

网络实验课程实用操作命令

1 基本命令	7
1.1 设备管理	7
1.1.1 查看当前配置	7
1.1.2 清除配置文件	7
1.1.3 重启设备	7
1.2 常用命令	7
1.2.1 进入系统视图	7
1.2.2 更改设备标号	7
1.2.3 显示设备端口	7
1.2.4 进入端口视图	7
1.2.5 配置端口IP	7
1.2.6 关闭/开启端口	7
1.2.7 查看路由表	8
1.2.8 更改端口转发速率	8
1.3 其它	8
1.3.1 特殊键的使用	8
1.3.2 清空交换机MAC地址表	8
1.3.3 清空交换机ARP缓存	8
2 LoopBack端口	8
2.1 添加LoopBack端口	8
2.2 删除LoopBack端口	8
3 VLAN配置	9
3.1 生成VLAN	9

3.2 添加端口	9
3.3 端口类型配置	9
3.4 配置端口聚合	10
4 网络地址转换	10
4.1 配置访问控制列表	10
4.2 配置地址池	10
4.3 配置NAT转换	10
4.4 配置静态路由	10
5 PPP协议配置	11
5.1 PAP验证方式	11
5.1.1 服务端	11
5.1.2 客户端	11
5.2 CHAP验证方式	12
5.2.1 服务端	12
5.2.2 客户端	12
5.3 重启端口以便命令生效	12
6 帧中继协议配置	12
7 OSPF协议配置	13
7.1 启用OSPF	13
7.2 修改端口的COST值	13
7.3 路由导入命令	13
7.3.1 导入直连路由	13

7.3.2 导入静态路由	13
7.4 查看OSPF路由	14
8 BGP协议配置	14
8.1 拓扑图	14
8.2 路由上的配置	14
8.3 交换机上的配置	14
8.4 注入路由信息	15
8.5 强制下一跳地址	15
8.6 路由聚合	15
8.6.1 同时通告聚合路由和具体路由	15
8.6.2 只通告聚合路由	15
8.7 BGP路由策略	15
8.7.1 基于ACL的路由过滤	15
8.7.2 基于AS-Path的路由过滤	15
8.7.3 基于Route Policy的路由过滤	16
8.8 查看BGP路由	16
8.9 其它相关命令	16
8.9.1 Debug bgp命令	16
8.9.2 取消debug dgp命令	16
8.9.3 重新启动BGP协议	17
8.9.4 显示BGP邻居状态	17
8.9.5 显示BGP路由表	17
9 SNMP协议配置	17

9.1 启用SNMP代理	17
9.2 配置trap	17
10 传输层实验	17
10.1 配置IP地址	17
10.2 开启FTP	18
10.2.1 直接使用root作为FTP账号	18
10.2.2 启动FTP服务	18
10.3 实时监控模块（TCPConnetion）	18
10.3.1 初始化	18
10.3.2 读取记录	18
10.4 启动丢包内核模块	18
10.5 启动TCPTest	19
11 组播实验	19
11.1 PIM协议配置	19
11.1.1 PIM-DM协议配置	19
11.1.2 PIM-SM协议配置	19
11.1.3 查看组播路由表	20
11.2 IGMP协议配置	20
11.2.1 启动IGMP	20
11.2.2 查看IGMP配置	20
12 其它知识点	20
12.1 网线类型的选择	20
12.2 IP地址分类	20

12.3 内网IP地址.....	21
12.4 组播IP地址.....	21

修订记录

版本	日期	作者	更改内容
0.1	2009-04-26	高宾	初稿

1 基本命令

1.1 设备管理

1.1.1 查看当前配置

[Quidway] display current-configuration

1.1.2 清除配置文件

<Quidway> reset saved-configuration

1.1.3 重启设备

<Quidway> reboot

1.2 常用命令

1.2.1 进入系统视图

<Quidway> system

1.2.2 更改设备标号

[Quidway] sysname R1

1.2.3 显示设备端口

此命令可以让你了解设备有哪些端口可以使用

[R1] disp ip int b

1.2.4 进入端口视图

[R1] interface e0/0

1.2.5 配置端口IP

[R1-Ethernet0/0] ip add 192.168.2.1 255.255.255.0

1.2.6 关闭/开启端口

[R1- Ethernet0/0] shutdown

[R1- Ethernet0/0] undo shutdown

1.2.7 查看路由表

```
[R1] display ip routing-table
```

1.2.8 更改端口转发速率

```
[R1- Ethernet0/0] qos lr cir 80000 # 将端口转发速率更改为 80Kbps
```

1.3 其它

1.3.1 特殊键的使用

TAB 键：补齐简写的命令

空格键：逐屏显示

回车键：逐行显示

1.3.2 清空交换机MAC地址表

```
[Quidway] undo mac-address
```

1.3.3 清空交换机ARP缓存

```
[Quidway] disp arp
```

```
[Quidway] undo arp 192.168.2.2
```

2 LoopBack端口

本地环回接口是一个逻辑接口，可以任意添加，删除。

配置方式跟物理接口相同。

2.1 添加LoopBack端口

```
[R1] int loop 2
```

```
[R1-LoopBack2] ip add 192.168.1.1 255.255.255.0
```

2.2 删除LoopBack端口

```
[R1] undo int loop 2
```


3 VLAN配置

3.1 生成VLAN

设备初始化时，默认所有端口都在 VLAN1 中

```
[S1] vlan 2
```

3.2 添加端口

```
[S1-vlan2] port e0/1
```

```
[S1-vlan2] port e0/1 e0/2
```

```
[S1-vlan2] port e0/1 to e0/3
```

3.3 端口类型配置

以太网端口有三种链路类型：access、hybrid 和 trunk。

access 类型的端口只能属于一个 VLAN，一般用于连接计算机的端口；

trunk 类型的端口可以属于多个 VLAN，用于接收和发送多个 VLAN 的报文，一般用

于交换机直接连接的端口；

hybrid 类型的端口同时具备 access 和 trunk 类型的端口的功能。

trunk 和 hybrid 不同之处在于：hybird 允许 VLAN 报文发送时不打标签；

trunk 只允许缺省的 VLAN 报文不打标签。

```
[S1-Ethernet0/1] port link-type access
```

```
[S1-Ethernet0/2] port link-type trunk
```

```
[S1-Ethernet0/2] port trunk permit vlan 2 3
```

```
[S1-Ethernet0/13]port hybrid pvid vlan 3      # 设置 Hybrid 端口的缺省 ID
```

```
[S1-Ethernet0/13]port hybrid vlan 2 tagged    # 将 Hybrid 端口加入已有 VLAN
```

```
[S1-Ethernet0/13]port hybrid vlan 3 untagged
```

3.4 配置端口聚合

端口聚合它可将多物理连接当作一个单一的逻辑连接来处理，它允许两个交换器之间通过多个端口并行连接同时传输数据以提供更高的带宽、更大的吞吐量和可恢复性的技术。

```
[S1] link-aggregation Ethernet 0/1 to Ethernet 0/2 both
```

4 网络地址转换

4.1 配置访问控制列表

这个访问控制列表定义了只允许发送 IP 源地址为 192.168.2.0/24 的外出数据包

```
<R1>system
```

```
[R1] acl number 2001
```

```
[R1-acl-2001] rule permit source 192.168.2.0 0.0.0.255 # 这里是反掩码
```

```
[R1-acl-2001] rule deny source any
```

4.2 配置地址池

定义一个包含 5 个公网地址（5~9）的地址池，地址池名称为 1。

```
[R1] nat address-group 1 192.168.5.5 192.168.5.9
```

4.3 配置NAT转换

```
[R1] interface e0/1
```

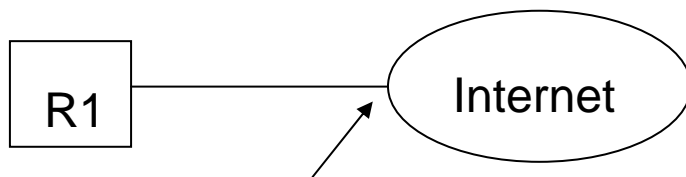
```
[R1-Ethernet0/1] nat outbound 2001 address-group 1
```

如果不添加 address-group，将使用网络地址端口转换 NAPT（Port-level NAT）模式。

```
[R1-Ethernet0/1] nat outbound 2001
```

4.4 配置静态路由

ip route-static 源地址网段 子网掩码 下一跳地址



IP:192.168.5.1

```
[R1] ip route-static 192.168.2.0 0.0.0.255 192.168.5.1
```

在路由表中添加缺省路由

```
[R1] ip route-static 0.0.0.0 0.0.0.0 192.168.5.1
```

5 PPP协议配置

PPP 协议的身份认证有 PAP 和 CHAP 两种方式。

5.1 PAP验证方式

5.1.1 服务端

```
[R1] local-user RTB # 用户名: RTB
```

```
[R1-user-RTB] service-type ppp
```

```
[R1-user-RTB] password simple aaa # 密码: aaa
```

```
#+++++
```

如果不能进入[R1-user-RTB] 视图，则使用如下配置命令配置用户列表、服务类型和用户密码。

```
[R1] local-user RTB service-type ppp
```

```
[R1] local-user RTB password simple aaa
```

```
#+++++
```

```
[R1] int s0/0
```

```
[R1-Serial0/0] link-protocol ppp
```

```
[R1-Serial0/0] ppp authentication-mode pap
```

5.1.2 客户端

```
[R2] int s0/0
```

```
[R2-Serial0/0] ppp pap local-user RTB password simple aaa
```

5.2 CHAP验证方式

5.2.1 服务端

```
[R1] local-user RTB # 用户名: RTB
```

```
[R1-user-RTB] service-type ppp
```

```
[R1-user-RTB] password simple aaa # 密码: aaa
```

```
[R1] int s0/0
```

```
[R1-Serial0/0] link-protocol ppp
```

```
[R1-Serial0/0] ppp authentication-mode chap
```

```
[R1-Serial0/0] ppp chap user RTA
```

5.2.2 客户端

```
[R2] local-user RTA # 用户名: RTA
```

```
[R2-user-RTA] service-type ppp
```

```
[R2-user-RTA] password simple aaa # 密码: aaa
```

```
[R2] int s0/0
```

```
[R2-Serial0/0] ppp chap user RTB
```

5.3 重启端口以便命令生效

```
[R1-Serial0/0] shutdown
```

```
[R1-Serial0/0] undo shutdown
```

6 帧中继协议配置

R1 为 DTE 端

```
[R1-Serial0/0] link-protocol fr # 封装帧中继接口
```

```
[R1-Serial0/0] fr interface-type DTE # 封装帧中继接口类型
```

R2 为 DCE 端

```
[R2] fr switching # 使能帧中继交换协议
```

```
[R2-Serial0/0] link-protocol fr          # 封装帧中继接口
```

```
[R2-Serial0/0] fr interface-type DCE    # 封装帧中继接口类型
```

```
[R2-Serial0/0] fr dlci 20               # 为接口分配 DLCI
```

DLCI(Data Link Connection Identifier): 数据链路连接标识, 用于标识节点与节点之间的逻辑链路、呼叫控制和管理信息。其中, 16~1007 分配给帧中继过程使用。

7 OSPF协议配置

7.1 启用OSPF

```
[R1] router id 1.1.1.1
```

```
[R1] ospf
```

```
[R1-ospf-1] area 0                      # 创建区域 0
```

```
[R1-ospf-1-area-0.0.0.0] network 1.1.1.0 0.0.0.255 # 将 1.1.1.0 网段分配到区域 0
```

7.2 修改端口的COST值

COST 值是最短路径树生成的关键参数。

使用 “display ospf ladb router” 查看时, metirc 项就是 COST 值。

```
[R1] interface e0/1
```

```
[R1-Ethernet0/1] ospf cost 100          # 设定 cost = 100
```

7.3 路由导入命令

7.3.1 导入直连路由

启用 **OSPF** 后, 如果导入直连路由, 可迅速实现全网连接。推荐!

```
[R1] ospf
```

```
[R1-ospf-1] import-route direct
```

7.3.2 导入静态路由

```
[R1] ospf
```

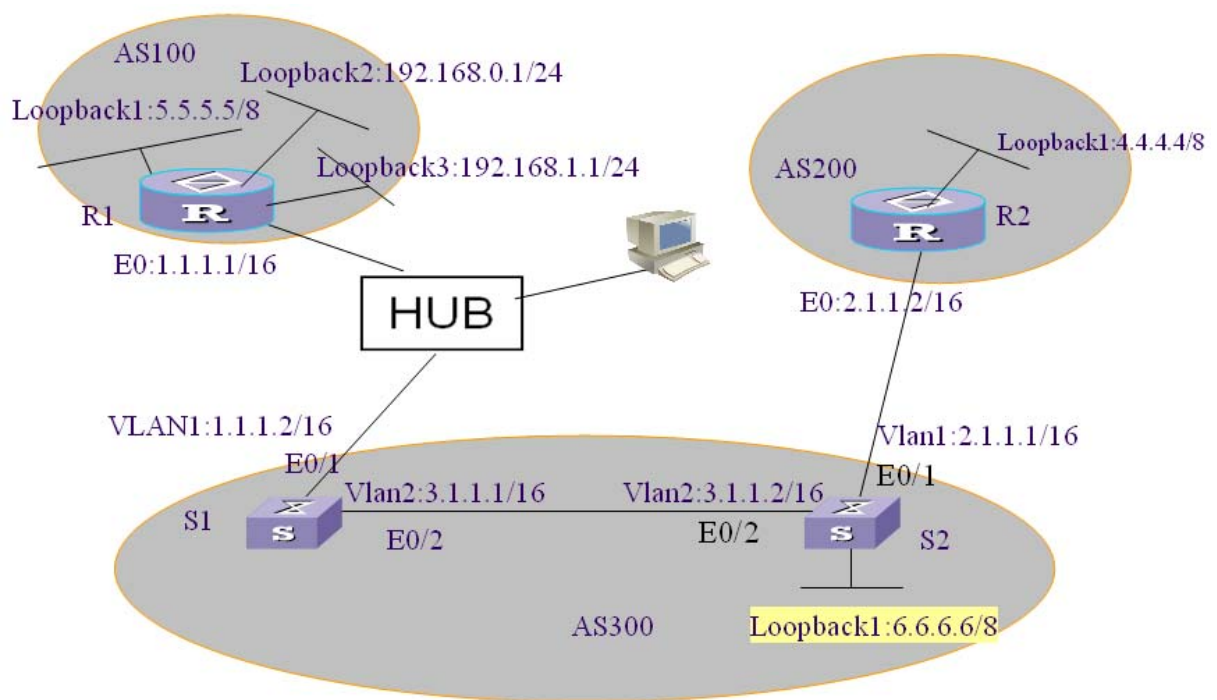
```
[R1-ospf-1] import-route static
```

7.4 查看OSPF路由

[R1] disp ospf routing-table

8 BGP协议配置

8.1 拓扑图



8.2 路由上的配置

[R1] bgp 100	# 启动 BGP ，自治系统号为 100
[R1-bgp] group R1S1 external	# 配置对等体组
[R1-bgp] peer R1S1 as-number 300	# 指定对等体组的自治系统号
[R1-bgp] peer 1.1.1.2 group R1S1	# 向对等体组中加入邻居组员
	# 注意，这里的端口是 1.1.1.2，参考拓扑图

8.3 交换机上的配置

[S1] bgp 300	# 启动 BGP ，自治系统号为 300
[S1-bgp] peer 1.1.1.1 as-number 100	# 加入 AS100 的邻居

```
[S1-bgp] peer 3.1.1.2 as-number 300 # 加入 AS300 的邻居(AS 内部邻居)
```

8.4 注入路由信息

```
[R1-bgp] network 5.0.0.0 255.0.0.0
```

8.5 强制下一跳地址

```
[S1-bgp] peer 3.1.1.2 next-hop-local # 强制下一跳地址
```

8.6 路由聚合

8.6.1 同时通告聚合路由和具体路由

```
[R1] bgp 100
```

```
[R1-bgp] aggregate 192.168.0.0 255.255.240.0
```

8.6.2 只通告聚合路由

```
[R1] bgp 100
```

```
[R1-bgp] aggregate 192.168.0.0 255.255.240.0 detail-suppressed
```

8.7 BGP路由策略

8.7.1 基于ACL的路由过滤

在 S2 上配置路由策略，阻止 AS100 的 5.0.0.0/8 网段的路由传给 AS200。

```
[S2] acl number 2001
```

```
[S2-acl-basic-1] rule 0 deny source 5.0.0.0 0.255.255.255
```

```
[S2-acl-basic-1] rule 1 permit source 0.0.0.0 255.255.255.255
```

```
[S2-acl-basic-1] quit
```

```
[S2] bgp 300
```

```
[S2- bgp] peer 2.1.1.2 filter-policy 2001 export
```

8.7.2 基于AS-Path的路由过滤

设置 S1 不通过来自 AS200 的路由

```
[S1] ip as-path-acl 1 deny \b200$ # 拒绝来自 AS200 的路由
```

[S1] ip as-path-acl 1 permit ^\$ # 允许本 AS 的路由

[S1] bgp 300

[S1-bgp] peer 1.1.1.1 as-path-acl 1 export

8.7.3 基于Route Policy的路由过滤

配置 S1 不向外通告 6.0.0.0/8 的路由信息, 并且向外通告的路由信息的 COST 为 888

[S1]acl number 2001

[S1-acl-1] rule 1 deny source 6.0.0.0 0.255.255.255

[S1-acl-1] rule 2 permit source any

[S1]route-policy deny6 permit node 10

[S1-route-policy] if-match acl 2001

[S1-route-policy] apply cost 888

[S1-bgp] peer 1.1.1.2 route-policy deny6 export

8.8 查看BGP路由

[R1] disp bgp routing-table

8.9 其它相关命令

8.9.1 Debug bgp命令

<R1> Debug bgp event

<R1> Debug bgp all

<R1> Terminal debugging # 打开终端调试

8.9.2 取消debug dgp命令

<R1> undo debuggingbgp even

<R1> undo terminal debugging

8.9.3 重新启动BGP协议

```
<R1> reset bgp all
```

8.9.4 显示BGP邻居状态

```
[R1] display bgp peer
```

8.9.5 显示BGP路由表

```
[R1]display bgp routing-table
```

9 SNMP协议配置

9.1 启用SNMP代理

```
[R1] snmp-agent
```

```
[R1] snmp sys ver v1          # 启用 SNMPv1
```

```
[R1] snmp com write private # 写密码: private, 不得写错、缩写
```

```
[R1] snmp com read public  # 读密码: public, 不得写错、缩写
```

9.2 配置trap

```
[S2]snmp trap enable
```

```
# 网管站的 IP 为 10.0.0.11
```

```
[S2]snmp target-host trap address udp-domain 10.0.0.11 params securityname public
```

10 传输层实验

Linux 系统的用户名: root, 密码: network;

10.1 配置IP地址

```
[root@localhost ~]# ifconfig eth0 192.168.1.99 netmask 255.255.255.0
```

如果 IP 配置未生效, 可以重启网络服务使之生效。

```
[root@localhost ~]# /etc/init.d/network restart
```

10.2 开启FTP

10.2.1 直接使用root作为FTP账号

要删除以下两个文件中的“root”字符串：

vsftp.ftputers

vsftp.user_list

可以用 gedit 打开并编辑它们：

```
[root@localhost ~]# gedit vsftp.ftputers
```

```
[root@localhost ~]# gedit vsftp.user_list
```

10.2.2 启动FTP服务

```
[root@localhost ~]# /etc/init.d/vsftpd start
```

```
[root@localhost ~]# /etc/init.d/vsftpd restart # 重启
```

10.3 实时监控模块（TCPConnetion）

10.3.1 初始化

```
[root@localhost ~]# cd /root/TCPLog/
```

```
[root@localhost TCPLog]# ./init.sh
```

10.3.2 读取记录

```
[root@localhost ~]# cd /root/TCPLog/
```

```
[root@localhost TCPLog]# ./read.sh # 此脚本将读取的 TCP 连接相关数据  
# 保存在/root/TCPLog/目录下  
# 的 tcpsndwnddata.txt 和 tcprtodata.txt 文件中。
```

10.4 启动丢包内核模块

```
[root@localhost ~]# cd /root/TCPDropPkt/
```

```
[root@localhost TCPDropPkt]# ./load.sh
```

10.5 启动TCPTest

```
[root@localhost ~]# cd /root/TCPTest/
```

```
[root@localhost TCPTest]# /root/j2re/bin/java TcpTest
```

11 组播实验

11.1 PIM协议配置

11.1.1 PIM-DM协议配置

启动组播路由协议

```
[S1] multicast routing-enable
```

在接口上启动 **PIM-DM**

```
[S1-VLAN-interface10] pim dm
```

```
[R1-Ethernet0] pim dm
```

11.1.2 PIM-SM协议配置

启动组播路由协议

```
[S1] multicast routing-enable
```

在接口上启动 **PIM-SM**

```
[S1-VLAN-interface10] pim sm
```

```
[R1-Ethernet0] pim sm
```

至少需要一台路由器为 **BSR** 候选者和 **RP** 候选者

```
[R1-pim] c-bsr E0/1 4 1 # '4'表明组播组为 244.0.0.0/4
```

'1'表明候选 **BSR** 的优先级，默认为 0

```
[R1-pim] c-rp E0/1
```

11.1.3 查看组播路由表

[S1] display pim routing-table

11.2 IGMP协议配置

11.2.1 启动IGMP

路由器每个接口上启动 IGMP

[R1-Ethernet0] igmp enable

11.2.2 查看IGMP配置

查看 IGMP 在接口上的相关信息

[R1] display igmp interface

查看 IGMP 组信息

[R1] display igmp group

12 其它知识点

12.1 网线类型的选择

RJ45 端口可分为 MDI 和 MDIX 两类。

通常主机和路由器的端口属于 MDI，交换机和集线器的端口属于 MDIX。

连接时：同类型的端口使用交叉线；不同类型的端口使用直连线。

12.2 IP地址分类

A, B, C, D, E 类 IP 地址



网络地址：202.112.138.0

广播地址：202.112.138.255

回环地址：127.*.*.*

12.3 内网IP地址

[RFC 1918]指明了一些专用地址，规定它们只能用作本地地址而不能作为因特网地址，因特网中的路由器对目的地址为专用地址的数据报一律不进行转发。

这些专用地址是：

10.0.0.0 到 10.255.255.255

172.16.0.0 到 172.31.255.255

192.168.0.0 到 192.168.255.255

12.4 组播IP地址

组播地址范围：224.0.0.0—239.255.255.255

保留组播地址：224.0.0.0—224.0.0.255

本地管理组地址：239.0.0.0—239.255.255.255

用户组播地址：224.0.1.0—238.255.255.255

组播 MAC 地址：01-00-5e-xx-xx-xx

组播 IP 到 MAC 映射：将 IP 组播地址中的低 23 位放入 MAC 地址的低 23 位；

由于高 5 位地址不作映射，因此有 32 个 IP 组播地址映射成一个 MAC 地址