

网络管理与维护技术习题参考答案

第 1 章

1. B
2. AB
3. BACD
4. 12.2(8)T5, 32M, 32K, 16384K, flash:C2600-i-mz.122-8.T5.bin, 0x2102
5. A
6. C
7. A
8. BCD
9. A
10. BA
11. D
12. DABCA
13. DCB
14. A
15. C
16. C
17. A

第 2 章

- 1-5: BCDAB
6-10: DDBCC
11-15: ACDDA
16-20: DBBDB
21-23: AAB

第 3 章

1-5: CDA(ABD)(ACD)
6-10: DA(ACD)AC
11-15(AB)(ABD)BA(ACD)
16-18: C(ABCD)C

第 4 章

1-5: (ABD)BD(ABD)A
6-10: (AC)(AD)(BCD)B(BD)
11-12: BB

第 5 章

1-5: (BD)BDCC
6-8: (ABD)B(ABCD)

第 6 章

1-5: (AD)C(ACD)DB
6-10: C(ABCD)(ABCD)(ABD)(ABC)
11-15: (ABCD)(BC)(ACD)(AC)(ABCD)
16-20: (AC)(BD)(ACD)(ABD)(BCD)
21-25: (ABCD)(ABCD)CAB
26-27: (BD)(ABC)

第 7 章

一、填空题

- (1) 自动分配 动态分配
- (2) 静态 IP 动态 IP

- (3) ipconfig
- (4) 递归查询 迭代查询 反向查询
- (5) DNS 域名空间 资源记录 DNS 服务器 DNS 客户机
- (6) 交叉式
- (7) 虚拟目录
- (8) 利用本地 IIS 管理器管理远程 IIS 服务器 使用终端服务管理远程 IIS 服务器
利用远程管理工具管理 IIS 服务器
- (9) 工作进程隔离模式 IIS5.0 隔离模式
- (10) 索引服务
- (11) 编录
- (12) Internet 连接共享 (ICS) 功能 网络地址转换 (NAT) 服务

二、选择题

- (1) A (2) B (3) C (4) D (5) A (6) D (7) A

三、判断正误

- (1) × (2) × (3) × (4) × (5) × (6) ×

四、问答题

(1) Windows Server 2003 家族的 4 个 32 位版本包括: Windows Server 2003 标准版、Windows Server 2003 企业版、Windows Server 2003 Datacenter 版和 Windows Server 2003 Web 版。

(2) DHCP 服务为动态主机配置协议, 建立 DHCP 服务器后, 网络管理员只需在该服务器上集中配置 IP 环境参数 (包括 IP 地址及子网掩码、网关、DNS 服务器地址等), 配置完成后, 网络中的计算机即可通过 DHCP 服务器获得其环境参数。其工作原理如图 T7-1 所示

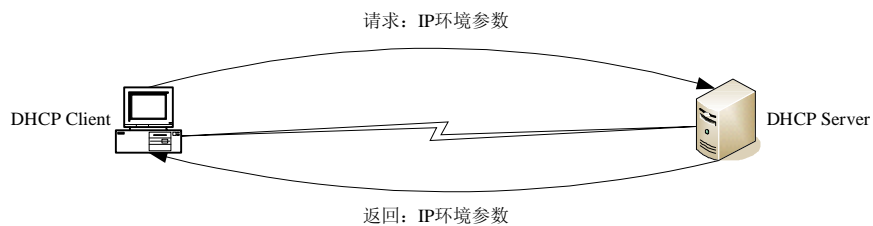


图 T7-1 DHCP 工作原理示意图

(3) 申请新的 IP 地址时, DHCP 客户机与服务器需要完成下列通信过程 (如图 T7-2 所示):

- 1) DHCP 客户机以广播方式将 DHCPDISCOVER (DHCP 探测) 信息发送到网络上, 寻找 DHCP 服务器。

- 2) DHCP 服务器收到 DHCPDISCOVER 信息后, 将自其地址池中选择一个未出租的 IP 地址, 锁定其所选择的 IP 地址, 然后构造 DHCPOFFER 信息并以广播的方式发送到网络上。
- 3) DHCP 客户机收到服务器的 DHCPOFFER 信息后, 再以广播的方式向 DHCP 服务器发送 DHCPREQUEST, 申请分配 IP 地址。如果网络中存在多个 DHCP 服务器, 客户机将选择使用其首先收到的 DHCPOFFER 信息。
- 4) DHCP 服务器收到客户机的信息后, 以广播方式将 DHCPACK (DHCP 确认) 信息发送给客户机, 除 IP 地址外, DHCPACK 信息中还可能包括其他 TCP/IP 配置数据, 如默认网关、DNS 服务器等。DHCP 客户机在收到 DHCPACK 信息后, 即可自动完成 IP 环境参数设置。

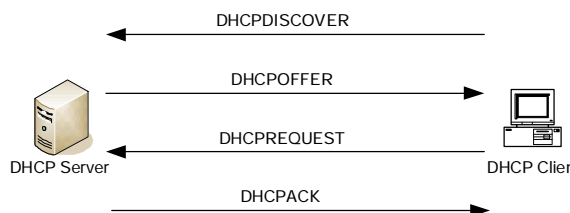


图 T7-2 申请新 IP 地址的过程

(4) 欲将一 IP 地址“保留”给某一 DHCP 客户, 在 DHCP 服务器上的操作步骤如下:

进入 DHCP 控制台, 依次选择服务器→作用域, 右击其中的“保留”, 于快捷菜单中选择“新建保留”, 打开“新建保留”对话框 (如图 T7-3 所示), 输入需要保留的 IP 地址、DHCP 客户机网卡的 MAC 地址等信息, 完成后单击“添加”按钮。当 DHCP 客户机可访问多个 DHCP 服务器时, 应确保在每一服务器上进行同样的设置。



图 T7-3 新建保留 IP 地址

(5) 若需要在 DHCP 服务器上增加一个作用域, 该作用域的地址范围与用于侦听 DHCP 服务请求的 IP 地址不在同一 IP 网段内, 但要求该作用域能正常工作, 可以创建超级作用域, 操作方法如下:

- 1) 进入 DHCP 控制台, 右击欲创建超级作用域的服务器, 于快捷菜单中选择“新建超级作用域”, 打开“欢迎使用新建超级作用域向导”。
- 2) 单击“下一步”按钮, 打开“超级作用域名”对话框, 输入超级作用域名称。

3) 单击“下一步”按钮,打开“选择作用域”对话框,选择欲加入超级作用域的作用域。

4) 单击“下一步”按钮,打开“正在完成新建超级作用域向导”对话框,查看超级作用域中的成员,确认无误后,单击“完成”按钮。

(6) 在为客户机分配 IP 地址与子网掩码的同时,DHCP 服务器还可将默认网关、DNS 服务器地址等 IP 环境参数一并分配给客户机。

(7) 当 DHCP 客户机请求 DHCP 服务失败时,可自动从保留的虚拟 IP 地址(又称“自动专用 IP 地址”)中取得并设定 IP 地址,其范围为 169.254.0.1~169.254.255.254,子网掩码为 255.255.255.0。

(8) DNS 是一种基于分布式数据库、采用客户/服务器模式完成主机名称与 IP 地址之间的转换的系统。通过建立 DNS 数据库,记录主机名称与 IP 地址的对应关系。DNS 驻留在服务器端,为客户端的主机提供 IP 地址解析服务,如图 T7-4 所示。

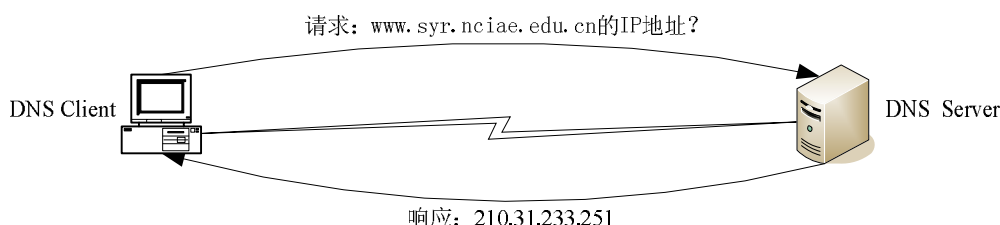


图 T7-4 DNS 服务器工作机制示意图

(9) DNS 客户向 DNS 服务器请求服务时,可能的查询方式有递归查询、迭代查询和反向查询 3 种。

1) 递归查询。不论解析是否成功,DNS 服务器都将结果提交给 DNS 客户机。DNS 服务器永远不会将其他 DNS 服务器的地址发送给 DNS 客户机,如图 T7-5 所示。

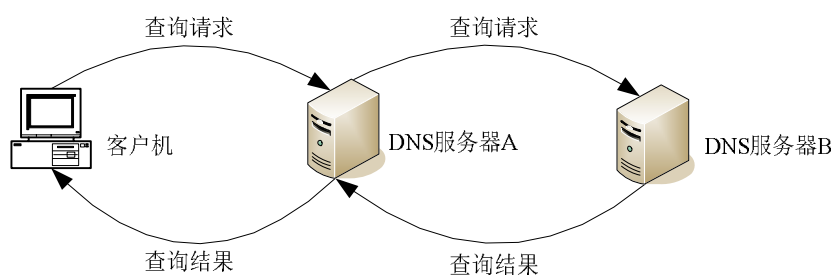


图 T7-5 递归查询示意图

2) 迭代查询。如果在 DNS 服务器本地进行的查询失败,则将另一 DNS 服务器的地址返回给客户机,然后 DNS 将查询请求提交这一新的 DNS 服务器,如图 T7-6 所示。

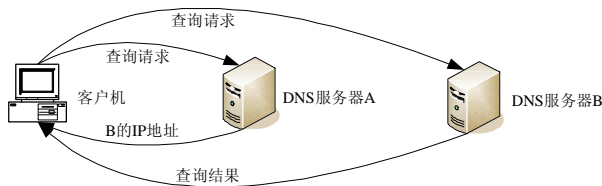


图 T7-6 迭代查询示意图

3) 反向查询。查询与 IP 地址对应的域名，如图 T7-7 所示。

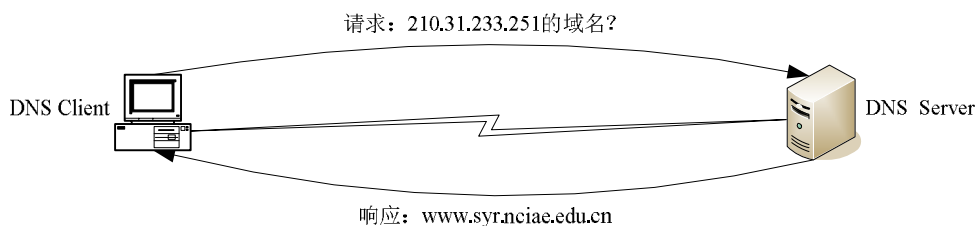


图 T7-7 反向查询示意图

(10) 在 DNS 服务器上为主机建立别名记录的主要步骤如下：

- 1) 建立区域、域及子域，自己命名。
- 2) 右击新建立的子域，选择“新建主机”命令，打开“新建主机”对话框。
- 3) 输入对应的 IP 地址，保持主机名称为空。
- 4) 单击“添加主机”按钮，在随后打开的“DNS”对话框中单击“确定”按钮。
- 5) 返回“新建主机”对话框，单击“完成”按钮。
- 6) 右击子域，选择“新建别名”命令，打开“新建资源记录”对话框。
- 7) 输入别名，输入（或通过单击“浏览”按钮选择）“目标主机的完全合格的名称”，完成后单击“确定”按钮。
- 8) 重复上述步骤，可以建立另一别名。

(11) Web 服务，是通过超链接技术，在位于不同位置的文件之间建立了链接，从而可以为用户提供一种交叉式（而非线性式）的访问方式。借助于这种更符合思维习惯的访问方式，人们可以十分便捷地访问各种资源。WWW Client 通过本机的浏览器访问 Web 服务器，服务器接收来自客户端的访问请求，返回适当的 HTML 文档（如图 T7-8 所示）。

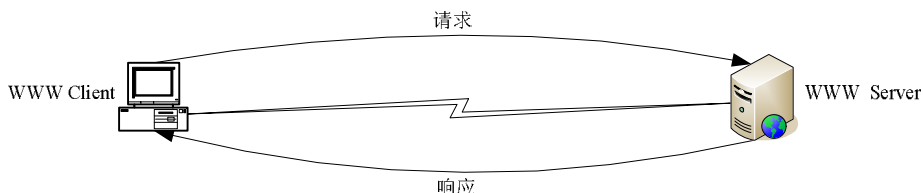


图 T7-8 WWW 客户与服务器的关系示意图

(12) 在选择 WWW 服务器软件时, 应重点考虑的因素:

- 1) 站点规模和用途。基于 Internet、访客众多的的大型站点, 应具备强大的多线程处理能力; 基于 Intranet 的企业站点一般对安全性有较高的要求; 小型站点一般在处理资源拮据的服务器上运行, 此时应选择轻量级的 WWW 服务器软件。
- 2) 操作系统。Unix 和 Windows 是目前的主流操作系统。若选择基于 Unix 的软件, 则需要考虑该软件是否支持所采用操作系统的版本。对于使用 Windows 平台的用户而言, 最好选择微软的 IIS, 能最大限度地体现 Windows 平台的优秀性能。
- 3) 商业软件和免费软件。一般商业 WWW 服务器软件的安装、管理比较方便, 能提供可靠、稳定和安全的服务, 可随时获得技术支持, 维护成本较低; 免费软件则相反。

(13) WWW 站点的实体是文件, 这些文件被组织在一个树形目录结构中, 其中位于最上层的目录就是站点的主目录。

(14) 在 WWW 服务器中, 虚拟目录实际上起指针的作用, 用于将分布在不同的存储位置的目录及其内容加入网站。

(15) 在一个 WWW 服务器上建立多个 Web 站点的技术称为虚拟主机技术, 可将一个物理主机分割成若干个逻辑主机。

在 IIS 的 WWW 服务器中, 可用 IP 地址、TCP 端口号和主机头名等方式来建立虚拟主机, 改变上述 3 个参数中的任何一个, 都可以得到新的站点标识。

使用同一 IP 地址、不同主机头架设多个 Web 站点是首选的虚拟主机技术。采用这种技术实现的多个虚拟主机拥有相同的 IP 地址, 这样可有效地节约 IP 地址资源。在客户端看来, 每个站点拥有不同的域名, 因此可以通过域名进行访问。

(16) 借助 Windows Server 2003 的索引服务为 WWW 站点建立全文搜索引擎的主要步骤如下:

- 1) 确认“索引服务”和“FrontPage 2002 Server Extensions”已经安装在 WWW Server 中。
- 2) 选择需要建立搜索引擎的 WWW 站点, 为其配置 Server Extensions 2002。
- 3) 在索引服务下新建编录。
- 4) 在索引服务下配置编录。
- 5) 启动索引服务。
- 6) 单击配置好的编录下的“查询编录”, 确认可在本地顺利进行查询。
- 7) 在“Windows Server 2003”上, 启动 FrontPage, 建立一个包含“搜索表单”的页面, 保存在目的站点的主目录下。
- 8) 在“WWW Client”端, 打开浏览器, 访问在上一步建立的页面, 即可对站点进行全文检索。

(17) FTP 服务实现在 Intranet 或 Internet 上传输文件的功能。FTP 服务器端的主目录存放被访问资源(可以设置访问权限), 客户端通过 FTP 协议访问或下载; 客户端除了可以下载服务器的资源外, 还可以通过客户端软件上传文件至 FTP 服务器。

(18) FTP 客户管理的主要内容为用户隔离和磁盘管理功能。

FTP 用户隔离功能用于限制用户只能访问自己目录，或称锁定用户主目录。启用用户隔离特性并经适当配置后，用户不能访问其他用户目录中的资源。

在用户目录所在磁盘的“属性”对话框的“配额”选项卡中启用“磁盘配额”，选择“拒绝将磁盘空间给超过配额限制的用户”，单击“配额项”，配置用户可用空间的大小。

(19) 利用 ICS 功能与利用 NAT 服务将局域网接入 Internet 的主要区别如下：

ICS 功能，要求内网成员必须使用私有子网 192.168.0.0 中的 IP 地址，且在 Internet 中不能访问内网中的任何资源，此外，当启用 Internet 连接共享功能后，还将导致 Windows Server 2003 的 DHCP 等服务不能正常运行。虽然有上述缺点，但因为设置简单，因此在网吧、家庭、学生寝室以及小型办公环境中，ICS 也得到了一定程度的应用。

NAT 的工作机制的核心是地址转换。网络地址转换是可以双向进行的。能够实现内部网络与外部网络之间的双向通信。当内部网络用户需要访问外部网络时，网络地址转换系统可将私有地址映射为合法的 IP 地址；当外部网络需要访问内部网络时，地址转换系统可根据外部数据包中的相关信息，向相关内网主机提出访问请求。只有使用 TCP/IP 协议的应用程序，才能使用网络地址转换功能。虽然设置相对较难，但是功能强大。

(20) NAT 服务器中的反向地址转换制外网主机访问内网资源，过程如图 T7-9 所示。

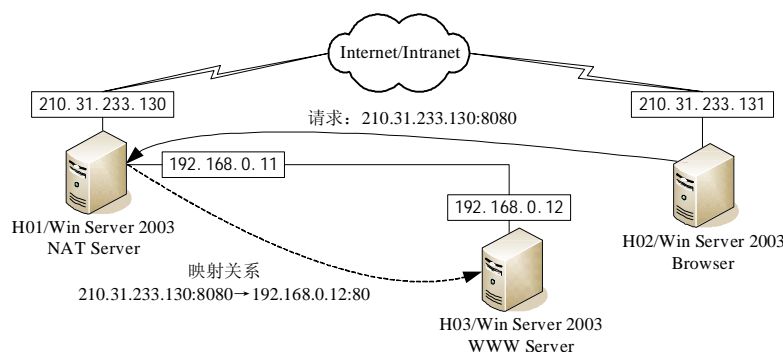


图 T7-9 反向地址转换过程示意图

为使外网中的机器能访问内网中的资源，需要为 NAT 明确指定反向地址映射关系。例如在图 7-6-4 中，为 NAT 指定了反向映射关系（210.31.233.130:8080→192.168.0.12:80），则外网主机（例如 H02）对资源 210.31.233.130:8080 的请求将首先被发往主机 H01，然后主机 H01 中的 NAT 服务就会将此请求转换为对 192.168.0.12:80 的请求并将请求发往主机 H03 以获取服务，主机 H03 的响应数据包又由 NAT 转交主机 H02，这样就完成了一次通信。

(21) VPN 是通过共享 IP 网中的“隧道”而建立的专用网络。通过 VPN 可在远程网络之间、专用网络与远程用户之间建立安全的、点对点的连接。VPN 是基于 C/S 模式工作的。典型的远程访问 VPN 的工作机制如图 T7-10 所示。

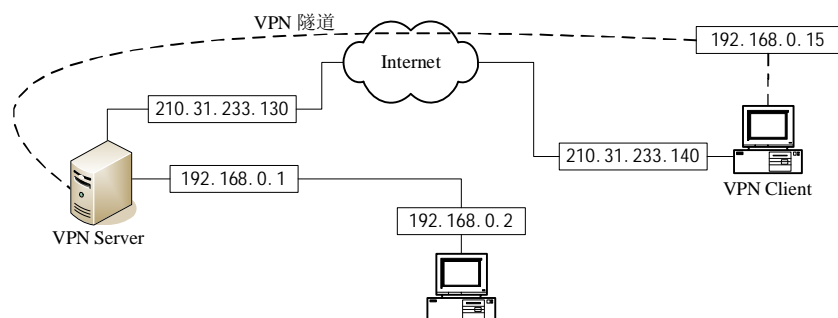


图 T7-10 远程访问 VPN 工作机制示意图

位于异地的 VPN 客户首先通过所在地的 ISP 接入 Internet，之后向 VPN 服务器发出连接申请以登录到专用网络。而 VPN 服务器在收到客户通过 Internet 发来的登录请求后，将首先确认用户身份，如果用户身份通过了验证，则服务器将与客户协商使用哪些隧道和加密协议，并根据协商的结果建立 VPN 连接。VPN 客户拥有两个 IP 地址，一个用于与 Internet 相连，另一个则用于与专用网相连。

(22) 建立远程访问 VPN 服务的实用价值体现在：

可在远程网络之间、专用网络与远程用户之间建立安全的、点对点的连接。例如可通过 VPN 技术将同属一个公司、分别位于北京和上海的两个专用网络通过 IP 网络连接起来；也可使漫游到美国的用户通过 IP 网络与北京的专用网络相连，成为专用网络的成员。

(23) 利用 Windows Server 2003 的路由和远程访问服务，可以建立 VPN 服务，主要步骤如下：

- 1) VPN Server 的设置。先设置外网卡和内网卡的 IP 参数，然后依次选择“开始”→“管理工具”→“路由和远程访问”，打开“路由和远程访问”控制台，在控制台左侧窗格中右击服务器，于呼出的快捷菜单中选择“配置并启用路由和远程访问”，在“配置”对话框中，选择“虚拟专用网络 (VPN) 访问和 NAT”，按提示，在打开的“VPN 连接”对话框中的“网络接口”列表中选择与外网的连接，单击“下一步”按钮，在打开的“IP 地址指定”对话框中，选择“来自一个指定的地址范围”，单击“下一步”按钮，在打开的“地址范围指定”对话框中，为远程客户分配 IP 地址范围。还可以设置访问权限。
- 2) VPN 本地计算机的设置。配置本地计算机，使其能与 VPN Server 正常通信。
- 3) VPN Client 的设置。设置网卡参数，依次选择“开始”→“所有程序”→“连接到”→“显示所有连接”，打开“网络连接”界面，在“网络任务”列表下选择“创建一个新的连接”，在“网络连接类型”对话框中选择“连接到我的工作场所的网络”，在打开的“网络连接”对话框中，选中“虚拟专用网络连接”，然后在打开的“连接名”对话框中，输入连接的名称，在打开的“公用网络”对话框中，选择“不拨初始连接”，在打开的“VPN 服务器选择”对话框中，输入 VPN Server 的域名或 IP 地址，在打开的连接对话框中，输入用户名和密码，如图 T7-11 所示，单击“连接”按

钮，将远程计算机连入专用网络。

- 4) 在远程计算机上访问虚拟专用网中的资源。在 VPN Client 上，以内网身份（连接 VPN Server 的内网卡）访问虚拟专用网中的资源。



图 T7-11 输入用户名和密码

第 8 章

1-7: D, B, D, B, B, C, D

8: ABC（这是多选题）

9-12: A, D, A, B

第 9 章

一、选择题

1. C
2. A
3. B
4. AB
5. A
6. B
7. A
8. B

二、简答题

1.

```
C2950(config)#monitor session 1 source interface fastEthernet 0/1
C2950(config)#monitor session 1 destination interface fastEthernet 0/24
```

2.

(1) 选择“Capture”菜单中的“Define Filter”命令，打开“Define Filter - Capture”对话框，选择“Address”选项卡。

(2) 在“Address”下拉列表中选择“IP”，在“Station1”和“Station2”中分别填写 any(表示所有主机)。

(3) 选择“Advanced”选项卡，依次选择“IP”→“TCP”→“FTP”。

(4) 按 F10 键或单击“Start”按钮，启动捕获。

第 10 章

1. 配置 cisco 路由器的只读字串为“reoly#!1”、读写字串为“wri*(!2”将路由器将所有类型 SNMP Trap 发送到 10.10.11.21 主机，发送 Trap 时采用“trancepc”作为字串、将 loopback 接口的 IP 地址作为 SNMP Trap 的发送源地址、将 log 记录发送到网管服务器的 IP (CW2K 10.11.11.23)上的 syslog server、将记录的事件严重级别从 informational 开始，一直到最紧急级别的事件全部发送到前边指定的 syslog server、将记录事件类型定义为 local6、发送记录事件的时候包含时间标记

```
Cisco#config terminal
Cisco(config)#snmp-server community reoly#!1 ro
Cisco(config)#snmp-server community wri*(!2 rw
Cisco(config)#snmp-server enable traps
Cisco(config)#snmp-server host 10.10.11.21 version 2c trancepc
Cisco(config)#snmp-server trap-source loopback0
Cisco(config)#logging on
Cisco(config)#logging 10.11.11.23
Cisco(config)#logging facility local6
Cisco(config)#logging trap Informational
Cisco(config)#service timestamps log datetime localtime
Cisco(config)#write terminal
```

2. 设置 cisco 路由器 secret 口令为“cissec#”控制台访问口令为“conlog” aux 端口访问口令为“auxadent” vty 访问采用 ssh 方式设置主机名为 router 主机域名为“netcent”用户名“netand”口令为“netvty!”；启用所有口令加密功能，并只有 ip 为 192.168.168.3 的主机可以

登录设备进行管理。配置完成后，用 **putty** 登录设备进行验证配置的正确性。

```
Cisco#config terminal
Cisco(config)#enable secret cissec
Cisco(config)#line console 0
Cisco((config-line)#password conlog
Cisco(config)#line aux 0
Cisco((config-line)#password auxadent
Cisco(config)#line vty 0 4
Cisco(config-line)#transport input SSH
Cisco(config-line)#access-class 3 in
Cisco(config-line)#access-list 3 permit 192.168.168.3 0.0.0.255
Cisco(config)#hostname router
router(config)#ip domain-name netcent
router(config)#crypto key generate rsa modulus 512
router(config)#aaa new-model
router(config)#username netand password netvty
router(config)#service password-encryption
router(config)#write terminal
```

3. 开启 cisco 设备 http 服务器并修改访问端口为 8080，启用本地身份认证，设置授权访问用户级别为 15 帐号为“httplogin”口令为“loginconfig”用 secret 加密，超过 2 分 20 秒中断会话，重试次数为 2 次。配置完成后验证正确性。

```
cisco#configure terminal
cisco(config)#ip http server
cisco(config)#ip http port 8080
cisco(config)#ip http authentication local
cisco(config)#username httplogin privilege 15 password 7 loginconfig
cisco(config)#enable secret loginconfig
cisco(config)#line vty 0 4
cisco(config-line)#login
cisco(config-line)#exec-timeout 2 20
cisco(config-line)#ip ssh authentication-retries 2
```

4. 配置 WAN 接口地址为 60.30.135.100/29，LAN 接口地址为 192.168.168.1/24，内部网络只有 192.168.168.0/23 网段对外访问，拒绝所有其他地源址的数据包进入 LAN 接口，禁止所有源地址为私有地址的数据包从 WAN 接口进入。

```
3640(Config)#access-list 120 deny ip 10.0.0.0 0.255.255.255 any log
3640(Config)#access-list 120 deny ip 172.16.0.0 0.15.255.255 any log
3640(Config)#access-list 120 deny ip 192.168.0.0 0.0.255.255 any log
3640(Config)#access-list 121 permit ip 192.168.168.0 0.0.1.255 any
3640(Config)#access-list 121 deny ip any any log
3640(Config)#access-list 122 deny ip 192.168.168.0 0.0.1.255 any
3640(Config)#access-list 122 permit ip any any log
3640(Config)#interface fastEthernet 0/0
3640(Config-if)#description "wan"
3640(Config-if)#ip address 60.30.135.100 255.255.255.248
3640(Config-if)#ip access-group 120 in
3640(Config-if)#ip access-group 121 out
3640(Config-if)#ip access-group 122 in
3640(Config)#interface fastEthernet 0/1
3640(Config-if)#description "lan"
3640(Config-if)#ip address 192.168.168.1 255.255.255.0
3640(Config-if)#ip access-group 121 in
```

5. 配置相关策略：从 2009 年 5 月 1 日 0 点到 2009 年 6 月 30 日晚 23 点 59 分。这一个月中，只有在周六早 7 点到周日晚 10 点才可以通过学校的网络访问 80 端口。

```
router #configure terminal
router(Config)# access-list 101
router(Config)# access-list 101 permit ip xxx.xxx.xxx.xxx xxx. xxx. xxx.
xxx any
router(Config)# access-list 101 deny ip any any log
router# config t
router(config)# interface ethernet 0
router(config-if)#ip access-group 101 in
router(config-if)#time-range http
router(config-if)#absolute start 0:00 1 May 2009 end 23:59 30 June 2009
periodic Saturday 7:00 to Sunday 22:00
router(config-if)#ip access-list 101 permit tcp any any eq 80 http
```