如果存在该文件，named 就要检查主域服务器，若数据有变化，更新本地数据，若无变化，就直接加载磁盘文件的内容
    masters   { 172.28.27.1; };  #指定主域名服务器的 IP 地址
    };
建立反向解析域：
zone "27.28.172.in-addr.arpa" {
    type slave;
    file "172.28.27.rev";
    masters   { 172.28.27.1; };
    };
```

配置完之后重新启动 DNS 服务即可。

（3）高速缓存域名服务器。

在 Internet 中主要使用名字进行连接，因此网络中的 DNS 查询会十分频繁。很多情况下，会有大量重复的 DNS 查询。尤其在使用拨号连接时，由于名字服务器位于 ISP 端，即使是曾经查询过的名字，其信息仍然保存在线路另一端名字服务器的缓冲区内，重复的 DNS 查询将占据部分线路带宽。因此，最好的办法是将查询结果保存在本地计算机上，以避免重复查询造成的网络流量。尽管很多客户机能够在本机内保存一个名字解析缓冲区，但这个缓冲区相对来说很小，起不到有效的作用，然而如果要将这个缓冲区设置得较大，就能及时刷新名字的解析数据。要想很好地缓冲 DNS 数据，最好的缓冲区还是 DNS 服务器本身，因为 DNS 的实现方式就是一种经常刷新的缓冲方式，并且 named 可以根据不同 zone 的不同设置来实现数据刷新。

因此，最简单的办法就是设置一个具备缓冲能力的名字服务器作为名字解析的缓冲。通常情况下，如果在 named.conf 中仅有默认的 zone "."，而没有 master 和 slave 定义的区域，则可以认为它是一个高速缓存服务器。默认的 zone "." 对应的 type hint 的区域文件是 named.ca。具体配置如下：

```
zone "." IN {                    #指定根域
    type hint;
    file "named.ca";
    };
```

named.ca 文件给出了 Internet 上所有根名字服务器的地址信息，用于初始化 named 的缓冲区。通过这些根域名服务器的帮助，每一台 DNS 服务器都能对整个 Internet 进行查询。一般不需要改变这些文件的内容，但是如果要建设一个不与 Internet 连接的内部网，就不需要 named.ca 中这些根名字服务器的地址，而是更改为自己网络内的根名字服务器的地址。

（4）DNS 服务器负载均衡配置。

在实际应用中还可以通过设置 DNS 的循环机制让多台服务器实现共用一个域名，以实现 DNS 负载均衡的目的。如有两台 Web 服务器，IP 地址分别为 61.187.55.34 和 61.187.55.35。这两台服务器由共同的域名 www.hunau.net 提供对外服务，只需在 DNS 服务器 hunau.net 区域对应的区域文件 hunau.net.db 中增加下列内容即可：

```
www1    IN   A        61.187.55.34
www2    IN   A        61.187.55.35
wwwIN   CNAME        www1
wwwIN   CNAME        www2
```

或者直接添加下列内容，效果是一样的。

```
www IN       A        61.187.55.34
www IN       A        61.187.55.35
```

## 18.2 DHCP 服务器配置

本部分主要讲解 DHCP 服务器的配置、测试和基本应用。

### 18.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：DHCP 服务器配置、客户端配置。

### 18.2.2 知识点精讲

1. DHCP 服务器配置

DHCP 是动态主机配置协议，用于向计算机自动提供 IP 地址、子网掩码和默认路由等基本配置信息。网络管理员通常会给局域网上的客户机分配某个范围内的 IP 地址。当 DHCP 客户接入网络时会向 DHCP 服务器请求一个 IP 地址，然后 DHCP 服务器为每个请求的设备分配一个地址，直到分配完该范围内的所有 IP 地址为止。已经分配的 IP 地址必须定时延长租用期。此过程确保了当客户机设备在正常释放 IP 地址之前突然从网络断开时，原来被分配的地址能够归还给服务器。

Linux 系统中 DHCP 服务器的配置相对比较简单，只需掌握/etc/dhcpd.conf 的配置即可，另外相关的辅助配置文件/lib/dhcpd.leases 用于记录所有已经分配出去的 IP 地址信息。

（1）/etc/dhcpd.conf 配置文件。

dhcpd 的配置文件是/etc/dhcpd.conf 文件。此配置文件包括两个部分：全局参数配置和局部参数配置。全局参数配置的内容对整个 DHCP 服务器起作用，如组织的域名、DNS 服务器的地址等；局部参数配置只针对相应的子网段或主机等局部对象起作用。所有配置的格式通常都包括三部分：parameters、declarations、option。系统中常用的主要参数、声明和选项如表 18-1～表 18-3 所示。

表 18-1　DHCP 参数表

| 选项 | 作用 |
| --- | --- |
| ddns-update-style | 配置 DHCP-DNS 更新模式 |
| default-lease-time | 指定默认租赁时间的长度，单位是秒 |
| max-lease-time | 指定最大租赁时间长度，单位是秒 |
| hardware | 指定网卡接口类型和 MAC 地址 |
| server-name | 通知 DHCP 客户服务器名称 |
| get-lease-hostnames flag | 检查客户端使用的 IP 地址 |
| fixed-address ip | 分配给客户端一个固定的地址 |
| authritative | 拒绝不正确的 IP 地址的要求 |

表 18-2　DHCP 声明参数表

| 选项 | 作用 |
| --- | --- |
| shared-network | 用来告知是否一些子网络共享相同网络 |
| subnet | 描述一个 IP 地址是否属于该子网 |
| range 起始 IP 终止 IP | 提供动态分配 IP 的范围 |
| host | 主机名称参考特别的主机 |
| group | 为一组参数提供声明 |
| Allow/deny unknown-clients; | 是否动态分配 IP 给未知的使用者 |
| Allow/ deny bootp | 是否响应激活查询 |
| allow/ deny booting | 是否响应使用者查询 |
| filename | 开始启动文件的名称，应用于无盘工作站 |
| next-server | 设置服务器从引导文件中装入主机名，应用于无盘工作站 |

表 18-3　DHCP 选项参数表

| 选项 | 作用 |
| --- | --- |
| subnet-mask | 为客户端设定子网掩码 |
| domain-name | 为客户端指明 DNS 名字 |
| domain-name-servers | 为客户端指明 DNS 服务器 IP 地址 |
| host-name | 为客户端指定主机名称 |
| routers | 为客户端设定默认网关 |
| broadcast-address | 为客户端设定广播地址 |
| ntp-server | 为客户端设定网络时间服务器 IP 地址 |
| time-offset | 为客户端设定与格林威治时间的偏移时间，单位是秒 |

- DHCP 配置文件中的 parameters（参数）：表明如何执行任务。参数说明见表 18-1。
- DHCP 配置文件中的 declarations（声明）：用来描述网络信息、提供给客户使用的 IP 地址等信息。参数说明如表 18-2 所示。
- DHCP 配置文件中的 option（选项）：用来配置 DHCP 可选参数，选项全部以 option 关键字开头。参数说明如表 18-3 所示。

一个典型的 dhcp 服务器的配置如下：

```
ddns-update-style interim;          #全局设置参数，允许 DNS 服务器动态更新
ignore client-updates;              #全局设置参数，忽略客户端更新
subnet 192.168.1.0 netmask 255.255.255.0 {
    option routers                  192.168.1.254;  #此处开始的是局部设置参数，只对子网 192.168.1.0 网段起
作用。此 routers 就只针对 192.168.1.0 网段的机器设置默认网关 192.168.1.254
    option subnet-mask              255.255.255.0;
    option broadcast-address        192.168.1.255;
    option domain-name-servers      192.168.1.3;
    option domain-name              "www.hunau.net";
    option domain-name-servers      192.168.1.3;
    option time-offset              -18000;     #指定与格林威治时间是偏移值
    range dynamic-bootp             192.168.1.128   192.168.1.255;
    default-lease-time 21600;
    max-lease-time 43200;
    host   xp {
            hardware Ethernet   00:19:21:D3:3B:05;
            fixed-address 192.168.1.17; #为一台 MAC 地址是 00:19:21:D3:3B:05 的主机固定分配 IP 地址 192.168.1.17.
             }
}
```

（2）dhcpd.leases。

dhcpd.leases 配置文件是 DHCP 服务器自动创建和维护的，不需要管理员参与配置。文件中自动记录了服务器已经分配了的所有 IP 地址的相关信息，在网路地址分配出现故障时，可以通过该文件中的信息了解网络地址的具体分配情况。

dhcpd.leases 文件的基本格式为：

leases ipaddress ｛statement｝

其中，｛ statement ｝是用于记录服务器分配给具体主机的各种配置信息，如开始租约时间、结束租约时间、客户机的 MAC 地址、客户机的主机名等。

一个典型的 dhcpd.leases 文件内容如下：

```
lease 192.168.1.17 {                    #DHCP 服务器分配的 IP 地址
  starts 1 20xx/05/02 03:02:26;         # lease  开始租约时间
  ends 1 20xx/05/02 09:02:26;           # lease  结束租约时间
  binding state active;
  next binding state free;
  hardware ethernet 00:19:21:D3:3B:05;  #客户机的 MAC 地址
  client-hostname "xp";                 #客户机名称
}
```

要注意开始租约时间和结束租约时间是格林威治标准时间，不是系统的本地时间。第一次运行 DHCP 服务器时，dhcpd.leases 是一个空文件，由系统自动创建和维护。作为网络工程师，只要能

看懂租约文件中的信息即可。

2. 启动和检查 DHCP 服务器

（1）使用命令启动 DHCP 服务器。

```
#service dhcpd start
```

（2）使用 ps 命令检查 dhcpd 进程。

```
#ps -ef | grep dhcpd
root      2402     1   0  14:25 ?        00:00:00  /usr/sbin/dhcpd
root      2764  2725   0  14:29 pts/2    00:00:00  grep dhcpd
```

（3）使用检查 dhcpd 运行的端口。

```
# netstat -nutap | grep dhcpd
udp    0   0 0.0.0.0：67          0.0.0.0：*      2402/dhcpd
```

3. Linux DHCP 客户端配置

可以手工配置/etc/sysconfig/network 和 /etc/sysconfig/network-scripts 目录中每个网络设备的配置文件。每个设备都有一个叫做 ifcfg-ethx 的配置文件，其中 x 表示网络设备的编号，如 eth0 表示第一块以太网卡。如果客户端希望在启动时就能联网，必须修改 NETWORKING，其变量必须为 yes。典型的/etc/sysconfig/network 文件如下：

```
NETWORKING=yes
DEVICE=eth0
BOOTPROTO=dhcp
ONBOOT=yes
```

其中 BOOTPROTO=dhcp 表明客户机启动时通过 DHCP 去获得自己的 IP 设置信息。在/etc/sysconfig/network-scripts/ifcfg-eth0 中就不要再指定客户机的 IP 地址了。

4. Windows 客户端配置

Windows 系统的 DHCP 客户端配置非常简单，只要将本地连接的 TCP/IP 属性设置为“自动获得 IP 地址”即可。系统运行后，要从服务器获得 IP 地址，可以用 ipconfig 指令看到 IP 的配置信息，配置方式和结果如图 18-2 图 18-3 示。

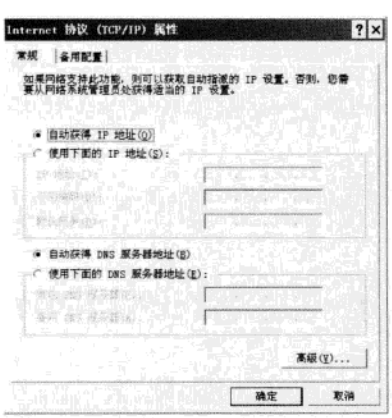



图 18-2 Windows DHCP 客户设置

```
Ethernet adapter 无线网络连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) Wireless WiFi Link
4965AG
        Physical Address. . . . . . . . . : 00-1F-3B-CD-29-DD
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.0.235
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DHCP Server . . . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 202.103.96.112
                                            211.136.17.108
        Lease Obtained. . . . . . . . . . : 20xx年10月6日 10:59:50
        Lease Expires . . . . . . . . . . : 20xx年10月6日 11:29:50
```

图 18-3 Windows DHCP 获得的设置信息

## 18.3 FTP服务器配置

本部分主要讲述FTP服务器配置、测试和基本应用。

### 18.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：FTP服务器配置、FTP服务管理。

### 18.3.2 知识点精讲

1. FTP服务器配置

在RedHat9以后的版本中，系统默认的FTP服务器是vsftp，原来的wuftp被取消，并且vsftp从XINETD中独立出来了。本书以vsftp为例讲述。

在访问FTP服务器时需要经过验证用户才能访问和传输文件。通常FTP服务器都可以提供以下3种不同的登录形式：

（1）anonymous。

anonymous就是匿名账户，是使用非常广泛的一种登录形式。对于没有FTP账户的用户可以用anonymous为用户名、任意字符（通常是自己电子邮件地址）为密码进行登录。当匿名用户登录FTP服务器后，其登录目录为匿名FTP服务器的根目录/var/ftp。在实际的服务器中，出于安全和负载压力的考虑，往往禁用匿名账号。

（2）普通账户。

普通账户也就是所谓的本地账户，就是用事先注册的用户名和密码进行登录。登录后，工作目录自动转移到用户自己在系统建立账户时自动创建的用户目录下。

（3）guest。

来宾账号，若用户在FTP服务器上有只能用于文件传输服务的账号，那就是guest，guest是普通账户的一种特殊形式，在guest登录FTP服务器后，不能访问除宿主目录以外的内容。在网络工程师考试中，与FTP服务器配置有关的文件是/etc/vsftpd/vsftpd.conf、/etc/vsftpd/ftpusers、/etc/vsftpd/user_list，在配置FTP服务器时，主要是修改这些文件中的相关语句。下面分别阐述这些基本配置文件的配置。

（1）vsftpd.conf文件。

vsftpd.conf文件是vsftp的主要配置文件，与服务器相关的全局设置都在此文件中，在Linux中可以使用vi /etc/vsftpd.conf查看和修改，具体内容如下：

```
[root@hunau ~]# vi /etc/vsftpd.conf
# Example config file /etc/vsftpd/vsftpd.conf
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit，to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
```

```
# READ THIS: This example file is NOT an exhaustive list of vsftpd options
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? （Beware - allowed by default if you comment this out）.
anonymous_enable=YES  #是否允许 anonymous 账户登录 FTP 服务器，默认值是允许的
#
# Uncomment this to allow local users to log in.
local_enable=YES   #是否允许本地用户登录 FTP 服务器，默认值是允许
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES  #是否开放本地用户的写权限，这个选项可以控制 FTP 的指令是否允许更改文件
#
# Default umask for local users is 077. You may wish to change this to 022，
# if your users expect that （022 is used by most other ftpd's）
local_umask=022  #设置本地用户的文件生成掩码为 022，默认值是 077
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also，you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES    #是否允许匿名账户在 FTP 服务器中创建目录
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES  #激活目录信息，当远程用户更改目录时将出现提示信息
#
# Activate logging of uploads/downloads.
xferlog_enable=YES  #启用上传和下载日志功能
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES    #启用 FTP 数据端口的连接请求
#
# If you want，you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.

#xferlog_file=/var/log/vsftpd.log  #设置日志文件的文件名和存储路径，这是默认的
#
# If you want, you can have your log file in standard ftpd xferlog format
xferlog_std_format=YES     #是否使用标准的 ftpd xferlog 日志文件格式
# You may change the default value for timing out an idle session.
```

```
#idle_session_timeout=600  #设置空闲的用户会话中断时间，默认值是 10 分钟
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120  #设置数据连接超时时间，默认值是 120 秒.
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it

# however，may confuse older FTP clients.

#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode.
# Beware that turning on ascii_download_enable enables malicious remote parties
# to consume your I/O resources，by issuing the command "SIZE /big/file" in
# ASCII mode.
# These ASCII options are split into upload and download because you may wish
# to enable ASCII uploads (to prevent uploaded scripts etc. from breaking)
# without the DoS risk of SIZE and ASCII downloads. ASCII mangling should be
# on the client anyway..
#ascii_upload_enable=YES
#ascii_download_enable=YES #是否允许使用 ASCII 格式来上传和下载文件
#
# You may fully customise the login banner string：
#ftpd_banner=Welcome to blah FTP service.#在 FTP 服务器中设置欢迎登录的信息
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES

#  （default follows）
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES,then this list becomes a list of
# users to NOT chroot().
#chroot_list_enable=YES
#如果希望用户登录后不能切换到自己目录以外的其他目录，需要设置该项，如果设置 chroot_list_enable=YES，那么只允许/etc/vsftpd.chroot_list 中列出的用户具有该功能。如果希望所有的本地用户都执行 chroot，可以增加一行：chroot_local_user=YES
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
```

```
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
pam_service_name=vsftpd     #设置 PAM 认证服务的配置文件名称，该文件存放在/etc/pam.d/目录下
userlist_enable=YES         #用户列表中的用户是否允许登录 FTP 服务器，默认是不允许
#enable for standalone mode
listen=YES  #若是 YES，则 vsftpd 将会以独立运作的方式运行;若是 vsftpd 包含在 xinetd 之中，则必须关闭此功能。
tcp_wrappers=YES  #将 vsftpd 与 TCP_wrapper 结合。如果启动，则会将 vsftpd 与 tcp wrapper 结合，也就是可以在
/etc/hosts.allow 与/etc/hosts.deny 中定义可访问或是拒绝的来源地址
```

（2）vsftpd.ftpusers 配置。

除了主配置文件/etc/vsftpd.conf 之外，FTP 服务器还使用/etc/vsftpd/ftpusers 文件用来记录“不允许”登录到 FTP 服务器的用户，通常是一些系统默认的用户。可以使用 vi /etc/vsftpd/ftpusers 命令查看，默认的设置如下：

```
[root@hunau  ~]# vi  /etc/vsftpd/ftpusers
# Users that are not allowed to login via ftp
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
```

在 FTP 的默认配置下，root 和上述用户不允许登录 FTP 服务器，通过这个文件，管理员可以将不允许登录的其他用户添加到此文件中，但是要注意，每个用户必须单独占用一行。

（3）vsftpd.user_list 配置。

vsftpd/user_list 文件与 vsftpd/ftpusers 文件的作用类似，在系统启动时会对主配置文件 vsftpd.conf 检查，根据其中的 userlist_deny=YES 选项的配置确定该配置文件是否生效，若主配置文件是 userlist_deny=YES，则 Vsftpd/user_list 配置文件必须存在。在系统中可以使用 vi /etc/vsftpd/vsftpd.user_list 命令查看，默认的设置如下：

```
[root@hunau  ~]# vi  /etc/vsftpd/ftpusers
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd.ftpusers
# for users that are denied.
root
bin
```

```
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
```

2. FTP 服务管理

管理 Linux 的 FTP 服务器，通常使用下面语句启动、停止和重启 FTP 服务。/etc/init.d/vsftpd stop 停止 FTP 服务，/etc/init.d/vsftpd start 启动 FTP 服务，或者/etc/init.d/vsftpd restart FTP 重启服务。

## 18.4 Web 服务器配置

本部分主要讲解 Web 服务器的配置和基本应用。

### 18.4.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：Apache 服务器的基本配置、虚拟主机的配置。

### 18.4.2 知识点精讲

1. Web 服务器配置

Linux 系统中常用的 Web 服务器软件主要是 Apache，网络工程师考试中与 Web 有关的考点也是与 Apache 服务器配置相关的知识点，因此本小节主要讲述 Apache 的配置。Apache 的主配置文件为/etc/httpd.conf。由于有两种安装方式，通常以源代码方式安装的配置文件保存在/usr/local/apache/conf/目录下，而以 RPM 包方式安装的配置文件保存在/etc/httpd/conf/目录下。在实际工作中通常以 RPM 包安装，因此可以直接修改/etc/httpd.conf 文件达到修改配置的目的。网络工程师考试中，Apache 的配置经常考，需要考生能熟练掌握。在系统中可以使用 vi/etc/httpd.conf 查看和修改基本配置，默认的基本配置参数如下：

```
[root@hunau ~]# vi/etc/httpd.conf
Port 80
#定义了 Web 服务器的侦听端口，默认值为 TCP 的 80 端口，可以保留多个端口，但以最后一个为准
User apache
#一般情况下，以 nobody 用户和 nobody 组来运行 Web 服务器
Group apache
#服务器发出的所有进程都是以 root 用户身份运行的，存在安全风险
```

```
ServerAdmin root@localhost
#指定服务器管理员的E-mail地址。服务器自动将错误报告到该地址
ServerRoot /etc/httpd
#服务器的根目录，一般情况下，所有的配置文件在该目录下
ServerName   new.host.name:80
#Web客户搜索的主机名称
KeepAliveTimeout   15
#规定了连续请求之间等待15秒，若超过15秒，则重新建立一条新的TCP连接
MaxKeepAliveRequests 100
#永久连接的HTTP请求数
MaxClients 150
#同一时间连接到服务器上的客户机总数
ErrorLog logs/error_log
#用来指定错误日志文件的名称和路径
PidFile run/httpd.pid
#用来存放httpd进程号，以便停止服务器
Timeout 300
#设置请求超时时间，若网速较慢，则应把值设大一些，效果更好
DocumentRoot /var/www/html
#用来存放网页文件
```

2. Web服务器配置虚拟主机

虚拟主机在一台WWW服务器上为多个单独的域名提供www服务，每个域名具有自己独立的目录和配置，相当于将一台主机分为多台主机。Apache有两种方式支持虚拟主机，一种是基于IP的虚拟主机；另一种是基于名字的虚拟主机。基于名字的虚拟主机使用相同的IP地址来配置不同的虚拟主机，这就弥补了因IP地址不足带来的问题。基于名字的虚拟主机的配置相当简单，只需配置DNS服务器使每个主机名对应正确的IP地址，然后再配置Apache HTTP Server，使其能认识不同的主机名。

【例18-1】Apache配置实例。

某公司因业务扩展，试图组建一台支持虚拟主机的Apache服务器，该服务器有一个IP地址：172.28.27.1，现在要建立两个虚拟主机，一个是公司的官方网站，域名为www.hunau.net；另一个是公司的培训业务网站，域名为www.hunau.edu.cn。因此需要先在DNS服务器中把域名www.hunau.net和www.hunau.edu.cn注册好。接下来修改Apache上的/etc/httpd.conf中的设置。

```
NameVirtualHost 172.28.27.1
< VirtualHost 172.28.27.1>
ServerAdmin root@hunau.net
ServerName www.hunau.net
DocumentRoot /var/www/html/gw
</VirtualHost >
< VirtualHost 172.28.27.1>
ServerAdmin root@hunau.edu.cnt
ServerName www.hunau.edu.cn
DocumentRoot /var/www/html/px
</VirtualHost >
```

而基于IP的虚拟主机则要求使用不同的IP地址来区别不同的虚拟主机，这就要求使用多块网卡把不同的IP地址捆绑到不同的网卡上，或者在一块网卡上捆绑多个IP地址。假设我们主机的IP

地址是 172.28.27.1（www.hunau.net），另一个 IP 地址是 172.28.27.3（www.hunau.edu.cn），只要修改 httpd.conf 关键配置即可。若服务器只有一个物理网卡，则需要使用 ifconfig eth0 172.28.27.1 和 ifconfig eth0:1 172.28.27.3 设置多个 IP 地址。

```
<Virtualhost 172.28.27.1:80>
ServerAdmin root@hunau.net
DocumentRoot /var/www/html/gw
ServerName www.hunau.net
ErrorLog /var/www/html/gw/logs/error_log
Customlog   /var/www/html/gw/logs/access_log common
</Virtualhost>
<Virtualhost 172.28.27.3:80>
ServerAdmin root@hunau.edu.cn
DocumentRoot /var/www/html/px
ServerName hunau.edu.cn
ErrorLog /var/www/html/px/logs/error_log
Customlog   /var/www/html/px/logs/access_log common
</Virtualhost>
```

修改完之后，用 service httpd restart 指令重启 Apache 即可生效。

3. Apache 的管理

启动和停止 Apache 服务的命令如下：

```
/etc/rc.d/init.d/httpd start        启动 Apache 服务
/etc/rc.d/init.d/httpd stop         停止 Apache 服务
```

# 第 4 天

# 再接再厉，案例实践

经过第 3 天的学习，我们已经掌握了各类应用服务器的基础知识，了解了一些重要的配置技巧和流程，并且能快速搭建常见的网络应用。第 4 天主要是学习网络基础硬件的搭建、管理和配置。重点讲解路由器、交换机、防火墙、硬件 VPN 的管理与配置。

## 第 1 学时　交换基础

第 4 天的第 1 学时主要学习交换基础知识。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 1～5 分之间。交换基础知识的考察主要集中在上午考试中。本章考点知识结构图如图 19-1 所示。


图 19-1　考点知识结构图

## 19.1　交换机概述

### 19.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：交换机分类、冲突域与广播域、吞吐量与背板带宽、交换机端口。

### 19.1.2 知识点精讲

交换机（Switch）是一种信号转发的设备，可以为交换机自身的任意两端口间提供独立的电信号通路。常见的交换机有以太网交换机、电话语音交换机等，考试只考查以太网交换机。

1. 交换机分类

（1）以管理划分。

以管理划分可分为网管交换机（智能机）和非网管交换机（傻瓜交换机）。能进行管理和配置的交换机都称为网管交换机，网管交换机**都有 console 口**；不能进行管理和配置的交换机都称为非网管交换机。

（2）以工作层次划分。

以交换机工作层次划分，可以分为 2 层交换机、3 层交换机和 4 层交换机。

1）2 层交换机。

**工作在数据链路层的交换机**通常称为 2 层交换机。2 层交换机**根据 MAC 地址进行交换**。如表 19-1 所示指出了各类交换机的交换依据。

表 19-1 交换机交换依据

| 交换机类别 | 交换依据 |
| --- | --- |
| 2 层交换机 | MAC 地址 |
| 3 层交换机 | IP 地址 |
| 4 层交换机 | TCP/UDP 端口 |
| 帧中继交换机 | 虚电路号（DLCI） |
| ATM 交换机 | 虚电路标识 VPI 和 VCI |

2）3 层交换机。

带有了路由功能的交换机工作在网络层，称为 3 层交换机。3 层交换机能加快数据交换，可以实现路由，能够做到“一次路由，多次转发”（Route Once，Switch Thereafter），即在第 3 层对数据报进行第一次路由，之后尽量在第 2 层交换端到端的数据帧。数据转发由高速硬件实现，路由更新、路由计算、路由确定等则由软件实现。3 层交换机根据 IP 地址进行交换，可以转发不同 VLAN 之间的通信。

多层交换（MultiLayer Switching，MLS）为交换机提供基于硬件的第 3 层高性能交换。它采用先进的专用集成电路（ASIC）交换部件完成子网间的 IP 包交换，可以大大减轻路由器在处理数据包时所引起的过高系统开销。MLS 是一种用硬件处理包交换和重写帧头，从而提高 IP 路由性能的技术。MLS 支持所有传统路由协议，而原来由路由器完成的帧转发和重写功能现在已经由交换机的硬件完成。MLS 将传统路由器的包交换功能迁移到第 3 层交换机上，这首先要求交换的路径必须存在。

3）4 层交换机。

第 2 层和第 3 层交换机分别基于 MAC 和 IP 地址交换，数据传输率较高，但却无法根据端口主机

的应用需求来自主确定或动态限制端口的交换过程和数据流量，即缺乏第4层智能应用交换需求。

第4层交换机除了可以完成第2层和第3层交换机功能外，还能依据传输层的端口进行数据转发。第4层交换机支持传输层以下的所有协议，可识别至少80个字节的数据包包头长度，可根据TCP/UDP端口号来区分数据包的应用类型，从而实现应用层的访问控制和服务质量保证。第4层交换机是以软件构建为主、以硬件支持为辅的网络管理交换设备。

（3）以网络拓扑结构划分。

依据交换机所处的网络拓扑结构，交换机分可为接入层交换机、汇聚层交换机、核心层交换机。

1）接入层交换机。

接入层交换机端口固定，一般拥有24～80个左右的百兆以太网口，12～24个左右的千兆以太网口，用于实现把用户的计算机和终端接入网络。老式的接入层交换机不带网管功能，现在越来越多的接入层交换机带网管功能。**MAC层过滤和IP地址绑定在接入层交换机层完成**。

2）汇聚层交换机。

汇聚层交换机将接入层交换机汇聚起来，与核心交换机连接。汇聚层交换机可以是固定配置，也可以是模块配置，千兆光纤口较多。汇聚层交换机一般都是可以网管的。**数据包过滤、协议转换、流量负载和路由应在汇聚层交换机层完成**。

3）核心层交换机。

核心层交换机属于高端交换机，背板带宽和包转发率高，且采用模块化设计。**核心层交换机可作为网络骨干构建高速局域网**。

（4）以交换方式划分。

以太网交换机的交换方式有三种：直通式交换、存储转发式交换、无碎片转发交换。

1）直通式交换（Cut-through）：只要信息有目标地址，就可以开始转发。这种方式没有中间错误检查的能力，但转发速度快。

2）存储转发式交换（Store-and-Forward）：将接收到的信息先缓存，检测正确性，确定正确后才开始转发。这种方式的中间节点需要存储数据，时延较大。

3）无碎片转发交换（Fragment Free）：接收到64字节之后才开始转发。

在一个正确设计的网络中，冲突的发现会在源发送64个字节之前，当出现冲突之后，源会停止继续发送，但是这一段小于64字节的不完整以太帧已经被发送出去了且没有意义，所以检查64字节以前就可以把这些“碎片”帧丢弃掉，这也是“无碎片转发”名字的由来。

有些交换机就只支持存储转发或直通转发，有些交换机支持多种模式。例如支持直通式交换和存储转发式交换的交换机，在每个交换端口设置一个错误值，超过时就自动调制模式，从直通转发切换到存储转发；低于某值时又恢复到直通转发。

2. 冲突域与广播域

（1）冲突域。

冲突域是物理层的概念，是指会发生物理碰撞的域。可以理解为连接在同一导线上的所有工作站的集合，也是同一物理网段上所有节点的集合，可以看作是以太网上竞争同一物理带宽或物理信

道的节点集合。**单纯复制信号的集线器和中继器是不能隔离冲突域的。**使用第 2 层技术的设备能分割 CSMA/CD 的设备，可以隔离冲突域。**网桥、交换机、路由器能隔离冲突域。**

（2）广播域。

广播域是数据链路层的概念，是能接收同一广播报文的节点集合。如设备广播的 ARP 报文，能接收到的设备都处于同一个广播域。隔离广播域需要使用第 3 层设备，**路由器、3 层交换机都能隔离广播域。**

3. 吞吐量与背板带宽

（1）吞吐量。

吞吐量是单位时间内网络中通过数据包的数量。对交换机而言，要实现满负荷运行，最小吞吐量计算公式如下：

吞吐量（Mp/s）=万兆端口数量×14.88 Mp/s+千兆端口数量×1.488 Mp/s+百兆端口数量×0.1488 Mp/s。

如果速率超过最小吞吐量，则交换机能实现线速交换。

这里的 14.88 Mp/s、1.488 Mp/s、0.1488 Mp/s 是如何得到的呢？这是通过用固定的数据速率除以最小帧长得到的，结果实际上就是单位时间内发送 64byte 数据包的个数。

由于以太网中的每个帧之间都要有帧间隙，即每发完一个帧之后要等待一段时间再发另外一个帧，在以太网标准中规定最小帧间隙是 12 个字节；同时以太帧报头长 20 个字节，因此 64byte 的数据包在数据链路层封装后大小变为了（64＋8＋12）=80byte。

这样千兆端口下数据包个数=1000Mb/s÷8bit÷(64+8+12)byte≈1.488Mp/s

（2）背板带宽。

带宽是交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量。全双工交换机背板带宽计算公式如下：

背板带宽（Mb/s）=万兆端口数量×10000Mp/s×2+千兆端口数量×1000Mb/s×2+百兆端口数量×100Mb/s×2+其他端口×端口速率×2

4. 交换机端口

交换机端口有很多，主要分为光纤端口、以太网端口、GBIC、SFP、万兆模块。

（1）光纤端口。

- 100Base-FX 光纤端口，速率为 100Mb/s，接多模光纤。
- 1000Base-SX 光纤端口，速率为 1000Mb/s，接多模光纤。

（2）以太网端口。

- 100Base-TX 以太网端口，速率为 100Mb/s，接双绞线。
- 1000Base-T 以太网端口，速率为 1000Mb/s，接双绞线。

（3）GBIC。

GBIC（Gigabit Interface Converter）是将千兆位电信号转换为光信号的接口器件，是千兆以太网连接标准。GBIC 在设计上可以为热插拔使用。目前 GBIC 基本被 SFP 取代。只要使用 GBIC 模

块，就能连接双绞线、单模光纤、多模光纤的介质。

- 1000Base-T GBIC 模块，接超五类和六类双绞线。
- 1000Base-SX GBIC 模块，接多模光纤。
- 1000Base-LX/LH GBIC 模块，接单模光纤。
- 1000Base-ZX GBIC 模块，接长波光纤，适合长距离传输，可达 100km。

GBIC 还可以作为级联模块，用于交换机的级联和堆叠。

（4）SFP。

SFP（Small Form-factor Pluggable）是 GBIC 的替代和升级版本，是小型的、新的千兆接口标准。

（5）万兆模块。

万兆模块是万兆的接口标准，万兆接口模块有多种，具体如表 19-2 所示。

表 19-2　万兆接口模块

| 模块名称 | 连接介质 | 可传输距离 |
| --- | --- | --- |
| 10GBase-CX4 | CX4 铜缆（属于屏蔽双绞线） | 15m |
| 10GBase-SR | 多模光纤 | 200m～300m，传输距离为 300m，则需要使用 50μm 的优化多模（Optimized Multimode 3，OM3） |
| 10GBase-LX4 | 单模、多模光纤 | 多模 300m，单模 10km |
| 10GBase-LR | 单模光纤 | 2～10km，可达 25km |
| 10GBase-LRM | 多模光纤 | 使用 OM3 可达 260m |
| 10GBase-ER | 单模光纤 | 2～40km |
| 10GBase-ZR | 单模光纤 | 80km |
| 10GBase-T | 屏蔽或非屏蔽双绞线 | 100m |

另外，SFP 还有 10GBase-KX4（并行方式）和 10GBase-KR（串行方式），用于背板。

## 19.2　交换机工作原理



### 19.2.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：2 层交换机工作流程、3 层交换机工作流程。

### 19.2.2　知识点精讲

1. 2 层交换机工作流程

2 层交换机具体的工作流程如下：

（1）交换机的某端口接收到一个数据包后，将源 MAC 地址与交换机端口对应关系存放到 MAC

地址表中。MAC 地址表存放 MAC 地址和端口对应关系，一个端口可以有多个 MAC 地址。

（2）读取该数据包头的目的 MAC 地址，并在交换机地址对应表中查 MAC 地址表。

（3）如果查找成功，则直接将数据转发到结果端口上。

（4）如果查找失败，则广播该数据到交换机所有端口上。如果有目的机器回应广播消息，则将该对应关系存入 MAC 地址表供以后使用。

2 层交换机识别数据中的 MAC 地址和转发数据到端口的功能，便于硬件实现。使用 ASIC 芯片可以实现高速数据查询和转发。

2. 3 层交换机工作流程

3 层交换机并非是路由器和 2 层交换机的简单物理组合，而是一个严谨的逻辑组合。某源主机发出的数据进行第 3 层交换后，相关信息保存到 MAC 地址与 IP 地址的映射表中。当同源数据再次交换时，3 层交换机则根据映射表直接转发到目的地址所在端口，无须通过路由计算。

这种方式简单、高效。相比“路由器+二层交换机”方式，配置更少、硬件空间更小、性能更高、管理更加方便。

# 第 2 学时　案例重点 1——交换机配置

第 4 天的第 2 学时主要学习交换配置知识。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 5～25 分之间。交换配置知识在上午和下午考试中均是重点，基本上每次考试均有一道 15 分的案例题。本章考点知识结构图如图 20-1 所示。

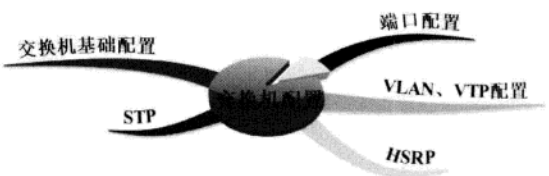



图 20-1　考点知识结构图

## 20.1　交换机基础配置

### 20.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：交换机连接、CLI 命令模式、交换机初始化配置、交换机静态路由配置。**注意本书中涉及的各类配置命令参数太多，因此在此只讲重要的、常考的参数。**

### 20.1.2 知识点精讲

1. 交换机连接

交换机连接有多种方式：

（1）基于 Console 口的命令行接口（Command Line Interface，CLI）配置方式。

（2）通过 Web 界面配置。

（3）通过 Cisco Works、CAN、SDM 等软件配置。

第一次初始配置必须使用基于 Console 口的 CLI 配置方式。使用 Console 配置方式需要使用超级终端，超级终端连接交换机，需要配置如图 20-2 所示的参数。

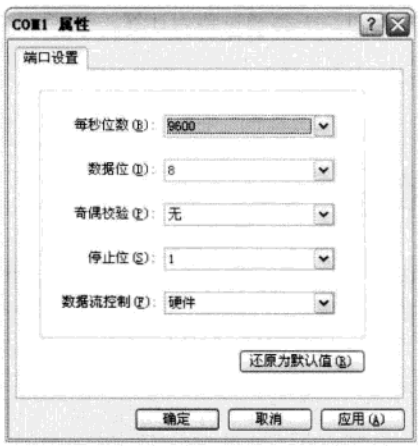



图 20-2 超级终端配置参数

具体参数值如下：

- 每秒位数：9600 波特。
- 数据位：8 位。
- 奇偶校验：无。
- 停止位：1 位。
- 数据流控制：无。

2. CLI 命令模式

考试一般以 Cisco 的 IOS 命令模式为准，不考虑 Catos 方式（几乎不再使用）。当然，考试不会严格依据 Cisco 的命令，有时历年试题出现细微的不同也是正常的。

IOS 主要包括六种不同的命令模式：

- User EXEC Mode（用户模式）
- Privileged EXEC Mode（特权模式）

- Global Configuration Mode（全局配置模式）
- VLAN Configuration Mode（VLAN 配置模式）
- Interface Configuration Mode（接口配置模式）
- Line Configuration Mode（Line 接口配置模式）

如表 20-1 所示列出了多个模式切换方法。

表 20-1 CLI 转换方式

| 模式 | 访问方法 | 提示符 | 退出方法 |
| --- | --- | --- | --- |
| 用户模式 | 登录交换机之后 | switch> | logout 或 quit |
| 特权模式 | 在**用户模式** switch>下，输入 **enable**（简写 en）命令 | switch# | disable |
| 全局配置模式 | **在特权模式** switch#下，输入 **config**（简写 con）命令 | switch(config)# | exit 或者 Ctrl+Z |
| VLAN 配置模式（VTP 透明模式下，可创建 ID>1005 的 VLAN） | 在 **全局模式** switch（config）#下，输入 vlan *vlan-id* 命令，vlan-id 表示 vlan 号 | Switch(config-vlan)# | （1）exit 退回到 switch（config）#；<br>（2）Ctrl+Z 或者 end 退回到 switch# |
| VLAN 配置（配置 ID 1～1005 的 VLAN） | **在特权模式** switch#下，输入 **Vlan database** 命令 | Switch(vlan)# | exit 退回到 switch# |
| 接口配置模式 | **在特权模式** switch#下，输入 **interface** 命令 | Switch(config-if)# | （1）exit 退回到 switch（config）#；<br>（2）Ctrl+Z 或者 end 退回到 switch# |
| Line 接口配置模式 | **在特权模式** switch#下，输入 **link console 0** 命令 | Switch(config-line)# | （1）exit 退回到 switch（config）#；<br>（2）Ctrl+Z 或者 end 退回到 switch# |

3. *交换机初始化配置*

如果要合理管理交换机，就应该配置 IP 地址（管理地址）和名称，并设置密码。管理一台新的交换机，首先要对其进行初始化配置。

Switch# **configure terminal**

*进入全局配置模式*

Switch（config）# **hostname** *name*

*配置交换机名称*

Switch（config）# **enable password** *password*

*为特权模式指定新的密码*

Switch（config）# **line vty 0 15**

*进入 Line 配置模式，15 是会话数，会话数可以是 0～15*

Switch（config）# **ip address** *ip_address subnet_mask*

*配置交换机 IP 地址及子网掩码*

Switch （config）#**ip default-gateway** ip default-gateway

*配置默认网关*

Switch （config）# **ip domain-name** *domain-name*

*配置域名*

Switch （config）# **ip name-server** *ip-address*

*配置域名服务器*

Switch（config-line）#**enable password** *password*

*配置 Telnet 访问时的 enable password 密码，长度可以是 1～25 个文字*

Switch（config-line）#**enable secret** *secret_password*

*配置 Telnet 访问时的 enable secret 密码*

Switch（config）# **interface vlan 1**

*配置 VLAN1，交换机默认 VLAN 是 VLAN1，交换机的指定 IP 必须在 VLAN1 中配置*

Switch（config-if）# **no shutdown**

*由于 VLAN 默认是关闭的，因此需要启用 VLAN1*

Switch（config）# **snmp-server host** *ipaddress | hostname*

*指定 SNMP 通知主机的 IP 地址*

Switch（config）# **snmp-server community** *string* [**ro**|**rw**]

*设置 SNMP 只读或读写字符串*

Switch（config）# **snmp-server enable traps**

*启用 SNMP 陷阱*

Switch（config）# **ip http server**

*启用交换机上的 HTTP 服务*

Switch（config）# **ip http secure-server**

*启用交换机上的 HTTPS 服务*

Switch（config）# **exit**

*返回特权模式*

Switch# **copy running-config startup-config**

*保存配置*

**注意**：配置使能口令（enable password）和使能密码（enable secret），可以在 Switch（config）#下配置完成。enable password 和 enable secret 的区别是使能口令以明文显示，而使能密码以密文形式显示。一般只需配置一个就可以了，当两者同时配置时，后者生效。

【例 20-1】下面给出了一个交换机基本配置过程。

```
Switch>                                          用户执行模式提示符
Switch >enable                                   进入特权模式
Switch #                                         特权模式提示符
Switch #config terminal                          进入全局配置模式
Switch(config)#                                  配置模式提示符
Switch(config)#enable password itct              设置 enable password 为 itct
Switch(config)#enable secret www.itct.com.cn     设置 enable secret 为 www.itct.com.cn
Switch(config)#hostname itct                     设置主机名为 itct
itct (config)#end                                退回到特权模式
itct #
```

4. 交换机静态路由配置

静态路由配置就是指定某一网络访问所需经过的路径，其中最关键的配置语句是：

```
Switch>                                          用户执行模式提示符
Switch >enable                                   进入特权模式
Switch #config terminal                          进入全局配置模式
Switch(config)# interface S0/0                   进入接口配置模式，这里以 S0 口为例
Switch(config-if)# ip address ip-address subnet-mask
Switch # ip route ip-address subnet-mask gateway
```

*ip-address* 为目标网络的网络地址，*subnet-mask* 为子网掩码，*gateway* 为网关。其中网关处的 IP 地址则说明了路由的下一站。

同时还要提一下默认路由。默认路由是一种特殊的静态路由，当路由表中与包的目的地址之间没有匹配的表项时，路由器能够做出选择。常考的默认路由配置命令如下：

```
Switch(config-if)# ip route 0.0.0.0   0.0.0.0   S0/0
```

如果没有默认路由，那么目的地址在路由表中没有匹配表项的包将被丢弃。默认路由会大大简化路由的配置，减轻管理员的工作负担，提高网络性能。

## 20.2　端口配置

### 20.2.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：接口命名、基本端口配置、端口工作模式设置。

### 20.2.2　知识点精讲

1. 接口命名

配置物理接口需要分别指定接口类型、堆叠成员号、模块号、交换机端口号。常见接口类型如表 20-2 所示。

- 堆叠成员号：标识堆叠的交换机成员，取值 1～9，默认为 1。并非所有交换机支持堆叠。
- 模块号：模块号是交换机模块或插槽号，非模块化交换机则不用标识模块号。
- 端口号：交换机端口总是从 1 开始。端口的标识都在交换机的面板上标出来，具体形式

如图 20-3 所示。

表 20-2　常见接口类型

| 接口类型 | 接口配置名称 | 简写 |
|---|---|---|
| 10/100Mb/s 网口 | fastethernet | fa |
| 10/100/1000Mb/s 网口 | gigabitethernet | gi |
| 10000Mb/s 以太网 | 10 gigabitethernet | te |
| SFP 模块千兆网口 | SFP | SFP |

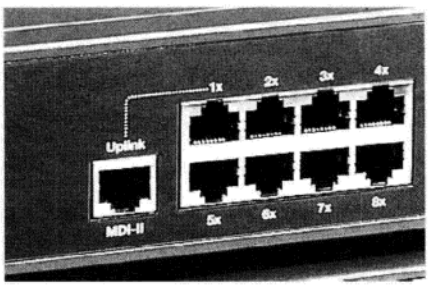



图 20-3　交换机端口标识

2. 基本端口配置

（1）堆叠交换机的接口标识为：堆叠成员号/模块号/接口号。Gigabitethernet3/0/23 表示交换机堆叠成员 3 的端口 4 的 10/100/1000Mb/s 网口，简写为 gi3/0/23。

进入该端口的配置命令为：

Switch(config)# **interface** *port*

例如，Switch(config)# **interface** gi3/0/23

（2）非堆叠交换机的接口标识为：模块号/接口号，如 fa0/1。配置接口完成后，可以通过 **show interface** 命令查看接口状态。

【例 20-2】使用 show interface fastEthernet0/1 switchport 命令查看交换机的 fa0/1 端口状态。

```
Switch # show interface fastEthernet0/1 switchport
Name: fa0/1
Switchport:Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1,2
Pruning VLANs Enabled: 2-1001
```

```
Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
```

例 20-2 中 Administrative mode：trunk 和 Operational Mode：trunk 两行说明了端口 fa0/1 的链路模式是 trunk 模式（中继模式）；Administrative Trunking Encapsulation：dot1q 和 Operational Trunking Encapsulation：dot1q 两行表示封装了 802.1Q 协议；Negotiation of Trunking：Disabled（default）表明不要求和对方建立中继连接；Trunking Native Mode VLAN：1（default）则表明默认 VLAN 为 VLAN1。

3. 端口工作模式设置

端口的工作模式一般有两种：访问 **Access** 模式（或接入模式）和 **Trunk** 模式，默认情况下为 Access 模式。

（1）Access 模式。

Access 口用于与计算机相连，只能运行设置一个 VLAN。Access 丢弃其他 VLAN 数据。

设置端口 Access 工作模式配置步骤为：

```
Switch #congfigure terminal
Switch(config-if)# Switchport mode access
```

（2）Trunk 模式。

Trunk 用于交换机之间的连接，把数据打上各类 VLAN 标签，带有标签的数据被转发到另一个交换机的 Trunk 口。

设置端口 Trunk 工作模式命令为：

```
Switch #congfigure terminal
Switch(config-if)# Switchport mode trunk                    配置中继模式
Switch(config-if)#switchport trunk encapsulation {isl|dot1q}
配置端口支持 isl、802.1q 封装
Switch(config-if)# switchport access vlan vlan-id
（可选）配置中继停止时，使用的默认 VLAN
Switch(config-if)# switchport trunk allowed vlan {add|all} vlan-list
生成 VLAN 许可列表，即允许部分或者全部 VLAN 通过 Trunk 口
Switch(config-if)# switchport trunk allowed vlan remove vlan-list
删除某 VLAN 出 VLAN 许可列表
```

Access 模式和 Trunk 模式在交换机端口上的应用如图 20-4 所示。


图 20-4 Access 模式和 Trunk 模式应用

【例 20-3】将交换机的 1～20 号端口设置为 Access 模式，并统一划到 VLAN 10 下。

```
Switch(config)# interface range fastethernet0/1-20        进入组配置状态
Switch(config-if)# switchport mode access                  设置端口工作在 Access 模式
Switch(config-if)# switchport access vlan 10               设置端口 1～20 为 VLAN 10 的成员
```

【例 20-4】配置交换机 24 口为中继模式，采用 IEEE 802.1Q 封装，允许所有 VLAN 从该端口交换数据。

```
Switch#config terminal                                     进入全局配置模式
Switch(config)#interface f0/24                             进入端口 24 配置模式
Switch(config-if)# switchport mode trunk
设置端口为中继（或 Trunk）模式
Switch (config-if)#switchport trunk encapsulation dotlq
设置 Trunk 采用 802.1q 格式（或 dot1q）
Switch(config-if)# switchport trunk allowed all
允许所有 VLAN 从该端口交换数据
```

## 20.3 VLAN、VTP 配置

### 20.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：VLAN 基础知识、VLAN 划分方法、VLAN 配置、将端口指定到 VLAN、 VTP 基础、VTP 协议、VTP 配置。

### 20.3.2 知识点精讲

1. VLAN 基础知识

虚拟局域网（Virtual Local Area Network，VLAN）是一种将局域网设备从逻辑上划分成一个个网段，从而实现虚拟工作组的数据交换技术。这一技术主要应用于 3 层交换机和路由器中，但主流应用还是在 3 层交换机中。

VLAN 是基于物理网络上构建的逻辑子网，所以构建 VLAN 需要使用支持 VLAN 技术的交换机。当网络之间的不同 VLAN 进行通信时，就需要路由设备的支持。这时就需要增加路由器、3 层交换机之类的路由设备。

一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，这样有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

2. VLAN 划分方法

VLAN 的划分方式有多种，主要有以下几种，但并非所有交换机都会支持，而且只能选择一种应用。

（1）根据端口来划分 VLAN。

这种划分方式是依据交换机端口来划分 VLAN 的，是最常用的 VLAN 划分方式，属于静态划分。例如，A 交换机的 1～12 号端口被定义为 VLAN1，13～24 号端口被定义为 VLAN2，25～48

号端口和 C 交换机上的 1～48 端口被定义为 VLAN3。VLAN 之间通过 3 层交换机或路由器保证 VLAN 之间的通信。

（2）根据 MAC 地址划分。

这种划分方法是根据每个主机的 MAC 地址来划分的，即对每个 MAC 地址的主机都配置其属于哪个组，属于**动态划分 VLAN**。这种方法的最大优点是当设备物理位置移动时，VLAN 不用重新配置，缺点是初始化时所有的用户都必须进行配置，配置工作量大；如果网卡更换或设备更新，又得重新配置。而且这种划分的方法也导致了交换机的端口都可能存在很多个 VLAN 组的成员，无法限制广播包，而导致广播太多，影响网络性能。

（3）根据网络层上层协议划分。

这种划分方法是根据每个主机的网络层地址或协议类型（如果支持多协议）划分的，属于动态划分 VLAN。这种划分方法根据网络地址（如 IP 地址），但与网络层的路由毫无关系。这种方法的优点是用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分，这对网络管理者来说很重要。此外，这种方法不需要附加帧标签来识别 VLAN，这样可以减少网络的通信量。这种方法的缺点是效率低，因为检查每一个数据包的网络层地址是需要消耗处理时间的（相对于前面两种方法），一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片能检查 IP 帧头，需要更高的技术，同时也更费时。

（4）根据 IP 组播划分 VLAN。

IP 组播实际上也是一种 VLAN 的定义，即认为一个组播组就是一个 VLAN，这种划分方法将 VLAN 扩展到了广域网，因此这种方法具有更大的灵活性，而且也很容易通过路由器进行扩展，当然这种方法不适合局域网，主要是效率不高。该方式属于**动态划分 VLAN**。

（5）基于策略的 VLAN。

根据 VLAN 划分规则发现感知加入新设备，并自动划分正确 VLAN。该方式属于**动态划分 VLAN**。

3. VLAN 配置

创建 VLAN 配置模式可以分为 VLAN 配置模式和 VLAN 数据库配置模式。一般情况下，交换机默认的 VLAN 是 VLAN1。

（1）VLAN 配置模式（Config Vlan Mode）。

VLAN 配置模式又称为全局配置模式，是目前主流的配置方式。该模式使用 **vlan** *vlan_id* 命令。

VLAN 配置模式创建 VLAN 步骤为：

| | |
|---|---|
| Switch #**config terminal** | 进入全局配置模式 |
| Switch(config)#**vlan** *vlan-id{[ vlan-id]}* | 创建 VLAN，可以同时创建多个 VLAN |
| 或 Switch(config)#**no vlan** *vlan-id* | 删除 VLAN |
| Switch(config-vlan)#**name** *vlan-name* | 配置 VLAN 名称 |
| Switch(config-vlan)#**mtu** *mtu-size* | 改变 MTU 大小 |

（2）VLAN 数据库配置模式。

该模式通过 vlan database 命令进入 VLAN 数据库配置模式。该模式只能配置 1～1005 号 VLAN

| | |
|---|---|
| Switch #vlan database | 进入 VLAN 数据库配置模式 |

| | |
|---|---|
| Switch(vlan)#vlan *vlan-id* name *vlan-name* | 创建 VLAN 并命名 |
| 或 Switch(vlan)#no vlan *vlan-id* | 删除 VLAN |
| Switch(vlan)# vlan *vlan-id* mtu *mtu-size* | 改变指定 MTU 大小 |

4. 将端口指定到 VLAN

当在交换机上创建了 VLAN 之后，接下来就需要根据规划将相应的端口指定至该 VLAN。指定可以是单一端口指定 VLAN 或者成批端口指定 VLAN。

（1）单一端口指定 VLAN。

| | |
|---|---|
| Switch(config)# **interface** *interface-id* | 指定欲配置的接口 |
| Switch(config-if)# **switchport mode access** | 设置端口工作在 Access 模式 |
| Switch(config-if)# **switchport access vlan** *vlan_id* | 将接口添加至指定的 VLAN |

（2）成批端口指定 VLAN。

| | |
|---|---|
| Switch(config)# **interface range** *port1-port2* | 进入组配置状态 |
| Switch(config-if)# **switchport mode access** | 设置端口工作在 Access 模式 |
| Switch(config-if)# **switchport access vlan** *vlan_id* | 设置 *port1-port2* 为 *vlan_id* 的成员 |

5. VTP 基础

VLAN 中继协议（VLAN Trunking Protocol，VTP）又称为虚拟局域网干道协议，是一种消息协议，用于在 VTP 域内同步 VLAN 信息（VLAN 的添加、删除和重命名）。可以系统地增加、删除、改变 VLAN 信息，并同时更新全网交换机，而无须一台一台地配置。VTP 是通过 ISL 帧或 Cisco 专有 DTP 帧来保持 VLAN 一致性的。

（1）VLAN 域。

VTP 域又称为 VLAN 管理域，是由若干相互联系的、相同 VTP 域名的交换机组成的。VTP 域结构如图 20-5 所示。

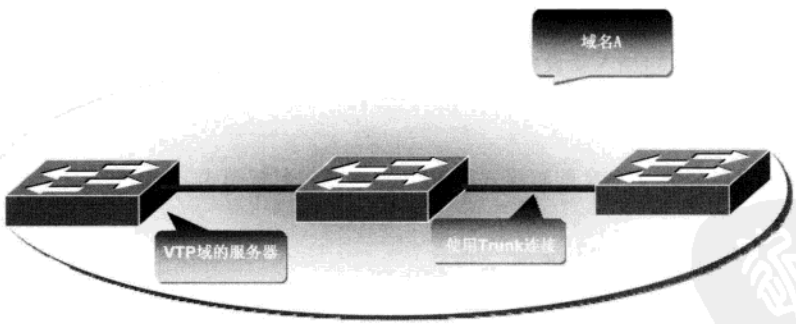



图 20-5　VTP 域结构

（2）VTP 模式。

VTP 分为三种模式，即 Server（服务器）模式、Client（客户端）模式、Transparent（透明）模式。

1）Server（服务器）模式。

VTP Server 模式**可以生成 VTP 消息（包含 VLAN ID、VLAN 名称），学习并转发相同域名的**

**VTP 消息，创建、删除、更改 VLAN。**交换机的**默认工作模式就是服务器模式**。局域网中的核心交换机往往被设置为 Server 模式。不相同的域名不转发 VTP 消息。如图 20-6 所示，左边交换机发送的 VTP 消息到中间就被丢弃。

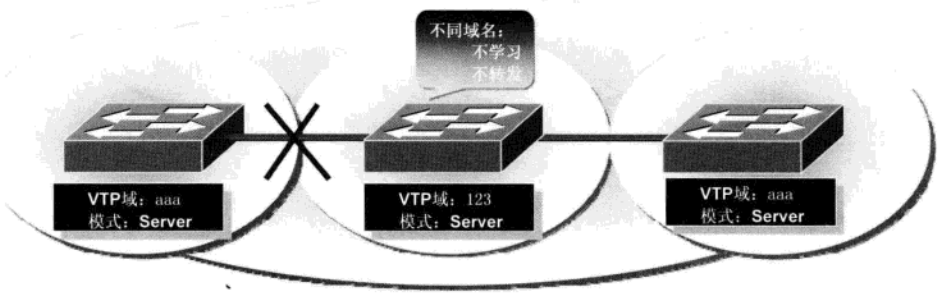



图 20-6 不同 VTP 名称，丢弃 VTP 消息

2）Client（客户端）模式。

VTP Client 模式**请求 VTP 消息，学习并转发相同域名的 VTP 消息，不可以创建、删除、更改 VLAN。**局域网中所有的汇聚交换机和接入交换机建议配置为 Client 模式。如图 20-7 所示说明了 Client 模式下不能创建 VLAN。

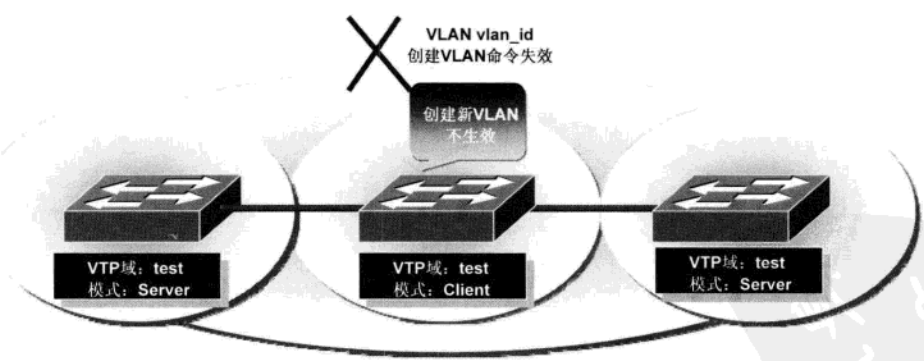



图 20-7 Client 创建 VLAN 失败

3）Transparent（透明）模式。

VTP Transparent 交换机不加入到 VTP 中，**不产生 VTP 消息，不学习 VTP 消息，可以转发 VTP 消息，可以添加、删除和更改 VLAN，但只在本地有效。**如图 20-8 所示可以看出，Server 端的 VTP 消息可以穿越 Transparent 端到达 Client。

（3）VTP 通告。

VTP 域中的交换机通过组播地址并使用中继端口发送通告。VTP 通告被相邻的交换机接收，并更新它们的 VTP 和 VLAN 配置。

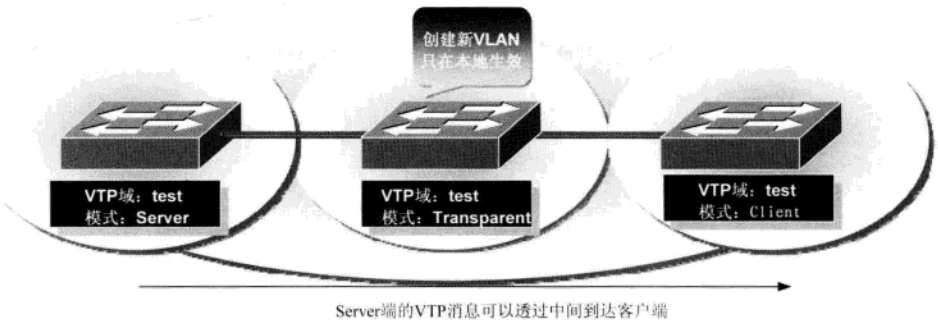



图 20-8　Transparent 模式可以透传 VTP 消息

VTP 通告包含 VLAN ID （ISL 和 802.1Q）、VTP 域名、VTP 配置版本号、VLAN 配置（包括每个 VLAN 的 MTU 大小）及帧格式。

（4）VTP 修剪。

VTP 修剪（VTP Pruning）通过减少不必要的广播（Broadcast Packet）、多播（Multicast Packet）等提高网络带宽。如图 20-9 和图 20-10 所示反应了开启 VTP Pruning 前后的网络交换情况。

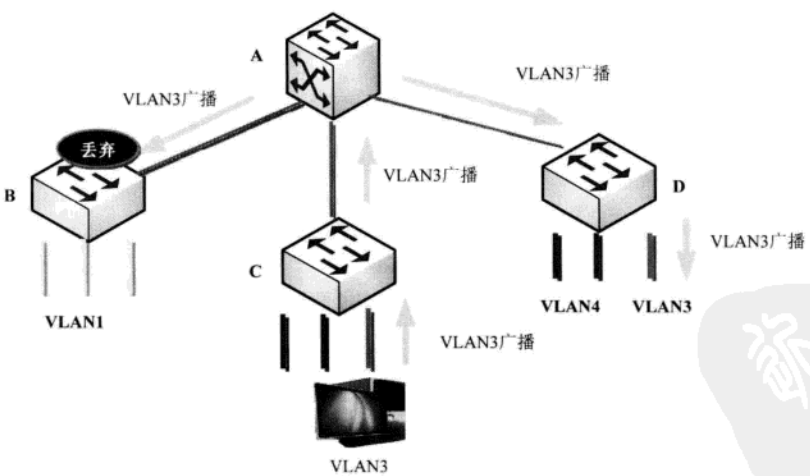



图 20-9　开启 VTP Pruning 前

- 修剪前，交换机 B 上没有 VLAN 3 的端口，交换机 B 丢弃这个广播包，浪费中继链路的带宽和交换机的处理资源。
- 采用 VTP 修剪后，只有交换机 B 通告了它使用 VLAN 3 的接口后，A 才把 VLAN 3 的广播转发到 B，否则不会转发 VLAN 3 广播给 B。即当启用 VTP 修剪功能后，如果交换端口中加入一个新的 VLAN，则该交换机会立即向周边交换机发送 VTP 连接报文。

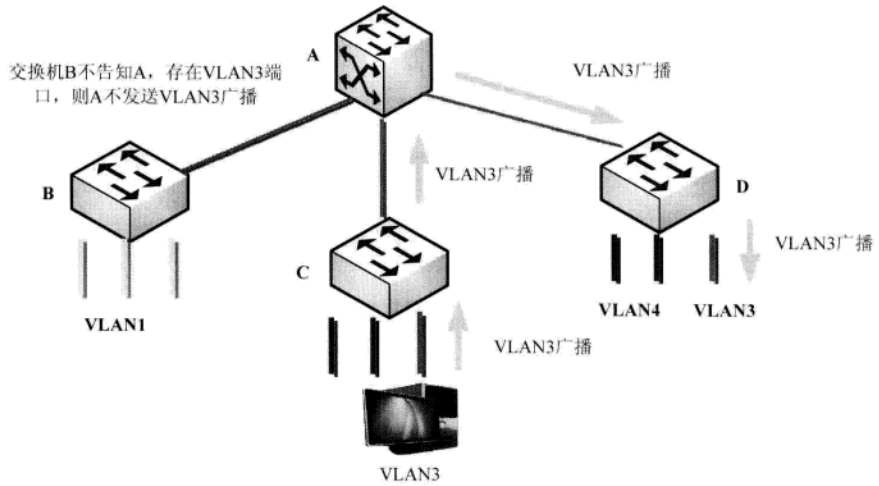



图 20-10　开启 VTP Pruning 后

6. VTP 协议

VTP 协议有两种链路封装协议：IEEE 802.1q 和 ISL。

（1）IEEE802.1q：俗称 dot1q，由 IEEE 创建。它是一个通用协议，在思科和非思科设备之间不能使用 ISL，必须使用 802.1q。802.1q 所附加的 VLAN 识别信息位于数据帧中的源 MAC 地址与类型字段之间。基于 IEEE802.1q 附加的 VLAN 信息，就像在传递物品时附加的标签。IEEE 802.1Q Vlan 最多可支持 4096 个 VLAN 组，并可跨交换机实现。

802.1q 协议在原来的以太帧中增加了 4 个字节的标记（Tag）字段，如图 20-11 所示。增加了 4 个字节后，交换机默认最大 MTU 应由 1500 个字节改为至少 1504 个字节。

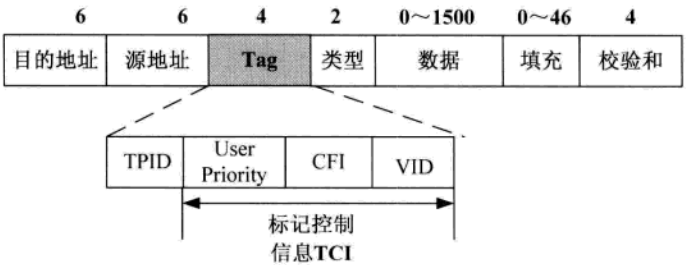



图 20-11　IEEE802.1q 格式

- TPID：值为 0x8100（hex），标记 IEEE 802.1Q 帧，hex 表示十六进制。
- TCI：标签控制信息字段，包括用户优先级（User Priority）、规范格式指示器（Canonical Format Indicator）和 VLAN ID。

- User Priority：定义用户优先级，3位，有8个优先级别。
- CFI：以太网交换机中，规范格式指示器总被设置为0。设置为1时，表示该帧格式并非合法格式，这类帧不被转发。
- VID：

VLAN ID标识VLAN，长度为12位，所以取值范围为[0～$2^{12}$–1]，即[0～4095]。VLAN ID在标准 802.1Q 中会被常常用到。在VID可能的取值范围[0～4095]中，VID=0用于识别帧优先级，4095（转换为十六进制为FFF）作为预留值，所以 **VLAN号的最大可能值为4094，最多可以配置4094个不同VLAN**。

（2）ISL（Inter-Switch Link）：属于思科私有协议，只能在快速和千兆以太网连接中使用。Trunk采用ISL格式时，**VLAN ID的最大值为1023**。

7. VTP配置

VTP2管理标准范围是VLAN 1～VLAN 1005，VTP3可以扩展到VLAN 1006～VLAN 4094。同一个VTP域中不能在多台交换机上手动配置同样的VLAN，也不能在多台交换机上为用一个VLAN配置信息。**VLAN只在一台交换机上手动配置**，否则可能会出现VLAN数据库的同步问题。

（1）配置VTP Server。

| | |
|---|---|
| Switch# **configure terminal** | 进入全局配置模式 |
| Switch(config)# **vtp mode server** | 配置为VTP服务器（默认模式） |
| Switch(config)# **vtp domain** *domain-name* | 配置VTP管理域名 |
| Switch(config)# **vtp password** *password* | 设置VTP域密码 |
| Switch(config)#**end** | 返回特权配置模式 |
| Switch# **show vtp status** | 查看并校验配置 |

（2）配置VTP Client。

| | |
|---|---|
| Switch# **configure terminal** | 进入全局配置模式 |
| Switch(config)# **vtp mode client** | |

配置为VTP客户端，需与VTP服务器域名相同。

| | |
|---|---|
| Switch(config)# **vtp domain** *domain-name* | 配置VTP管理域名 |
| Switch(config)# **vtp password** *password* | 设置VTP域密码 |
| Switch(config)#**end** | 返回特权配置模式 |
| Switch# **show vtp status** | 查看并校验配置 |

（3）配置VTP Transparent。

| | |
|---|---|
| Switch# **configure terminal** | 进入全局配置模式 |
| Switch(config)# **vtp mode transparent** | 配置为VTP透明模式 |

（4）配置VTP pruning。

| | |
|---|---|
| Switch# **configure terminal** | 进入全局配置模式 |
| Switch(config)# **vtp pruning** | 在VTP管理域中启用VTP修剪 |

## 20.4 STP

### 20.4.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：STP 的作用、STP 交换机接口状态、STP 工作原理、STP 配置、Trunk 端口负载均衡、端口汇聚。

### 20.4.2 知识点精讲

生成树协议（Spanning Tree Protocol，STP）是一种链路管理协议，为网络提供路径冗余，同时防止产生环路。交换机之间使用网桥协议数据单元（Bridge Protocol Data Unit，BPDU）来交换 STP 信息。**BPDU** 包含了实现 STP 必要的根网桥 ID、根路径成本、发送网桥 ID、端口 ID 等信息，具有配置 BPDU 和通告拓扑变化的功能。

1. STP 的作用

STP 的作用有以下几点：

（1）逻辑上断开环路，防止广播风暴的产生。

（2）当线路出现故障，断开的接口被激活，恢复通信，起备份线路的作用。

（3）形成一个最佳的树形拓扑。

2. STP 交换机接口状态

启动了 STP 的交换机的接口状态和作用如表 20-3 所示。

表 20-3 接口状态和作用

| 状态 | 用途 |
| --- | --- |
| 阻塞（Blocking） | 接收 BPDU、不转发帧 |
| 侦听（Listening） | 接收 BPDU、不转发帧、接收网管消息 |
| 学习（Learning） | 接收 BPDU、不转发帧、接收网管消息、把终端站点位置信息添加到地址数据库（构建网桥表） |
| 转发（Forwarding） | 发送和接收用户数据、接收 BPDU、接收网管消息、把终端站点位置信息添加到地址数据库 |
| 禁用（Disable） | 端口处于 shutdown 状态，不转发 BPDU 和数据帧 |

其中，**阻塞状态到侦听状态需要 20 秒，侦听状态到学习状态需要 15 秒，学习状态到转发状态需要 15 秒。**

3. STP 工作原理

STP 首先选举根网桥（Root Bridge），然后选择根端口（Root Ports），最后选择指定端口（Designated Ports）。

下面讲述具体的 STP 选择过程。

（1）选择根网桥。

每台交换机都有一个唯一的网桥 ID（BID），**最小 BID 值**的交换机为根交换机。其中 BID，是由 2 字节网桥优先级字段和 6 字节的 MAC 地址字段组成。图 20-12 描述了根网桥的选择过程。

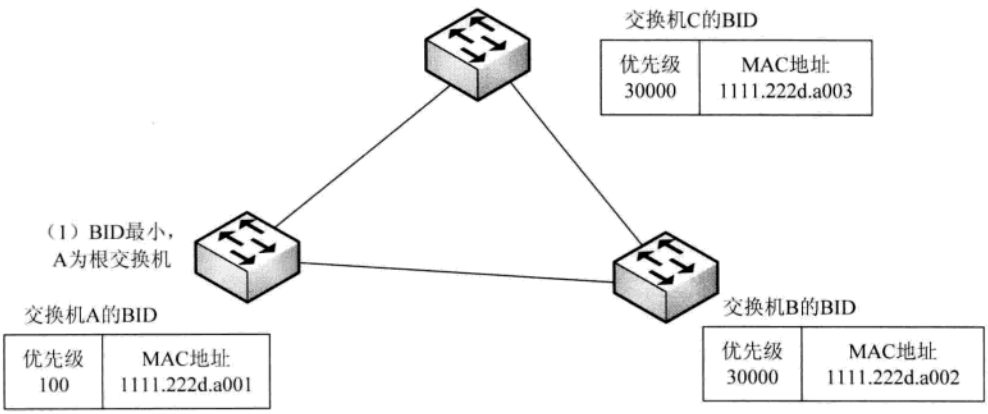



图 20-12　根网桥的选择

（2）选择根端口。

选择根网桥后，其他的非根网桥选择一个距离根桥最近的端口为根端口。

选择根端口的依据如下：

1）交换机中到根桥**总路径成本**最低的端口。**路径成本**根据带宽计算得到，如 10Mb/s 的路径成本为 100，100Mb/s 的路径成本为 19，1000Mb/s 的路径成本为 4。

2）直连的网桥 ID 最小的端口。

3）直连的邻居端口 ID 最小的端口。端口 ID 由端口优先级（8 位）和端口编号（8 位）组成。

如图 20-13 所示描述了根端口的选择过程。

（3）选择指定端口。

每个网段选择一个指定端口，根桥端口均为指定端口。

选定非根桥的指定端口的依据如下：

1）到根路径成本最低。

2）端口所在的网桥的 ID 值较小。

3）端口 ID 值较小。

如图 20-14 所示描述了指定端口的选择过程。

交换机中所有的根端口和指定端口之外的端口称为非指定端口。此时非指定端口被 STP 协议设置为阻塞状态，这时没有环的网络就生成了。

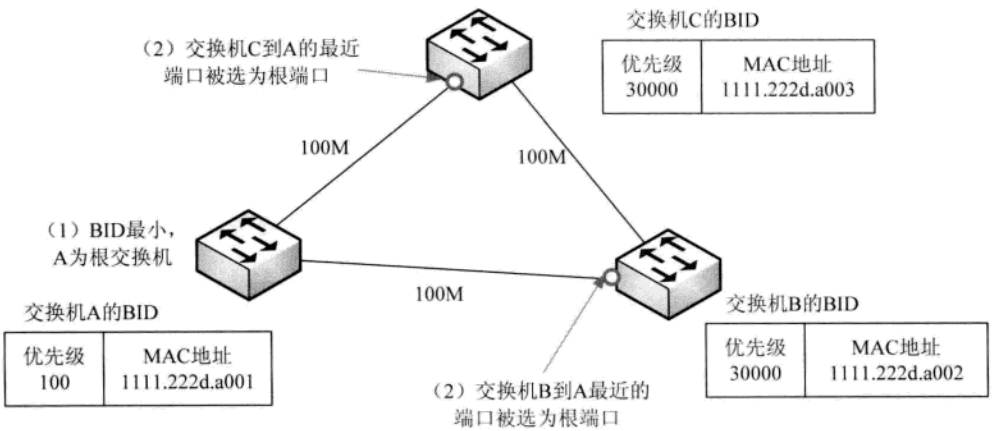



图 20-13　根端口的选择

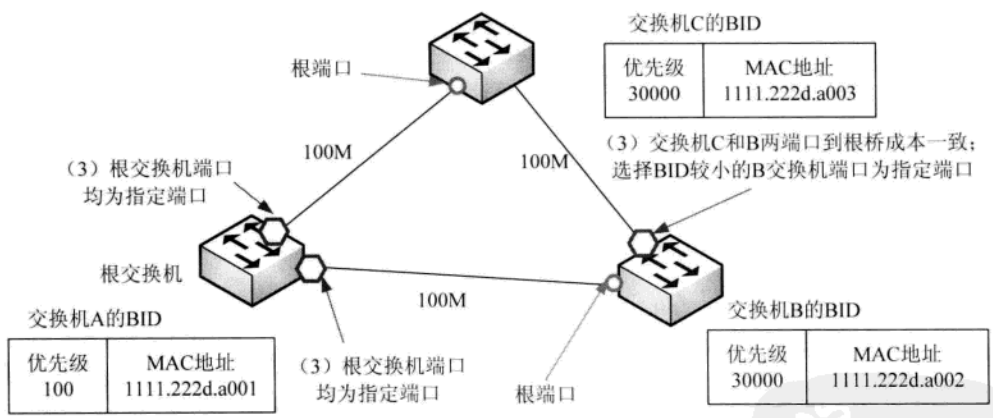



图 20-14　指定端口的选择

4. STP 配置

默认的交换机优先级为 32768，STP 端口的优先级默认为 128。

（1）配置根交换机。

```
Switch# configure terminal                                    进入全局配置模式
Switch(config)# spanning-tree vlan vlan_id root primary [diameter hops]
配置交换机为指定某个 VLAN 的根交换机，hops 表示网络直径（根桥到终端间交换机的数量）
Switch(config-if)# end
```

（2）配置端口优先值。

```
Switch# configure terminal                                    进入全局配置模式
Switch(config)# interface port-id                             选择要配置的接口
Switch(config-if)# spanning-tree port-priority priority       配置优先级，默认值为 128
```

或者

```
Switch(config-if)# no spanning-tree port-priority          重置优先级，恢复默认值 128
Switch(config-if)# spanning-tree vlan vlan-id port-priority port_priority
为网段接口配置 VLAN 端口优先值，默认 128
或者
Switch(config-if)# no spanning-tree vlan vlan-id port-priority
重置 VLAN 端口优先值
Switch(config)# end
```

（3）配置路径成本。

```
Switch# configure terminal                                 进入全局配置模式
Switch(config)# interface port-id                          选择要配置的接口
Switch(config-if)# spanning-tree cost cost                 配置接口连接路径成本
Switch(config-if)# spanning-tree vlan vlan_id cost cost
为 VLAN 接口配置 VLAN 端口连接路径成本
```

（4）配置 PortFast。

配置 PortFast 可以使得端口从阻塞状态直接到转发状态，而无须经过侦听和学习状态，大大减少了延时等待时间。连接了终端的交换机端口可以配置 PortFast。

```
Switch# configure terminal                                 进入全局配置模式
Switch(config)# interface port-id                          选择要配置的接口
Switch(config-if)# spanning-tree portfast                  启用 portfast
```

5. Trunk 端口负载均衡

通过设置 STP 端口优先级或路径成本两种方式实现 Trunk 的负载均衡。

（1）设置 STP 端口优先级实现。如图 20-15 所示描述了该方式。

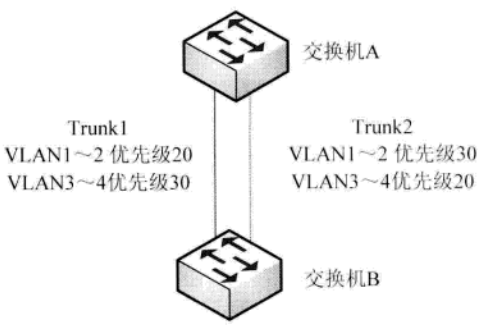



图 20-15　STP 端口优先级实现负载均衡

VLAN1～2 的数据通过 Trunk1，VLAN3～4 的数据通过 Trunk2。

交换机 A 的配置步骤如下：

1）配置两个端口为 Trunk 口。

2）在各自 Trunk 口下，使用 Switch（config-if）# **spanning-tree vlan** *vlan-id* **port-priority**

*port_priority* 命令配置 STP 端口优先级。

3）连接 Trunk1 端口上 VLAN1～2 的优先级设置一定低于 VLAN3～4；连接 Trunk2 端口上 VLAN1～2 的优先级设置一定高于 VLAN3～4。

交换机 B 的配置同交换机 A。

（2）设置 STP 路径成本优先级实现。如图 20-16 所示描述了该方式。

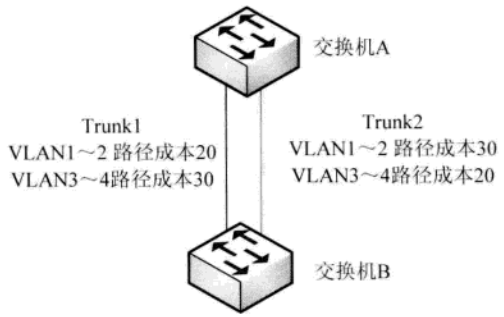



图 20-16 STP 路径成本实现负载均衡

VLAN1～2 的数据通过 Trunk1，VLAN3～4 的数据通过 Trunk2。

交换机 A 的配置步骤如下：

1）配置两个端口为 Trunk 口。

2）在各自 Trunk 口下，使用 Switch（config-if）# **spanning-tree vlan** *vlan_id* **cost** *cost* 命令配置每个 VLAN 的 STP 路径成本。

3）连接 Trunk1 端口上 VLAN1～2 的路径成本设置一定低于 VLAN3～4；连接 Trunk2 端口上 VLAN1～2 的路径成本设置一定高于 VLAN3～4。

交换机 B 的配置同交换机 A。

6. 端口汇聚

STP 只能在设备间保证一条活动链路，而其他链路将处于备用闲置状态，因此，在很大程度上浪费了宝贵的硬件和链路资源。端口汇聚多个物理链路，组成一个逻辑链路，成倍地提高设备间带宽。

## 20.5 HSRP

### 20.5.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：HSRP。

### 20.5.2 知识点精讲

热备份路由协议（Hot Standby Router Protocol，HSRP）可以配置一个交换机群集。HSRP 允许两台或多台交换机使用同一个虚拟的 MAC 地址和 IP 地址，看起来多台交换机就像是一台大交换机，其实这台大交换机并不存在，只是多台互为备份的交换机。

HSRP 配置如下

| | |
|---|---|
| Switch# **configure terminal** | 进入全局配置模式 |
| Switch(config)# **interface** port-id | 选择要配置的接口 |
| Switch (config) # **standby** number **ip** ip_address | 创建 HSRP 组，分配组号和虚拟 IP 地址 |
| Switch (config)# **standby** number **priority** priority<br>设置优先级，默认值为 100。数值越高，优先权越高 | |
| Switch (config)# **standby** number **preempt** | 设置抢占模式，即当路由器比活动路由器有较高的优先权时，它便升为一个活动路由器 |

# 第 3 学时　路由基础

第 4 天的第 3 学时主要学习路由基础知识。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 1～3 分之间。路由基础知识在上、下午考试中均有涉及。本章考点知识结构图如图 21-1 所示。**注意本书中涉及的各类配置命令参数太多，因此在此只讲重要的、常考的参数。**


图 21-1　考点知识结构图

## 21.1　路由器概述

### 21.1.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：路由器基本功能、路由器分类、路由器组成。

### 21.1.2 知识点精讲

路由器（Router）是连接网络中各类局域网和广域网的设备，它会根据信道的情况自动选择和设定路由，以最佳路径按前后顺序发送信号的设备。**路由器工作在 OSI 模型的网络层。路由**就是指通过相互连接的网络把信息从源地点移动到目标地点的活动。

1. 路由器基本功能

路由器功能有：连接各类网络；隔离子网和广播，抑制广播风暴；路由；转发；网络安全；实现网络地址转换，把私有地址转换为共有地址。

2. 路由器分类

（1）从性能上来分，路由器可以分为高性能路由器、中端路由器和低端路由器。

（2）从结构上来分，路由器可以分为模块结构路由器和非模块结构路由器。

（3）从网络位置来分，路由器可以分为核心路由器、分发路由器和接入路由器。

3. 路由器组成

路由器有多种内存，ROM 存储引导软件，Flash 用来存储 IOS，RAM 是主存，NVRAM 保存启动配置。路由器中，当前运行配置（running-config）存储在 RAM 中，设备掉电则配置就消失；备份配置（start-config）存储在 NVRAM 中，掉电则不消失，设备启动时就使用该配置。

Copy 命令可以完成 RAM、NVRAM、TFTP 直接复制文件。Copy 命令格式为：

```
Switch> copy startup-config|running-config    startup-config|running-config
将第一个参数指定的文件复制到第二个参数指定的文件
```

## 21.2 路由器原理

### 21.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：路由器原理、松散源路由、严格源路由。

### 21.2.2 知识点精讲

1. 路由器原理

路由器的主要功能是进行路由处理和包转发。

（1）路由处理。

通过运行路由协议来学习网络的拓扑结构，通过一定的规则建立和维系路由表，保持信息有效。通过特定算法依据路由表决定最佳路径。

（2）包转发。

1）接收数据包，检查、解释和处理 IP 版本号、头长度、头校验等数据包报头，对数据报文的长度和完整性进行验证。

2）依据目的 IP 地址检查下一跳（Next Hop）IP 地址。修改 TTL 值，重新计算校验和。

3）新数据附加新数据链路层报头并转发。

2. 松散源路由（Loose Source Route）

松散源路由只给出IP数据报**必须经过源站指定的路由器**，并不给出一条完备的路径，没有直连的路由器之间的路由需要有寻址功能的软件支撑。

3. 严格源路由（Strict Source Route）

严格源路由选项IP数据报要经过路径上的每一个路由器，相邻路由器之间不得有中间路由器，并且所经过路由器的顺序不可更改。

## 21.3 端口种类

### 21.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：路由器端口种类。

### 21.3.2 知识点精讲

常见的路由器端口有以下几种：

（1）RJ45端口。

RJ45端口指的是由IEC（60）603-7标准化使用由国际性的接插件标准定义的8个位置（8针）的模块化插孔或插头。RJ这个名称代表已注册的插孔（Registered Jack）。如图21-2所示给出了RJ45端口的外形。

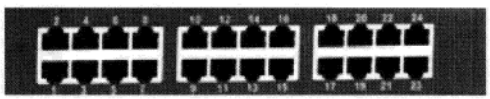


图21-2 RJ45端口

（2）高速同步串口（Serial Peripheral Interface）。

在路由器的广域网连接中，高速同步串口（Serial Peripheral Interface，SPI）应用较多。这种端口主要是用于连接DDN、帧中继（Frame Relay）、X.25、PSTN（模拟电话线路）等网络。如图21-3所示给出了高速同步串口的外形。这种同步端口一般要求速率非常高，因为一般通过这种端口所连接的网络的两端都要求实时同步。

（3）ISDN BRI。

ISDN BRI端口通过ISDN线路实现路由器与Internet或其他网络的远程连接。ISDN BRI端口采用RJ-45标准，与ISDN NT1的连接使用RJ-45 to RJ-45直通线。如图21-4所示给出了ISDN BRI的外形。

（4）异步串口（ASYNC）。

异步串口适合Modem间的连接，实现PSTN的拨号接入。该端口速率不高，工作在异步传输

模式下。如图 21-5 所示给出了异步串口的外形。

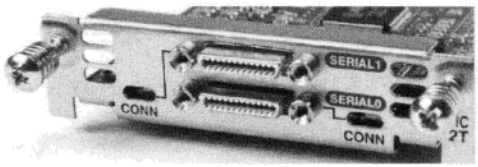



图 21-3　高速同步串口


图 21-4　ISDN BRI 口

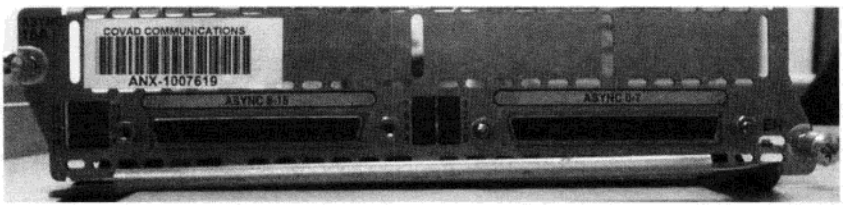



图 21-5　异步串口

（5）Console 口。

Console 线连接 PC 机的串口和设备 Console 口，可以通过超级终端配置设备。如图 21-6 所示给出了 Console 口的外形。

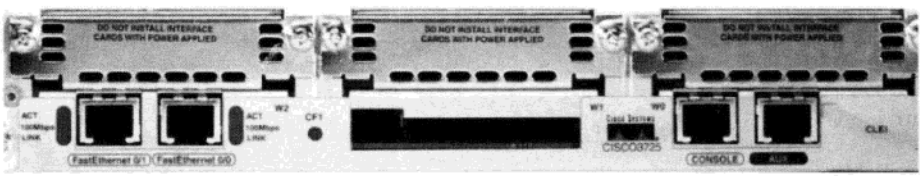



图 21-6　Console 口与 AUX 口

（6）AUX 端口。

AUX 端口在外观上与 RJ-45 端口一样，只是内部电路不同，实现的功能也不一样。通过 AUX 端口与 Modem 进行连接时必须借助 RJ-45 to DB9 或 RJ-45 to DB25 适配器进行转换。

（7）E1/T1 端口。

E1/T1 用于连接运行商网络。如图 21-7 所示给出了 E1/T1 口的外形。

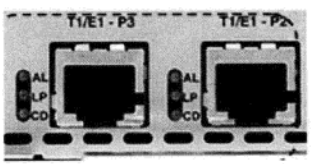



图 21-7　E1/T1 口

（8）光纤接口。

用于连接光纤，提供千兆速率。如图 21-8 所示给出了 SC 光纤接口和光纤的外形。

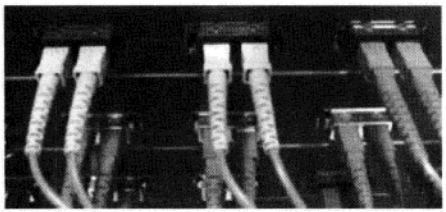


图 21-8　SC 光纤接口

# 第 4 学时　案例重点 2——路由配置

第 4 天的第 4 学时主要学习路由配置知识。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 5～20 分之间。路由配置知识在上、下午考试中均是重点，基本上每次考试常有一道 15 分左右的案例题。本章考点知识结构图如图 22-1 所示。

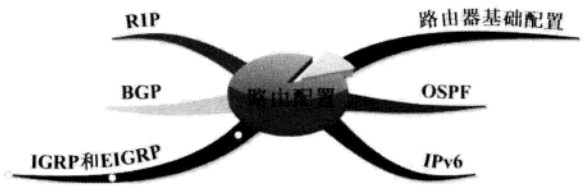



图 22-1　考点知识结构图

## 22.1　路由器基础配置



### 22.1.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：路由器连接、CLI 命令模式、路由表、路由器基本配置。

### 22.1.2　知识点精讲

1. 路由器连接

和连接交换机一样，连接路由器也有多种方式。

（1）基于 Console 口的命令行接口（Command Line Interface，CLI）配置方式。

（2）通过 Web 界面配置。

（3）通过 Cisco Works、CAN、SDM 等软件配置。

第一次初始配置必须使用基于 Console 口的 CLI 配置方式。使用 Console 配置方式时需要使用超级终端，超级终端连接路由器，需要配置如图 22-2 所示的参数。

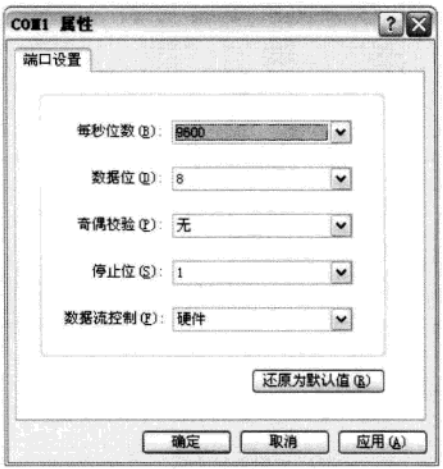



图 22-2 超级终端配置参数

- 每秒位数：9600 波特。
- 数据位：8 位。
- 奇偶校验：无。
- 停止位：1 位。
- 数据流控制：无。

2. CLI 命令模式

和交换机配置类似，路由器的 IOS 主要有以下六种不同命令模式：

- User EXEC Mode（用户模式）
- Privileged EXEC Mode（特权模式）
- Global Configuration Mode（全局配置模式）
- Router Configuratio Mode（路由器配置模式）
- Interface Configuration Mode（接口配置模式）
- Line Configuration Mode（Line 接口配置模式）

如表 22-1 所示表示了多个模式切换方法。

另外，在路由器的特权模式下键入命令 setup，则路由器进入**设置对话状态**模式。

3. 路由表

路由表（Routing Table）供路由选择时使用，路由表为路由器进行数据转发提供信息和依据。路由表可以分为静态路由表和动态路由表。

表 22-1 CLI 转换方式

| 模式 | 访问方法 | 提示符 | 退出方法 |
| --- | --- | --- | --- |
| 用户模式 | 登录路由器之后 | router> | logout 或 quit |
| 特权模式 | 在**用户模式** router>下，输入 **enable**（简写 en）命令 | router# | disable |
| 全局配置模式 | **在特权模式** router#下，输入 **config**（简写 con）命令 | router（config）# | exit 或者 Ctrl+Z |
| 接口配置模式 | **在全局模式** router（config）#下，输入带有指定接口的 **interface** 命令 | router（config-if）# | （1）exit 退回到 router（config）#；<br>（2）Ctrl+Z 或者 end 退回到 router# |
| 路由器配置模式 | **在全局模式** router（config）#下，输入 rip、ospf 等 | router（config-router）# | （1）exit 退回到 router（config）#；<br>（2）Ctrl+Z 或者 end 退回到 router# |
| Line 接口配置模式 | **在特权模式** router#下，输入 **link console 0** 命令 | router（config-line）# | （1）exit 退回到 router（config）#；<br>（2）Ctrl+Z 或者 end 退回到 router# |

（1）静态路由表。

由系统管理员事先设置好固定的路由表称为静态（Static）路由表，一般是在系统安装时就根据网络的配置情况预先设定的，不会随网络结构的改变而改变。

（2）动态路由表。

动态（Dynamic）路由表是路由器根据网络系统的运行情况自动调整的路由表。路由器根据路由选择协议（Routing Protocol）提供的功能自动学习和记忆网络运行情况，在需要时自动计算数据传输的最佳路径。

使用 show ip route 命令可以查看路由表信息。如表 22-2 所示给出了一个虚构的路由表，用于说明路由表结构。

```
Router# show ip route
Codes:I - IGRP derived,R - RIP derived,H – Hello derived,O - OSPF derived
      C - connected,S - static,E - EGP derived,B - BGP derived
      * - candidate default route,IA - OSPF inter area route
      E1 - OSPF external type 1 route,E2 - OSPF external type 2 route
```

```
Gateway   of last resort is 131.119.254.240 to network 129.140.0.0
192.168.0.0/24 is subnetted,6 subnets
C       192.168.1.0 is directly connected,Ethernet0
C       192.168.65.0 is directly connected,Serial0
C       192.168.67.0 is directly connected,Seriall
R       192.168.69.0 [120/1]        via   192.168.67.2,00:00:15,Seriall
                     [120/1]        via   192.168.65.2,00:00:24,Serial0
R       192.168.5.0[120/1]          via   192.168.07.2,00:00:15,Seriall
R       192.168.3.0[120/1]          via   192.168.65.2,00:00:24,Serial0
0  E2   117.150.150.0 [160/5]      via   121.119.254.6 ,0:01:00 ,Ethernet2
0  E2   130.130.0.0 [160/5]        via   121.119.254.6 ,0:00:59,Ethernet2
E       128.128.0.0 [200/128]       via   121.119.254.224 ,0:02:22,Ethernet2
E       129.129.0.0 [200/128]       via   121.119.254.220 ,0:02:22,Ethernet2
```

- 路由表第 1 列：指出路由是通过哪种**协议**得到的。C 为直连，R 为 RIP 协议，O 为 OSPF 协议，S 为静态路由。
- 路由表第 2 列：指出协议的特有信息。如 E1 表示 OSPF 外部是 1 型路由，E2 表示 OSPF 外部是 2 型路由。

注意：OE1 和 OE2 的区别是，OE2 开销=外部开销，OE1 开销=外部开销+内部开销。

- 路由表第 3 列：目的网段。
- 路由表第 4 列：格式为**目的网段地址 [管理距离]/度量值**，例如[120/1] 表示 RIP 协议的管理距离为 120，1 是路由的度量值，即跳数。管理距离表示路由协议的优先级，其中 RIP 默认值为 120、OSPF 默认值为 110、IGRP 默认值为 100、EIGRP 默认值为 90、静态路由默认值为 1、直连路由默认值为 0。由此可见，直连路由的优先级最高，静态路由次之。
- 路由表第 5 列（紧接关键词 via 之后）：达到目的网段的下一跳 IP 地址。
- 路由表第 6 列：表示路由产生的时间，格式为**小时:分钟:秒**。
- 路由表第 7 列：该路由接口是该路由信息的物理出口。Serial 为串口，Ethernet 为以太口。

4. 路由器基本配置

（1）配置路由器名称。

```
Router(config)# hostname R1                    设置路由器名为 R1
R1(config)#                                    修改后的配置模式提示符
```

（2）配置以太网口。

配置接口命令形式为 **ip address** *ip_addr subnet_mask*。

```
Router>                                        用户模式
Router> enable
Router #                                       特权模式
Router # config terminal                       准备进入全局配置模式
Router(config)# interface fastethernet0/1      对指定接口进行配置
Router(config-if)# ip address ip_address   subnet_mask
配置 IP 地址和子网掩码
Router(config-if)# no shutdown                 启动接口
```

*10：19：11：%LINK-3-UPDOWN：Interface FastEthernet 0/1 changed state to up*
Router(config-if)# **exit** 返回全局配置模式

（3）配置串口。

Router> 用户模式
Router> **enable**
Router # 特权模式
Router # **config terminal** 准备进入全局配置模式
Router(config) # **interface serial** *interface-id* 对指定串口进行配置
Router(config-if)#**async default ip address** *ip_address subnet_mask*
配置串口 IP 地址和掩码
Router(config-if)#**encapsulation** *{ppp|frame-relay|hdlc|lapb|x.25}*
封装链路协议，可以是 ppp、frame-relay、hdlc、lapb、x.25
Router(config-if)# exit 返回全局配置模式

（4）静态路由配置。

Router> 用户模式
Router> **enable**
Router # 特权模式
Router # **ip routing** 启动路由协议
Router # **config terminal** 进入全局模式
Router(config)# **ip route** *ip-address subnet-mask gateway*
指定到达目的网络的地址、子网掩码、下一条（网关）地址或路由器接口

（5）Show 命令。

Router> **show ip protocol** 显示路由器配置的路由协议
Router> **show ip route** 命令显示路由信息
Router> **show version** 查看版本及引导信息
Router> **show running-config** 查看运行设置
Router> **show startup-config** 查看开机设置
Router> **show interface** *type port/number* 检查端口配置参数和统计数据
Router>**show history** 功能和上下箭头键，查看历史输入的命令

## 22.2 RIP



### 22.2.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：RIP 基本概念、路由收敛、RIP 配置。

### 22.2.2 知识点精讲

路由信息协议（Routing Information Protocol，RIP）是使用最广泛的**距离矢量路由**协议。距离矢量名称的由来是因为路由是以矢量（距离、方向）的方式被通告出去的，这里的距离是根据度量来决定的。距离矢量路由算法是动态路由算法。它的工作流程是：每个路由器维护一张矢量表，表中列出了当前已知的到每个目标的最佳距离以及所使用的线路。通过在邻居之间相互交换信息，路

由器不断更新它们内部的表。

1. RIP 基本概念

**RIP 协议基于 UDP，端口号为 520。RIPv1 报文基于广播，RIPv2 基于组播（组播地址 224.0.0.9）。**RIP 路由的更新周期为 **30 秒**，如果路由器 **180 秒**没有回应，则标志路由不可达，如果 **240 秒**内没有回应，则删除路由表信息。RIP 协议的最大跳数为 15 条，16 条表示不可达，直连网络跳数为 0，每经过一个节点跳数增 1。

RIP 分为 RIPv1、RIPv2 和 RIPng 三个版本，其中 RIPv2 相对 RIPvl 的改进点有：**使用组播**而不是广播来传播路由更新报文；RIPv2 属于**无类协议**，支持可变长子网掩码（VLSM）和无类别域间路由（CIDR）；采用了**触发更新机制来加速路由收敛**；**支持认证**，使用经过散列的口令字来限制更新信息的传播。RIPng 协议支持 IPv6。

2. 路由收敛

好的路由协议必须能够快速收敛，收敛就是网络设备的路由表与网络拓扑结构保持一致，所有路由器再判断最佳路由达到一致的过程。

距离矢量协议容易形成路由循环、传递好消息快、传递坏消息慢等问题。解决这些问题可以采取以下几个措施：

（1）水平分割（Split Horizon）。

路由器某一个接口学习到的路由信息，不再反方向传回。

（2）路由中毒（Router Poisoning）。

路由中毒又称为反向抑制的水平分割，不马上将不可达网络从路由表中删除该路由信息，而是将路由信息度量值置为无穷大（RIP 中设置跳数为 16），该中毒路由被发给邻居路由器以通知这条路径失效。

（3）反向中毒（Poison Reverse）。

路由器从一个接口学习到一个度量值为无穷大的路由信息，则应该向同一个接口返回一条路由不可达的信息。

（4）抑制定时器（Holddown Timer）。

一条路由信息失效后，一段时间内都不接收其目的地址的路由更新。路由器可以避免收到同一路由信息失效和有效的矛盾信息。通过抑制定时器可以有效避免链路频繁起停，增加了网络有效性。

（5）触发更新（Trigger Update）。

路由更新信息每 30 秒发送一次，当路由表发生变化时，则应立即更新报文并广播到邻居路由器。

3. RIP 配置

RIP 协议配置如下：

```
Router # config terminal                    进入全局模式
Router(config)# ip routing                  启动路由协议
Router(config)# router rip                  启动 RIP 协议进程
Router(config)# network network
配置该 RIP 路由器邻接的网络（多个邻接网络要配置多次）
Router(config)# version {1|2}               配置 RIP 协议版本
```

Router(config)# **no auto summary**
禁止路由自动汇总（可选）。路由汇总指的是将通往某个网络的多个子网的路由汇总成一条 A 类、B 类或 C 类路由。可以大大缩小路由表规模。路由汇总分为自动和手动。当 RIP 路由器接的子网不连续时，使用路由自动汇总往往会出错
Router(config-router)# **end** 返回特权模式

## 22.3 OSPF

### 22.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：基本概念、OSPF 的 5 类报文、OSPF 工作流程、BR 与 BDR 选举、OSPF 网络类型、OSPF 配置。

### 22.3.2 知识点精讲

开放式最短路径优先（Open Shortest Path First，OSPF）是一个**内部网关协议**（Interior Gateway Protocol，IGP），用于在**单一自治系统**（Autonomous System，AS）内决策路由。OSPF 适合小型、中型、较大规模网络。OSPF 采用 Dijkstra 的**最短路径优先算法**（Shortest Path Firs，SPF）计算最小生成树，确定最短路径。OSPF 基于 IP，协议号为 89，采用组播方式交换 OSPF 包。OSPF 的组播地址为 224.0.0.5（全部 OSPF 路由器）和 224.0.0.6（指定路由器）。OSPF 使用链路状态广播（Link State Advertisement，LSA）传送给某区域内的所有路由器。

1. 基本概念

（1）AS。

自治系统（AS）是指使用同一个内部路由协议的一组网络。Internet 可以被分割成许多不同的自治系统。换句话说，Internet 是由若干自治系统汇集而成的。每个 AS 由一个长度为 16 位的编码标识，由 Internet 地址授权机构（Internet Assigned Numbers Authority，IANA）负责管理分配。AS 编号分为公用 AS（编号范围 1～64511）和私有 AS（编号范围 64512～65535），公有 AS 编号需要向 IANA 申请。

（2）IGP。

内部网关协议（Interior Gateway Protocol，IGP）在同一个自治系统内交换路由信息。IGP 的主要目的是发现和计算自治域内的路由信息。**IGP 使用的路由协议有 RIP、OSPF、IS-IS、EIGRP、IGRP。**

（3）EGP。

外部网关协议（Exterior Gateway Protocol，EGP）是一种连接不同自治系统的相邻路由器之间交换路由信息的协议。**EGP 使用的路由协议有 BGP。**三者关系如图 22-3 所示。

（4）链路状态路由协议。

运行距离矢量路由协议的路由器会将所有它知道的**路由信息与邻居共享**，当然只是与直连邻

居共享。运行链路状态路由协议的路由器只将它所**直连的链路状态与邻居共享**。如表 22-2 所示给出了链路状态路由协议和距离矢量路由协议。

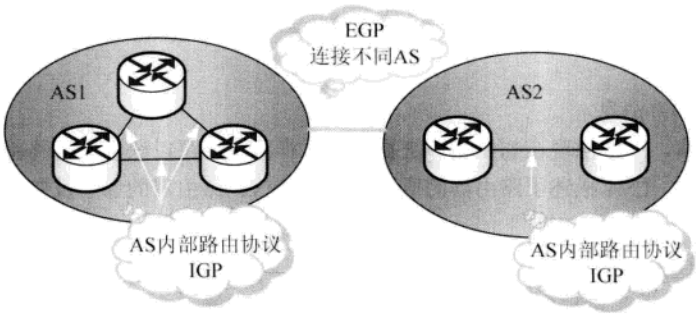



图 22-3 IGP、EGP、AS 三者关系

表 22-2 链路状态路由协议和距离矢量路由协议对比

| | 距离矢量路由协议 | 链路状态路由协议 |
|---|---|---|
| 发布路由触发条件 | 周期性发布路由信息 | 网络扑拓变化发布路由信息 |
| 发布路由信息的路由器 | 所有路由器 | 指定路由器（Designated Router，DR） |
| 发布方式 | 广播 | 组播 |
| 应答方式 | 不要求应答 | 要求应答 |
| 支持协议 | RIP、IGRP、BGP（增强型距离矢量路由协议） | OSPF、IS-IS |

**注意**：RIPv2 既支持广播，也支持组播；每一个接口都可以配置为使用不同的路由协议，但它们必须能够通过重分布路由来交换路由信息。

（5）区域（Area）。

OSPF 是分层路由协议，每个 AS 中，网络被分为不同的区域，每个区域拥有特定的标识符。OSPF 的区域中必须包含 Area 0，其他区域必须连接 Area 0。不能连接 Area 0 的区域需要通过虚链路，通过中间区域连接。

2. OSPF 的 5 类报文

OSPF 使用 IP 包头封装了 5 类报文，用来交换链路状态广播（Link State Advertisement，LSA）。

**注意**：LSA 本身不是 OSPF 的消息，它是一类数据结构，存放在路由器的链路状态库（Link-State DataBase，LSDB）中，并可包含在 LSU 消息中进行交换。LSA 包括有关邻居和通道成本的信息。接收路由器用 LSA 维护其路由选择表。

（1）Hello。

Hello 用于**发现邻居**，保证邻居之间 keeplive，能在 NBMA 上**选举指定路由器**（DR）、备份指定路由器（BDR）。**默认的 Hello 报文的发送间隔时间是 10 秒，默认的无效时间间隔是 Hello 时间**

**间隔的4倍**，即如果在**40秒**内没有从特定的邻居接收到这种分组，路由器就认为那个邻居不存在了。Hello包应该包含：源路由器的RID、源路由器的Area ID、源路由器接口的掩码、源路由器接口的认证类型和认证信息、源路由器接口的Hello包发送的时间间隔、源路由器接口的无效时间间隔、优先级、DR/BDR接口IP地址、五个标记位、源路由器的所有邻居的RID。**Hello组播地址为224.0.0.5。**

（2）数据库描述（DD或DBD）消息。

用来交换每个LSA的摘要版本，一般出现在初始拓扑交换中，这样路由器可以获悉邻接路由器的LSA列表并用于选择主从关系。LSA描述了路由器的所有链路、接口、路由器的邻居及链路状态信息。

（3）链路状态请求（LSR）消息。

请求一个或多个LSA，通告邻接路由器提供LSA的详细信息给发送路由器。

（4）链路状态更新（LSU）消息。

包含LSA的详细信息，一般用来响应LSR消息。

（5）链路状态应答（LSAck）消息。

用来确认已收到LSU消息。

上述消息可以支持路由器发现邻接路由器（Hello），学习其本身链路状态库（LSDB）中没有的LSA（DD），请求并可靠交换LSA（LSR/LSU），监测邻接路由器是否发生拓扑改变。**LSA每30分钟重传1次。**

3. OSPF工作流程

（1）启动OSPF进程的接口，发送Hello消息。

（2）交换Hello消息建立邻居关系。

（3）每台路由器对所有邻居发送LSA。

（4）路由器接收邻居发过来的LSA并保存在LSDB中，发送一个LSAcopy给其他邻居。

（5）LSA泛洪扩散到整个区域，区域内所有路由器都会形成相同的LSDB。

（6）当所有路由器的LSDB完全相同时，每台路由器将以自身为根，使用最短路径算法算出到达每个目的地的最短路径。

（7）每台路由器通过最短路径构建出自己的路由表，包含区域内路由（最优）、区域间路由、E1外部路由和E2外部路由。

4. BR与BDR选举

在DR和BDR出现之前，每一台路由器和其所有邻居成为全连接的OSPF邻接关系，关系数为**n×(n-1)**。在多址网络中，路由器发出的LSA从邻居的邻居发回来，导致网络上产生很多LSA的复制，所以基于这种考虑产生了DR和BDR。网段中的所有路由器都从DR和BDR交换信息，而不是彼此交换信息。DR和BDR将信息转交给其他所有路由器，用DR和BDR方式的连接数为**2×(n-1)**。

OSPF选举Router-id的规则：

（1）手动配置的 Router-id 为首选。

（2）用所有 loopback 中最大的 IP 作为 Router-id。

（3）用所有活动物理接口中最大的 IP 作为 Router-id（用作 Router-id 的接口不一定非要运行 OSPF 协议）。

DR/BDR 的选举过程如下：

（1）选举路由器必须进入双向会话（Two-way）状态，优先级别必须大于 0（优先级为 0，则不参与选举）。

（2）选举优先级最高的路由器为 DR，次优的为 BDR。

（3）如果优先级相同，则选举 Router-id 最大的路由器。

（4）如果 DR/BDR 已经存在，而又有新的 OSPF 路由器加入，即使该路由器优先级最高，也不剥夺现有 DR/BDR 的角色。

（5）如果 DR 失效，则 BDR 接管 DR，并重新激活一个新 BDR 选举进程。

**注意**：DR 的数据包通过 224.0.0.5 发往所有路由器，DR、BDR 监听使用地址 224.0.0.6；DROther 监听使用地址 224.0.0.5。网络上允许有 DR 却不存在 BDR 的情况。

DR/BDR 的作用是减少网络通信量、负责为整个网络生成 LSA、减少链路状态数据库的大小。

5. OSPF 网络类型

OSPF 网络类型分为点到点网络（Point-to-Point）、广播型网络（Broadcast）、非广播型（NBMA，Non Broadcast Multiaccess）网络、点到多点网络（Point-to-Multicast）、虚链接（Virtual Link）。各类网络特点对比如表 22-3 所示。

表 22-3 OSPF 网络类型

| OSPF 网络类型 | 特点 | 数据传输方式 |
| --- | --- | --- |
| 点到点网络（Point-to-Point） | 有效邻居总是可以形成邻居关系 | 组播地址为 224.0.0.5，该地址称为 AllSPFRouters |
| 点到多点网络（Point-to-Multicast） | 不选举 DR/BDR，可看作是多个 Point-to-Point 链路的集合 | 单播（Unicast） |
| 广播型网络（Broadcast） | 选举 DR/BDR，所有路由器和 BR/BDR 交换信息。DR/BDR 不能被抢占。广播型网络有：以太网、Token Ring 和 FDDI | DR、BDR 组播到 224.0.0.5；DR/BDR 侦听 224.0.0.6，该地址称为 AllDRouters |
| 非广播型（NBMA） | 没有广播，需手动指定邻居，Hello 消息单播。NBMA 网络有 X.25、Frame Relay 和 ATM | 单播 |
| 虚链接（Virtual Link） | 虚链路一旦建立，就不再发送 Hello 消息。应用：通过一个非 Area 0 连接到 Area 0；一个非 Area 0 连接 Area 0 的两个分段骨干区域 | 单播 |

6. OSPF 配置

（1）基本配置。

```
Router # config terminal                    进入全局模式
Router(config)# ip routing                  启动路由协议
```

Router(config)# **router ospf** *process-id*
启动 OSPF 协议进程，*process-id* 是进程号，一台路由器可以开启多个 OSPF 进程，但最好不要这样做
Router(config-router)# **network** *address wildcard-mask* **area** *area-id*
配置接口网络、反掩码、接口 ID
Router(config-router) # **end** 返回特权模式

**注意**：OSPF 配置掩码时，应该使用反掩码（wildcard-mask），反掩码是掩码按位取反的结果。例如：255.255.255.0 的反掩码为 0.0.0.255。

（2）配置 OSPF 区域。

Router # **config terminal** 进入全局模式
Router(config)# **ip routing** 启动路由协议
Router(config) # **router ospf** *process-id*
启动 OSPF 协议进程，process-id 是进程号，一台路由器可以开启多个 OSPF 进程，但最好不要这样做
Router(config-router)# **network** *address wildcard-mask* **area** *area-id*
配置接口网络、反掩码、接口 ID
Router (config) # **area** *area-id* **stub [no-summary]**
（可选）配置末梢区域（完全末梢区域）
Router (config) # **summary-address** *address mask*
（可选）配置外部汇总路由。当外部路由重分布到 OSPF 中时，可以缩减汇总之后通告给 OSPF 路由器
Router (config) # **area** *area-id* **vitual-link** *router-id*
（可选）创建虚拟连接
Router (config-router) # **end** 返回特权模式

（3）配置环回接口。

Router # **config terminal** 进入全局模式
Router(config) # **ip routing** 启动路由协议
Router(config) # **router ospf** *process-id*
Router(config) # **interface loopback** *num*
创建 Loopback 接口
Router(config-if) # **ip address** *address mask*
指定 loopback 接口 IP 地址
Router(config-router) # **end** 返回特权模式

## 22.4 BGP

### 22.4.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：对等体、BGP 消息、BGP 基本配置。

### 22.4.2 知识点精讲

BGP 是边界网关协议，目前版本为 BGP4，是一种增强的距离矢量路由协议。该协议运行在不同 AS 的路由器之间，用于选择 AS 之间花费最小的协议。BGP 协议基于 TCP 协议，端口为 179。

使用面向连接的 TCP 可以进行身份认证，可靠地交换路由信息。BGP4+支持 IPv6。

BGP 特点：

（1）不用周期性发送路由信息。

（2）路由变化，发送增量路由（变化了的路由信息）。

（3）周期性发送 Keepalive 报文效验 TCP 的连通性。

1. 对等体（Peer）

在 BGP 中，两个路由器之间的相邻连接称为对等体连接，两个路由器互为对等体。如果路由器对等体在同一个 AS 中，就称为 IBGP 对等体；否则称为 EBGP 对等体。BGP4 网关向对等实体发布可以到达的 AS 列表。

2. BGP 消息

BGP 常见四种报文：OPEN 报文、KEEPLIVE 报文、UPDATE 报文和 NOTIFICATION 报文。

（1）OPEN 报文：建立邻居关系。

（2）KEEPLIVE 报文：保持活动状态，周期性确认邻居关系，对 OPEN 报文回应。

（3）UPDATE 报文：发送新的路由信息。

（4）NOTIFICATION 报文：报告检测到的错误。

发送过程如图 22-4 所示。

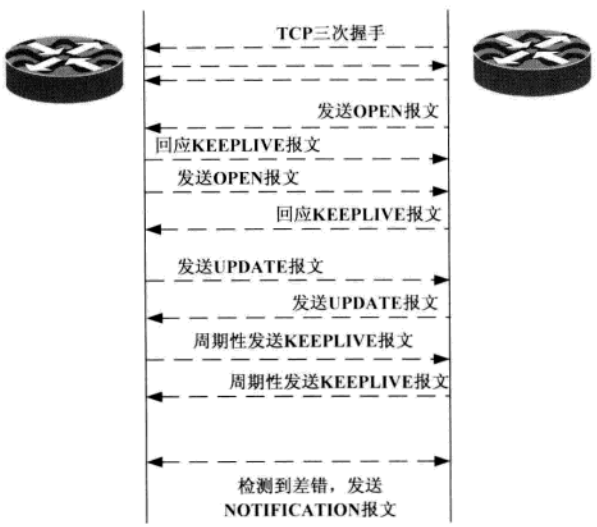



图 22-4 BGP 报文工作流程

BGP 工作流程：

（1）BGP 路由器直接进行 TCP 三次握手，建立 TCP 会话连接。

（2）交换 OPEN 信息，确定版本等参数，建立邻居关系。

（3）路由器交换所有 BGP 路由，直到平衡，之后只交换变化了的路由信息。

（4）路由更新由 UPDATE 完成。

（5）通过 KEEPALIVE 验证路由器是否可用。

（6）出现问题，发送 NOTIFICATION 消息通知错误。

3. BG 基本 P 配置

BGP 基本配置如下：

```
Router # config terminal                          进入全局配置模式
Router(config) # ip routing                       启动路由协议
Router (config) # router bgp autonomous-system-number
启动 BGP 协议进程，autonomous-system-number 用来指定自治区号
Router (config-router) # network network-address mask network-mask
配置接口网络、掩码
Router (config-router) # end                      返回特权模式
```

## 22.5 IGRP 和 EIGRP

### 22.5.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：IGRP、EIGRP。

### 22.5.2 知识点精讲

1. IGRP

IGRP 是 Cisco 公司开发的路由协议，它们采用的路由度量（metric）方法是由带宽、延时、负载、可靠性和最大传输单元通过加权计算而来的，可以简化为跳步数。IGRP 是**距离矢量路由协议**，其发布路由更新信息的周期是 **90 秒**。

2. EIGRP

EIGRP 是 Cisco 公司开发的路由协议，是最典型的**平衡混合路由选择协议**，它融合了距离矢量和链路状态两种路由选择协议的优点，快速达到网络收敛。采用不定期更新，即只在路由器改变计量标准或拓扑出现变化时发送部分更新路由。和 IGRP 一样，EIGRP 采用的路由度量包括带宽、延迟、可靠性、负载等因素。

## 22.6 IPv6

### 22.6.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：IPv6 基本配置、VLAN 配置、

IPv6-over-IPv4 GRE 隧道、ISATAP 隧道。

### 22.6.2 知识点精讲

1. IPv6 基本配置

Router (config) # **IPv6 unicast-routing**　　开启 IPv6 单播路由
Router (config)#**Interface** *port_num*　　进入接口配置
Router (config-if)#**IPv6 address** *IPv6-prefix/prefix-length*
配置端口 IPv6 地址，如 2002:2fcc::1/64
Router (config-if)#**IPv6 route** *IPv6-prefix/prefix-length* *IPv6_gateway*
配置端口静态路由，如 **IPv6 route** 2002：2fcc：：1/64　2002：2fcc：：f1c1

2. VLAN 配置

Router (config)#**Interface** *VLAN_num*　　进入 VLAN 接口配置
Router (config-if)#**IPv6 enable**
启动 IPv6。如果没有执行这条命令，给接口配置 IPv6 地址时会自动打开 IPv6 协议
Router (config-if)#**IPv6 address** *IPv6-prefix/prefix-length*
配置 VLAN 的 IPv6 地址
Ruijie(config-if)# **show IPv6 Interface** *vlan_num*

3. IPv6-over-IPv4 GRE 隧道

通用路由封装协议定义了，在任意一种网络层协议上封装另一个协议(或同一种协议)的协议。如把 IPv6 的数据包进行封装并在 IPv4 网络上传输。

（1）GRE。

通用路由封装协议（Generic Routing Encapsulation，GRE）是第三层隧道协议，即在协议层之间采用了一种被称为隧道（Tunnel）的技术。

隧道是一个虚拟的点对点的连接，这个接口提供了一条通路，使封装的数据报能够在这个通路上传输，并且在一个隧道的两端分别对数据报进行封装和解封。

GRE 通常和 IPSec 联合使用。IPSec 是一种点对点的隧道协议，无法支持对多播报文的封装，而 GRE 可以，所以我们通常用 GRE over IPSec，即先用 GRE 封装多播报文，再用 IPSec 封装 GRE 报文来进行多播数据的加密传输。

（2）IPv6-over-IPv4 隧道（6to4 隧道）。

IPv6-over-IPv4 隧道是将 IPv6 报文封装在 IPv4 报文中发送，封装后，报文穿越 IPv4 网络，目的 IPv6 路由器将封装数据包解封装。

（3）IPv6-over-IPv4 相关配置命令。

Router(config)# **Interface tunnel** *tunnel_number*　　创建虚拟隧道接口
Router(config-if)# **ip address** *ip_address mask*　　配置隧道接口 IPv4 地址
或者
Router(config-if)# **ipv6 address** *ipv6_address mask*　　配置隧道接口 IPv6 地址
Router(config-if)#**tunnel source** *Port_num*　　配置隧道源接口
Router(config-if)#**tunnel source** *source_ip*　　定义隧道源地址
Router(config-if)# **tunnel destination** *destination_ip*　　定义隧道目标地址
Router(config-if)# **tunnel mode** *gre ipv6*

隧道模式为6to4的GRE隧道

4. ISATAP隧道

站内自动隧道寻址协议（Intra-Site Automatic Tunnel Addressing Protocol，ISATAP）是一种站点内部的IPv6网络将IPv4网络视为一个非广播型多路访问（NBMA）链路层的IPv6隧道技术，即将IPv4网络当作IPv6的虚拟链路层。

双栈主机使用ISATAP隧道时，IPv6报文的目的地址和隧道接口的IPv6地址都要采用特殊的ISATAP地址。在ISATAP地址中，**前64位是向ISATAP路由器发送请求得到的**；后64位中由两部分构成，其中前32位是**0:5efe**，后32位是**IPv4单播地址**，即ISATAP接口ID必须为**::0:5ffe:IPv4地址**的形式。具备该地址形式的双栈主机可以和同一子网内的其他ISATAP主机进行IPv6通信。如果要跨网段，ISATAP路由器还需要使用全球单播地址（2xxx::/4或3xxx::/4）。

ISATAP隧道技术不要求隧道节点拥有公网IPv4地址，只要求双栈主机具有IPv4地址。

（1）路由器端配置。

| | |
|---|---|
| Router (config)# **Interface tunnel** *tunnel_number* | 创建虚拟隧道接口 |
| Router (config-if)# **ipv6 address** *ipv6_address mask* | 配置隧道接口IPv6地址 |
| Router(config-if)#**no ipv6 nd suppress-ra** | 启用了隧道口的路由器广播 |
| Router (config-if)#**tunnel source** *Port_num* | 配置隧道源接口 |
| Router (config-if)# **tunnel mode ipv6ip isatap** | 隧道模式为ISATAP隧道 |

（2）客户端配置。

客户端可以使用netsh配置，具体如图22-5所示。


图22-5 netsh配置ISATAP客户端

其中，命令***netsh interface ipv6 isatap>set router*** *.*.*.*中的*.*.*.*是设置ISATAP路由器的地址。可以合并为一条命令C:/>netsh interface ipv6 isatap set router *.*.*.*。

## 22.7 NAT

### 22.7.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：静态NAT 、动态NAT、网络地址端口转换。

### 22.7.2 知识点精讲

1. 静态 NAT

静态 NAT 将合法 IP 地址和内部 IP 地址进行绑定，这种绑定的好处就是外网可以访问内网主机，内网可以访问外网。

配置过程如下：

（1）配置外部端口。

```
Router> enable
Router # config terminal                          准备进入全局配置模式
Router(config)# interface port1_num               对指定接口进行配置
Router(config-if)#ip address ipv4_address  mask
配置外部接口的 IP 地址和子网掩码。其中 IP 地址为公网合法 IP
Router(config-if)#ip nat outside
```

（2）配置内部端口。

```
Router> enable
Router # config terminal                          准备进入全局配置模式
Router(config)# interface port1_num               对指定接口进行配置
Router(config-if)#ip address ipv4_address mask
配置内部接口的 IP 地址和子网掩码。其中 IP 地址为内网 IP
Router(config-if)#ip nat inside
```

（3）内、外网地址建立一一对应关系。

```
Router> enable
Router # config terminal                          准备进入全局配置模式
Router(config)# ip nat inside source static local_ipv4_address global_ipv4_address
建立内、外网地址的一一对应关系
```

2. 动态 NAT

动态 NAT 就是内部私有 IP 地址动态地转换为合法 IP 地址池内的 IP 地址，但是对应关系不固定。

配置过程如下：

（1）配置外部端口。

```
Router> enable
Router # config terminal                          准备进入全局配置模式
Router(config)# interface port1_num               对指定接口进行配置
Router(config-if)#ip address ipv4_address mask
配置外部接口的 IP 地址和子网掩码。其中 IP 地址为公网合法 IP
Router(config-if)#ip nat outside
```

（2）配置内部端口。

```
Router> enable
Router # config terminal                          准备进入全局配置模式
Router(config)# interface port1_num               对指定接口进行配置
Router(config-if)#ip address ipv4_address mask
配置内部接口的 IP 地址和子网掩码。其中 IP 地址为内网 IP
Router(config-if)#ip nat inside
```

（3）定义合法 IP 地址。

Router> **enable**
Router # **config terminal** 准备进入全局配置模式
Router(config)# **ip nat pool** *name start_ipv4_address end_ipv4_address* **netmask** *mask*
建立地址池，设置地址池名称、起始 IP 地址、终止 IP 地址、子网掩码

（4）定义访问列表（ACL）。

Router(config)# **access-list** access-list_num **permit** source_ip source_wildcard
配置访问列表，设置允许访问 Internet 的地址；source_wildcard 表示反掩码

（5）关联前面设置的 ACL，并进行地址转换（全局模式下）

Router(config)# **ip nat inside source list** *access-list_num* **pool** *name*
进行地址转换，*name* 是外部地址池名，在（3）处应用，*access-list_num* 是 ACL 名，在（4）处设置

3. 网络地址端口转换

（1）配置外部端口。

Router> **enable**
Router # **config terminal** 准备进入全局配置模式
Router(config)# **interface** *port1_num* 对指定接口进行配置
Router(config-if)#**ip address** *ipv4_address mask*
配置外部接口的 IP 地址和子网掩码。其中 IP 地址为公网合法 IP
Router(config-if)#**ip nat outside**

（2）配置内部端口。

Router> **enable**
Router # **config terminal** 准备进入全局配置模式
Router(config)# **interface** *port1_num* 对指定接口进行配置
Router(config-if)#**ip address** *ipv4_address mask*
配置内部接口的 IP 地址和子网掩码。其中 IP 地址为内网 IP
Router(config-if)#**ip nat inside**

（3）定义复用的合法 IP 地址。

Router> **enable**
Router # **config terminal** 准备进入全局配置模式
Router(config)# **ip nat pool** *name start_ipv4_address end_ipv4_address* **netmask** *mask*
建立地址池，设置地址池名称、起始 IP 地址、终止 IP 地址、子网掩码

（4）定义访问列表（ACL）。

Router(config)# **access-list** access-list_num **permit** source_ip source_wildcard
配置访问列表，设置允许访问 Internet 的地址；source_wildcard 表示反掩码

（5）关联前面设置的 ACL，并进行地址转换（全局模式下）。

Router(config)# **ip nat inside source list** *access-list_num* **pool** *name* **overload**
进行地址转换，*name* 是外部地址池名，在（3）处应用，*access-list_num* 是 ACL 名，在（4）处设置

## 第 5 学时　案例难点 3——防火墙配置

第 4 天的第 5 学时主要学习防火墙配置知识。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 5～17 分之间。防火墙配置知识在上、下午考试中均是重点，ACL 知识又是考查的重中之重。每年的两次考试中都会有一道 15 分左右的案例题。本章考点知识结构图如图 23-1 所示。


图 23-1 考点知识结构图

## 23.1 防火墙基本知识

### 23.1.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：常见的三种防火墙技术、防火墙区域结构。

### 23.1.2 知识点精讲

防火墙（Fire Wall）是网络关联的重要设备，用于控制网络之间的通信。外部网络用户的访问必须先经过安全策略过滤，而内部网络用户对外部网络的访问则无须过滤。现在的防火墙还具有隔离网络、提供代理服务、流量控制等功能。

1. 常见的三种防火墙技术

常见的三种防火墙技术：包过滤防火墙、代理服务器式防火墙、基于状态检测的防火墙。

（1）包过滤防火墙。

包过滤防火墙主要针对 OSI 模型中的网络层和传输层的信息进行分析。通常包过滤防火墙用来控制 IP、UDP、TCP、ICMP 和其他协议。包过滤防火墙对通过防火墙的数据包进行检查，只有满足条件的数据包才能通过，对数据包的**检查内容**一般包括**源地址、目的地址和协议**。包过滤防火墙通过规则（如 ACL）来确定数据包是否能通过。配置了 ACL 的防火墙可以看成包过滤防火墙。

（2）代理服务器式防火墙。

代理服务器式防火墙对**第四层到第七层的数据**进行检查，与包过滤防火墙相比，需要更高的开销。用户经过建立会话状态并通过认证及授权后，才能访问到受保护的网络。压力较大的情况下，代理服务器式防火墙工作很慢。ISA 可以看成是代理服务器式防火墙。

（3）基于状态检测的防火墙。

基于状态检测的防火墙检测每一个 TCP、UDP 之类的会话连接。基于状态的会话包含特定会话的源、目的地址、端口号、TCP 序列号信息以及与此会话相关的其他标志信息。基于状态检测的防火墙工作基于数据包、连接会话和一个基于状态的会话流表。基于状态检测的防火墙的性能比包过滤防火墙和代理服务器式防火墙要高。思科 PIX 和 ASA 属于基于状态检测的防火墙。

2. 防火墙区域结构

防火墙按安全级别不同可划分为内网、外网和 DMZ 区，具体结构如图 23-2 所示。

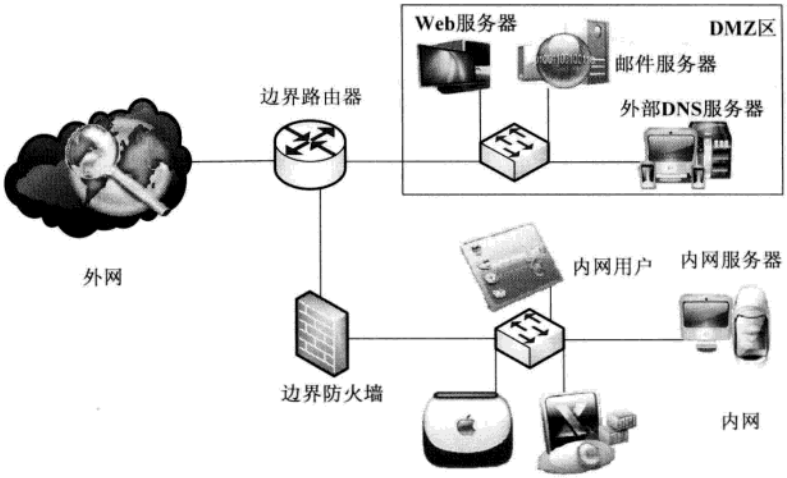



图 23-2　防火墙区域结构

（1）内网。

内网是防火墙的重点保护区域，包含单位网络内部的所有网络设备和主机。该区域是可信的，内网发出的连接较少进行过滤和审计。

（2）外网。

外网是防火墙重点防范的对象，针对单位外部访问用户、服务器和终端。外网发起的通信必须按照防火墙设定的规则进行过滤和审计，不符合条件的则不允许访问。

（3）DMZ 区（Demilitarized Zone）。

DMZ 区是一个逻辑区，从内网中划分出来，包含向外网提供服务的服务器集合。DMZ 中的服务器有 Web 服务器、邮件服务器、FTP 服务器、外部 DNS 服务器等。DMZ 区保护级别较低，可以按要求放开某些服务和应用。

## 23.2　ACL



### 23.2.1　考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：标准访问控制列表、扩展访问控制列表。

### 23.2.2　知识点精讲

访问控制列表（Access Control Lists，ACL）是目前使用最多的访问控制实现技术。访问控制列表是路由器接口的指令列表，用来控制端口进出的数据包。ACL 适用于所有的被路由协议，如

IP、IPX、AppleTalk 等。访问控制列表可以分为**标准访问控制列表**和**扩展访问控制列表**。ACL 的默认执行顺序是自上而下，在配置时要遵循最小特权原则、最靠近受控对象原则及默认丢弃原则。

1. 标准访问控制列表

标准访问控制列表**基于 IP 地址**，列表取值为 1～99，分析数据包的源地址决定允许或拒绝数据报通过。

（1）标准访问控制表配置。

```
Router> enable
Router # config terminal                                    准备进入全局配置模式
Router(config)#access-list access-list_num {permit|deny} source_ip source_wildcard_mask
access-list_num 取值为 1～99；permit 表示允许，deny 表示拒绝，source_wildcard_mask 表示反掩码
```

access-list 可以配置多条，但用这种方式时，如果列表要插入或删除一行，就必须删除所有 ACL 并重新配置。这种方式容易出错，建议使用文本方式编辑 ACL，通过 TFTP 上传或拷贝+粘贴方式到路由器。在配置 ACL 时，如果删除一项 ACL 条目，就会删除所有 ACL。

（2）启动标准访问控制表。

进入需要应用的接口时使用 access-group 命令启动标准访问控制表。

```
Router> enable
Router # config terminal                                    准备进入全局配置模式
Router(config)# interface port_num                          进入要配置标准访问控制表的接口
Router(config-if)# ip access-group access-list_num in|out
在指定接口上启动标准访问控制表，标明方向是 in 还是 out
```

这里 in 和 out 是针对防火墙接口而言的，部署方式如图 23-3 所示。

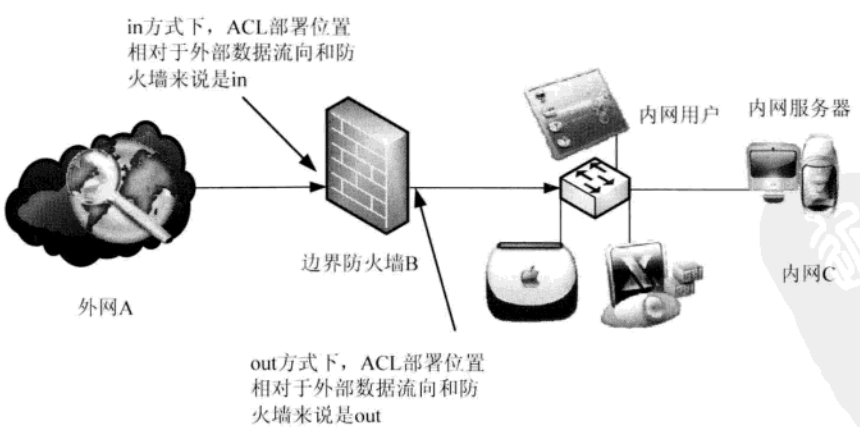



图 23-3 ACL 的 in 和 out 方式

假设网络管理员拒绝外网黑客 A 通过防火墙 B 访问内网 C，网络管理员可以使用 in 方式或 out 方式启动 ACL。

（1）使用 in 方式，外网黑客 A 甚至不能进入 B。

（2）使用 out 方式，外网黑客 A 虽然不能进入内网 C，但是可以进入防火墙 B，而且消耗了

防火墙B的运算资源。

2. 扩展访问控制列表

（1）通用扩展访问控制列表配置。

Router> **enable**

Router # **config terminal** 准备进入全局配置模式

Router(config)# **access-list** *access-list_num* **{permit|deny}** *IP_protocol source_ip source_wildcard_mask destionation_ip destionation _wildcard_mask*

*access-list_num* 取值为100～199，**permit** 表示允许，**deny** 表示拒绝

*IP_protocol* 包括IP、ICMP、TCP、GRE、UDP、IGRP、EIGRP、IGMP、NOS、OSPF

*source_ip source_wildcard_mask* 表示源地址及其反掩码

*destionation_ip destionation _wildcard_mask* 表示目的地址及其反掩码

（2）针对TCP和UDP的扩展访问控制列表配置。

Router> **enable**

Router # **config terminal** 准备进入全局配置模式

Router(config)# **access-list** *access-list_num* **{permit|deny}** *IP_protocol source_ip source_wildcard_mask[operator source_port] destionation_ip destionation _wildcard_mask [operator destination_port]* **[established]**

*access-list_num* 取值为100～199；**permit** 表示允许，**deny** 表示拒绝

*IP_protocol* 包括：IP、ICMP、TCP、GRE、UDP、IGRP、EIGRP、IGMP、NOS、OSPF

*source_ip source_wildcard_mask* 表示源地址及其反掩码

*destionation_ip destionation _wildcard_mask* 表示目的地址及其反掩码

*[operator source_port]*和*[operator destination_port]*是操作符+端口号方式，操作符可以是lt（小于）、gt（大于）、neq（不等于）、eq（等于）、range（端口号范围）

关键词 **established** 仅用于TCP连接，此关键词可以允许（拒绝）任何TCP数据段报头中RST或ACK位设置为1的TCP流量

（3）针对ICMP的扩展访问控制列表配置。

Router> **enable**

Router # **config terminal** 准备进入全局配置模式

Router(config)# **access-list** *access-list_num* **{permit|deny}** *IP_protocol source_ip source_wildcard_mask destionation_ip destionation _wildcard_mask [icmp_message]*

*access-list_num* 取值为100～199；**permit** 表示允许，**deny** 表示拒绝

*source_ip source_wildcard_mask* 表示源地址，及其反掩码

*destionation_ip destionation _wildcard_mask* 表示目的地址及其反掩码

*icmp_message* 可以是

·*Administratively-prohibited* 表示分组被过滤的消息

·*Echo* 表示ping命令消息

·*Echo-reply* 对ping命令产生的Echo消息回应

·*Host-unreachable* 子网可达，但主机不可达

·*Net-unreachable* 子网不可达

·*traceroute* 表示traceroute上的过滤信息

（4）启动扩展访问控制表。

进入需要应用的接口，使用access-group命令启动扩展访问控制表。

Router> **enable**

Router # **config terminal** 准备进入全局配置模式

Router(config)# **interface** *port_num* 进入要配置扩展访问控制表的接口

Router(config-if)# **ip access-group** *access-list_num* **in|out**

在指定接口上启动扩展访问控制表，标明方向是in还是out

## 23.3 防火墙基本配置

### 23.3.1 考点分析

历年网络工程师考试试题涉及本部分的相关知识点有：配置防火墙接口、配置接口参数、配置接口地址、配置公网地址范围和定义地址池、地址转换（NAT）、路由配置、配置静态地址映射、侦听。

### 23.3.2 知识点精讲

和路由器、交换机类似，防火墙具有 4 种命令模式，本部分以 PIX 防火墙为蓝本，介绍防火墙的配置，具体如表 23-1 所示。

表 23-1 防火墙 4 类命令模式

| 模式 | 访问方法 | 提示符 |
| --- | --- | --- |
| 用户模式 | 登录防火墙之后 | Firewall> |
| 特权模式 | 在**用户模式** Firewall >下，输入 **enable** 命令 | Firewall# |
| 全局配置模式 | **在特权模式** Firewall #下，输入 **configure terminal** 命令 | Firewall(config)# |
| 监视模式模式 | 防火墙开机或重启过程中按住 Esc 键，可更新操作系统映像文件恢复口令 | monitor> |

1. 配置防火墙接口

使用 nameif 命令配置防火墙接口名称，并制定接口的安全级别。

```
Firewall > enable
Firewall # config terminal                          准备进入配置模式
Firewall(config)#nameif port_num interface_name security security _num
配置端口名并指定优先级，security _num 越大安全级别越高
例如：
nameif ethernet0 outside   security 0          配置 e0 名字为 outside 优先级 0（默认为 0）
nameif ethernet1 inside    security 100        配置 e1 名字为 inside 优先级 100（默认为 100）
nameif ethernet2 dmz    security 10            配置 e2 名字为 outside 优先级 10
```

防火墙规则是：dmz 可以访问 outside，inside 可以访问 dmz 和 inside，配置访问控制列表可以让 outside 访问 inside。

2. 配置接口参数

```
Firewall > enable
Firewall # config terminal                          准备进入配置模式
Firewall(config)# interface port_num auto|100full [shutdown]
配置端口为自适应（auto）模式、100Mb/s（100full）模式、关闭该接口（shutdown）
```

3. 配置接口地址

```
Firewall(config)# ip address interface_name ipaddress mask
配置接口地址
```

例如：Firewall(config)#**ip address** inside 10.0.0.1 255.255.255.0

4. 配置公网地址范围和定义地址池

Firewall > **enable**
Firewall # **config terminal** 准备进入配置模式
Firewall(config)#**global** (*interface_name*) *nat_id ip_address-ip_address [global_ip_mask]*
*interface_name* 为外网接口名字，一般为 outside；nat_id 为公网地址池名，供 **nat** 命令使用；ip_address-ip_address 为公网地址段；[*global_ip_mask*]为公网地址掩码

5. 地址转换（NAT）

使用 NAT 配置，可以将私有 IP 转换为公网 IP。做 NAT 后，只有私有 IP 的主机可以访问外网。

Firewall > **enable**
Firewall # **config terminal** 准备进入配置模式
Firewall(config)# **nat** *(interface_name) nat_id local_ip [local_ip_mask]*
*interface_name* 为内网接口名字，一般为 inside；*nat_id* 为公网地址池名，会在 **global** 命令中配置；*local_ip* 为内网网络地址；[*local_ip_mask*]为掩码
例如：
Firewall(config)#**global** (*outside*) *1 123.1.1.1-123.1.254*
Firewall(config)#**nat** (*inside*) *1 192.168.1.1-192.168.1.254*

6. 路由配置

使用 route 命令定义静态路由。

Firewall(config)# **route** (interface_name) ip_address netmask gateway_ip_address
其中 interface_name 为接口名，可以是 inside、outside、dmz；ip_address netmask 为 IP 地址和子网掩码；gateway_ip_address 为网关地址

7. 配置静态地址映射

使用 static 命令配置静态地址映射，使得内外部地址一一对应。

Firewall(config)#**static**(internal_interface_name,external_interface_name)outside_ip_address inside_ip_address
其中 internal_ interface _name 表示内部网络接口，安全级别较高，如 inside；
external_ interface _name 表示外部网络接口，安全级别较低，如 outside；
outside_ip_address 表示共有 IP 地址；inside_ip_address 表示被转换的 IP 地址
例如
Firewall(config)#**static** (inside,outside) 123.1.1.1 192.168.1.1
Firewall(config)#**static** (dmz,outside) 123.1.1.2 192.168.1.2

8. 侦听

使用侦听 fixup 命令可以启用或者禁止特定的服务和协议。

Firewall(config)#**fixup protocol** *protocol_name protocol_port_num*
*protocol_name* 表示协议名称，可以是 ftp、http 等；*protocol_port_num* 表示协议端口号
例如：
Firewall (config)#**fixup protocol** http 8080
Firewall (config)#**no fixup protocol** http 80
启用 http 协议 8080 端口，禁止 80 端口



## 第 6 学时　案例难点 4——VPN 配置

第 4 天的第 6 学时主要学习 VPN 配置知识。根据历年考试的情况来看，每次考试涉及相关知识点的分值约在 0～6 分之间。VPN 配置知识在上、下午考试中均是重点，基本每次考试常有一道 15 分左

右的案例题。本节只讲 IPSec 的 VPN 配置。本章考点知识结构图比较单一，具体如图 24-1 所示。


图 24-1 考点知识结构图

## 24.1 IPSec VPN 配置基本知识

前面章节中介绍了 IPSec 的两种模式，提到了 AH 和 ESP 基本知识，大体知道了 IPSec 能实现加密、完整性判断。完整的 IPSec 协议由**加密、摘要、对称密钥交换、安全协议**四个部分组成。

两台路由器要建立 IPSec VPN 连接，就需要保证各自采用加密、摘要、对称密钥交换、安全协议的参数是一致的。但是 IPSec 协议并没有确保这些参数一致的手段。同时，IPSec 没有规定身份认证，无法判断通信双方的真实性，这就有可能出现假冒。

因此，在两台 IPSec 路由器交换数据之前就要建立一种约定，这种约定就称为 SA。安全关联（Security Association，SA）是单向的，在两个使用 IPSec 的实体（主机或路由器）间建立的逻辑连接，定义了实体间如何使用安全服务（如加密）进行通信。**SA 包含了安全参数索引（Security Parameter Index，SPI）、IP 目的地址、安全协议（AH 或者 ESP）三个部分。**

使用 IKE 建立 SA 分为两个阶段，即前面提到的“IKE 使用了两个阶段的 ISAKMP”。

1. 构建 IKE SA（第一阶段）

协商创建一个通信信道（IKE SA），并对该信道进行验证，为双方进一步的 IKE 通信提供机密性、消息完整性及消息源验证服务，**即构建一条安全的通道**。

第一阶段分为以下几步：

（1）参数协商。

该阶段协商以下几个参数：

- 加密算法：可以选择 DES、3DES、AES 等。
- 摘要（hash）算法：可以选择 MD5 或 SHA1。
- 身份认证方法：可以选择预置共享密钥（pre-share）认证或 Kerberos 方式认证。
- Diffie-Hellman 密钥交换（DH，Diffie-Hellman key exchange）算法：一种确保共享密钥安全穿越不安全网络的方法，该阶段可以选择 DH1（768bit 长的密钥）、DH2（1024bit 长的密钥）、DH5（1536bit 长的密钥）、DH14（2048bit 长的密钥）、DH15（3072bit 长的密钥）、DH16（4096bit 长的密钥）。
- 生存时间（life time）：选择值应小于 86400 秒，超过生存时间后，原有的 SA 就会被删除。

上述参数集合就称为 IKE 策略（IKE Policy），而 IKE SA 就是要在通信双方之间找到相同的 Policy。

（2）交换密钥。

（3）双方身份认证。

（4）构建安全的 IKE 通道。

2. 构建 IPSec SA（第二阶段）

使用已建立的 IKE SA，协商 IPSec 参数，为数据传输建立 IPSec SA。

构建 IPSec SA 的步骤如下：

（1）参数协商。

该阶段协商以下几个参数：

- 加密算法：可以选择 DES、3DES。
- Hash 算法：可以选择 MD5、SHA1。
- 生存时间（life time）。
- 安全协议：可以选择 AH 或 ESP。
- 封装模式：可以选择传输模式或隧道模式。

上述参数被称为变换集（Transform Set）。

（2）创建、配置加密映射集并应用，构建 IPSec SA。

第二阶段如果响应超时，则重新进行第一阶段的 IKE SA 协商。

## 24.2 IPSec VPN 配置

配置 IPSec VPN 分为四步，下面以图 24-2 为例讲述 IPSec VPN 的具体配置过程。


图 24-2 IPSec 配置实例



1. 连通性测试

（1）确认路由器 A 和路由器直接的联通性，保证之间的路由信息正常。

（2）确定路由器 A 和 B 上的 ACL 允许 AH（IP 协议，端口 50）、ESP（IP 协议，端口 51）和 ISAKMP（UDP 协议，端口 500）通过。

2. 配置 IKE（ISAKMP/IKE）阶段

（1）启动 IKE（ISAKMP/IKE）配置。

```
Router> enable
Router # config terminal                    准备进入全局配置模式
Router(config)# crypto isakmp enable
全局模式下对所有端口启用，路由器 IKE 默认开启，如果阻止端口开放 IKE，可以使用 ACL 屏蔽端口号为 500 的 UDP
```

（2）配置 IKE 策略（IKE Policy）。

Router（config）# **crypto isakmp policy** *priority*

定义一个 IKE 策略，进入 ISAKMP 配置模式，*priority* 取值为 1～10000，用来唯一标识 IKE 策略，并为 IKE 策略分配优先级，1 为最高优先级

Router（config-isakmp）# **encryption {des|3des|aes|aes 192| aes 256}**

指定加密算法

Router（config-isakmp）#**hash {sha|md5}**

指定摘要算法

Router（config-isakmp）# **group {1|2|5|14|15|16}**

指定 Diffie-Hellman 密钥交换（DH）算法，参数 1 表示 DH1（768bit 长的密钥），2 表示 DH2（1024bit 长的密钥），5 表示 DH5（1536bit 长的密钥），14 表示 DH14（2048bit 长的密钥），15 表示 DH15（3072bit 长的密钥），16 表示 DH16（4096bit 长的密钥）

Router（config-isakmp）# **authentication {pre-share|rsa-sig|rsa-encr}**

配置认证方法。参数 pre-share 通过手工配置预共享密钥；rsa-sig 默认值，要求使用 CA 并使用 RSA 防抵赖；rsa-encr 不需要 CA，使用 RSA 防抵赖

Router（config-isakmp）#**lifetime** *seconds*

指定 IKE SA 生存时间。*seconds* 单位秒，取值为 60～86400，默认为 86400，并且越短越安全

例如，RouterA 可以配置如下：

```
RouterA（config）# crypto isakmp policy 100
RouterA（config-isakmp）# encryption des
RouterA（config-isakmp）# hash md5
RouterA（config-isakmp）# group 1
RouterA（config-isakmp）# authentication pre-share
RouterA（config-isakmp）# lifetime 86400
```

（3）配置 IKE 身份认证。

IKE 身份认证可以有 RSA 签名方式（RSA signature）、随机 RSA 加密（RSA encrypted nonce）、预共享密钥（preshared key）三种方式。

考试只涉及预共享密钥（preshared key）方式。

Router（config-isakmp）# **crypto isakmp identity address**

表明用 IP 地址指定本地 peer 的 ISAKMP 标识，此时接口 IP 地址需要事先配置好

Router（config-isakmp）# **crypto isakmp key** *keystring* **address** *peer_address*

指定本地 peer 与特定远程 peer 要使用的共享密钥。*Keystring* 是指定预共享密钥，*peer_address* 是远端 peer 的 IP 地址。

例如，RouterA 可以配置如下：

```
RouterA（config-isakmp）# crypto isakmp identity address
RouterA（config-isakmp）# crypto isakmp key S1 address 202.1.1.2
```

RouterB 可以配置如下：

```
RouterB（config-isakmp）# crypto isakmp identity address
RouterB（config-isakmp）# crypto isakmp key S1 address 202.1.1.1
```

（4）检测 IKE 配置。

使用 show 命令检测 IKE 配置。

```
Router> enable
Router # show crypto isakmp policy
```

3. 配置 IPSec SA 阶段

（1）配置 IPSec SA 变换集（Transform Set）。

```
Router # config terminal                    准备进入全局配置模式
Router（config）#crypto ipsec transform-set transform_set_name transform1 [transform2 [transform3]]
```

定义一个变换集，*transform_set_name* 表示变换集名，*transform1[transform2 [transform3]]*表示变换集合方式。

其中 *transform1[transform2 [transform3]] 形式如下*：

- 认证方式：ah-md5-hmac（AH 采用 MD5 认证）、ah-sha-hmac、esp-md5-hmac、esp-sha-hmac
- 加密方式：esp-aes（esp 协议采用 128AES 加密算法）、esp-aes 192、esp-aes 256、esp-des、esp-3des、esp-null（不加密）

router（cfg-crypto-trans）#**mode {tunnel|transport}**

（可选）配置变换集关联模式，**tunnel** 表示隧道模式，**transport** 表示传输模式

例如，RouterA 可以配置如下：

RouterA（config）# **crypto ipsec transform-set** mine esp-des

RouterA （cfg-crypto-trans）#**mode tunnel**

（2）创建 ACL，对 IPSec 进行控制。

创建访问控制列表对 IPSec 流量进行控制。

（3）创建加密映射集合（crypto map）。

Router # **config terminal** 准备进入全局配置模式

Router（config）#**crypto map** *map_name seq_num* **ipsec-isakmp**

命名要创建的加密映射条目，并对加密映射集进行配置。例如：crypto map S1map 100 ipsec-isakmp

Router（config-crypto-map）#**match address** *access_list_id*

用应用之前创建的 ACL 进行流控

Router（config-crypto-map）#**set-peer** ip_address

配置 IPSec SA 协商的远程 peer。此配置语句可以重复

Router（config-crypto-map）#**set transform-set** *transform_set_name transform1 [transform2 [transform3]]*

指定变换集

Router（config-crypto-map）# **set security-association lifetime** *seconds*

指定 IPSec SA 生存时间（可选）

例如，RouterA 可以配置如下：

RouterA（config）# crypto map mymap 100 ipsec-isakmp

RouterA（config-crypto-map）# match address 100

RouterA（config-crypto-map）# set peer 202.1.1.2

RouterA（config-crypto-map）# set transform-set mine

RouterA（config-crypto-map）# set security-association lifetime 86400

（4）应用加密映射集（crypto map）

Router（config-if）#**crypto map** *map_name*

在某接口下应用加密映射集

例如，RouterA 可以配置如下：

RouterA（config）# **interface** ethernet0/1

RouterA（config-if）# **crypto map** S1map

4. 检测命令

Router（config）# show crypto ipsec transform-set

显示 IPSec 变换集

Router（config）# show crypto map

显示 crypto maps

Router（config）# show crypto ipsec sa

显示 IPSec SA 的状态

# 第5天

## 模拟测试，反复操练

经历过前4天的学习后，进入最后一天的学习了。今天最主要的任务就是做模拟题、熟悉考题风格、检验自己的学习成果。考生一定摩拳擦掌好久了吧？下面就一起来进入吧。

### 第1~2学时　模拟测试1（上午试题）

- 以下关于CPU的叙述中，正确的是（ 1 ）。

（1）A．ALU属于运算单元

B．程序计数器PC用于存放临时运算结果

C．逻辑运算部件主要用于控制信号的处理

D．寄存器是CPU中的控制部件

- 以下关于PIO与DMA的描述中，正确的是（ 2 ）。

（2）A．PIO模式是一种主要依赖CPU运算完成数据传输的方式

B．PIO模式不依赖CPU指令完成数据传送

C．DMA的传输速度比PIO慢

D．DMA相对PIO模式而言需要更多的CPU指令来实现

- 以下关于校验码的叙述中，正确的是（ 3 ）。

（3）A．海明码对数位进行分组，奇偶校验码进行纠错

B．海明码的码距必定大于1

C．奇偶校验码具有很强的检错能力

D．循环冗余校验码的码距一定是1

- 以下关于Cache的叙述中，正确的是（ 4 ）。

（4）A．Cache 容量越大，性能越好

B．Cache 采用预读取技术，尽可能保证 CPU 需要读取的数据预先读入 Cache

C．Cache 的存取速度与硬盘的读取速度相等

D．CPU 内部 Cache 容量应大于或等于外部所有 Cache 容量之和

- 下列面向对象概念中，成为了业界统一标准的是（ 5 ）。

（5）A．Coad　　B．Booch

C．OMT　　D．UML

- 结构化程序设计中，适合解决阶乘计算的基本结构是（ 6 ）。

（6）A．顺序　　B．循环　　C．堆栈　　D．选择

- 为了验证软件的功能是否满足应用要求的测试称为（ 7 ）。

（7）A．单元测试　　B．集成测试

C．回归测试　　D．确认测试

- 下列选项中，属于系统软件的是（ 8 ）。

（8）A．系统工具软件、财务软件和数据库管理系统软件

B．汇编程序、统计分析软件和 Java 解释器

C．数据库管理系统软件和电梯控制程序

D．编译程序、数据库管理系统软件

- 某报刊编辑于 2011 年 5 月 1 日将我国的《中华人民共和国著作权法》译成英文，投递给某刊物，于 2011 年 9 月 1 日发表。相关国家机关认为该译文质量很高，经与该编辑协商，于 2011 年 10 月 1 日发文将该译文定为官方正式译文。该编辑对其译文（ 9 ）。

（9）A．自 2011 年 10 月 1 日起一起享有著作权

B．自 2011 年 9 月 1 日起一起享有著作权

C．自 2011 年 5 月 1 日至 2011 年 9 月 1 日期间享有著作权

D．不享有著作权

- 在 Windows Server 2003 系统中，下列能代表本机地址的是（ 10 ）。

（10）A．127.0.0.1　　B．local host　　C．selfhost　　D．hosts

- 一个速度为 1.544Mb/s 的标准 T1 载波的时隙是 125μs，则该基本帧由（ 11 ）个子信道组成，每一个基本帧所包含的二进制 bit 是（ 12 ）。

（11）A．32　　B．16　　C．24　　D．23

（12）A．128　　B．184　　C．193　　D．192

- 下列关于网络应用服务的说法中，正确的是（ 13 ）。

（13）A．在 DNS 应用中数据交换频繁且流量相对较大

B．FTP 服务中数据交换频繁，但数据流量相对较小

C．VOD 服务对数据传输实时性要求不高

D．OA 应用的数据交换频繁，但对数据的实时性要求高

● 8B/10B 编码是一种常用的局域网编码方案，其原理是先把 8 位分为一组的代码变换成 10 位一组，然后再传输，则这种编码的效率是（ 14 ）。

（14）A．0.4　　B．0.5　　C．0.8　　D．1.0

● STP 协议中，交换机端口状态总是保持在某种状态，当交换机端口处于（ 15 ）状态时，不把接收到的 MAC 帧转发出去，但是可以检测交换机环路状态。

（15）A．阻塞（blocking）　　B．学习（learning）
　　C．转发（forwarding）　　D．监听（listening）

● IP 地址为全 1 的是（ 16 ）。

（16）A．公用 IP 地址　　B．专用 IP 地址
　　C．受限广播地址　　D．直接广播地址

● 在标准 PCM 调制方式中，每一路标准语音信号是（ 17 ）kb/s，若该信号使用 128 级量化，则一路语音信号的传输速率为（ 18 ）。

（17）A．32　　B．64　　C．128　　D．256

（18）A．64kb/s　　B．128kb/s
　　C．56kb/s　　D．56kb/s

● 在相隔 500km 的两地间，若通过电缆以 9600b/s 的速率传送 1000Byte 的数据包，从开始发送到接收完数据需要的时间是（ 19 ）；同样的数据，若用 512kb/s 的卫星信道传送，则需要的时间是（ 20 ）。

（19）A．833.5ms　　B．135.5ms
　　C．835.5ms　　D．1250ms

（20）A．156.3ms　　B．183.3ms
　　C．285.6ms　　D．585.6ms

● IOS 中，要执行 show running 的提示符是（ 21 ）。

（21）A．>　　B．#　　C．%　　D．@

● 在网络工程师的实际操作中，为了检测服务器的某个基于 TCP 协议的服务是否正常开启，可以使用下列（ 22 ）命令。

（22）A．Telnet IP 端口　　B．show ip route
　　C．show interface　　D．route print

● 在普通的二层交换机中，（ 23 ）总是向所有端口转发。

（23）A．冲突碎片　　B．已知的单播
　　C．广播　　D．组播

● 在 OSPF 协议中，为了限制路由信息传播的范围，常采用分区的机制来处理，各个区域必须要与主干区域直接连接才可以正常通信，主干区域通常用（ 24 ）表示，若某个区域没有直接连接主干区域，则必须使用（ 25 ）来联系主干区域。

（24）A．area 0.0.0.0　　B．backbone

C．virtual-link　　D．router ospf

（25）A．组播机制　　B．广播机制

C．路由重发布　　D．虚连接

- MPLS VPN 中，与用户端连接的设备是（ 26 ）。

（26）A．CE　　B．PE　　C．P　　D．VRF

- 某 Windows 系统的 PC 用 ipconfig 看到的本地连接信息如下：

```
C：\Documents and Settings\Administrator>ipconfig
Windows IP Configuration
Ethernet adapter 本地连接：
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . :  192.168.10.1
        Subnet Mask . . . . . . . . . . . :  255.255.255.0
        Default Gateway . . . . . . . . . :  192.168.0.254
用 ping 192.168.0.254 之后，显示的信息如下：
C：\Documents and Settings\Administrator>ping 192.168.0.254
Pinging 192.168.0.254 with 32 bytes of data：
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Ping statistics for 192.168.0.254：
    Packets：Sent = 3,Received = 0,Lost = 3 （100% loss）
```

则该 PC 的 IP 地址为（ 27 ），若该机的 IP 地址与子网掩码设置正确，则其默认网关可能是（ 28 ）。Ping 不通过网关的可能原因是（ 29 ）。

（27）A．192.168.10.1　　B．192.168.10.0

C．192.168.10.128　　D．192.168.10.255

（28）A．192.168.10.255　　B．192.168.10.254

C．192.168.10.0　　D．192.168.0.254

（29）A．默认网关与本机 IP 地址不在同一个网段

B．TCP/IP 协议内部故障

C．子网掩码设置错误

D．DNS 服务器设置错误

- 在 Linux 系统中，修改了 sshd 的配置文件之后，若想要新配置生效，可以通过查看进程命令获得以下信息：

```
[root@hunau ~]# ps -A
  PID TTY          TIME CMD
    1 ?        00:00:02 init
    2 ?        00:00:00 ksoftirqd/0
    3 ?        00:00:00 watchdog/0
    4 ?        00:00:00 events/0
    5 ?        00:00:00 khelper
    6 ?        00:00:00 kthread
    8 ?        00:00:00 kblockd/0
```

```
11 ?        00:00:00 khubd
68 ?        00:00:00 pdflush
69 ?        00:00:00 pdflush
974 ?       00:00:00 udevd
2074 ?      00:00:00 sshd
```

则以下命令（ 30 ）可以实现，从中也可以看出系统启动时最先运行的进程是（ 31 ）。

（30）A．kill udevd;udevd　　B．kill 2074 ;sshd

C．kill sshd ;sshd　　D．kill 974;udevd

（31）A．0　　B．syslogd

C．init　　D．sshd

- 若在路由器中检查接口时，发现接口的状态是 serial 0 is up,line protocol is down，则说明（ 32 ）。

（32）A．物理接口已经连接正常　　B．数据链路层已经连接正常

C．应用层协议端口连接正常　　D．路由协议连接正常

- Linux 操作系统中，网络管理员可以通过修改（ 33 ）文件控制 Linux 的启动。

（33）A．inetd.conf　　B．lilo.conf

C．httpd.conf　　D．resolv.conf

- Linux 操作系统中，若用户的口令丢失，则可以由 root 用户修改加密口令的文件（ 34 ）得以解决。

（34）A．/etc/sam　　B．/etc/shadow

C．/etc/group　　D．/etc/security

- 在 Windows 中运行（ 35 ）命令后得到如下图所示的结果，从中可以看出，目前用户 102.217.112.0/24 的分组经 102.217.115.1 发出，需增加一条路由，正确的命令为（ 36 ）

```
TCP    192.168.1.100：2959    124.228.175.10：80     ESTABLISHED
TCP    192.168.1.100：2961    124.228.175.10：80     ESTABLISHED
TCP    192.168.1.100：3077    220.181.112.34：80     TIME_WAIT
TCP    192.168.1.100：3079    219.148.35.4：80       ESTABLISHED
TCP    192.168.1.100：3081    219.148.35.44：80      ESTABLISHED
TCP    192.168.1.100：3105    220.181.112.75：80     ESTABLISHED
TCP    192.168.1.100：3109    220.181.112.75：80     ESTABLISHED
TCP    192.168.1.100：3113    220.181.112.34：80     TIME_WAIT
TCP    192.168.1.100：3115    220.181.112.34：80     TIME_WAIT
TCP    192.168.1.100：3119    220.181.112.34：80     TIME_WAIT
TCP    192.168.1.100：3137    220.181.112.34：80     TIME_WAIT
```

（35）A．ipconfig /all　　B．ping

C．nslookup　　D．netstat -n

（36）A．访问 Web 网站　　B．下载 FTP 文件

C．发送电子邮件　　D．接收电子邮件

- 下列关于 Microsoft 管理控制台（MMC）的说法中，错误的是（ 37 ）。

（37）A．MMC 集成了用来管理网络、计算机、服务及其他系统组件的管理工具

B．MMC 创建、保存并打开管理工具单元

C．MMC 可以运行在 Windows XP 和 Windows 2000 操作系统上

D．MMC 是用来管理硬件、软件和 Windows 系统的网络组件

- 下列 RAID 技术中，磁盘利用率最高的是（ 38 ）。

（38）A．RAID0　　B．RAID1

C．RAID3　　D．RAID5

- 在 xDSL 技术中，适合作为小型公司员工上网并提供公司 Web 服务器连接的是（ 39 ）。

（39）A．ADSL 和 HDSL　　B．ADSL 和 VDSL

C．SDSL 和 VDSL　　D．SDSL 和 HDSL

- 对于开启了匿名访问功能的 FTP 服务器，匿名用户登录时需要输入的用户名是（ 40 ）。

（40）A．root　　B．user　　C．guest　　D．anonymous

- 在 Windows Server 2003 中安装 Web 服务器，若需要启用 SSL 协议，则必须为 Web 服务器（ 41 ）。

（41）A．申请一个数字证书　　B．申请一对公开密钥

C．申请一个普通的会话密钥　　D．申请由 KDC 颁发一个密钥

- 下列几种病毒中，能感染 Office 文件的是（ 42 ）。

（42）A．worm.a79　　B．Win32.CIH

C．Trojan. Generic　　D．Macro.Xls.3mcab

- 下列关于 ACL 配置规则的说法中，错误的是（ 43 ）。

（43）A．每个 ACL 语句中的最后都隐含一句 deny any

B．设置 ACL 时要先设定主机，再设定整个网段

C．扩展访问列表才可以指定目的地址和协议

D．标准 ACL 适合限制具体的应用协议

- 某商业银行向 CA 申请数字证书用于其网上银行，普通网银用户可以通过（ 44 ）来确认其网上银行网站不是被仿冒的钓鱼网站。在网银用户与网银网站进行安全通信时，用户向网站提交的支付信息可以使用（ 45 ）进行加密，网银网站可以通过（ 46 ）进行解密，完成安全支付。

（44）A．CA 的签名　　B．证书中的公钥

C．网银网站的私钥　　D．用户的公钥

（45）A．CA 的签名　　B．证书中的公钥

C．网银网站的私钥　　D．用户的公钥

（46）A．CA 的签名　　B．证书中的公钥

C．网银网站的私钥　　D．用户的公钥

- IPSec 的防重放攻击主要由（ 47 ）来实现。

（47）A．ESP　　B．PKI　　C．KDC　　D．AH

- 下列是利用 SSL 协议登录网上银行进行网上支付的页面地址的是（ 48 ）。

（48）A．http://ssl.aaa.com.cn　　B．ssl://www. aaa.com.cn

C．shttp://www. aaa.com.cn　　D．https://www. aaa.com.cn

● 某高校从运营商处分配到的网络地址为 222.169.0.0/24～222.169.7.0/24，这个地址块可以用（ 49 ）表示，则该高校最多可用计算数为（ 50 ）。

（49）A．222.169.0.0/20　　B．222.169.0.0/21

C．222.169.0.0/16　　D．222.169.0.0/24

（50）A．2032　　B．2048　　C．2000　　D．2056

● 能够表示 4 个网络 192.168.12.0/24、192.168.13.0/24、192.168.14.0/24 和 192.168.15.0/24 的一个地址是（ 51 ）。

（51）A．192.168.8.0/22　　B．192.168.12.0/22

C．192.168.8.0/21　　D．192.168.12.0/21

● 有 10 个部门的某 IT 公司，要求每个部门都用独立的 IP 网段，现从 ISP 处获得 210.43.192.0/18 的地址段，则下列地址段中，不属于该公司的地址的是（ 52 ）。

（52）A．210.43. 236.0/22　　B．210.43.224.0/22

C．210.43.208.0/22　　D．210.43.254.0/22

● 某单位的域名为 Hunau.net，其对应的 Web 服务器的 IPv6 地址为 FEDC:BA99:8888:7777:6666:5555:4444:3333，对应的 DNS 主机名为 www，则用户访问该服务器的正确形式是（ 53 ）。

（53）A．http://[ FEDC:BA99:8888:7777:6666:5555:4444:3333]

B．http:// FEDC:BA99:8888:7777:6666:5555:4444:3333

C．http6://www.hunau.net

D．https://www.hunau.net

● 下列关于 IPv6 的优点中，错误的是（ 54 ）

（54）A．地址长度为 128bit，容量大大地扩展了

B．能够真正地实现无状态地址自动配置

C．基本报头格式大大简化

D．利用流标签可以实现网络安全通信

● 一个 IPv6 地址可以有不同的缩写方式，若存在 IPv6 地址 20F1:00D3:0000:0000:0F3A:0000:0000:8731，则以下表示错误的是（ 55 ）

（55）A．20F1:D3:0:0:F3A:0:0:8731

B．20F1:D3::F3A:0:0:8731

C．20F1:D3::F3A::8731

D．20F1:D3:0:0:F3A::8731

● 下列关于 ADSL 的描述中，正确的是（ 56 ）。

（56）A．ADSL 是一种基于传统电话线路的模拟通信技术

B．ADSL 可以采用模拟信道数字调制方式实现高速通信

C．ADSL 的最大下行速度可以达到 8Mb/s

D．ADSL 是一种上下行速率对称的通信技术

- SNMP 代理进程可以向管理进程发送的操作指令是（ 57 ）。

（57）A．get-request　　B．get-next-request

C．set-request　　D．get-response

- 以下关于单臂路由的说法正确的是（ 58 ）。

（58）A．在路由器接口充足的情况下，尽可能考虑使用单臂路由

B．在路由器里通过使用子接口，每个子接口对应一个 VLAN

C．使用单臂路由，路由器至少应该有 2 个以上的物理接口

D．若只使用一个物理接口，则是无法实现

- 交换机命令 Switch >enable 的作用是（ 59 ）。

（59）A．配置 enable 访问口令　　B．进入全局配置模式

C．进入特权模式　　D．显示当前模式

- 下列关于 VLAN 的说法，正确的是（ 60 ）。

（60）A．VLAN ID 是唯一区分 VLAN 的标识

B．网络中最多允许的 VLAN 数量为 1024 个

C．VLAN ID 的长度是 2 个字节

D．普通 PC 能够识别出 VLAN ID

- 下列关于 CSMA/CD 协议几种不同的监听算法的描述中，正确的是（ 61 ）。

（61）A．非坚持型监听算法有利于减少网络空闲时间

B．坚持型监听算法有利于减少冲突的概率

C．坚持型监听算法无法减少网络的空闲时间

D．坚持型监听算法能够及时抢占信道

- 在 DHCP 客户端释放原来 IP 地址的指令是（ 62 ）

（62）A．ipconfig/all　　B．ipconfig/release

C．ipconfig/renew　　D．ipconfig/flushdns

- 用户 A 的 IP 地址为 172.28.0.253/24，主机设置的默认网关为 172.28.0.254，工程师小张在用户 A 的计算机上 ping 默认网关时，显示的是 request timeout，于是小张继续在用户 A 的计算机上使用 arp -a 指令，可以看到如下信息：

```
Interface:  172.28.0.253 --- 0x20002
  Internet Address      Physical Address      Type
  172.28.0.254          00-1F-3B-CD-29-DD     dynamic
```

则说明（ 63 ）。

（63）A．主机 A 与默认网关之间不可以相互通信

B．默认网关已经关机

C．主机 A 可以与默认网关通信

D．主机 A 与主机 B 之间连线故障

- 下列关于 RAID5 阵列的说法中，正确的是（ 64 ）。

（64）A．至少需要 2 块以上的硬盘

B．使用奇偶校验确保数据的完整性

C．其磁盘利用率是 80%

D．最小磁盘数配置时，损坏 2 块硬盘还可以保证数据完整

- 下列关于 802.3 的以太网帧中最小帧长的说法中，不正确的是（ 65 ）。

（65）A．以太网的最小帧长是 64 字节

B．若数据内容部分小于 46 字节，可以通过填充部分确保最小帧长满足条件

C．若数据帧长度小于最小帧长，则数据帧一定不是合法数据帧

D．设置最小帧长的目的是杜绝冲突

- 建筑物综合布线系统中的工作区子系统是指（ 66 ）。

（66）A．由终端到信息插座之间的连线系统

B．楼层配线间的配线架和线缆系统

C．各楼层设备之间的互连系统

D．连接各个建筑物的通信系统

- 根据 EIA/TIA-568 标准规定，最适合交叉线连接的设备是（ 67 ）。

（67）A．路由器与交换机　　B．PC 与交换机

C．集线器与路由器　　D．路由器与路由器

- 下列不属于常用备份设备的是（ 68 ）。

（68）A．磁盘阵列　　B．光盘塔或光盘库

C．磁带机或磁带库　　D．Flash 盘

- 下列关于网络分层设计模型的说法中，正确的是（ 69 ）。

（69）A．网络分层模型包括接入层、分布层和路由层三个层次

B．接入层主要实现用户接入、Mac 地址绑定、端口安全等功能

C．因为所有数据都要经过核心层，因此核心层应当使用高速设备，而不是路由设备

D．汇聚层是各个区域的分中心，因此安全认证和快速路由转发是该层的主要功能

- 网络系统设计过程中，需求分析阶段的任务是（ 70 ）。

（70）A．确认需求分析说明书，总结个人与单位的需求

B．分析现有网络的各类资源分布，掌握网络所处的状态

C．根据用户需求描述网络行为和性能

D．网络设计者确定具体的软件、硬件、连接设备、服务和布线

- The server site shall （ 71 ） on the specified data socket. The FTP request command determines the direction of data transfer，and the socket number which is to be used in establishing the

data connection. The server on receiving the appropriate store or retrieve （ 72 ） shall initiate the data connection to the specified user data socket in the specified byte size （default byte size is 8 bits） and send a reply indicating that file transfer may proceed. Prior to this the server should send a reply indicating the server socket for the data connection. The user may use this server socket information to （ 73 ） the security of his data transfer. The server may send this （ 74 ） either before of after initiating the data connection.

The byte size for the data connection is specified by the TYPE，or TYPE and BYTE commands. It is not required by the protocol that servers accept （ 75 ） possible byte size. The user of various byte size is for efficiency in data transfer and servers may implement only those byte size for which their data transfer is efficient. It is however recommended that servers implement at least the byte size of 8 bits.

（71）A．monitor　　B．listen
　　C．find　　D．accept
（72）A．request　　B．command
　　C．data　　D．order
（73）A．support　　B．ensure
　　C．keep　　D．hold
（74）A．accept　　B．reply
　　C．information　　D．byte
（75）A．more　　B．one
　　C．part　　D．all

## 第3～4学时　模拟测试1（下午试题）

**试题一**、某企业试图在全国范围内的分公司之间部署视频系统，总部通过2.5Gb/s的POS技术连接ISP，POS接口使用SONET技术实现连接，并要求在R1上禁止所有目的端口号为5002的UDP数据包进入企业总部的内部网络。拓扑连接如图1所示。

**【问题1】**阅读运营商R1的配置信息，将相关的配置内容补充完整。

R1的配置信息如下：

```
R1 #conf  t
R1 (config)#interface pos 0/0
R1 (config-if)#description To ISP
R1 (config-if)#bandwidth____（ 1 ）____
R1 (config-if)#ip address 10.0.0.2 ____（ 2 ）____
R1 (config-if)#pos  framing  sonet
R1 (config-if)#no shutdown
R1 (config-if)#exit
```

```
R1 (config)#access-list 110 deny udp ____( 3 )____ eq 5200
R1 (config)#access-list 110 permit ____( 4 )____ any any
R1 (config)#interface pos 0/0
R1 (config-if)#ip access-group ____( 5 )____
R1 (config-if)#exit
```

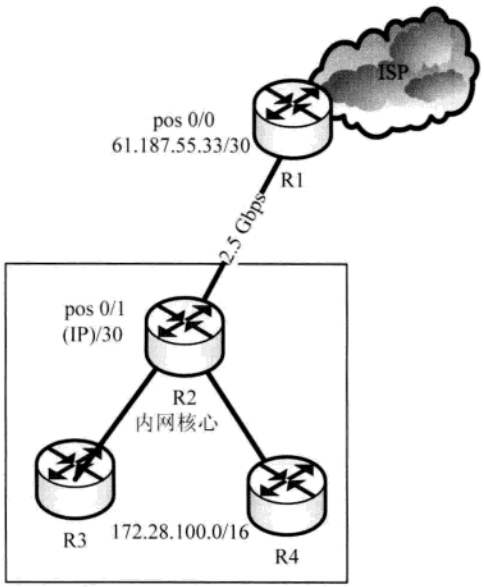



图 1　拓扑图

**【问题 2】**企业总部网与 ISP 相连的 2.5Gb/s 线路中，R2 的 pos0/1 接口的 IP 应该使用（ 6 ）。

（6）A．61.187.55.32/30　　B．61.187.55.34/30

C．61.187.55.35/30　　D．61.187.55.36/30

**【问题 3】**企业网与 ISP 相连的线路使用/30 的掩码的原因是（ 7 ）。

（7）A．节省 IP 地址资源　　B．提高访问效率

C．降低广播，提高安全性　　D．降低管理成本

**【问题 4】**若企业网内部与全国各地 31 个省级分公司之间采用 VPN 连接，全公司网络构成了一个自治系统，则该系统适合的路由协议是（ 8 ）。

（8）A．RIP　　B．OSPF　　C．IS-IS　　D．BGP

**试题二、**某高校校园网的拓扑图如图 2 所示，其他基本访问要求如表 1 所示。

该校在校园网建设中的基本要求如下：

1．要求主干链路 1000Mb/s 连接，桌面主机 100Mb/s 连接到接入交换机，其中网络中心距离学生宿舍区最远不超过 2000 米，距离教学楼区最远不超过 400 米。

2．教学楼区的汇聚交换机置于教学楼的机房内，各层信息点数如表 2 所示。

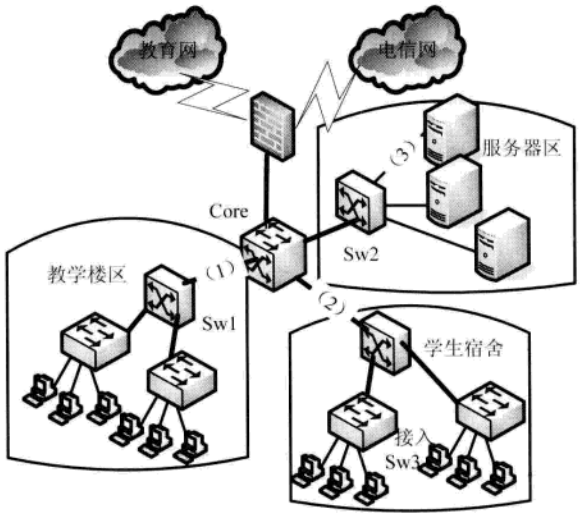



图2　校园网拓扑结构图

表2　教学楼信息点分布

| | |
|---|---|
| 1 | 24 |
| 2 | 30 |
| 3 | 19 |
| 4 | 22 |
| 5 | 18 |

3．教学楼区的所有计算机采用静态IP地址，其他区域采用DHCP分配方式，DHCP服务器采用千兆光口网卡。

4．信息中心有两条百兆出口线路，在防火墙上根据外网IP设置出口策略，分别从两个出口访问Internet。

**【问题1】**根据网络的需求和拓扑图，在满足网络功能的前提下，本着最节约成本的布线方式，传输介质1应采用（ 1 ），传输介质2应采用（ 2 ），传输介质3应采用（ 3 ）。

（1）～（3）A．单模光纤　　B．多模光纤

C．基带同轴电缆　　D．宽带同轴电缆

E．3类双绞线　　F．5类双绞线

**【问题 2】**网络工程师小张根据网络需求选择了三种类型的交换机，其基本参数如表3所示。

表 3 交换机配置表

| | |
|---|---|
| 1 | 12 端口 1000Mb/s 光电自适应接口 |
| 2 | 24 端口 100Mb/sRJ-45 接口，一端口 1000Mb/s SFP |
| 3 | 5 插槽模块化三层交换机 |

根据网络需求、拓扑图和交换机参数类型，在图中，Switch 1 应采用（ 4 ）类型交换机，Switch 2 应采用（ 5 ）类型交换机，Switch 3 应采用（ 6 ）类型交换机。

根据需求描述和所选交换机类型，则教学楼的 4 楼至少需要（ 7 ）类交换机（ 8 ）台。

**【问题 3】**工程师小张根据层次化网络设计的思想部署网络设计，在（ 9 ）层设置了大量的访问控制列表，以实现精确的网络访问控制；为了实现用户的 PC 能安全的使用网络，在（ 10 ）层实现 MAC 与 IP 地址绑定，（ 11 ）层完成数据的高速转发。

**【问题 4】**若将防火墙上根据内网 IP 设置出口的策略由路由器来实现，其中 192.168.0.0/25 的数据由 s3/0 转发，其余的由 S3/1 转发，配置如下，请补充完整。

```
access-list 70 permit ip 192.168.0.0 ____（ 12 ）____
access-list 80 permit ip 192.168.128.0  0.0.127.255

route-map Cernet permit  70
match ip address ____（ 13 ）____
set interface Serial3/0
!

route-map Cernet permit 80
match ip address 80
set interface Serial3/1  !
!
```

**试题三、**某企业欲搭建基于 Linux 系统的 Qmail 作为公司的邮件服务器，其安装要求如下：

1．要求新装的服务器在/var/mailbox 下。

2．使用 mail 服务的基本用户组为 Qmail。

**【问题 1】**下列选项中，能创建/var/mailbox 的是（ 1 ），创建 Qmail 用户组的指令是（ 2 ）。

（1）A．mv /var/mailbox　　B．rmdir /var/mailbox

C．cp /var/mailbox　　D．mkdir /var/mailbox

（2）A．addgroup qmail　　B．groupadd qmail

C．add qmail group　　D．group add qmail

**【问题 2】**为了确保 Qmail 的工作正常，可以先检测其 DNS 解析配置是否正常，通常测试命令是（ 3 ）。

（3）A．ping　　B．nslookup

C．tracert　　D．pathping

**【问题 3】**由于近期垃圾邮件特别多，管理员添加了反垃圾邮件网关，为了确保邮件先经过反

垃圾邮件网关检查再交给邮件服务器，进行如下检查：

```
Default Server:  ns.domain.com
Address:  172.28.1.10
>;set type=  ____(4)____

>;domain.com
domain.com MX preference = 10,  mail exchanger = mail.domain.com
mail.domain.com internet address =172.28.1.100
domain.com MX preference =5,  mail exchanger = mail1.domain.com
mail1.domain.com internet address =172.28.1.101
>;exit
```

使用 nslookup 指令检查 DNS 服务器是否能正常地解析邮件服务器，使用>;set type= （ 4 ）。

（4）A．A　　B．MX　　C．PTR　　D．NS

从检查结果来看，下列反垃圾邮件网关的地址中，正确的是（ 5 ）。

（5）A．172.28.1.100　　B．172.28.1.101

C．随意选择这两个地址中的一个　　D．172.28.1.10

**【问题 4】**用户接收电子邮件所使用的在线协议 IMAP 使用的端口是（ 6 ）。

（6）A．25　　B．110　　C．143　　D．随机

**试题四、**某 IT 公司的 Web 服务访问量非常大，因此考虑采用 DNS 负载均衡实现一个高速的 Web 服务器。若公司的域名为 www.mydomain.com，三台服务器的地址分别是 192.168.1.1、192.168.2.1 和 192.168.3.1，并且这三台服务器分别是公司三个部门的部门服务器，以下关于 Windows Server 2003 服务器配置 DNS 负载均衡的过程，根据题意回答下列问题。

**【问题 1】**采用 Windows 默认安装的 DNS 服务器时，进入 DNS 服务器配置的正确步骤是（ 1 ）。

A．执行“开始”→“运行”命令并输入 MMC 启动

B．执行“开始”→“所有程序”→“管理工具”→DNS 命令启动

C．在 Windows Server 2003 系统光盘中双击 dnssetup.exe 图标

D．执行“开始”→“运行”命令并输入 dns.exe 启动

**【问题 2】**要实现这三台服务器的 DNS 负载均衡，下列说法正确的是（ 2 ）。

A．在 mydomain.Com 中创建一个名为 www1 的主机，IP 地址为 192.168.1.1，www2 的主机对应 192.168.2.1，依此类推

B．在 DNS 的“属性-高级”选项中选中 enable round robin 选项

C．在客户端访问时输入 http://www1.mydomain.com 访问 192.168.1.1

D．客户端 DNS 地址必须指定本 DNS 服务器的地址

**【问题 3】**若为了确保每个部门内的主机访问公司域名时，都能对应解析到本部门的部门服务器地址上，则下列操作正确的（ 3 ）。

A．在 DNS 服务器上建立反向地址解析即可

B．在 DNS 的“属性-高级”选项中选中 enable subnet ordering 选项

C．在客户端访问时输入 http：//www.mydomain.com:x，其中的 x 表示自己所在的部门编号

D．客户端 DNS 地址必须指定本 DNS 服务器的地址

**【问题 4】**Windows Server 2003 中，DNS 服务器的区域配置文件默认保存在（ 4 ）中。

A．windows\system32\dns　　B．windows\system\dns

C．windows\server\dns　　D．windows \dns

**试题五、**某 IT 公司为了方便客户下载软件升级包和操作手册，因此建立了 FTP 服务器。请回答以下问题。

**【问题 1】**根据客户的情况，部分客户希望在没有账号的情况下也可以获得下载，则服务器管理员必须开通匿名下载，匿名下载的用户名是（ 1 ）。

A．anonymous　　B．root

C．administrator　　D．guest

**【问题 2】**在公司的 FTP 运行过程中，发现一个名为 aaa 的用户经常使用 172.28.0.0/24 的网段地址大量地下载公司的升级服务包，严重影响 FTP 服务器的性能，管理员若要解决此问题，需要修改的配置文件是（ 2 ），需要添加的内容是（ 3 ）。

（2）A．/etc/ftpusers　　B．/etc/ftpconversions

C．/etc/ftpgroups　　D．/etc/ftpphosts

（3）A．allow aaa 172.28.0.0/24　　B．aaa allow 172.28.0.0/24

C．deny aaa 172.28.0.0/24　　D．aaa deny 172.28.0.0/24

**【问题 3】**若管理员为了便于联系客户，要求每个匿名用户登录时必须输入一个有效的电子邮件地址作为密码，则可以在服务器的/etc/ftpaccess 文件中设置 passwd-check，其中能满足管理员要求的是（ 4 ）。

（4）A．None　　B．Trivial

C．RFC822　　D．In “@”

## 第 5～6 学时　模拟测试 1 点评（上午试题）

上午部分的考试侧重的是基础理论，总的涉及面较广，因此要求考生掌握这些相关知识点的基础理论。本小节给出每道题的详细的分析和解答，供考生进一步掌握。

1．试题解析：

本题考查考生对 CPU 内部基本结构的了解，主要掌握控制单元、运算单元、寄存器等几个主要部分的作用。运算器是计算机对数据进行处理的基本部件，它主要由算术逻辑部件（Arithmetic and Logic Unit，ALU）、寄存器组和状态寄存器组成；CPU 中的寄存器组用来保存操作数和运算的中间结果；控制器是计算机的控制中心，决定了计算机运行过程的自动化。

试题答案：A

2．试题解析：

DMA（Direct Memory Access）是一种不经过CPU、直接从内存存取数据的数据交换模式。PIO模式下硬盘和内存之间的数据传输是由CPU来控制的；DMA模式与PIO模式的最大区别在于，DMA很少依赖CPU。

试题答案：A

3．试题解析：

海明码实际上是一种多重奇偶校验码，其工作原理是：在有效信息位中加入校验位形成海明码，并把海明码的每一个二进制位分配到不同的奇偶校验组中。当某一位出错后，就会引起有关校验位的值发生变化，因此不但可以发现错误，还能指出错误的位置，所以还可以进行纠错。码字之间的海明距离是一个码字要变成另一个码字时必须改变的最小位数。如果一个码字的海明距离为D，则所有小于或等于D-1位的错误都可以被检测出来，而所有小于或等于(D-1)/2位的错误都可以被纠正。所以海明码的码距必须大于1。

试题答案：B

4．试题解析：

高速缓冲存储器Cache位于CPU和内存之间，其目的是尽可能提高CPU读取数据的速率，Cache的特点是容量小、速度快，接近CPU的工作速度。容量相对较大的Cache的命中率会相应提高，但容量过大，成本会提高很多，因此关键是要保证Cache中数据的命中率。

当CPU访问内存时，它首先访问Cache，检查所需要的数据或指令是否在Cache中，若在，则说明可以从Cache中找到需要的数据或指令，称为命中；若不在，则称为未命中，需要从内存中读取。若CPU需要的指令或数据在Cache中，则不需要等待，Cache可以将信息传送给CPU，同时在Cache中拷贝一份副本。已备CPU以后再访问同一信息时又会出现不命中的情况，从而尽量降低CPU访问内存的概率。因此，CPU访问Cache的命中率越高，系统性能就越好。

试题答案：B

5．试题解析：

面向对象开发方法有Coad方法、Booch方法和OMT方法等。

（1）Booch方法：最先描述了面向对象的软件开发方法的基础问题，指出面向对象开发是一种完全不同于传统的功能分解的设计方法。

（2）Coad方法：其主要优点是通过大量大系统开发的经验与面向对象概念的有机结合，在对象、结构、属性和操作的认定方面制定了一套系统的原则。该方法完成了从需求角度进一步进行类和类层次结构的认定。

（3）OMT方法：是一种新兴的面向对象的开发方法，开发工作的基础是对真实世界的对象建模，然后围绕这些对象使用分析模型来进行独立于语言的设计，面向对象的建模和设计促进了对需求的理解，有利于开发更清晰、更容易维护的软件系统。

（4）UML：统一了Booch方法、OMT方法、OOSE方法的表示方法，并且对其做了进一步的发展，最终统一为大众接受的标准建模语言。

试题答案：D

6．试题解析：

这是考查程序设计的基本知识，要求考生对结构化程序设计中的三种基本结构的作用有所了解，本题是考控制结构的作用。

试题答案：B

7．试题解析：

集成测试是对源代码实现的每一个程序单元进行测试，检查各个程序模块是否正确地实现了规定的功能。集成测试把已测试过的模块组装起来，主要对与设计相关的软件体系结构的构造进行测试。确认测试则是要检查已实现的软件是否满足了需求规格说明中确定了的各种需求，以及软件配置是否完全、正确。

试题答案：D

8．试题解析：

要特别注意的是系统软件除了操作系统之外，还有编译程序和数据库管理系统软件这一类系统软件。

试题答案：B

9．试题解析：

本题主要考察《中华人民共和国著作权法》。根据《中华人民共和国著作权法》的第2条："中国公民、法人或者非法人单位的作品，不论是否发表，依照本法享有著作权"和第12条："改编、翻译、注释、整理已有作品而产生的作品，其著作权由改编、翻译、注释、整理人享有，但行使著作权时，不得侵犯原作品的著作权"的规定可以断定，该编辑自2011年5月1日起享有译文的著作权。

但是2011年10月1日后，该译文被定为官方正式译文，而根据《中华人民共和国著作权法》第5条第1款规定"本法不适用于：（一）法律、法规，国家机关的决议、决定、命令和其他具有立法、行政、司法性质的文件，及其官方正式译文"，此时，由于国家的法律、法规及其官方正式译文的著作权不能归个人所有，故自2011年10月1日后，该编辑不再享有译文的著作权。正确答案应该为C。

试题答案：C

10．试题解析：

在Windows系统中，通常由于hosts文件中会指定127.0.0.1对应的主机名是localhost，因此本机地址可以是127.0.0.1和localhost。但是要注意，B选项中的空格是不对的。

试题答案：A

11～12．试题解析：

T1的一个时分复用帧划分为24个相等的时隙，其中23个时隙用于传输数据，1个时隙用于传输控制信令，每个基本帧之间增加1bit的间隔，因此每个时隙传送的bit为24*8+1=193bit。

试题答案：C、C

13．试题解析：

考查考生是否对常用的服务的访问情况和流量情况有所了解，我们知道，日常应用中的 DNS 服务和 OA 服务数据交换频繁，但流量相对较小，实时性要求不高；VOD 服务数据负担重，实时性要求高。

试题答案：D

14．试题解析：

通过编码之后，每传输 10 个 bit，其中有效的只有 8 个，因此效率是 8/10×100%=80%，即 0.8。

试题答案：C

15．试题解析：

运行生成树协议的交换机时，每个端口总是处于 STP 协议规定的四个状态中的一个。在正常工作状态下，端口总处于转发或阻塞状态。只有当网络拓扑结构变化时，交换机才会使端口暂时处于监听和学习状态。STP 协议中规定的端口的基本状态如下：

监听状态：不转发，检测 BPDU。

学习状态：不转发，学习 MAC 地址表。

转发状态：转发和接收数据。

阻塞状态：不转发，接收 BPDU。

试题答案：D

16．试题解析：

在广播地址中有两类：直接广播地址就是在标准的有类（A、B、C 三类）地址中，主机号全为 1 的；受限广播地址是 IP 地址所有 bit 全部是 1 的，也就是 255.255.255.255。

试题答案：D

17～18．试题解析：

标准 PCM 调制中，每一路语音信号的速度是 64kb/s，采样频率是 8000Hz，每个采样若用 128 级量化，则说明各个状态可以用 7 个 bit 来表示。而采样频率还是 8KHz，因此该信号的速率是 7×8=56kb/s。

试题答案：B、C

19～20．试题解析：

网络中电信号的传输速度在计算时可以使用常数 200000km/s 计算，则总时间=发送时间+传播时间=1000×8 /9600+500/200000=833ms+2.5ms=835.5ms。

卫星信道传输信息的过程中，不管两个站点之间的地面直线距离是多少，其传播时延也是常数（270ms）。从题目可知，数据帧长度为 1000×8=8000 比特，卫星信道的数据传输速率为 512kb/s，可计算出其传输时延为 15.63ms，所以总时间为 15.63ms+270ms=285.63ms。

试题答案：C、C

21．试题解析：

“>”表明正处于用户 EXEC 模式中，“#”表示正处于特权 EXEC 模式中或全局配置模式。而

show 指令必须是在特权模式之下，因此 B 正确，“%”和“@”是无效的提示符。

试题答案：B

22．试题解析：

测试某个 TCP 服务是否开启，其实只要检测这个服务对应的 TCP 端口是否有响应即可，通常可以使用“Telnet IP 服务端口”的形式看是否可以建立 TCP 连接，若可以建立，则说明服务是正常的。本题中的其他命令都是用于测试网络层信息的。

试题答案：A

23．试题解析：

如果目的 MAC 地址在 MAC 地址表中，单播流量只会转发到指定端口。但是为了维持 2 层设备的透明性，所有广播类型和未知单播类型的数据包总是向所有端口转发。

答案：C

24～25．试题解析：

OSPF 协议采用了分层路由的设计思想，可以将网络分割成由一个“主干”部分连接的一组相互独立的小网络，其中每个小网络都被称为“区域”(Area)。在配置过程中，通常使用 area 0.0.0.0 来表示主干区域。为了解决部分区域不能直接连接主干区域的问题，可以通过虚连接的形式建立通信。

试题答案：A、D

26．试题解析：

从图 3 的 MPLS VPN 结构可以看出，与用户端连接 CE，CE 连接 PE。

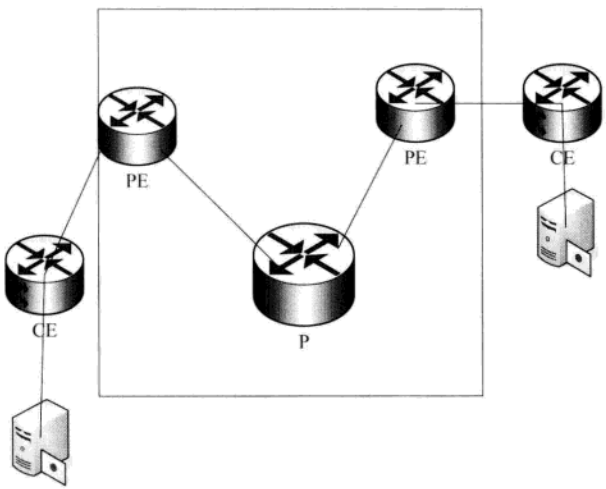



图 3　MPLS VPN 示意图

试题答案：A

27～29．试题解析：

作为网络工程师，对基本的网络管理命令及其参数必须要掌握，如 ipconfig、route 等。在实际应用中，必须让 IP 地址与默认网关在同一个 IP 网段才能让计算机连接到外网。本题中，从 ipconfig 可以看到主机的 IP 地址与默认网关的地址不在同一个网段，因此只有 B 是正确的，而不能上网的原因则是 A。

试题答案：A、B、A

30～31．试题解析：

要使配置立即生效，只要重启进程即可，因此可以先结束进程，然后再重新启动该服务进程。结束进程可以使用 kill 进程号实现。

作为系统的第一个进程，init 的进程 ID（PID）为 1。它将完成系统的初始化工作，并维护系统的各种运行级别，包括系统的初始化、系统结束、单用户运行模式和多用户运行模式。

试题答案：B、C

32．试题解析：

serial 0 is up 说明物理层基本正常；line protocol is down 表明数据链路层可能故障。因此答案选 A。

试题答案：A

33．试题解析：

Linux 操作系统中，网络管理员可以通过修改 lilo.conf 文件对系统启动进行配置。

试题答案：C

34．试题解析：

/etc/passwd 文件记录了用户的基本属性，但是由于该文件所有用户可读，因此安全性不高，安全性较高的系统通常把加密后的口令字分离出来，单独存放在/etc/shadow 文件中。该文件只有 Root 用户才能访问，因此可以选择 B。

试题答案：B

35～36．试题解析：

从题目可以看出，显示的是系统建立网络连接的情况，因此是使用了 netstat 指令。从题中显示的信息可以知道远程主机的端口是 80，所以是访问 Web 服务。

试题答案：D、A

37．试题解析：

Microsoft 管理控制台 （MMC） 集成了用来管理网络、计算机、服务及其他系统组件的管理工具。可以使用 Microsoft 管理控制台 （MMC） 创建、保存并打开管理工具（称为“管理单元”），这些管理工具用来管理 Windows 系统的硬件、软件和网络组件。

试题答案：D

38．试题解析：

独立冗余磁盘阵列（Redundant Array of Independent Disks，RAID）技术是一种用多个较小的磁盘替换单一的大容量磁盘，并通过合理地在多个磁盘上存放数据以提高系统的I/O性能。

RAID中共分以下几个级别：

（1）RAID 0级（无冗余和无校验的数据分块）：具有最高的I/O性能和最高的磁盘空间利用率，但系统的故障率高，属于非冗余系统。

（2）RAID 1级（磁盘镜像阵列）：由磁盘对组成，每一个工作盘都有其对应的镜像盘，上面保存着与工作盘完全相同的数据拷贝，具有最高的安全性，但磁盘空间利用率只有50%。

（3）RAID 2级（采用纠错海明码的磁盘阵列）：采用了海明码纠错技术，用户需增加校验盘来提高可靠性，在大量数据传输时，I/O性能较高，但不利于小批量数据传输。

（4）RAID 3级和RAID 4级（采用奇偶校验码的磁盘阵列）：把奇偶校验码存放在一个独立的校验盘上。如果有一个盘失效，其数据可以通过对其他盘上的数据进行异或运算得到。读数据很快，但写入数据时要计算校验位，速度较慢。

（5）RAID 5级（无独立校验盘的奇偶校验码磁盘阵列）：没有独立的校验盘，校验信息分布在组内所有盘上，对于大批量和小批量数据的读写性能都很好。

试题答案：A

39．试题解析：

xDSL是DSL（Digital Subscriber Line）的统称，是以电话线为传输介质的点对点传输技术。在小型公司员工上网和提供公司Web服务器要求上传和下载的速度都要高，因此对称的线路技术是首选。通常的DSL技术中，不对称传输包括ADSL（非对称数字用户环路）、VDSL（甚高速数字用户环路）、RADSL（速率自适应数字用户线路）、G.LITE（通用ADSL）等；而支持对称传输包括HDSL（高比特率数字用户线路）、SDSL、MDSL（多速率数字用户线路）、和G.SHDSL（单对高速数字用户线）等。因此正确答案选择D。

试题答案：D

40．试题解析：

匿名FTP专用的用户名为anonymous，可以使用自己的电子邮件地址或任意字符作为密码均可。

试题答案：D

41．试题解析：在Windows Server 2003的Web服务器安装过程中，若需要使用SSL协议，必须先申请数字证书。

试题答案：A

42．试题解析：

现代反病毒软件公司为了方便管理，通常按照病毒的特性将病毒进行分类命名。利用病毒名来表明一个病毒的家族特征，尽管不同的反病毒公司的命名规则不完全一样，但基本采用比较统一的命名方法来命名。

命名一般格式为：<病毒前缀>.<病毒名>.<病毒后缀>

系统病毒的前缀为Win32、Win95、W32、W95等。这些病毒一般共有的特性是可以感染Windows操作系统的 *.exe 和 *.dll 文件，并通过这些可执行文件进行传播。

蠕虫病毒的前缀是Worm，通常是通过网络或系统漏洞进行传播。

木马病毒其前缀是Trojan，木马病毒的共有特性是通过网络或系统漏洞进入用户的系统并隐藏，然后向外泄露用户的信息。

宏病毒的前缀是Macro，通常感染Office文档。

试题答案：C

43.试题解析：

IOS中的ACL有两类，分别是标准ACL和扩展ACL。其中标准ACL是通过使用IP包中的源IP地址进行过滤，其编号从1到99；扩展ACL是基于源地址、目标地址、协议等参数进行控制的，其编号为100到199。

配置ACL时要注意以下两个基本规则：

（1）最靠近受控对象原则。

ACL在检查规则时是采用自上而下在列表中逐条检测的，只要发现符合条件的立刻执行，而不继续检测后面的语句。因此必须要先指定最小的范围（如主机），然后才是网段。

（2）默认丢弃原则。

在ACL中默认的最后一句是DENY ANY，也就是丢弃所有不符合条件的数据包。当然可以修改这个默认规则。

因此本题中的选项D显然不正确。

试题答案：D

44～46．试题解析：

认证中心（Certificate Authority，CA）是网络活动中负责发放和管理数字证书的权威机构，并作为交易中受信任的第三方，承担公钥体系中公钥的合法性检验。CA为每个用户发放一个数字证书，该证书的作用是证明证书中列出的用户合法拥有证书中列出的公开密钥。CA的数字签名使得攻击者不能伪造和篡改证书。如用户通过CA的签名来验证证书的合法性，从而确认拥有该证书的网站的合法性。在用户与网站进行安全通信时，用户可以通过证书中的公钥进行加密和验证，该网站通过网站的私钥进行解密和签名。

试题答案：A、B、C

47．试题解析：

IPsec体系中，两个主要的协议是认证头（Authentication Header，AH）和封装安全载荷（Encapsulating Security Payload，ESP），其中AH主要为IP数据报提供完整性检查与数据源认证，并可以有效防止重放攻击；ESP则主要提供加密服务。可以实现数据内容的加密，根据具体的安全需求，既可以用于加密IP数据报中的内容部分（不包含IP头），也可以用于加密整个IP数据报。

试题答案：D

48．试题解析：

目前国内网上银行的支付页面基本都采用 SSL 协议，其标准访问格式为 https://ip 或域名。

试题答案：D

49～50．试题解析：

CIDR 是一种将网络合并的技术其作用就是把小的网络汇聚成大的网段。题中的 222.169.0.0/24～222.169.7.0/24 这个地址块中，可以看到其网络位占 21 位，主机位占 11 位，子网掩码为 255.255.248.0。

222.169.0.0:11000000 00011000 00000 000 00000000

222.169.7.0:11000000 00011000 00000 111 00000000

其中排除掉各网段的全 0 全 1 地址，则 254×8=2032。

试题答案：B、A

51．试题解析：

路由汇聚算法的实现过程如下：

假设有 4 个路由：192.168.12.0/24、192.168.13.0/24、192.168.14.0/24、192.168.15.0/24，如果这 4 个路由进行路由汇聚，则能覆盖这 4 个路由的是 192.168.12.0/22。具体算法为：12 的二进制代码是 00001100，13 的二进制代码是 00001101，14 的二进制代码是 00001110，15 的二进制代码是 00001111。这 4 个二进制数的前 6bit 相同，都是 000011。根据最大匹配原则可知，加上前面的 192.168 这两部分相同的位数，网络位就是 8+8+6=22bit。而 00001100 的十进制数是 12，所以汇聚的 IP 地址就是 192.168.12.0。

试题答案：B

52．试题解析：

某公司网络的地址是 210.43.192.0/18，划分成 10 个子网，则需要继续从主机位中拿出 4bit（$2^4$=16）进行划分。则这 16 个子网地址分别为：

210.43.11000000 0

210.43.11000100 0

210.43.11001000 0

210.43.11001100 0

……

210.43.11111100 0

其中不包括 210.43.254.0/22。

试题答案：D

53．试题解析：

要在一个 URL 中使用 IPv6 文本地址，则必须用符号“[”和“]”来引用。例如本题中服务器的 IPv6 地址写成 URL 的标准形式就是 http://[ FEDC:BA99:8888:7777:6666:5555:4444:3333]:80/index.html。

试题答案：A

54．试题解析：

（1）地址长度由原来的32位扩充到128位，容量大大地扩展了。

（2）大容量的地址空间能够真正地实现无状态地址自动配置，IPv6 终端能够无需人工配置，直接连接到网络上实现即插即用。

（3）报头格式大大简化，从而极大地减少路由器或交换机对报头的处理开销，提高效率。

（4）加强了对扩展报头和选项部分的支持，能支持更多的新应用。

（5）流标签能够为数据包所属类型提供个性化的服务，并保障业务的服务质量。

试题答案：D

55．试题解析：

IPv6地址中，每个16位分组中的前导零可以做简化表示，但必须保证每个分组至少保留一位数字。本题中的地址去除前导零位后可写成20F1:D3:0:2F3B:F3A:FF:FE28:8731。

某些地址中可能包含很长的零序列，为进一步简化表示，还可以将冒号十六进制格式中相邻的连续零位进行合并，用双冒号“::”表示。但是“::”符号在一个地址中只能出现一次，该符号可以用来压缩表示地址中相邻的连续零位。

试题答案：C

56．试题解析：

ADSL采用离散多音频（DMT）技术，将原来电话线路的1.1MHz频段以下的带宽划分成256个子频道。其中，4KHz以下频段保留给传统电话业务，而20KHz到138KHz的频段用来传送上行信号，138KHz到1.1MHz的频段用来传送下行信号。DMT技术可根据线路的情况自动调整在信道上所调制的比特数，可以更充分地利用线路。因此ADSL可达到最大上行640kb/s、下行8Mb/s的数据传输率。

试题答案：C

57．试题解析：

SNMP一共定义了5种不同功能的PDU，用于管理进程和代理之间的数据交换，其中get-request可以从代理进程处提取一个或多个数值，get-next-request从代理进程处提取当前参数值的下一个参数值，set-request设置代理进程的参数值，get-response返回参数值，trap代理进程主动发出的报文，通知管理进程有某些事件发生。其中前面三个操作是响应操作，由管理进程向代理进程发出的，后面的2个操作是代理进程发给管理进程的。

试题答案：D

58．试题解析：

本题考查考生对单臂路由概念的理解，在只有一个接口的路由器上要实现多个VLAN路由，则应该使用子接口形式，也就是常称的单臂路由。

试题答案：B

59．试题解析：

交换机配置状态与转换命令。

（1）用户模式：登录到交换机时就会自动进入该模式，此时只能运行一些简单指令。

（2）特权模式：此模式下的命令非常丰富，命令集包含用户模式下的大部分命令，而且能进行检查配置文件、重新启动交换机等特权操作。

（3）全局配置模式：配置交换机全局特性的模式。

（4）子配置模式：单独针对某个特殊的进程或接口进行配置的模式。

试题答案：C

60．试题解析：

本题考的是VLAN基础概念，也就是VLAN的唯一标识VLAN ID的长度是12bit，故网络中最多能支持2^12个不同的VLAN。

试题答案：A

61．试题解析：

IEEE 802.3标准所采用的CSMA/CD协议虽然无法完全避免冲突，但可以通过精心设计的监听算法来缓解，其中非坚持型监听算法无法在第一时间获得空闲的总线，效率较低。坚持型算法会一直坚持监听信道，直到获得空闲的信道为止，因此可以及时抢占信道，提高利用率。但有两个以上主机同时监听到信道空闲时则一起发送，不能减低线缆的空闲，通常会选择一个合适的发送概率P，由P来决定抢占空闲信道之后是否立即发送数据，这就是P坚持算法。

试题答案：D

62．试题解析：

本题考查对ipconfig基本参数的掌握。all表示显示ip配置有关的所有信息，release表示释放原来的IP地址，renew续借IP地址，ipconfig/flushdns删除DNS缓存内容。

试题答案：B

63．试题解析：

从ARP的工作原理可知，在用户A与默认网关之间，尽管ping时显示time out，但是从arp表可知，在用户A的主机中已经有默认网关的IP和MAC的对应关系。说明用户A的主机与默认网关之间至少来回通信过一次。因此选C。

试题答案：C

64．试题解析：

RAID5把数据和生成的奇偶校验信息存到RAID的每个磁盘上，并且校验信息和相对应的数据分开存放在不同的磁盘上，能保证其中任意N-1块磁盘上都有完整的数据，一旦RAID5的任意一个磁盘出现故障后，通过其他的N-1个磁盘RAID可以自动重建数据。

试题答案：B

65．试题解析：

802.3的CSMA/CD协议中，定义最短帧长的目的就是要保证CSMA/CD协议能正常工作。因此对于数据长度较短的帧，通过填充信息的形式使其满足最短帧长。在以太网中设定的最短帧长是

64字节，因此信息的最少长度要保持在64-18=46字节以上。

试题答案：D

66．试题解析：

综合布线系统通常由工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群主干子系统6个部分组成。

（1）工作区子系统：是连接用户终端设备到信息插座之间的子系统，简单地说就是指电脑和墙上网线插口之间的部分。

（2）水平子系统：是连接工作区与主干的子系统，简单来说就是指从楼层弱电井里的配线架到每个房间的墙上网线插口之间的部分，由于其布线是在天花板上，与楼层平行，所以叫水平子系统。

（3）管理子系统：就是对布线电缆进行端接及配置管理的部分。

（4）干线子系统：是用来连接管理间和设备间的子系统。简单来说就是将接入层交换机连接到汇聚层或核心层交换机的网络线缆，因为其往往在大楼的弱电井里面垂直上下，因此称为垂直子系统。

（5）设备间子系统：是安装在设备间内的子系统，或者说是大楼中集中安装设备的场所。

（6）建筑群主干子系统：是用来连接园区内不同楼群之间的子系统，因为这一部分在户外，也称为户外子系统。通常包括地下管道、直埋沟、架空线三种方式。

试题答案：D

67．试题解析：

交叉线适合连接两种相同性质的设备，本题的4个选项中，只有D是正确答案。尽管有些交换机能够识别连接线缆的类型，不管是直连线还是交叉线都可以使用，但是本题中给出的是根据EIA/TIA-568标准规定最适合的。

试题答案：D

68．试题解析：

常用备份设备包括磁盘阵列、光盘塔、光盘库、磁带机、磁带库、光盘网络服务器等。

试题答案：D

69．试题解析：

通常，网络结构分为接入层、汇聚层和核心层。

（1）接入层：提供网络基本接入功能，如基本的二层交换、安全认证、QoS标记等功能。

（2）汇聚层：汇聚来自接入层的流量并执行流分类、QoS策略、负载均衡、快速收敛等；

（3）核心层：网络的最核心部分，往往提供高速数据转发和快速路由，要求有高的可靠性、稳定性和可扩展性。

试题答案：B

70．试题解析：

网络系统设计过程分为五个步骤：

（1）需求分析。

确认需求分析说明书，清楚并细致地了解和总结单位及个人的需求、意愿，但不涉及提供建议解决方法和设计方案的问题。

（2）分析现有网络。

分析阶段是需求收集阶段的有意补充，分析网络现在处于什么阶段。

（3）逻辑网络设计。

逻辑网络设计阶段描述用户需求的网络行为和性能，详细说明数据是如何在网络上传输的，但并不涉及网络元素的物理位置。

（4）物理网络设计。

物理网络设计阶段体现如何根据逻辑网络设计的意图，确定具体的软件、硬件、连接设备、服务和布线等。

（5）安装和维护。

安装和维护阶段需要完善文档，如更新最后修改过的网络图，清晰标记的线缆、连接器和设备，以及整理所有能为以后的维护和纠错带来方便的记录和文档，如测试结果和数据流量记录等。

试题答案：A

71～75．试题解析：

略。

试题答案：

（71）B（72）A（73）B（74）B（75）D

## 第7～8学时　模拟测试1点评（下午试题）

**试题一：**

【问题1】试题解析：

本题是网络工程师考试的基本配置题。除了基本的VLAN、STP、RIP、OSPF、ACL配置之外，还需要注意VPN的配置。

试题答案：

（1）2500000　　（2）255.255.255.252　　（3）any any 4.ip 5.110 in

【问题2】试题解析：

由于此企业网与ISP之间使用/30的掩码，ISP端的地址是61.187.55.33/30，按照IP子网的计算，与此IP地址在同一子网的可用IP是61.187.55.34/30。

试题答案：B

【问题3】试题解析：

运营商与用户之间的连接使用/30的掩码主要就是为了节省运营商宝贵的IP地址。

试题答案：A

【问题4】试题解析：

RIP由于其16跳的路由跳数限制，只适合小型的网络，OSPF是一种链路状态的路由协议，通过分区可以实现较大规模的网络使用，本题中OSPF是较好的选择。

试题答案：B

**试题二**

【问题1】试题解析：

根据题目给出的距离和主干链路的速度，可知2必须使用单模光纤，其余都用多模光纤即可。

试题答案：B、A、B

【问题2】试题解析：

Switch 1处于教学区汇聚层位置，可以使用1000Mb/s光电自适应接口；Switch 2位于服务区，但是dhcp服务器是1000Mb/s的网卡，因此也要求使用1000Mb/s光电自适应接口交换机；Switch 3属于接入层，用接入层交换机。办公区22台计算机中至少要使用1台24端口的接入层交换机。

试题答案：1、1、2、2、1

【问题3】试题解析：

层次化网络设计的思想中，汇聚层用于做访问控制策略，接入层完成基本接入控制，核心层完成数据的高速转发。

试题答案：汇聚层、接入层、核心层

【问题4】试题解析：

策略路由基本配置题。

试题答案：0.0.127.255、70

**试题三**

【问题1】试题解析：

本题考查考生对Linux服务器的基本系统管理指令的了解，建立目录的操作和创建用户、用户组等命令，同时也考查考生对服务器的配置过程是否熟悉。本题中创建目录使用mkdir，添加用户组使用group add即可。

试题答案：D、B

【问题2】试题解析：

检查DNS解析是否正常可以使用nslookup。通过nslookup可以了解DNS服务器关于域名的详细配置信息，如MX记录的设置、MX的优先级设置等。nslookup是一个检查DNS的专用工具。实际应用中有一种简单的方式检查DNS服务器能否解析，就是ping域名的方式，但是该方式不能了解详细的DNS设置信息。

试题答案：B

【问题3】试题解析：

nslookup指令中可以通过set type=x指令指定要查询的域名上某种类型记录的设置情况，本题中查询邮件服务器的邮件交换记录，也就是MX记录，因此选B。而从检查的结果可以看到

MX preference = 10，address =172.28.1.100，MX preference =5，address =172.28.1.101，因此可以知道邮件是先发给 172.28.1.101，也就是这个地址是反垃圾邮件网关的地址。

试题答案：B、B

【问题 4】试题解析：

邮件接收有两个协议：pop3 和 Imap4，使用的端口分别是 110 和 143。

试题答案：C

**试题四**

【问题 1】试题解析：

本题是基本操作题，正确的步骤是执行“开始”→“所有程序”→“管理工具”→DNS 命令启动。

试题答案：B

【问题 2】试题解析：

本题考查考生对 DNS 负载均衡的概念理解和配置方法的掌握。Windows Server 2003 DNS 服务器配置中，要显示 DNS 负载均衡，只要在域中多次新建一个名为 www 的主机，对应多个不同的 IP 地址，并且在 DNS 的“属性-高级”选项中选中 enable round robin 选项即可实现，在客户端只要直接输入公司域名即可分别轮流地访问这三台服务器上的内容，当然这三台服务器的 Web 的内容要是一致的。

试题答案：B

【问题 3】试题解析：

DNS 的高级选项中，有一项可以针对子网的解析设置的，即 enable subnet ordering，确保每个子网解析同一个域名时，解析到自己所在子网的对应服务器。

试题答案：B

【问题 4】试题解析：

Windows Server 2003 中 DNS 服务器的区域配置文件是一个普通文本文件，默认情况下保存在 windows\system32\dns 文件夹中。

试题答案：A

**试题五**

【问题 1】试题解析：

本题考查有关 FTP 的基本常识，也就是匿名用户的账号。FTP 中的匿名账号就是 anonymous，密码可以是用户的邮箱或任意字符。

试题答案：A

【问题 2】试题解析：

/etc/ftpusers：用于限制用户是否可以通过 FTP 登录服务器，因此可以将需要禁止的用户账号写入文件。

/etc/ftpconversions：用来配置压缩/解压缩程序。

/etc/ftpgroups：创建用户组，预先定义哪些成员可以访问 FTP 服务器。

/etc/ftpphosts：用来设置禁止或允许的远程主机对特定账户的访问，因此选择 D。

Ftphosts 文件中使用的规则的基本格式是：

Allow/deny　username　　ip/mask

分别表示允许或禁止某个用户名从某个 IP 网段登录服务器。因此本题中的进制用户 aaa 从 172.28.0.0 的网段登录，则可以选择 C。

试题答案：D、C

【问题 3】试题解析：

/etc/ftpaccess 文件中对 passwd-check 的基本格式：passwd-check (type) warn

此配置用于对匿名用户的密码使用方式进行检查，其中(type)有三种取值，分别是 None、Trivial 和 RFC822。其中 None 表示将不对口令做任何检查；Trivial 表示口令中至少要有一个@符号，但不检查其是否是一个合法的邮件地址；而 RFC822 则要求 E-mail 地址必须严格遵守 RFC822 报文标题标准，也就是必须是合法的邮件地址格式。因此选择 C。

试题答案：C

# 后记

完成“5天修炼”后，您感受如何？是否觉得更加充实了？是否觉得意犹未尽？这5天的天学习并不能保证您100%通过考试，但可以让您心中倍感踏实。基于此，还想再啰嗦几句，提出几点建议供参考：

（1）做历年的试题，做完网络工程师考试的，可以接着做网络规划设计师的（除论文考试），因为这两个不同级别考试的基础知识和案例分析可以相互借鉴。

（2）该背的背，该记的记，如果可以整本书都背下来。

（3）多做题，做历年试题是确保通过考试的重要手段。

（4）经济条件许可的情况下，参加辅导培训，这并不是广告，而是最好的建议，良师益友，可以少走很多弯路。

最后，再祝“准网工”们一声：“祝您顺利过关”，通过了记得发个邮件给老师报个喜。

# 附录一　网络工程师考试常考公式、要点汇总表

- 码元：在数字通信中常用时间间隔相同的符号来表示一位二进制数字，这样的时间间隔内的信号称为二进制码元。
- 码元速率（波特率）：即单位时间内载波参数（相位、振幅、频率等）变化的次数，单位为波特，常用符号 Baud 表示，简写成 B。
- 比特率（信息传输速率、信息速率）：是指单位时间内在信道上传送的数据量（即比特数），单位为比特每秒（bit/s），简记为 b/s 或 bps。
- 波特率与比特率有如下换算关系：

比特率=波特率×单个调制状态对应的二进制位数=波特率× $\log_2^N$，其中 N 是码元总类数。

- 信道带宽 W=最高频率-最低频率
- 信噪比与分贝关系 1dB=10× $\log_{10}$ S/N
- 无噪声情况下，数据速率依据尼奎斯特定理计算：

$$\text{最大数据速率}=2W\log_2 N=B\log_2 N$$

其中，W 是带宽，B 是波特率，N 是码元总的种类数。

- 有噪声情况下，数据速率依据香农公式计算：

$$\text{极限数据速率}=\text{带宽}\times\log_2(1+S/N)$$

其中，S 是信号功率，N 是噪声功率。

- 误码率：是指接收到的错误码元数在总传送码元数中所占的比例。

$$P_C=\frac{\text{错误码元数}}{\text{码元总数}}$$

- 异步通信数据速率=每秒钟传输字符数×(起始位+终止位+校验位+数据位)

- 异步通信有效数据速率=每秒钟传输字符数×数据位
- E1 的一个时分复用帧（其长度 T=125us）共划分为 32 相等的时隙，每秒传送 8000 个帧，因此 PCM 一次群 E1 的数据率就是 2.048Mb/s。
- T1 系统共有 24 个语音话路，每个时隙传送 8bit（7bit 编码加上 1bit 信令），因此共用 193bit（192bit+1bit 帧同步位）。每秒传送 8000 个帧，因此 PCM 一次群 T1 的数据率=8000×193b/s＝1.544Mb/s
- E1 和 T1 可以使用复用方法，4 个一次群可以构成 1 个二次群（称为 E2、T2）。
- SONET 和 PCM 都是每秒钟传送 8000 帧，STS-1 的帧长为 810 字节，因此基础速率为 8000×810×8=51.84Mb/s。
- SONET 中 OC-1 为最小单位，值为 51.84Mb/s，OC-N 则代表 N 倍的 51.84Mb/s。
- STM-1 速率为 155.2Mb/s，与 OC-3 速率相同，STM-N 则代表 N 倍的 STM-1。
- 一帧包含 m 个数据位（报文）和 r 个冗余位（校验位）。假设帧总长度为 n，则有 n=m+r。包含数据和校验位的 n 位单元通常称为 n 位码字（codeword）。
- 海明码距（码距）：两个码字中不相同的位的个数。
- 两个码字的码距：一个编码系统中任意两个合法编码（码字）之间不同的二进制位数。
- 编码系统的码距：整个编码系统中任意两个码字的码距的最小值。
- 为了检测 d 个错误，则编码系统码距≥d+1；为了纠正 d 个错误，则编码系统码距>2d。
- 设海明码校验位为 k，信息位为 m，则它们之间的关系应满足 $m+k+1 \leqslant 2^k$。
- 以太帧头长 18 个字节，以太帧的数据字段最长为 1500 字节，以太网最小帧长为 64 字节。
- MAC 地址为 48 位，前 24 位是厂商编号。
- 以太网规定了帧间最小间隔为 9.6μs。
- 电磁波在 1km 电缆传播的时延约为 5μs。
- 冲突检测最长时间为两倍的总线端到端的传播时延（2τ），2τ 称为争用期（contention period），又称为碰撞窗口。
- 10Mb/s 以太网争用期为 51.2μs。对于 10Mb/s 网络，51.2μs 可以发送 512bit 数据，即 64 字节。
- 以太网规定 10Mb/s 以太网最小帧长为 64 字节，最大帧长为 1518 字节（如果还带有 4 个字节的 VLAN 标签，则应该是 1522 字节），最大传输单元（MTU）为 1500 字节。小于 64 字节的都是由于冲突而异常终止的无效帧，接收这类帧后应该丢弃（千兆以太网和万兆以太网的最小帧长为 512 字节）。
- 最小帧长=网络速率×2×(最大段长/信号传播速度+站点延时)，往往站点延时为 0。
- 吞吐率：单位时间实际传送数据位数。

吞吐率=帧长/(传输数据帧所花费的时间+1 帧发送到网络所花费的时间)=帧长/(网络段长/传播速度+1 帧长/网络数据速率)

- 网络利用率=吞吐率/网络数据速率

- 强化碰撞：当发生碰撞时，发送数据的站除了立刻停止发送当前数据外，还需要发送 32bit 或 48 比特的干扰信号（Jamming Signal），所有站都会收到阻塞信息（连续几个字节的全 1）。
- 快速以太网（Fast Ethernet）：快速以太网的最小帧长不变，数据速率提高了 10 倍，所以冲突时槽缩小为 5.12μs。以太网计算冲突时槽的公式为

$$slot \approx 2S/0.7C+2tphy$$

其中，S 表示网络的跨距（最长传输距离），0.7C 为 0.7 倍光速（信号传播速率），tphy 是发送站物理层时延，由于往返需要通过站点两次，所以取其时延的两倍值。

- IP 报头固定长度为 20 字节。
- A 类地址范围：1.0.0.0～126.255.255.255。
- 10.X.X.X 是私有地址。
- 127.X.X.X 是保留地址，用做环回（Loopback）地址。
- B 类地址范围：128.0.0.0～191.255.255.255。
- 172.16.0.0～172.31.255.255 是私有地址。
- 169.254.X.X 是保留地址。
- C 类地址范围：192.0.0.0～223.255.255.255。
- 192.168.X.X 是私有地址。地址范围：192.168.0.0～192.168.255.255。
- D 类地址范围：224.0.0.0～239.255.255.255。
- E 类地址范围：240.0.0.0～247.255.255.255。
- 早期 IP 地址结构为两级地址：IP 地址::={<网络号>,<主机号>}。
- RFC 950 文档发布后，增加一个子网号字段，变成三级网络地址结构。
  IP 地址::={<网络号>,<子网号>,<主机号>}
- 子网能容纳的最大主机数=$2^{\text{主机位}}-2$
- 子网范围=[子网地址]～[广播地址]
- IPv6 地址为 128 位长，但通常写作 8 组，每组为 4 个十六进制数的形式。
- IPv6 全球单播地址最高位为 001（二进制）。
- IPv6 链路本地单播地址起始 10 位固定为 1111111010（FE80::/10）。
- IPv6 地区本地单播地址起始 10 位固定为 1111111011（FE8C::/10）
- IPv6 组播分组的前 8 比特设置为 1，十六进制值为 FF。
- TCP 的头部长度为 20 字节。
- 传输层系统端口取值范围为[0,1023]
- 传输层登记端口取值范围为[1024,49151]
- 传输层客户端使用端口[49152,65535]
- 假定 SNMP 网络管理中，轮询周期为 N，单个设备轮询时间为 T，网络没有拥塞，则

$$\text{支持的设备数 } X=\frac{\text{轮询周期为 N}}{\text{单个设备轮询时间为 T}}$$

- MTTF、MFBF、MTTR 三者之间的关系：MTBF= MTTF+ MTTR
- 失效率：单位时间内失效元件和元件总数的比率，用 λ 表示，MTBF=1/λ
- 可靠性和失效率的关系 $R=e^{-\lambda}$
- 可靠性和失效率的计算如下表：

| | 可靠性 | 失效率 |
|---|---|---|
| 串联系统 | $\prod_{i=1}^{n} R_i$ | $\sum_{i=1}^{n} \lambda_i$ |
| 并联系统 | $R = 1 - \prod_{i=1}^{n} (1 - R_i)$ | $\frac{1}{\frac{1}{\lambda} \sum_{j=1}^{n} \frac{1}{j}}$ |
| 模冗余系统 | $R = \sum_{i=n+1}^{m} C_m^i \times R^i \times (1-R)^{m-i}$ | |

- DES 明文分为 64 位一组，密钥 64 位（实际位是 56 位的密钥和 8 位奇偶校验）。

**注意：**考试中填写实际密钥位（即 56 位）。

- 3DES 是 DES 的扩展，是执行了三次的 DES。其中，在第一次和第三次加密使用同一密钥的方式下，密钥长度扩展到 128 位（112 位有效）；三次加密使用不同密钥，密钥长度扩展到 192 位（168 位有效）。
- IDEA 明文和密文均为 64 位，密钥长度为 128 位。
- 消息摘要算法 5（MD5）把信息分为 512 比特的分组，并且创建一个 128 比特的摘要。
- 安全 hash 算法（SHA-1）把信息分为 512 比特的分组，并且创建一个 160 比特的摘要。
- 网络需要的传输速率=用户数×每单位时间产生事务的数量×事务量大小
- 吞吐量（Mp/s）=万兆端口数量×14.88 Mp/s+千兆端口数量×1.488 Mp/s+百兆端口数量×0.1488 Mp/s
- 背板带宽（Mb/s）=万兆端口数量×10000Mp/s×2+千兆端口数量×1000Mb/s×2+百兆端口数量×100Mb/s×2+其他端口×端口速率×2
- 阻塞状态到侦听状态需要 20 秒，侦听状态到学习状态需要 15 秒，学习状态到转发状态需要 15 秒。
- RIP 路由更新周期为 30 秒，如路由器 180 秒没有回应，则标志路由不可达；如 240 秒内没有回应，则删除路由表信息。RIP 协议的最大跳数为 15 条，16 条则表示不可达，直连网络跳数为 0，每经过一个节点跳数增 1。
- OSPF 默认的 Hello 报文发送间隔时间是 10 秒，默认无效时间间隔是 Hello 时间间隔的 4 倍，即如果在 40 秒内没有从特定的邻居接收到这种分组，路由器就认为那个邻居不存在了。Hello 组播地址为 224.0.0.5。

- ISATAP 地址中，前 64 位是向 ISATAP 路由器发送请求得到的；后 64 位由两部分构成，其中后 64 位中的前 32 位是 0:5EFE，后 32 位是 IPv4 单播地址，即 ISATAP 接口 ID 必须为::0:5ffe:IPv4 地址的形式。
- 1 字节（B）=8bit
- 1MB=1024KB、1GB=1024MB、1TB=1024GB。
- 1Mb=1024Kb、1Gb=1024Mb、1Tb=1024Gb。
- 1Mb/s=1024kb/s、1Gb=1024Mb/s、1Tb=1024Gb/s。
- 总线数据传输速率=[时钟频率（HZ）/每个总线包含的时钟周期数]×每个总线周期传送的字节数（b）
- 每秒指令数=时钟频率/(每个总线周期包含时钟周期数×指令平均占用总线周期数)
- 每秒总线周期数=主频/时钟周期
- 执行程序所需时间=编译后产生的机器指令数×指令所需平均周期数×每个机器周期时间
- 流水线周期值等于最慢的那个指令周期。
- 流水线执行时间=首条指令的执行时间+(指令总数–1)×流水线周期值
- 流水线吞吐率=任务数/完成时间
- 流水线加速比=不采用流水线的执行时间/采用流水线的执行时间
- 存储器带宽=每周期可访问的字节数/存储器周期（ns）
- 需要内存片数=（W/w）×（B/b）

其中，W 和 B 分别表示要组成的存储器的字数和位数，w 和 b 表示内存芯片的字数和位数；

- 存储器地址编码=(第二地址–第一地址)+1，如(CFFFFH-90000H)+1
- Cache 平均访存时间=Cache 命中率×Cache 访问周期时间+Cache 失效率×主存访问周期时间
- Cache 访存命中率=Cache 存取次数/(Cache 存取次数+主存存取次数)
- **磁带**数据传输速率（B/s）=磁带记录密度（B/mm）×带速（mm/s）
- **磁盘**非格式化容量＝位密度×π×最内圈址径×总磁道数
- 总磁道数=记录面数×磁道密度×(外直径–内直径)/2
- **磁盘**格式化容量＝每道扇区数×扇区容量×总磁道数
- 寻道时间=移动道数×每经过一条磁道所需时间
- 等待时间=移动扇区数×每转过一道扇区所需时间
- 读取时间=目标的块数×读一块数据的时间
- 数据读出时间=等待时间+寻道时间+读取时间
- 平均等待时间=(最长时间+最短时间)/2
- 平均寻道时间=(最大磁道的平均最长寻道时间+最短时间)/2
- 位：计算机中采用二进制代码来表示数据，代码只有 0 和 1 两种，无论是 0 还是 1，在

CPU 中都是 1 位。

- 字长：CPU 在单位时间内能一次处理的二进制数的位数叫字长。通常能一次处理 16bit 数据的 CPU 通常就叫 16 位的 CPU。
- 设流水线由 N 段组成，每段所需时间分别为 $\Delta t_i$（$1 \leqslant i \leqslant N$），完成 M 个任务的实际时间可以计算如下：$\sum_{i=1}^{n} \Delta t_i + (M-1)\Delta t_j$，其中 $\Delta t_j$ 为时间最长的那一段的执行时间。
- **吞吐率**：指的是计算机中的流水线在单位时间内可以处理的任务或执行指令的个数。
- **加速比**：是指某一流水线采用串行模式的工作速度和流水线模式的工作速度的比值。
- **效率**：是指流水线中各个部件的利用率。
- 高速缓存中，若直接访问主存的时间为 M 秒，访问高速缓存的时间为 N 秒，CPU 访问内存的平均时间为 L 秒，设命中率为 H，则满足下列公式：L=M×(1–H)+N×H。
- 内存容量=最高地址–最低地址+1
- 存储器的地址总线中，地址线的根数与存储器的容量大小之间有密切的关系，若设地址线的根数为 N，则此地址总线可以访问的最大存储容量 $M=2^N$ 字节。

# 附录二　网络工程师考试常用术语汇总表

**OSI 参考模型**

系统网络体系结构（System Network Architecture，SNA）
国际标准化组织（International Standard Organized，ISO）
开放系统互连基本参考模型（Open System Interconnection Reference Model，OSI/RM）
物理层（Physical Layer）
数据终端设备（Data Terminal Equipment，DTE）
数据通信设备（Data Communications Equipment，DCE）
数据链路层（Data Link Layer）
逻辑链路控制（Logical Link Control，LLC）
介质访问控制（Media Access Control，MAC）
网络层（Network Layer）
传输层（Transport Layer）
会话层（Session Layer）
表示层（Presentation Layer）
应用层（Application Layer）
公共应用服务元素（CASE，Common Application Service Element）
特定应用服务元素（SASE，Specific Application Service Element）
协议数据单元（PDU，Protocol Data Unit）
服务数据单元（SDU，Service Data Unit）

**物理层**

分贝（decibel，dB）
脉冲编码调制（Pulse Code Modulation，PCM）

幅移键控（Amplitude Shift Keying，ASK）
频移键控（Frequency Shift Keying，FSK）
相移键控（Phase Shift Keying，PSK）
交替反转编码（Alternate Mark Inversion，AMI）
归零码（Return to Zero，RZ）
不归零码（Not Return to Zero，NRZ）
不归零反相编码（No Return Zero-Inverse，NRZ-I）
通用串行总线（Universal Serial Bus，USB）
时分复用（Time Division Multiplexing，TDM）
波分复用（Wavelength Division Multiplexing，WDM）
频分复用（Frequency Division Multiplexing，FDM）
同步光纤网（Synchronous Optical Network，SONET）
第 1 级同步传送信号（Synchronous Transport Signal，STS-1）
第 1 级光载波（Optical Carrier，OC-1）
同步数字系列（Synchronous Digital Hierarchy，SDH）
混合光纤－同轴电缆（Hybrid Fiber-Coaxial，HFC）
电缆调制解调器（Cable Modem，CM）
有线电视网络（Cable TV，CATV）
电缆调制解调器终端系统（Cable Modem Terminal System，CMTS）
光线路终端（Optical Line Terminal，OLT）
光网络单元（Optical Network Unit，ONU）
光网络终端（Optical Network Terminal，ONT）
光纤到交换箱（Fiber To The Cabinet，FTTCab）
光纤到路边（Fiber To The Curb，FTTC）
光纤到大楼（Fiber To The Building，FTTB）
光纤到户（Fiber To The Home，FTTH）
无源光纤网络（Passive Optical Network，PON）
以太网无源光网络（Ethernet Passive Optical Network，EPON）
千兆以太网无源光网络（Gigabit-Capable PON，GPON）
美国电子工业协会（Electrical Industrial Association，EIA）
异步传输模式（Asynchronous Transfer Mode，ATM）
固定比特率（Constant Bit Rate，CBR）
可变比特率（Variable Bit Rate，VBR）
有效比特率（Available Bit Rate，ABR）
不定比特率（Unspecified Bit Rate，UBR）

**数据链路层**

循环冗余校验码（Cyclical Redundancy Check，CRC）
点到点协议（the Point-to-Point Protocol，PPP）
链路控制协议（Link Control Protocol，LCP）
网络控制协议（Network Control Protocol，NCP）
密码验证协议（Password Authentication Protocol，PAP）
挑战一握手验证协议（Challenge Handshake Authentication Protocol，CHAP）
逻辑链路控制（Logical Link Control，LLC）
媒体接入控制层（Media Access Control，MAC）
载波监听多路访问/冲突检测（Carrier Sense Multiple Access/Collision Detect，CSMA/CD）
生成树协议（Spanning Tree Protocol，STP）
虚拟局域网（Virtual Local Area Network，VLAN）
多生成树协议（Multiple Spanning Tree Protocol，MSTP）
快速生成树协议（Rapid Spanning Tree Protocol，RSTP）
快速以太网（Fast Ethernet）
千兆以太网（Gigabit Ethernet）
万兆以太网（10 Gigabit Ethernet）
令牌总线网（Token-Passing Bus）
集成数据和语音网络（Voice over Internet Protocol，VoIP）
无线个人局域网（Personal Area Network，PAN）
宽带无线接入（Broadband Wireless Access）

**网络层**

互连协议（Internet Protocol，IP）
数据报头（Packet Header）
区分服务（Differentiated Services，DS）
区分代码点（DiffServ Code Point，DSCP）
显式拥塞通知（Explicit Congestion Notification，ECN）
可变长子网掩码（Variable Length Subnet Masking，VLSM）
无类别域间路由（Classless Inter-Domain Routing，CIDR）
路由汇聚（Route Summarization）
Internet 控制报文协议（Internet Control Message Protocol，ICMP）
地址协议（Address Resolution Protocol，ARP）
反向地址解析（Reverse Address Resolution Protocol，RARP）
IPv6（Internet Protocol Version 6）
网络地址转换（Network Address Translation，NAT）

网络地址端口转换（Network Address Port Translation，NAPT）
传输控制协议（Transmission Control Protocol，TCP）
初始序号（Initial Sequence Number，ISN）
协议端口号（Protocol Port Number）

**应用层**

域名系统（Domain Name System，DNS）
顶级域名（Top Level Domain，TLD）
动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）
万维网（World Wide Web，WWW）
统一资源标识符（Uniform Resource Locator，URL）
超文本传送协议（HyperText Transfer Protocol，HTTP）
文本标记语言（HyperText Markup Language，HTML）
万维网协会（World Wide Web Consortium，W3C）
Internet 工作小组（Internet Engineering Task Force，IETF）
电子邮件（electronic mail，E-mail）
简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）
邮局协议（Post Office Protocol，POP）
Internet 邮件访问协议（Internet Message Access Protocol，IMAP）
文件传输协议（File Transfer Protocol，FTP）
简单文件传送协议（Trivial File Transfer Protocol，TFTP）
性能管理（Performance Management）
配置管理（Configuration Management）
故障管理（Fault Management）
安全管理（Security Management）
计费管理（Accounting Management）
公共管理信息服务/公共管理信息协议（Common Management Information Service/Protocol，CMIS/CMIP）
管理信息库（Management Information Base，MIB）
简单网络管理协议（Simple Network Management Protocol，SNMP）
管理信息结构（Structure of Management Information，SMI）
对象命名树（Object Naming Tree）
TCP/IP 终端仿真协议（Telnet，TCP/IP Terminal Emulation Protocol）
网络虚拟终端（Net Virtual Terminal，NVT）
代理服务器（Proxy Server）
安全外壳协议（Secure Shell，SSH）

## 网络安全

平均无故障时间（Mean Time To Failure，MTTF）

平均修复时间（Mean Time To Repair，MTTR）

平均失效间隔（Mean Time Between Failure，MTBF）

拒绝服务（Denial of Service，DOS）

分布式拒绝服务攻击（Distributed Denial of service，DDOS）

报文摘要算法（Message Digest Algorithms）

证书颁发机构（Certification Authority，CA）

注册机构（Registration Authority，RA）

证书撤销列表（certification revocation list，CRL）

身份鉴别（Authentication）

密钥分配中心（Key Distribution Center，KDC）

票据（ticket-granting ticket）

单点登录（Single Sign On，SSO）

鉴别服务器（Authentication Server，AS）

票据授予服务器（Ticket-Granting Server，TGS）

公钥基础设施（Public Key Infrastructure，PKI）

安全电子交易（Secure Electronic Transaction，SET）

安全套接层（Secure Sockets Layer，SSL）

传输层安全（Transport Layer Security，TLS）

安全超文本传输协议（HyperText Transfer Protocol over Secure Socket Layer，HTTPS）

远程用户拨号认证系统（Remote Authentication Dial In User Service，RADIUS）

虚拟专用网络（Virtual Private Network，VPN）

Internet 协议安全协议（Internet Protocol Security，IPSec）

Internet 密钥交换协议（Internet Key Exchange Protocol，IKE）

Internet 安全关联和密钥管理协议（Internet Security Association and Key Management Protocol，ISAKMP）

认证头（Authentication Header，AH）

封装安全载荷（Encapsulating Security Payload，ESP）

多协议标记交换（Multi-Protocol Label Switching，MPLS）

边缘路由器（Label Edge Router，LER）

标记交换通路（Label Switch Path，LSP）

标签交换路由器（Lab Switch Router，LSR）

统一威胁管理（Unified Threat Management，UTM）

入侵检测系统（Intrusion Detection System，IDS）

## 无线

基础设施网络（Infrastructure Networking）
自主网络（Ad Hoc Networking）
基本服务集（Basic Service Set，BSS）
基本服务区（Basic Service Area，BSA）
分配系统（Distribution System，DS）
扩展服务集（Extended Service Set，ESS）
服务集标识符（Service Set Identifier，SSID）
无线电通信部门（ITU Radio Communication Sector，ITU-R）
跳频（Frequency-Hopping Spread Spectrum，FHSS）
红外技术（InfraRed，IR）
直接序列（Spread Spectrum，DSSS）
正交频分复用技术（Orthogonal Frequency Division Multiplexing，OFDM）
高速直接序列扩频（High Rate Direct Sequence Spread Spectrum，HR-DSSS）
载波侦听多路访问/冲突避免协议（Carrier Sense Multiple Access/Collision Avoidance，CSMA/CA）
分布协调功能（Distributed Coordination Function，DCF）
点协调功能（Point Coordination Function，PCF）
帧间隔（InterFrame Space，IFS）
无线网的安全协议（Wired Equivalent Privacy，WEP）
Wi-Fi 保护接入（Wi-Fi Protected Access，WPA）
码分多址（Code-Division Multiple Access，CDMA）
宽带分码多址存取（Wideband CDMA，WCDMA）
时分同步的码分多址技术（Time Division-Synchronous Code Division Multiple Access，TD-SCDMA）
3GPP 长期演进技术（3GPP Long Term Evolution，LTE）
存储技术基础
独立磁盘冗余阵列（Redundant Array of Independent Disks，RAID）
网络附属存储（NAS，Network Attached Storage，）
存储区域网络及其协议（Storage Area Network and SAN Protocols，SAN）

## 交换机

多层交换（MultiLayer Switching，MLS）
命令行接口（Command Line interface，CLI）
User EXEC（用户模式）
Privileged EXEC Mode（特权模式）
Global Configuration Mode（全局配置模式）

VLAN Configuration Mode（VLAN 配置模式）
Interface Configuration Mode（接口配置模式）
Line Configuration Mode（line 接口配置模式）
虚拟局域网（Virtual Local Area Network，VLAN）
VLAN 中继协议（VLAN Trunking Protocol，VTP）
VTP 修剪（VTP Pruning）
规范格式指示器（Canonical Format Indicator）
生成树协议（Spanning Tree Protocol，STP）
网桥协议数据单元（Bridge Protocol Data Unit，BPDU）
根网桥（Root Bridge）
根端口（Root Ports）
指定端口（Designated Ports）
热备份路由协议（Hot Standby Router Protocol，HSRP）

**路由器**

松散源路由（Loose Source Route）
严格源路由（Strict Source Route）
已注册的插孔（Registered Jack，RJ）
高速同步串口（Serial Peripheral Interface，SPI）
路由表（Routing Table）
路由选择协议（Routing Protocol）
路由信息协议（Routing Information Protocol，RIP）
水平分割（Split Horizon）
路由中毒（Router Poisoning）
反向中毒（Poison Reverse）
触发更新（Trigger Update）
开放式最短路径优先（Open Shortest Path First，OSPF）
单一自治系统（Autonomous System，AS）
最短路径优先算法（Shortest Path Firs，SPF）
OSPF 使用链路状态广播（Link State Advertisement，LSA）
因特网地址授权机构（Internet Assigned Numbers Authority，IANA）
内部网关协议（Interior Gateway Protocol，IGP）
外部网关协议（Exterior Gateway Protocol，EGP）
链路状态库（Link-State DataBase，LSDB）
链路状态广播（Link State Advertisement，LSA）
点到点（Point-to-Point）

广播型（Broadcast）
非广播型（Non-Broadcast，NB）
点到多点（Point-to-Multicast）
虚链接（Virtual Link）
路由度量（metric）
通用路由封装协议（Generic Routing Encapsulation，GRE）
站内自动隧道寻址协议（Intra-Site Automatic Tunnel Addressing Protocol，ISATAP）

**防火墙**

防火墙（Fire Wall）
DMZ 区（Demilitarized Zone）
访问控制表（Access Control Lists，ACL）

**VPN**

安全关联（Security Association，SA）是单向的
安全参数索引（Security Parameter Index，SPI）
IKE 策略（IKE Policy）
变换集（Transform Set）

**计算机硬件知识**

中央处理单元（Central Processing Unit）
微处理器（Microprocessor）
复杂指令集（Complex Instruction Set Computer，CISC）
精简指令集（Reduced Instruction Set Computer，RISC）
一级缓存（L1 Cache）
二级缓存（L2 Cache）
三级缓存（L3 Cache）
流水线（pipeline）
随机存取存储器（Random Access Memory，RAM）
只读存储器（Read Only Memory，ROM）
顺序存取存储器（Sequential Access Memory，SAM）
相联存储器（Content Addressable Memory，CAM）

**计算机软件知识**

代码行（line of code）
功能点分析法（Function Point Analysis，FPA）
国际功能点用户协会（International Function Point Users' Group，IFPUG）
德尔菲法（Delphi technique）
构造性成本模型（Constructive Cost Model，COCOMO）

模型描述图（diagram）
软件开发模型（Software Development Model）
元模型（meta-model）
系统测试（System Testing）
α 测试（Alpha Testing）
β 测试 （Beta Testing）
白盒测试（White Box Testing）
黑盒测试（Black Box Testing）
计划评审技术（Program Evaluation and Review Technique，PERT）

**Windows 部分**

域（Domain）
域控制器（DC，Domain Controller）。
活动目录（Active Directory）
主文件目录 MFD（Master File Directory）
用户目录 UFD（User File Directory）
文件配置表（File Allocation Table，FAT）
新网络技术文件系统（New Technology File System，NTFS）
nslookup 命令（name server lookup）
管理控制台（Microsoft Management Console，MMC）

# 参考文献


[1] （美）Jeff Doyle 著．TCP/IP 路由技术．葛建立等译．北京：人民邮电出版社，2009．

[2] （美）Justin Menga 著．CCNP 实战指南：交换．李莉等译．北京：人民邮电出版社，2011．

[3] 谢希仁．计算机网络（第五版）．北京：电子工业出版社，2008．

[4] 王达．路由器配置与管理完全手册（Cisco 篇）．武汉：华中科技大学出版社，2011．

[5] 王达．交换机配置与管理完全手册（Cisco/H3C）．北京：中国水利水电出版社，2009．

[6] （美）Andrew S.Tanenbaum 著．计算机网络（第四版）．潘爱民译．北京：清华大学出版社，2009．

[7] 黄传河．网络规划设计师教程．北京：清华大学出版社，2009．

[8] 刘晓辉．网络设备规划、配置与管理大全．北京：电子工业出版社，2009．

[9] 丁奇．大话无线通信．北京：人民邮电出版社，2010．

[10] 杨波．大话通信．北京：人民邮电出版社，2009．

[11] （美）Shun Harris 著．CISSP 认证考试指南．石华耀译．北京：科学出版社，2009．

[12] 王奎．PPP 身份验证协议．中国互动出版网，2001．

[13] （美）RichardDeal 著．CCNA 学习指南．邢京武、何陶译．北京：人民邮电出版社，2004．

[General Information]
书名=软考课程5天通关　网络工程师的5天修炼
作者=朱小平编著
页码=335
ISBN=335
SS号=13039820
dxNumber=000008281869
出版时间=2012.03
出版社=该引擎未能查询到
定价：38.00
试读地址=http://book.szdnet.org.cn/bookDetail.jsp?dxNumber=000008281869&d=7EE0D34E84BFDBF92E268F7A49DCDD27&fenlei=1817041103&sw=%CD%F8%C2%E7%B9%A4%B3%CC%CA%A6
全文地址=http://nb.5read.com/image/ss2jpg.dll?did=t1&pid=B7CDA5E35F9391F01AF975463D4DB3605B1D4BE97C9B1A8D37A8406FB765794B2386D6504D0769E1C55E2315FDAFC228DD00D934D1B30277D0B66F3CABF684AC48A3C4228772DA0CD92E49554C375ADBA7B527AC6F5C766AB9FC336D762BA3892A8D6ECD93632A65950148C17BB895F0348B&jid=/