第 3 章　企业网设计实验

企业网设计的关键是内部网络私有 IP 地址分配、网络地址转换(Network Address Translation,NAT)和访问控制策略实现。私有 IP 地址使得内部网络对于外部网络(Internet 和行业服务网)是透明的。NAT 允许配置私有 IP 地址的内部网络终端访问外部网络资源。访问控制策略严格限制内部网络与 Internet 之间的信息交换过程。

3.1　企业网结构和实施过程

3.1.1　企业网结构

企业网结构如图 3.1 所示,由内部网络、DMZ、Internet 和行业服务网组成。防火墙端口 3 连接 Internet,路由器 R2 成为防火墙通往 Internet 的默认网关。同样,路由器 R1 端口 3 连接行业服务网,路由器 R3 成为路由器 R1 通往行业服务网的默认网关。交换机 S7 和 Web 服务器 1、E-mail 服务器构成 DMZ。内部网络终端通过三层交换机 S5 和 S6 连接防火墙和路由器 R1,三层交换机 S5 和 S6 构成冗余网关。内部网络终端分为普通终端、业务员终端和管理层终端,允许所有类型终端访问 Internet,只允许业务员终端和管理层终端访问行业服务网。

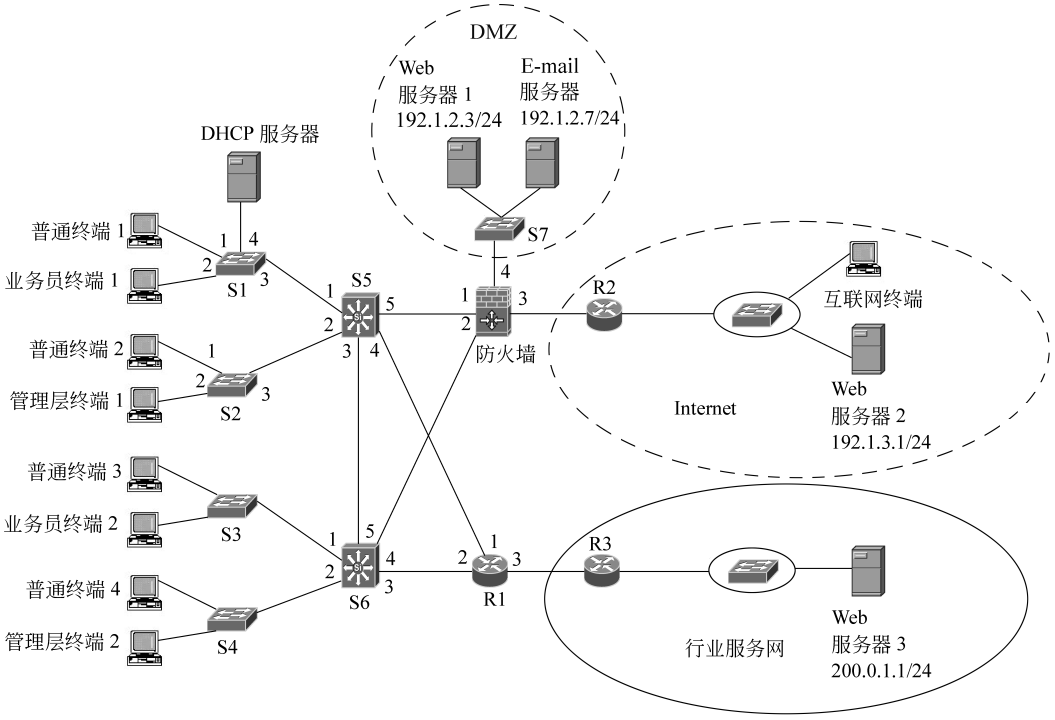


图 3.1　企业网结构

3.1.2　实施过程

实施过程分为两个阶段：数据通信网络配置实验和防火墙配置实验。

1. 数据通信网络配置实验

将不同类型的终端划分到不同的 VLAN，连接到不同 VLAN 的终端通过 DHCP（动态主机配置协议）自动从 DHCP 服务器获取网络信息。S5 和 S6 通过虚拟路由冗余协议（Virtual Router Redundancy Protocol，VRRP）组成冗余网关。内部网络使用私有 IP 地址，内部网络终端访问 Internet 和行业服务网时，分别由防火墙和路由器 R1 完成端口地址转换（Port Address Translation，PAT）过程。

2. 防火墙配置实验

防火墙配置实验用于实现以下安全策略。

（1）允许内部终端发起访问 Internet 中的 Web 服务器。

（2）允许内部终端发起访问 DMZ 中的 Web 服务器。

（3）允许内部终端通过 SMTP 和 POP3 发起访问 DMZ 中的邮件服务器。

（4）允许 DMZ 中的邮件服务器通过 SMTP 发起访问外部网络中的邮件服务器。

（5）允许外部网络中的终端以只读方式发起访问 DMZ 中的 Web 服务器。

（6）允许外部网络中的邮件服务器通过 SMTP 发起访问 DMZ 中的邮件服务器。

3.2　数据通信网络配置实验

3.2.1　实验内容

（1）在接入交换机 S1、S2、S3、S4 中创建 VLAN 2、VLAN 3 和 VLAN 4，分别用于连接普通终端、业务员终端和管理员终端。在三层交换机 S5 和 S6 中创建 VLAN 2、VLAN 3 和 VLAN 4，分别用于定义 VLAN 1、VLAN 2、VLAN 3 和 VLAN 4 对应的 IP 接口。在三层交换机 S5 中创建分别用于连接防火墙和路由器 R1 的 VLAN 5 和 VLAN 6。在三层交换机 S6 中创建分别用于连接防火墙和路由器 R1 的 VLAN 7 和 VLAN 8。

（2）在三层交换机 S5 和 S6 中分别定义 VLAN 1、VLAN 2、VLAN 3 和 VLAN 4 对应的 IP 接口。三层交换机 S5 和 S6 成为 VLAN 1、VLAN 2、VLAN 3 和 VLAN 4 的冗余网关。在三层交换机 S5 中定义 VLAN 5 和 VLAN 6 对应的 IP 接口。在三层交换机 S6 中定义 VLAN 7 和 VLAN 8 对应的 IP 接口。

（3）通过配置路由信息协议（Routing Information Protocol，RIP）和静态路由项生成用于指明通往内部网络各个子网、Internet 和行业服务网的传输路径的路由项。

（4）通过配置 OSPF（开放式最短路径优先）协议分别生成用于指明通往 Internet 和 DMZ 的传输路径的路由项。

（5）完成防火墙和路由器 R1 有关 PAT 的配置过程。

（6）在 DHCP 服务器中创建 VLAN 2、VLAN 3 和 VLAN 4 对应的作用域，使得各种类型终端可以通过 DHCP 自动从 DHCP 服务器获取网络信息。

（7）本实验由路由器 AR0 代替 DHCP 服务器。

3.2.2 实验目的

(1) 掌握 VLAN 配置过程。
(2) 掌握三层交换机 VRRP 配置过程。
(3) 掌握 RIP 配置过程。
(4) 掌握 OSPF 配置过程。
(5) 掌握静态路由项配置过程。
(6) 掌握路由器 PAT 配置过程。
(7) 掌握 DHCP 服务器配置过程。

3.2.3 实验原理

DHCP 服务器(由路由器 AR0 仿真)接入 VLAN 1,普通终端、业务员终端和管理员终端分别接入 VLAN 2、VLAN 3 和 VLAN 4,建立 DHCP 服务器、各种类型终端与三层交换机 S5 和 S6 中各个 VLAN 对应的 IP 接口之间的交换路径。通过在三层交换机 S5 和 S6 中完成 VRRP 配置过程,使得三层交换机 S5 和 S6 成为 VLAN 1、VLAN 2、VLAN 3 和 VLAN 4 的冗余网关。三层交换机 S5 和 S6 分别建立与防火墙和路由器 R1 之间的传输路径。防火墙和路由器 R1 完成 PAT 配置过程,使得所有内部网络终端都可以访问 Internet,但只有业务员终端和管理员终端可以访问行业服务网。在 DHCP 服务器中创建 VLAN 2、VLAN 3 和 VLAN 4 对应的作用域,在三层交换机 S5 和 S6 VLAN 2、VLAN 3 和 VLAN 4 对应的 IP 接口中启动 DHCP 中继功能,配置 DHCP 服务器地址。

3.2.4 关键命令说明

1. RIP 配置命令

以下命令序列用于完成图 3.2 中三层交换机 LSW5 的 RIP 配置过程。

```
[Huawei]rip
[Huawei-rip-1]network 192.168.1.0
[Huawei-rip-1]network 192.168.2.0
[Huawei-rip-1]network 192.168.3.0
[Huawei-rip-1]network 192.168.4.0
[Huawei-rip-1]network 192.168.5.0
[Huawei-rip-1]network 192.168.6.0
[Huawei-rip-1]quit
```

rip 是系统视图下使用的命令,该命令的作用是启动 RIP 进程,并进入 RIP 视图。由于没有给出进程编号,因此启动编号为 1 的 rip 进程。

network 192.168.1.0 是 RIP 视图下使用的命令,紧随命令 network 的参数通常是分类网络地址。192.168.1.0 是 C 类网络地址,其 IP 地址空间为 192.168.1.0～192.168.1.255。该命令的作用有两个:一是启动所有配置的 IP 地址属于网络地址 192.168.1.0 的路由器接口的 RIP 功能,允许这些接口接收和发送 RIP 路由消息;二是如果网络 192.168.1.0 是该路由器直接连接的网络,或者划分网络 192.168.1.0 后产生的若干个子网是该路由器直接连接

的网络，网络 192.168.1.0 对应的直连路由项（启动路由项聚合功能情况），或者划分网络 192.168.1.0 后产生的若干个子网对应的直连路由项（取消路由项聚合功能情况）参与 RIP 建立动态路由项的过程，即其他路由器的路由表中会生成用于指明通往网络 192.168.1.0（启动路由项聚合功能情况），或者划分网络 192.168.1.0 后产生的若干个子网（取消路由项聚合功能情况）的传输路径的路由项。

2. 静态路由项配置命令

```
[Huawei]ip route-static 200.0.1.0 24 192.168.6.253
[Huawei]ip route-static 0.0.0.0 0 192.168.5.253
```

ip route-static 200.0.1.0 24 192.168.6.253 是系统视图下使用的命令，该命令的作用是配置一项静态路由项，其中 200.0.1.0 是目的网络的网络地址，24 是目的网络的网络前缀长度，这两项用于确定目的网络的网络地址 200.0.1.0/24。192.168.6.253 是下一跳 IP 地址。由于下一跳结点连接在该三层交换机某个 IP 接口连接的网络中，根据下一跳结点的 IP 地址，可以确定下一跳结点所连接的网络，进而确定连接该网络的 IP 接口。如三层交换机 VLAN 6 对应的 IP 接口所连接的网络是 VLAN 6 对应的网络 192.168.6.0/24，由于下一跳 IP 地址 192.168.6.253 属于网络 192.168.6.0/24，因而可以确定输出接口是 VLAN 6 对应的 IP 接口，因此，只要在静态路由项配置命令中给出了下一跳 IP 地址，就无须给出输出接口。

ip route-static 0.0.0.0 0 192.168.5.253 是系统视图下使用的命令，该命令的作用是配置一项默认路由项，默认路由项是特殊的静态路由项，该路由项的目的网络与任意 IP 地址匹配。默认路由项的网络地址为 0.0.0.0，网络前缀长度为 0，即子网掩码为 0.0.0.0。由于任意 IP 地址和子网掩码“0.0.0.0”进行“与”操作的结果都是“0.0.0.0”，因此，任意 IP 地址都属于目的网络地址 0.0.0.0 和子网掩码 0.0.0.0 指定的目的网络。192.168.5.253 是下一跳 IP 地址。

3. VRRP 配置命令

以下命令序列用于完成三层交换机 LSW5 中连接 VLAN 1 的 IP 接口的 VRRP 配置过程。

```
[Huawei]interface vlanif 1
[Huawei-Vlanif1]vrrp vrid 1 virtual-ip 192.168.1.250
[Huawei-Vlanif1]vrrp vrid 1 priority 120
[Huawei-Vlanif1]vrrp vrid 1 preempt-mode time delay 20
[Huawei-Vlanif1]quit
```

vrrp vrid 1 virtual-ip 192.168.1.250 是接口视图下使用的命令，该命令的作用是在指定接口（这里是 VLAN 1 对应的 IP 接口）中创建编号为 1 的 VRRP 备份组，并为该 VRRP 备份组分配虚拟 IP 地址 192.168.1.250。

vrrp vrid 1 priority 120 是接口视图下使用的命令，该命令的作用是配置接口所在设备在编号为 1 的 VRRP 备份组中的优先级值。默认优先级值是 100，优先级值越大，则优先级越高，优先级最高的设备成为 VRRP 备份组的主路由器。执行该命令前，必须先创建编号为 1 的 VRRP 备份组。

vrrp vrid 1 preempt-mode timer delay 20 是接口视图下使用的命令，该命令的作用是

在编号为 1 的 VRRP 备份组中，将接口所在设备设置成延迟抢占方式，即如果接口所在设备的优先级值大于当前主路由器的优先级值，经过 20s 延时后，接口所在设备成为主路由器。执行该命令前，必须先创建编号为 1 的 VRRP 备份组。

4. 路由器 PAT 配置命令

1）确定需要地址转换的内网私有 IP 地址范围

以下命令序列通过基本过滤规则集将内网需要转换的私有 IP 地址范围定义为 CIDR 地址块 192.168.3.0/24 和 192.168.4.0/24。

```
[Huawei]acl 2000
[Huawei-acl-basic-2000]rule 10 permit source 192.168.3.0 0.0.0.255
[Huawei-acl-basic-2000]rule 20 permit source 192.168.4.0 0.0.0.255
[Huawei-acl-basic-2000]quit
```

acl 2000 是系统视图下使用的命令，该命令的作用是创建一个编号为 2000 的基本过滤规则集，并进入基本 acl 视图。

rule 10 permit source 192.168.3.0 0.0.0.255 是基本 acl 视图下使用的命令，该命令的作用是创建允许源 IP 地址属于 CIDR 地址块 192.168.3.0/24 的 IP 分组通过的过滤规则。这里，该过滤规则的含义变为对源 IP 地址属于 CIDR 地址块 192.168.3.0/24 的 IP 分组实施地址转换过程。

2）建立基本过滤规则集与公共接口之间的联系

```
[Huawei]interface GigabitEthernet0/0/2
[Huawei-GigabitEthernet0/0/2]nat outbound 2000
[Huawei-GigabitEthernet0/0/2]quit
```

nat outbound 2000 是接口视图下使用的命令，该命令的作用是建立编号为 2000 的基本过滤规则集与指定接口（这里是接口 GigabitEthernet0/0/2）之间的联系。建立该联系后，一是如果某个 IP 分组从该接口输出，且该 IP 分组的源 IP 地址属于编号为 2000 的基本过滤规则集指定的允许通过的源 IP 地址范围，则对该 IP 分组实施地址转换过程；二是指定该接口的 IP 地址作为 IP 分组完成地址转换过程后的源 IP 地址。

5. 防火墙 USG6000V PAT 配置命令

1）定义 IP 地址对象

以下命令序列用于创建一个名为 aa，涵盖 CIDR（无类别域间路由）地址块 192.168.2.0/24、192.168.3.0/24 和 192.168.4.0/24 的地址对象。

```
[USG6000V1]ip address-set aa type object
[USG6000V1-object-address-set-aa]address 10 192.168.2.0 0.0.0.255
[USG6000V1-object-address-set-aa]address 20 192.168.3.0 0.0.0.255
[USG6000V1-object-address-set-aa]address 30 192.168.4.0 0.0.0.255
[USG6000V1-object-address-set-aa]quit
```

ip address-set aa type object 是系统视图下使用的命令，该命令的作用是创建一个名为 aa 的地址对象，并进入地址对象视图。类型 object 表明创建的是地址对象。

address 10 192.168.2.0 0.0.0.255 是系统视图下使用的命令，该命令的作用是在地址对

象中添加 CIDR 地址块 192.168.2.0/24。其中 10 是添加的地址块的序号，192.168.2.0 是 CIDR 地址块 192.168.2.0/24 的起始地址，0.0.0.255 是反掩码，对应子网掩码 255.255.255.0，用于将 CIDR 地址块网络前缀长度确定为 24。

2）将接口加入安全区域中

以下命令序列用于将接口 GigabitEthernet1/0/0 和 GigabitEthernet1/0/3 加入名为 trust 的安全区域中。USG6000V 默认状态下存在 4 个安全区域，分别是安全区域 trust、untrust、dmz 和 local，这些安全区域的优先级是固定的。local 的优先级最高，之后依次是 trust、dmz 和 untrust。安全区域 local 中不能分配接口。

```
[USG6000V1]firewall zone trust
[USG6000V1-zone-trust]add interface GigabitEthernet1/0/0
[USG6000V1-zone-trust]add interface GigabitEthernet1/0/3
[USG6000V1-zone-trust]quit
```

firewall zone trust 是系统视图下使用的命令，该命令的作用是进入名为 trust 的安全区域视图。

add interface GigabitEthernet1/0/0 是安全区域视图下使用的命令，该命令的作用是将接口 GigabitEthernet1/0/0 加入当前安全区域（这里是名为 trust 的安全区域）。

3）配置安全策略

默认状态下，允许信息流从高优先级安全区域传输到低优先级安全区域，禁止信息流从低优先级安全区域传输到高优先级安全区域。通过配置安全策略，可以实现双向传输过程，即安全策略一旦允许访问请求从 x 安全区域传输到 y 安全区域，即允许该访问请求对应的访问响应从 y 安全区域传输到 x 安全区域。

```
[USG6000V1]security-policy
[USG6000V1-policy-security]rule name policy1
[USG6000V1-policy-security-rule-policy1]source-zone trust
[USG6000V1-policy-security-rule-policy1]destination-zone untrust
[USG6000V1-policy-security-rule-policy1]source-address address-set aa
[USG6000V1-policy-security-rule-policy1]action permit
[USG6000V1-policy-security-rule-policy1]quit
[USG6000V1-policy-security]quit
```

security-policy 是系统视图下使用的命令，该命令的作用是进入安全策略视图。

rule name policy1 是安全策略视图下使用的命令，该命令的作用是创建一条名为 policy1 的规则，并进入安全策略规则视图。policy1 是规则名称。

source-zone trust 是安全策略规则视图下使用的命令，该命令的作用是为当前规则（这里是名为 policy1 的规则）指定源安全区域。这里指定的源安全区域是区域 trust。

destination-zone untrust 是安全策略规则视图下使用的命令，该命令的作用是为当前规则（这里是名为 policy1 的规则）指定目的安全区域。这里指定的目的安全区域是区域 untrust。

source-address address-set aa 是安全策略规则视图下使用的命令，该命令的作用是为当前规则（这里是名为 policy1 的规则）指定源 IP 地址范围。这里指定的源 IP 地址范围是

名为 aa 的地址对象所涵盖的地址范围，即 CIDR 地址块 192.168.2.0/24、192.168.3.0/24 和 192.168.4.0/24。

action permit 是安全策略规则视图下使用的命令，该命令的作用是为当前规则（这里是名为 policy1 的规则）指定动作。这里的动作是允许，即允许继续转发符合规则中所有条件的 IP 分组。

需要说明的是，对于实现允许内部网络访问 Internet 的访问控制策略的规则，只需要在区域 trust 至区域 untrust 方向配置允许传输与内部网络访问 Internet 有关的请求报文的规则，无须在区域 untrust 至区域 trust 方向配置允许传输 Internet 发送给内部网络的响应报文的规则，这是有状态分组过滤器的特点，在区域 trust 至区域 untrust 方向已经传输内部网络发送给 Internet 的请求报文后，区域 untrust 至区域 trust 方向自动添加允许传输 Internet 发送给内部网络的响应报文的规则，且该规则的条件根据监测到的内部网络发送给 Internet 的请求报文的字段值产生。

4）配置 NAT 策略

```
[USG6000V1]nat-policy
[USG6000V1-policy-nat]rule name policy2
[USG6000V1-policy-nat-rule-policy2]source-zone trust
[USG6000V1-policy-nat-rule-policy2]destination-zone untrust
[USG6000V1-policy-nat-rule-policy2]source-address address-set aa
[USG6000V1-policy-nat-rule-policy2]action source-nat easy-ip
[USG6000V1-policy-nat-rule-policy2]quit
[USG6000V1-policy-nat]quit
```

nat-policy 是系统视图下使用的命令，该命令的作用是进入 NAT 策略视图。

rule name policy2 是 NAT 策略视图下使用的命令，该命令的作用是创建一条名为 policy2 的规则，并进入 NAT 策略规则视图。policy2 是规则名称。

action source-nat easy-ip 是 NAT 策略规则视图下使用的命令，该命令的作用是为当前规则（这里是名为 policy2 的规则）指定动作。这里的动作是基于 PAT 实施源地址转换，用信息流的输出接口的 IP 地址作为转换后的信息流的源 IP 地址。

3.2.5 实验步骤

（1）启动 eNSP，按照如图 3.1 所示的企业网结构放置和连接设备。完成设备放置和连接后的 eNSP 界面如图 3.2 所示。启动所有设备。图 3.2 中的防火墙 FW1 是 USG6000V。

（2）完成交换机 LSW1～LSW6 VLAN 配置过程和端口分配过程。LSW1、LSW5 和 LSW6 中创建的 VLAN 和分配给各个 VLAN 的交换机端口如图 3.3～图 3.5 所示。LSW1 中创建分别用于连接普通终端和业务员终端的 VLAN 2 和 VLAN 3，默认 VLAN（这里是 VLAN 1）连接作为 DHCP 服务器的 AR0。LSW5 和 LSW6 中创建分别用于连接普通终端、业务员终端和管理层终端的 VLAN 2、VLAN 3 和 VLAN 4。创建这些 VLAN 的目的是定义这些 VLAN 对应的 IP 接口。LSW5 中还创建了分别用于连接 FW1 和 AR1 的 VLAN 5 和 VLAN 6。LSW6 中还创建了分别用于连接 FW1 和 AR1 的 VLAN 7 和 VLAN 8。

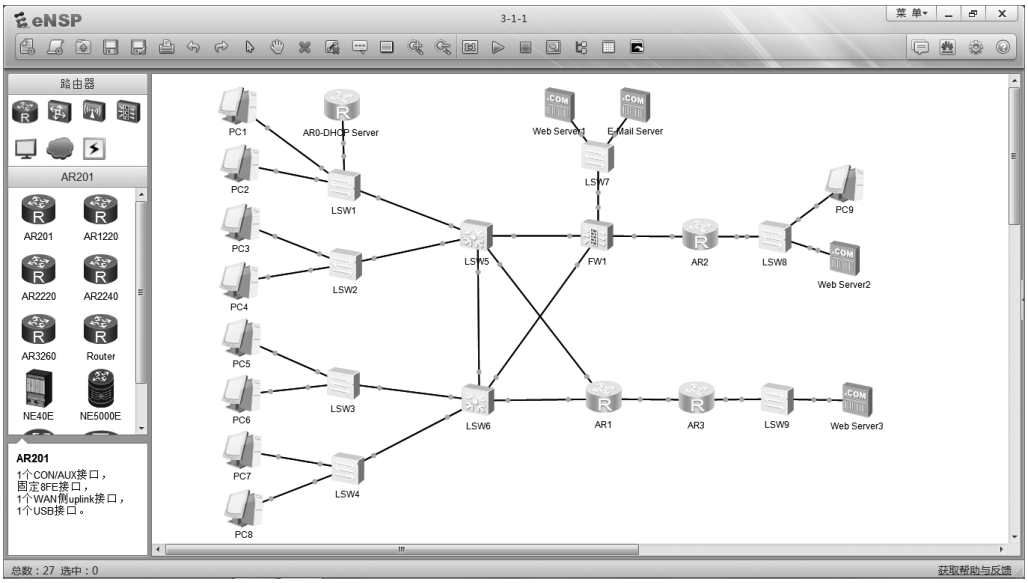


图 3.2　完成设备放置和连接后的 eNSP 界面

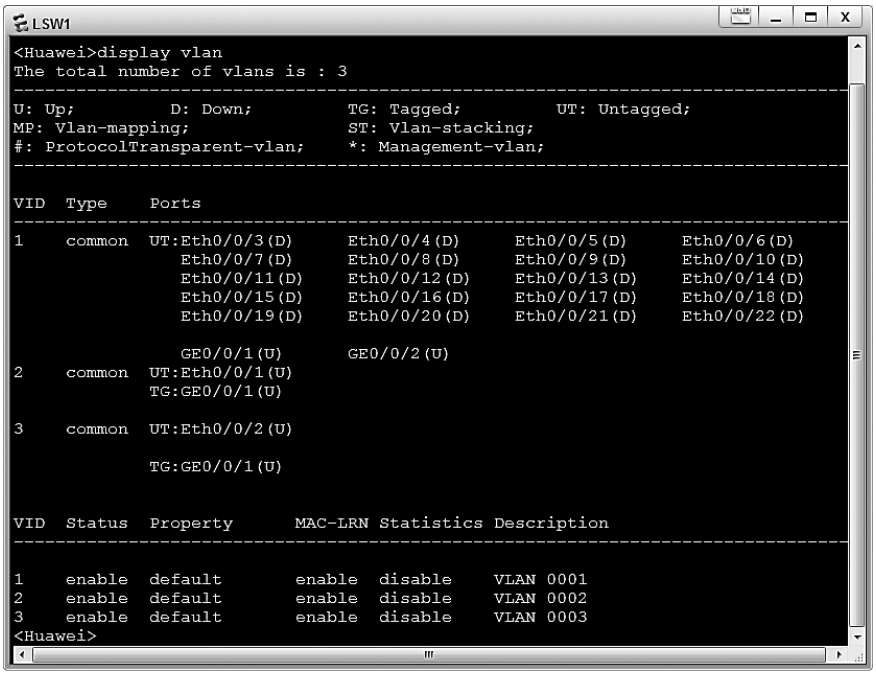


图 3.3　LSW1 有关 VLAN 的状态

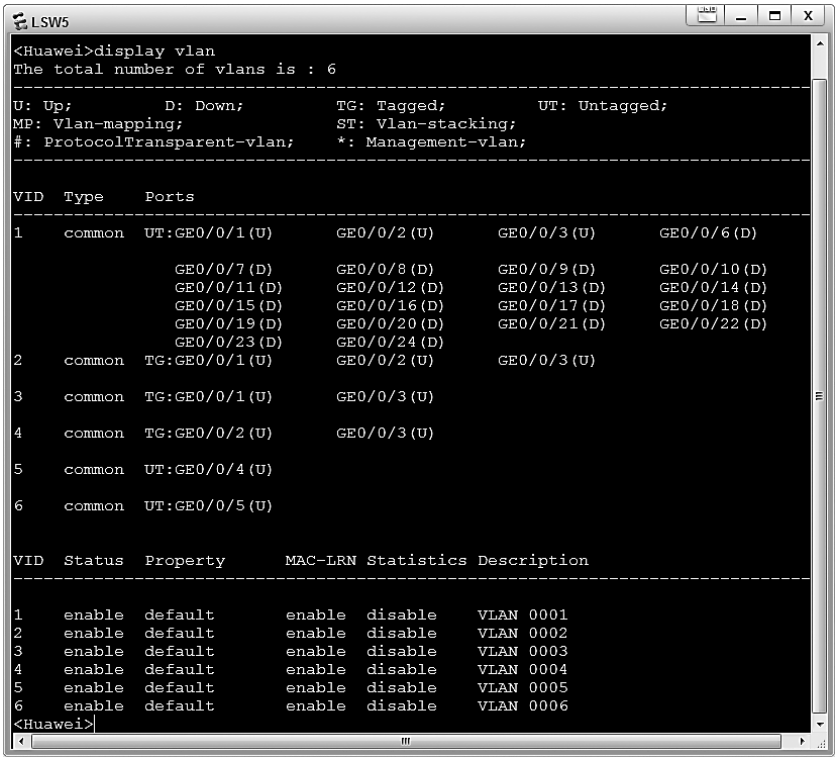


图 3.4　LSW5 有关 VLAN 的状态

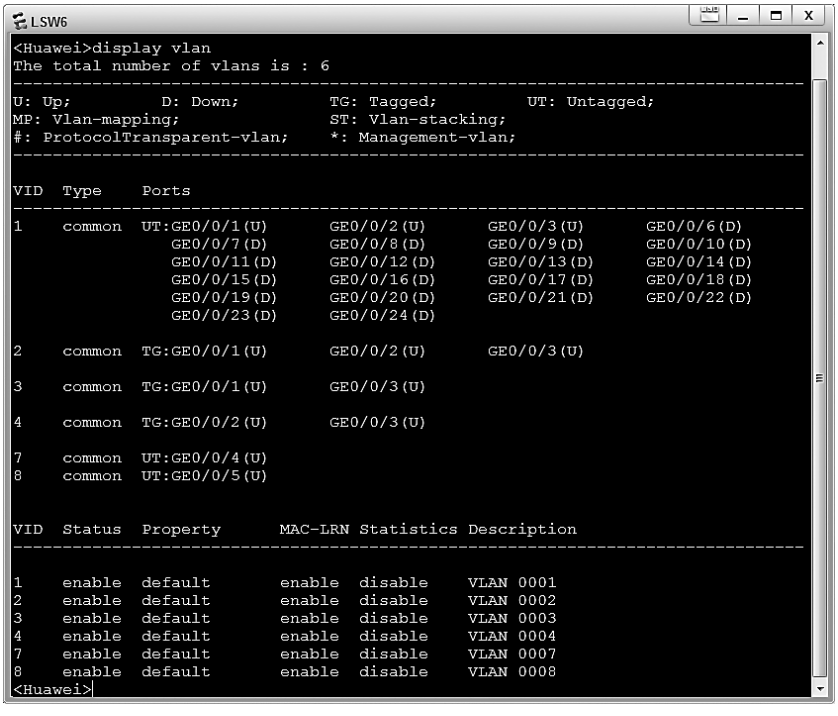


图 3.5　LSW6 有关 VLAN 的状态

(3) 在三层交换机 LSW5 和 LSW6 中定义各个 VLAN 对应的 IP 接口,为这些 IP 接口分配 IP 地址和子网掩码。LSW5 和 LSW6 中各个 VLAN 对应的 IP 接口的状态分别如图 3.6 和图 3.7 所示。需要说明的是,LSW5 和 LSW6 中分别定义了 VLAN 1～VLAN 4 对应的 IP 接口,针对同一个 VLAN 对应的 IP 接口,LSW5 和 LSW6 分别分配网络号相同、主机号不同的 IP 地址,如针对 VLAN 1 对应的 IP 接口,LSW5 和 LSW6 分别分配 IP 地址和子网掩码 192.168.1.254/24 和 192.168.1.253/24。FW1、AR2、AR1 和 AR3 各个 IP 接口配置的 IP 地址和子网掩码如图 3.8～图 3.11 所示。

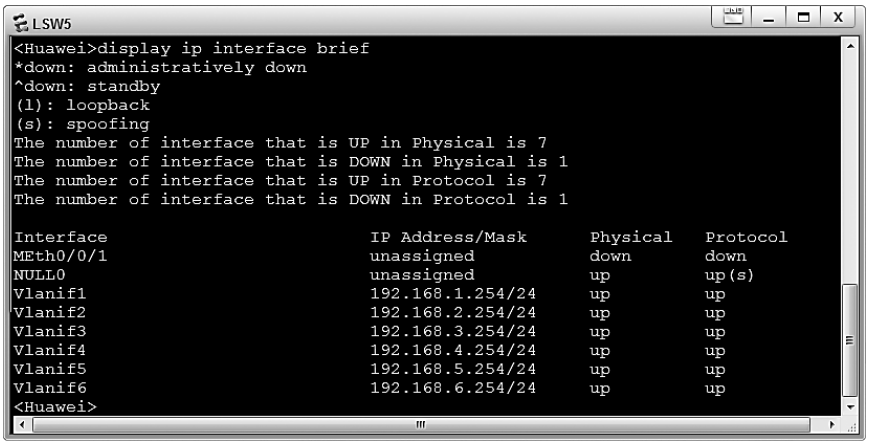


图 3.6　LSW5 中各个 VLAN 对应的 IP 接口的状态

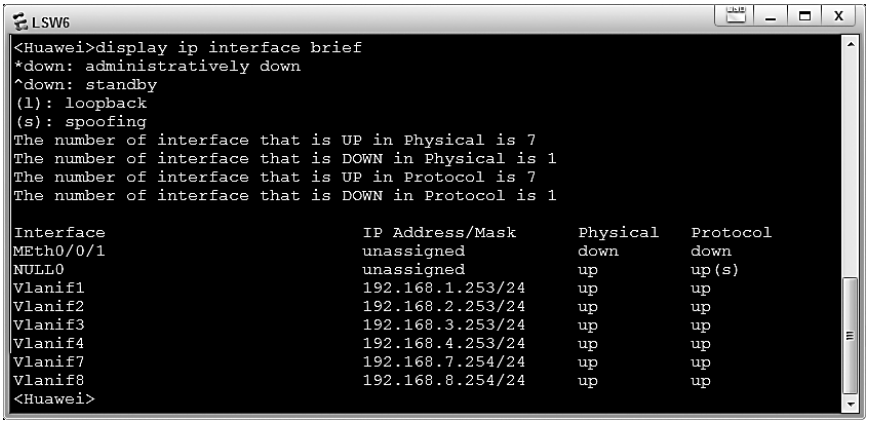


图 3.7　LSW6 中各个 VLAN 对应的 IP 接口的状态

(4) 针对 VLAN 1～VLAN 4,配置冗余网关,将 LSW5 中这 4 个 VLAN 对应的 IP 接口作为活跃 IP 接口,将 LSW6 中这 4 个 VLAN 对应的 IP 接口作为备份 IP 接口。图 3.12 所示的 LSW5 冗余网关信息表明,VRID 分别为 1、2、3 和 4 的虚拟路由器接口都是主路由器接口。图 3.13 所示的 LSW6 冗余网关信息表明,VRID 分别为 1、2、3 和 4 的虚拟路由器接口都是备份路由器接口。

VLAN 1～VLAN 4 对应的冗余网关的虚拟 IP 地址(Virtual IP)分别是 192.168.1.250、192.168.2.250、192.168.3.250 和 192.168.4.250。

FW1

```
<USG6000V1>display ip interface brief
2020-12-03 04:15:09.410
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(d): Dampening Suppressed
(E): E-Trunk down
The number of interface that is UP in Physical is 6
The number of interface that is DOWN in Physical is 4
The number of interface that is UP in Protocol is 6
The number of interface that is DOWN in Protocol is 4

Interface                         IP Address/Mask      Physical   Protocol
GigabitEthernet0/0/0              unassigned           down       down
GigabitEthernet1/0/0              192.168.7.253/24     up         up
GigabitEthernet1/0/1              192.1.1.1/30         up         up
GigabitEthernet1/0/2              192.1.2.254/24       up         up
GigabitEthernet1/0/3              192.168.5.253/24     up         up
GigabitEthernet1/0/4              unassigned           down       down
GigabitEthernet1/0/5              unassigned           down       down
GigabitEthernet1/0/6              unassigned           down       down
NULL0                             unassigned           up         up(s)
Virtual-if0                       unassigned           up         up(s)

<USG6000V1>
```

图 3.8　防火墙 FW1 各个 IP 接口配置的 IP 地址和子网掩码

AR2

```
<Huawei>display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 3
The number of interface that is DOWN in Protocol is 0

Interface                         IP Address/Mask      Physical
GigabitEthernet0/0/0              192.1.1.2/30         up
GigabitEthernet0/0/1              192.1.3.254/24       up
NULL0                             unassigned           up
<Huawei>
```

图 3.9　路由器 AR2 各个 IP 接口配置的 IP 地址和子网掩码

AR1

```
<Huawei>display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 4
The number of interface that is DOWN in Physical is 0
The number of interface that is UP in Protocol is 4
The number of interface that is DOWN in Protocol is 0

Interface                         IP Address/Mask      Physical
GigabitEthernet0/0/0              192.168.6.253/24     up
GigabitEthernet0/0/1              192.168.8.253/24     up
GigabitEthernet0/0/2              200.0.0.1/30         up
NULL0                             unassigned           up
<Huawei>
```

图 3.10　路由器 AR1 各个 IP 接口配置的 IP 地址和子网掩码

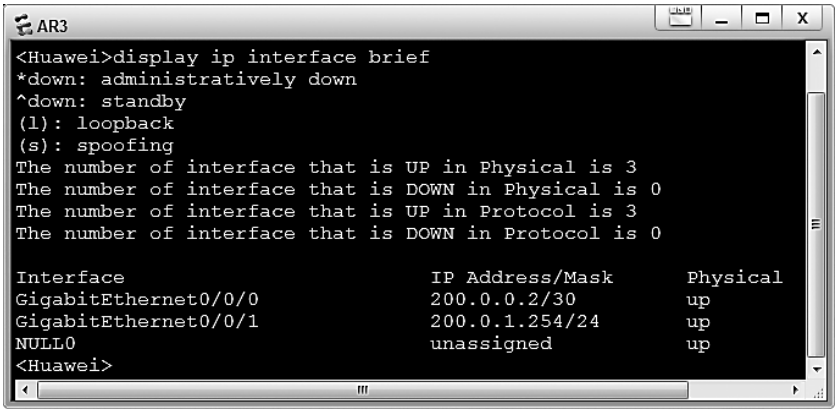


图 3.11　路由器 AR3 各个 IP 接口配置的 IP 地址和子网掩码

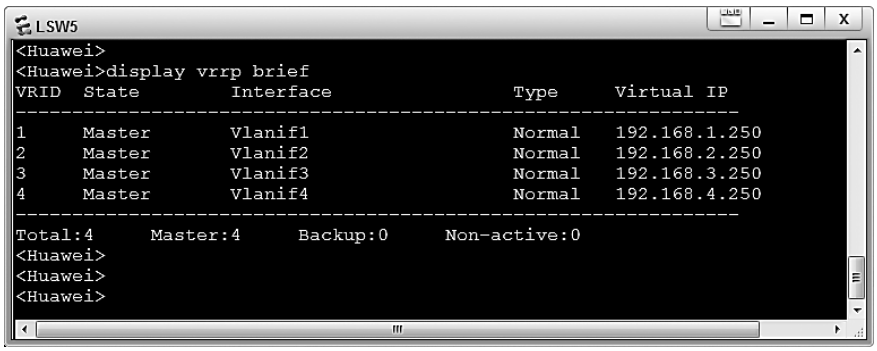


图 3.12　LSW5 冗余网关信息

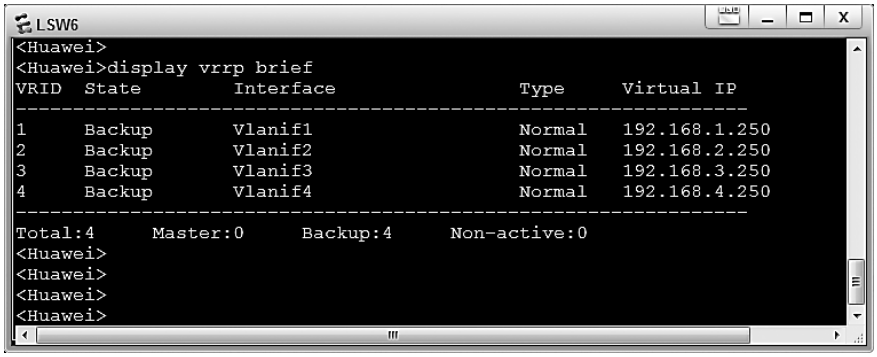
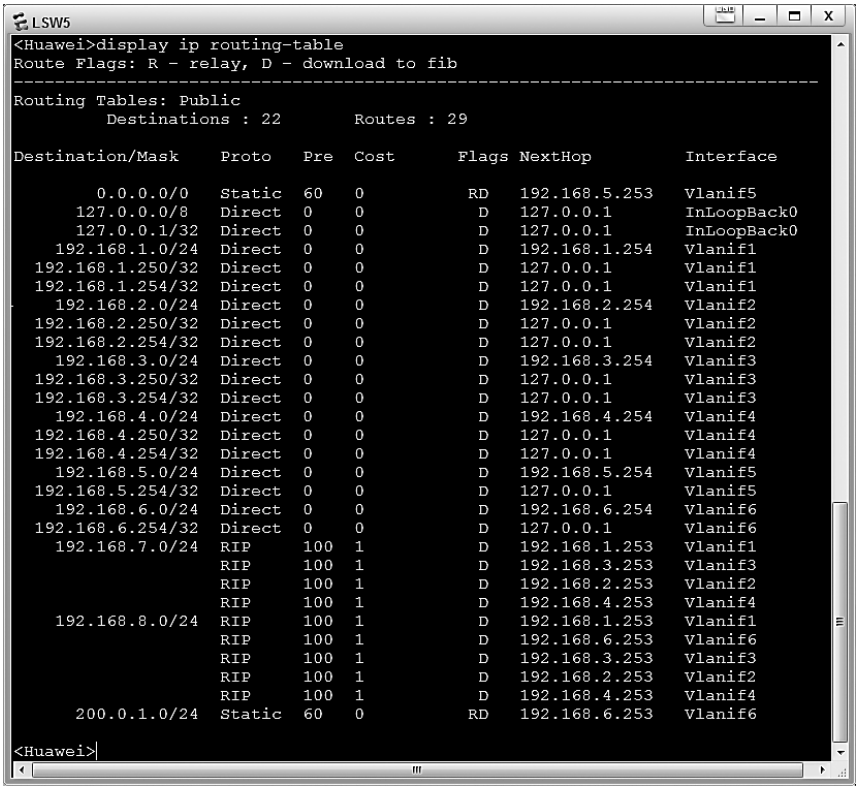


图 3.13　LSW6 冗余网关信息

（5）完成 LSW5、LSW6、防火墙 FW1 和路由器 AR1 的 RIP 配置过程。完成防火墙 FW1，路由器 AR2、AR1 和 AR3 的 OSPF 配置过程。LSW5、LSW6、防火墙 FW1 和路由器 AR1 通过 RIP 创建用于指明通往内部网络各个子网的传输路径的路由项。防火墙 FW1，路由器 AR2、AR1 和 AR3 通过 OSPF 创建用于指明通往 Internet 和行业服务网的传输路径的路由项。LSW5、LSW6、FW1、AR2、AR1 和 AR3 的完整路由表如图 3.14～图 3.20 所



LSW5

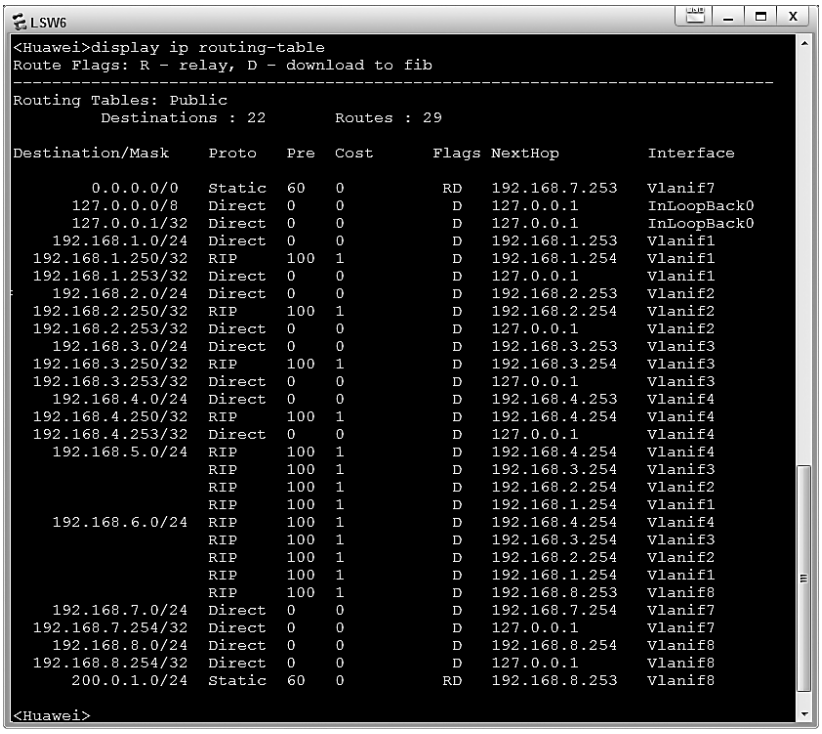
```
<Huawei>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 22        Routes : 29

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD   192.168.5.253   Vlanif5
      127.0.0.0/8   Direct  0    0           D    127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D    127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D    192.168.1.254   Vlanif1
  192.168.1.250/32  Direct  0    0           D    127.0.0.1       Vlanif1
  192.168.1.254/32  Direct  0    0           D    127.0.0.1       Vlanif1
    192.168.2.0/24  Direct  0    0           D    192.168.2.254   Vlanif2
  192.168.2.250/32  Direct  0    0           D    127.0.0.1       Vlanif2
  192.168.2.254/32  Direct  0    0           D    127.0.0.1       Vlanif2
    192.168.3.0/24  Direct  0    0           D    192.168.3.254   Vlanif3
  192.168.3.250/32  Direct  0    0           D    127.0.0.1       Vlanif3
  192.168.3.254/32  Direct  0    0           D    127.0.0.1       Vlanif3
    192.168.4.0/24  Direct  0    0           D    192.168.4.254   Vlanif4
  192.168.4.250/32  Direct  0    0           D    127.0.0.1       Vlanif4
  192.168.4.254/32  Direct  0    0           D    127.0.0.1       Vlanif4
    192.168.5.0/24  Direct  0    0           D    192.168.5.254   Vlanif5
  192.168.5.254/32  Direct  0    0           D    127.0.0.1       Vlanif5
    192.168.6.0/24  Direct  0    0           D    192.168.6.254   Vlanif6
  192.168.6.254/32  Direct  0    0           D    127.0.0.1       Vlanif6
    192.168.7.0/24  RIP     100  1           D    192.168.1.253   Vlanif1
                    RIP     100  1           D    192.168.3.253   Vlanif3
                    RIP     100  1           D    192.168.2.253   Vlanif2
                    RIP     100  1           D    192.168.4.253   Vlanif4
    192.168.8.0/24  RIP     100  1           D    192.168.1.253   Vlanif1
                    RIP     100  1           D    192.168.6.253   Vlanif6
                    RIP     100  1           D    192.168.3.253   Vlanif3
                    RIP     100  1           D    192.168.2.253   Vlanif2
                    RIP     100  1           D    192.168.4.253   Vlanif4
     200.0.1.0/24   Static  60   0           RD   192.168.6.253   Vlanif6

<Huawei>
```

图 3.14　LSW5 的完整路由表



LSW6

```
<Huawei>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 22        Routes : 29

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD   192.168.7.253   Vlanif7
      127.0.0.0/8   Direct  0    0           D    127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D    127.0.0.1       InLoopBack0
    192.168.1.0/24  Direct  0    0           D    192.168.1.253   Vlanif1
  192.168.1.250/32  RIP     100  1           D    192.168.1.254   Vlanif1
  192.168.1.253/32  Direct  0    0           D    127.0.0.1       Vlanif1
    192.168.2.0/24  Direct  0    0           D    192.168.2.253   Vlanif2
  192.168.2.250/32  RIP     100  1           D    192.168.2.254   Vlanif2
  192.168.2.253/32  Direct  0    0           D    127.0.0.1       Vlanif2
    192.168.3.0/24  Direct  0    0           D    192.168.3.253   Vlanif3
  192.168.3.250/32  RIP     100  1           D    192.168.3.254   Vlanif3
  192.168.3.253/32  Direct  0    0           D    127.0.0.1       Vlanif3
    192.168.4.0/24  Direct  0    0           D    192.168.4.253   Vlanif4
  192.168.4.250/32  RIP     100  1           D    192.168.4.254   Vlanif4
  192.168.4.253/32  Direct  0    0           D    127.0.0.1       Vlanif4
    192.168.5.0/24  RIP     100  1           D    192.168.4.254   Vlanif4
                    RIP     100  1           D    192.168.3.254   Vlanif3
                    RIP     100  1           D    192.168.2.254   Vlanif2
                    RIP     100  1           D    192.168.1.254   Vlanif1
    192.168.6.0/24  RIP     100  1           D    192.168.4.254   Vlanif4
                    RIP     100  1           D    192.168.3.254   Vlanif3
                    RIP     100  1           D    192.168.2.254   Vlanif2
                    RIP     100  1           D    192.168.1.254   Vlanif1
                    RIP     100  1           D    192.168.8.253   Vlanif8
    192.168.7.0/24  Direct  0    0           D    192.168.7.254   Vlanif7
  192.168.7.254/32  Direct  0    0           D    127.0.0.1       Vlanif7
    192.168.8.0/24  Direct  0    0           D    192.168.8.254   Vlanif8
  192.168.8.254/32  Direct  0    0           D    127.0.0.1       Vlanif8
     200.0.1.0/24   Static  60   0           RD   192.168.8.253   Vlanif8

<Huawei>
```

图 3.15　LSW6 的完整路由表

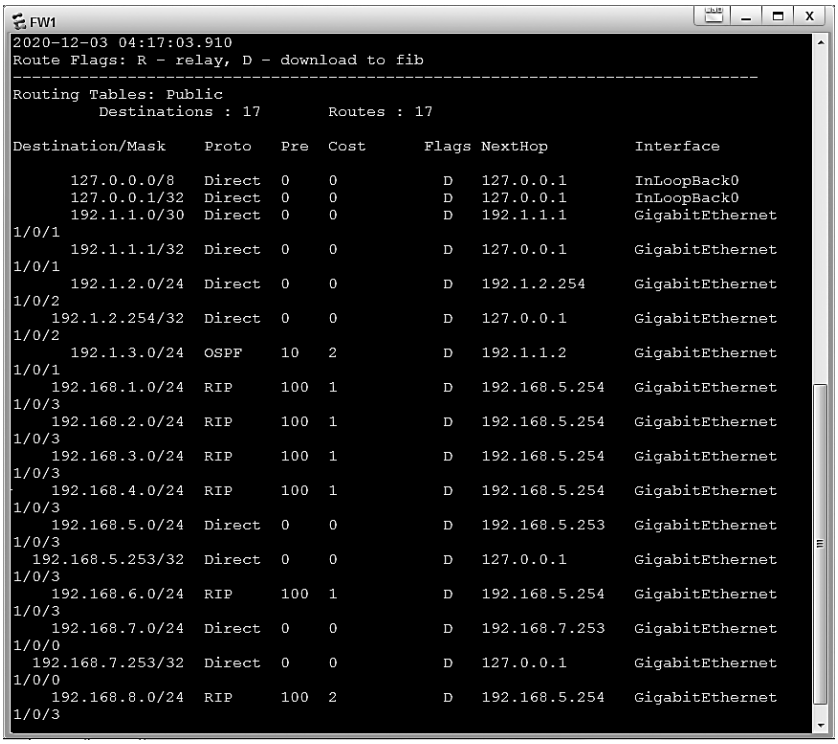


图 3.16　防火墙 FW1 的完整路由表

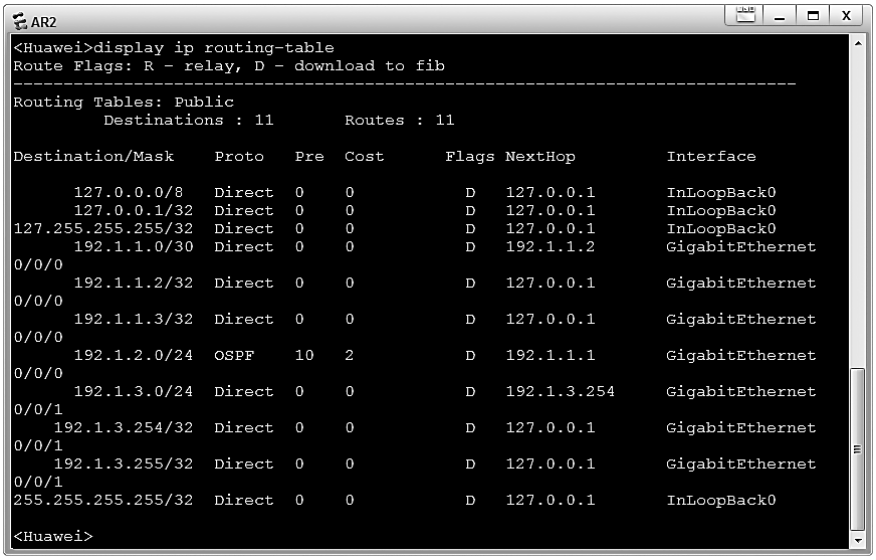


图 3.17　AR2 的完整路由表

AR1

```
<Huawei>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 20        Routes : 24

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
    192.168.1.0/24  RIP     100  1           D   192.168.6.254   GigabitEthernet
0/0/0
                    RIP     100  1           D   192.168.8.254   GigabitEthernet
0/0/1
    192.168.2.0/24  RIP     100  1           D   192.168.6.254   GigabitEthernet
0/0/0
                    RIP     100  1           D   192.168.8.254   GigabitEthernet
0/0/1
    192.168.3.0/24  RIP     100  1           D   192.168.6.254   GigabitEthernet
0/0/0
                    RIP     100  1           D   192.168.8.254   GigabitEthernet
0/0/1
    192.168.4.0/24  RIP     100  1           D   192.168.6.254   GigabitEthernet
0/0/0
                    RIP     100  1           D   192.168.8.254   GigabitEthernet
0/0/1
    192.168.5.0/24  RIP     100  1           D   192.168.6.254   GigabitEthernet
0/0/0
    192.168.6.0/24  Direct  0    0           D   192.168.6.253   GigabitEthernet
0/0/0
  192.168.6.253/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
  192.168.6.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
    192.168.7.0/24  RIP     100  1           D   192.168.8.254   GigabitEthernet
0/0/1
    192.168.8.0/24  Direct  0    0           D   192.168.8.253   GigabitEthernet
0/0/1
```

图 3.18　AR1 的完整路由表(一)

AR1

```
  192.168.8.253/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
  192.168.8.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
      200.0.0.0/30  Direct  0    0           D   200.0.0.1       GigabitEthernet
0/0/2
      200.0.0.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
      200.0.0.3/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/2
      200.0.1.0/24  OSPF    10   2           D   200.0.0.2       GigabitEthernet
0/0/2
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

<Huawei>
```

图 3.19　AR1 的完整路由表(二)

AR3

```
<Huawei>display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10        Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      200.0.0.0/30  Direct  0    0           D   200.0.0.2       GigabitEthernet
0/0/0
      200.0.0.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
      200.0.0.3/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/0
      200.0.1.0/24  Direct  0    0           D   200.0.1.254     GigabitEthernet
0/0/1
    200.0.1.254/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
    200.0.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet
0/0/1
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

<Huawei>
```

图 3.20　AR3 的完整路由表

示。LSW5 和 LSW6 完整路由表中不但有 RIP 建立的用于指明通往内部网络各个子网的传输路径的路由项，还有用于指明通往 Internet 和行业服务网的传输路径的静态路由项。防火墙 FW1 的路由表中，不仅包含 RIP 生成的用于指明通往内部网络各个子网的传输路径的路由项，还包含 OSPF 生成的用于指明通往 DMZ 和 Internet 的传输路径的路由项。路由器 AR2 的路由表中，只包含 OSPF 生成的用于指明通往 DMZ 和 Internet 的传输路径的路由项，内部网络对 AR2 是透明的。同样，路由器 AR1 的路由表中，不仅包含 RIP 生成的用于指明通往内部网络各个子网的传输路径的路由项，还包含 OSPF 生成的用于指明通往行业服务网的传输路径的路由项。路由器 AR3 的路由表中，只包含用于指明通往路由器 AR1 连接行业服务网的接口和行业服务网 200.0.1.0/24 的传输路径的路由项，内部网络对 AR3 也是透明的。

（6）在仿真 DHCP 服务器的路由器 AR0 上创建 VLAN 2、VLAN 3 和 VLAN 4 对应的作用域，这 3 个作用域对应的 IP 地址池如图 3.21 所示。分别在三层交换机 LSW5 和 LSW6 中 VLAN 2、VLAN 3 和 VLAN 4 对应的 IP 接口上启动 DHCP 中继功能，配置 DHCP 服务器的 IP 地址。三层交换机 LSW5 和 LSW6 配置的中继信息分别如图 3.22 和图 3.23 所示。完成 DHCP 配置过程后，各个终端可以自动获取网络信息。如图 3.24 所示为 PC1 的基础配置界面，选择 DHCP 自动获取网络信息方式。如图 3.25 所示为 PC1 自动获取的网络信息。如图 3.26 所示为 PC2 自动获取的网络信息。PC1 是普通用户终端，连接在 VLAN 2 上。PC2 是业务员终端，连接在 VLAN 3 上。

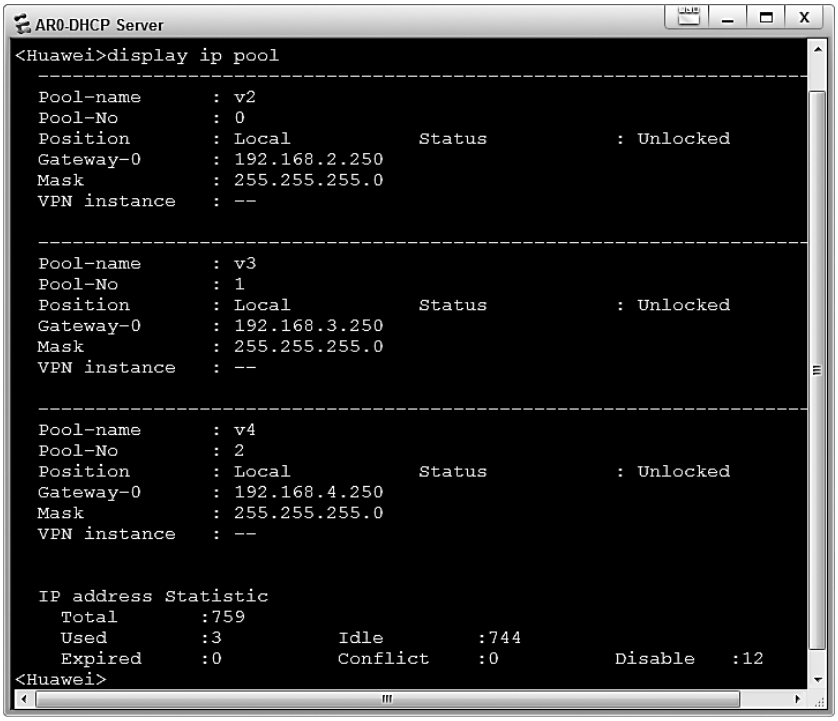


图 3.21　仿真 DHCP 服务器的 AR0 配置的作用域

（7）在防火墙 FW1 和路由器 AR1 中完成有关 PAT 的配置过程，允许连接在 VLAN 2、VLAN 3 和 VLAN 4 上的终端访问 Internet，允许连接在 VLAN 3 和 VLAN 4 上的终端访问行

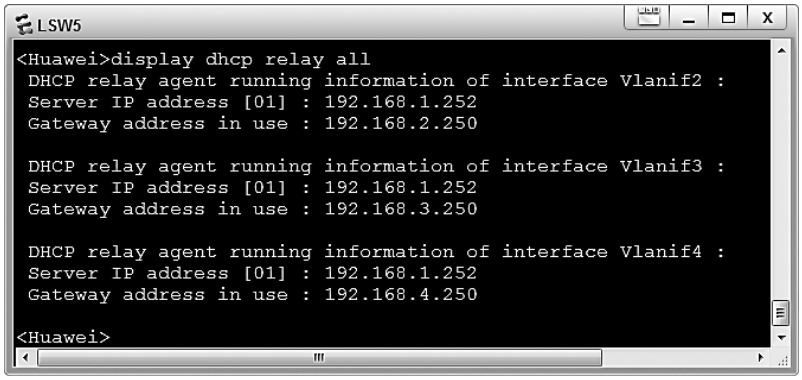


图 3.22　LSW5 配置的中继信息

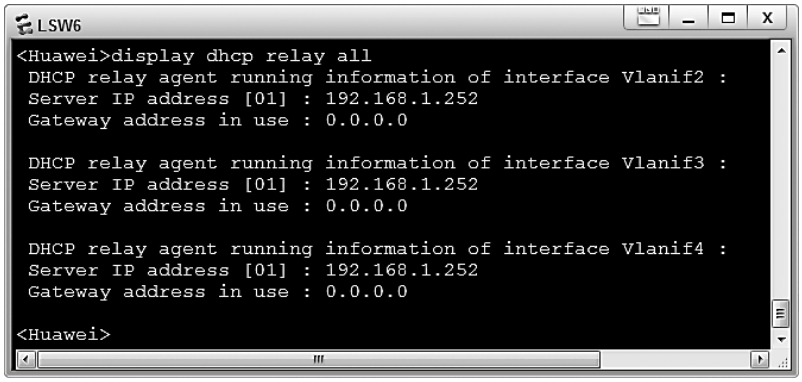


图 3.23　LSW6 配置的中继信息

图 3.24　PC1 的基础配置界面

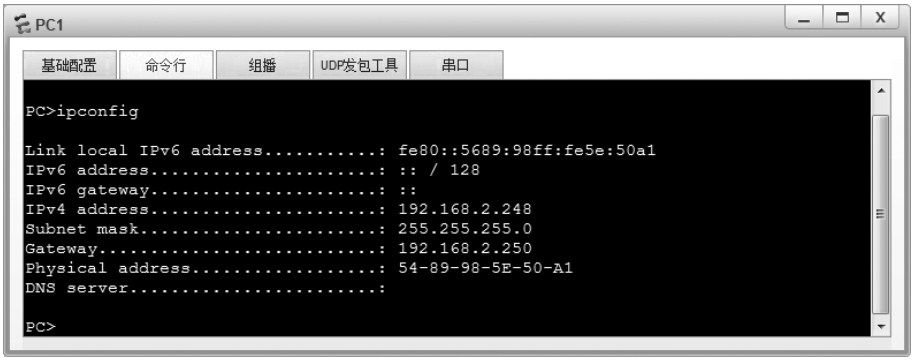


图 3.25　PC1 自动获取的网络信息

图 3.26　PC2 自动获取的网络信息

业服务网。防火墙通过地址转换策略完成 PAT 配置过程，指定允许进行地址转换的内部网络私有 IP 地址范围的 IP 地址集如图 3.27 所示，涵盖内部网络中的子网 192.168.2.0/24、192.168.3.0/24 和 192.168.4.0/24。为了实现内部网络访问 Internet 的过程，需要配置允许内部网络访问 Internet 的安全策略。为了通过 OSPF 建立用于指明通往 Internet 的传输路径的路由项，需要配置允许 OSPF 消息传输给防火墙 FW1 的安全策略。防火墙 FW1 配置的安全策略如图 3.28 所示。防火墙 FW1 配置的 NAT 策略如图 3.29 所示，easy-ip 表明采用 PAT 方式。

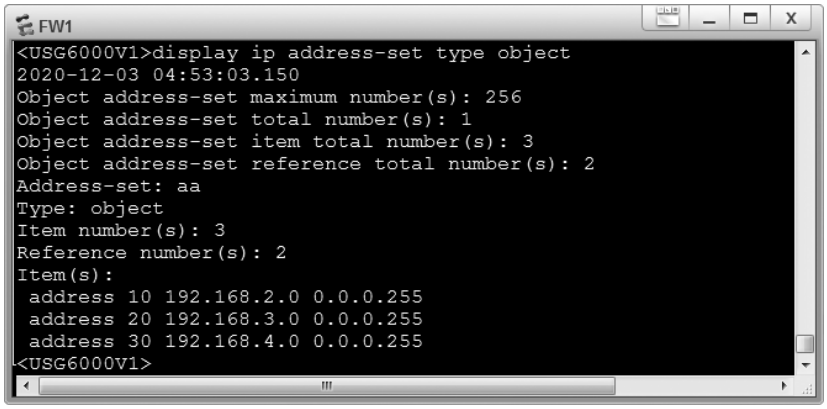


图 3.27　防火墙 FW1 配置的地址集

```
FW1
<USG6000V1>display security-policy rule name policy1
2020-12-03 04:44:26.310
 (0 times matched)
 rule name policy1
  source-zone trust
  destination-zone untrust
  source-address address-set aa
  action permit
<USG6000V1>display security-policy rule name policy3
2020-12-03 04:44:37.650
 (0 times matched)
 rule name policy3
  source-zone untrust
  source-address 192.1.1.2 mask 255.255.255.255
  service protocol 89
  action permit
<USG6000V1>
```

图 3.28　防火墙 FW1 配置的安全策略

```
FW1

<USG6000V1>display nat-policy rule name policy2
2020-12-03 04:46:05.040
 (0 times matched)
 rule name policy2
  source-zone trust
  destination-zone untrust
  source-address address-set aa
  action source-nat easy-ip
<USG6000V1>
<USG6000V1>
<USG6000V1>
<USG6000V1>
```

图 3.29　防火墙 FW1 配置的 NAT 策略

路由器 AR1 通过配置访问控制列表(ACL)指定允许进行地址转换的内部网络私有 IP 地址范围,访问控制列表指定的私有 IP 地址范围是 192.168.3.0/24 和 192.168.4.0/24,如图 3.30 所示。在路由器 AR1 连接行业服务网的接口启动 PAT 功能,如图 3.30 所示。

```
AR1
<Huawei>display acl all
 Total quantity of nonempty ACL number is 1

Basic ACL 2000, 2 rules
Acl's step is 5
 rule 10 permit source 192.168.3.0 0.0.0.255
 rule 20 permit source 192.168.4.0 0.0.0.255

<Huawei>display nat outbound
 NAT Outbound Information:
 --------------------------------------------------------------------------
 Interface                   ACL     Address-group/IP/Interface      Type
 --------------------------------------------------------------------------
 GigabitEthernet0/0/2        2000                    200.0.0.1    easyip
 --------------------------------------------------------------------------
  Total : 1
<Huawei>
```

图 3.30　路由器 AR1 配置的 ACL 和实施 PAT 的接口

(8) 验证连接在 VLAN 2、VLAN 3 和 VLAN 4 上的终端可以访问 Internet，只有连接在 VLAN 3 和 VLAN 4 上的终端可以访问行业服务网。因此，PC1 只能 ping 通连接在 Internet 上的 Web Server2，PC2 可以 ping 通连接在 Internet 上的 Web Server2 和连接在行业服务网上的 Web Server3。Web Server2 和 Web Server3 的基础配置界面分别如图 3.31 和图 3.32 所示。PC1 和 PC2 的命令行操作界面分别如图 3.33 和图 3.34 所示。

图 3.31　Web Server2 的基础配置界面

图 3.32　Web Server3 的基础配置界面