



计算机网络实用技术人才培养丛书
锐 捷 职 业 认 证 系 列

设备调试与网络优化

Debugging and Optimizing Networking Devices (DOND)

实验指南



◎ 张选波 王 东 张国清 编著

 科学出版社
www.sciencep.com



计算机网络实用技术人才培养丛书
锐 捷 职 业 认 证 系 列

设备调试与网络优化

Debugging and Optimizing Networking Devices (DOND)

实验指南

© 张选波 王 东 张国清 编著

 科学出版社
www.sciencep.com

内 容 简 介

本书是《设备调试与网络优化学习指南》的配置套教材,内容涉及《设备调试与网络优化学习指南》课程中所阐述的理论知识。全书以实际的网络环境为依托,结合工程项目中的实践经验,对现在最流行的网络技术进行了综合性的实践。书中提供的真实案例和项目解决方案会使读者在学习理论知识的基础上,通过实践操作加深对网络技术的理解和领悟。

本书既可以作为本科类院校、高职类院校教学的教材,也可以作为网络设计师、网络工程师、系统集成工程师以及相关技术人员在实际构建园区网络中的技术参考用书。由于具备很强的专业性、实用性、易读性,本书现已被选为锐捷网络有限公司 RCCP(锐捷认证资深网络调试工程师)认证的指定教材。

本书配套电子课件、各章的复习题答案可以通过访问 <http://labclub.ruijie.com.cn>、<http://university.ruijie.com.cn> 获得。

需要本书或技术支持的读者,请与北京清河 6 号信箱(邮编:100085)发行部联系,电话:010-62978181(总机)、010-82702660,传真:010-82702698, E-mail: tbd@bhp.com.cn。

图书在版编目(CIP)数据

设备调试与网络优化实验指南 / 张选波, 王东, 张国清编
著. —北京: 科学出版社, 2009.4
(计算机网络实用技术人才培养丛书)

ISBN 978-7-03-024168-9

I. 设... II. ①张... ②王... ③张... III. 计算机网络—实验—指南 IV. TP393-62

中国版本图书馆 CIP 数据核字 (2009) 第 027005 号

责任编辑: 刘 芯 / 责任校对: 马 君
责任印刷: 密 东 / 封面设计: 青青果园

科学出版社 出版

北京东黄城根北街 16 号
邮政编码: 100717

<http://www.sciencep.com>

北京市密东印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2009 年 4 月第 一 版 开本: 787×1092 1/16
2009 年 4 月第一次印刷 印张: 15
印数: 1-1000 册 字数: 343 000

定价: 32.00 元

《设备调试与网络优化实验指南》编委会

Debugging and Optimizing Networking Devices (DOND)

主 编：张选波 王 东 张国清

策 划：安淑梅

编 委：方 洋 周 超 高 峡 石 林

“计算机网络实用技术人才培养丛书”

编审委员会

主 任：安淑梅

副主任：汪双顶

委 员：（按姓氏拼音排序）

鲍 蓉	常小刚	陈斌斌	陈红松	陈希球	陈小中	陈智罡	邓朝辉
邓国斌	方 洋	高海侠	高 峡	巩军华	郭 彬	郭拯危	韩家伟
何 力	贺 平	黄传河	金汉均	赖 庆	李向来	李永俊	李战波
林 楠	刘冬萍	刘 亮	刘 萍	刘 琪	刘任熊	龙冬云	卢 朴
马宏伟	孟晓景	闵 林	齐锁来	邵 丹	石 林	宋贤钧	万长征
汪 涛	王 东	王继龙	王向军	王晓东	王昭顺	王 忠	吴经龙
吴丽征	武俊生	武志刚	武 装	肖广维	谢 杰	徐亚峰	许如志
杨 靖	杨 磊	杨 璐	杨 威	杨文利	姚 羽	于凌云	余明辉
俞黎阳	喻 涛	袁宗福	张国清	张恒杰	张 军	张旭兰	张选波
钟啸剑	周 超	周金玲	左 凌				

前 言

随着信息化的高速发展,人们已经把更多的生活、娱乐和学习等事务转移到网络这个平台上去开展。小到一个家庭,大到一个企业,甚至是一所高校,为了提高工作效率,并进行更多的信息交流,都需要构建一个园区网,从而实现内部的高效沟通。如果希望能进一步地能够和互联网中的其他地区甚至国家的人群、组织进行信息交流,则需要将内部的园区网接入到互联网中。

本书详细介绍了构建园区网所涉及的各项交换、路由、安全等方面的知识,以及如何将园区网接入到互联网的相关技术,包括 VLAN、STP/RSTP/MSTP、VRRP、RIP、OSPF、局域网安全设计、网络出口设计、远程接入、VPN 等。另外,在最后一章还介绍了在网络故障维护中常用的思路、工具与命令,使读者在对网络进行维护与故障排除中进行借鉴。在本书的各个章中,不仅对相关技术进行了详细的介绍,而且还介绍了为了实现和部署这些技术在网络设备上的配置方式,并且章节的末尾提供了复习题目,以帮助读者巩固所学的内容和达到自我测试的目的。

本书的规划思想是使所需知识具有专业化、体系化、全面化的特征,能够体现和代表当前最新的网络技术发展方向。因此,在课程规划和内容选择上与传统的网络专业教材有很大的区别,本书从各个方面都能满足各级、各类不同专业院校教学与实践的要求。

本书由资深网络技术专家张选波和具有多年教学经验的王东、张国清在基于多年的网络工程经验、教学经验以及对网络技术的深刻理解上联合编写而成。

本书目标

本书在完成理论知识和技术原理学习的同时,通过大量的真实项目案例和项目示例,以达到理论和实践相结合的目的,帮助读者对所学的知识的掌握程度进行评估和验证,对本科类院校、高职类院校培养技能型、实用型人才有很大的帮助。

本书读者

本书的读者对象可以是本科类院校、高职类院校的学生、教师,也可以为准备参加 RCCP 考试的专业人士,以及希望学习更多园区网构建知识的技术人员。

我们推荐阅读本书的读者具有基本的网络技术知识,或者具备 RCNA 认证或者具有与 RCNA 同等水平的网络知识,以便更好地理解本书中所涉及的内容。

阅读方法

本书将所有内容分为 38 个实验案例,每个实验案例都对一项或几项协议及技术用项目案例来加深对知识点的理解。由于后续章节内容的理解需要掌握前面章节的知识,所以推荐读者根据章节的顺序依次阅读。具有一定基础的读者也可以灵活地有选择地对某些章节进行阅读。

本书资源

为了保证课程在学校的有效实施,及课程教学资源的长期提供,还建设了专门的课程实施教学俱乐部的网络资源共享基地,用来支持在课程实施过程中的项目资源更新。读者可以访问 <http://labclub.ruijie.com.cn>、<http://university.ruijie.com.cn>, 免费获得配套电子课件、各章节的复习题答案以及更多的教学资源。

本书结构

本书通过 38 个实验项目实例对园区网相关技术进行了介绍，其中实验 32～实验 38 为本书的扩展部分，不列为此次认证的考试范围，具体结构如下所示。

实验 1～实验 3 是关于 VLAN 技术的实验案例，包括单臂路由、使用 SVI 实现 VLAN 间路由、跨交换机实现 VLAN 间路由等实验，理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 1 章 VLAN 技术”。

实验 4～实验 5 是关于生成树协议的实验案例，包括配置 RSTP、配置 MSTP 等。理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 2 章 生成树协议”。

实验 6～实验 8 是关于虚拟路由器冗余协议（VRRP）的实验案例，包括配置 VRRP 单备份组、配置 VRRP 多备份组、配置基于 SVI 的 VRRP 备份组等。理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 3 章 虚拟路由器冗余协议（VRRP）”。

实验 9 是关于路由信息协议（RIP）的实验案例，包括配置 RIP 版本、汇总、定时器等。理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 4 章 路由信息协议（RIP）”。

实验 10～实验 11 是关于开放式最短路径优先协议（OSPF）的实验案例，包括 OSPF 单区域配置、OSPF 多区域配置等。理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 5 章 开放式最短路径优先协议（OSPF）”。

实验 12～实验 15 是关于路由重发布与路由控制的实验案例，包括配置 RIP 被动接口、配置 OSPF 被动接口、调整路由的 AD 值、配置 RIP 与 OSPF 路由重发布等。理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 6 章 路由重发布与路由控制”。

实验 16～实验 23 是关于网络安全控制的实验案例，包括配置 ARP 检查、配置 DHCP 监听、配置动态 ARP 检测、配置标准 IP ACL、配置扩展 IP ACL、配置基于 MAC 的 ACL、配置基于时间的 ACL 等。理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 7 章 网络安全控制”。

实验 24～实验 26 是关于 AAA 和 802.1x 的实验案例：包括配置远程登录的 AAA 认证、配置 PPP 链路的 AAA 认证、接入层 802.1x 等。理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 8 章 AAA 和 802.1x”。

实验 27～实验 31 是关于网络出口设计的实验案例，包括配置静态 NAT、配置动态 NAT、配置 NAT 地址复用（NAPT）、配置 TCP 负载分配、配置策略路由等。理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 9 章 网络出口设计”。

实验 32～实验 36 是关于远程接入技术的实验案例，包括广域网协议的封装、PPP PAP 认证、PPP CHAP 认证、帧中继基本配置、帧中继交换机配置等。理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 10 章 远程接入技术”。

实验 37～实验 38 是关于虚拟专用网（VPN）的实验案例，包括 IPSec VPN 简单配置、Site To Site IPSec VPN 多站点配置等。理论知识可以参阅《设备调试与网络优化学习指南》一书中的“第 11 章 虚拟专用网（VPN）”。

命令语法规范

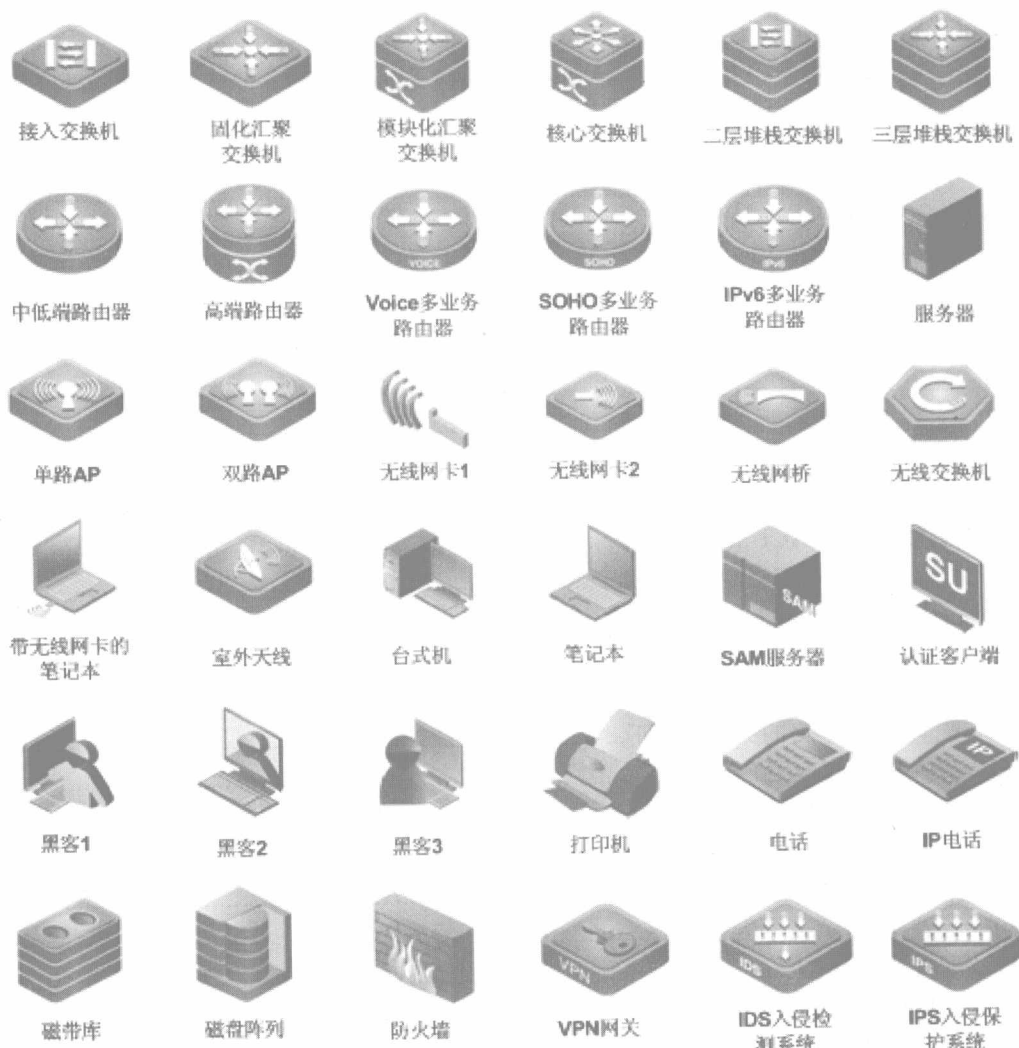
本书中使用的命令语法规范与产品命令参考手册中的命令语法相同。

- 竖线“|”表示分隔符，用于分开可选择的选项。
- 星号“*”表示可以同时选择多个选项。

- 方括号 “[]” 表示可选项。
- 大括号 “{ }” 表示必选项。
- **粗体字**表示按照显示的文字输入的命令和关键字。在配置的示例和输出中，粗体字表示需要用户手工输入的命令（例如 **show** 命令）。
- *斜体字*表示需要用户输入的具体值。

本书使用的图标

本书中所使用的图标示例如下所示。



目 录

实验 1 单臂路由	1
实验 2 使用 SVI 实现 VLAN 间路由	5
实验 3 跨交换机实现 VLAN 间路由	9
实验 4 配置 RSTP	15
实验 5 配置 MSTP	21
实验 6 配置 VRRP 单备份组	30
实验 7 配置 VRRP 多备份组	35
实验 8 配置基于 SVI 的 VRRP 备份组	40
实验 9 配置 RIP 版本、汇总、定时器	52
实验 10 OSPF 单区域配置	59
实验 11 OSPF 多区域配置	64
实验 12 配置 RIP 被动接口	71
实验 13 配置 OSPF 被动接口	77
实验 14 调整路由的 AD 值	83
实验 15 配置 RIP 与 OSPF 路由重发布	89
实验 16 配置 ARP 检查	97
实验 17 配置 DHCP 监听	103
实验 18 配置动态 ARP 检测	112
实验 19 配置标准 IP ACL	125
实验 20 配置扩展 IP ACL	130
实验 21 配置基于 MAC 的 ACL	136
实验 22 配置专家 ACL	141
实验 23 配置基于时间的 ACL	146
实验 24 配置远程登录的 AAA 认证	150
实验 25 配置 PPP 链路的 AAA 认证	155
实验 26 接入层 802.1x	160
实验 27 配置静态 NAT	168
实验 28 配置动态 NAT	171
实验 29 配置 NAT 地址复用 (NAPT)	174
实验 30 配置 TCP 负载分配	177
实验 31 配置策略路由	181
实验 32 广域网协议的封装	186
实验 33 PPP PAP 认证	190
实验 34 PPP CHAP 认证	194
实验 35 帧中继基本配置	198
实验 36 帧中继交换机配置	202
实验 37 IPSec VPN 简单配置	211
实验 38 Site To Site IPSec VPN 多站点配置	218
锐捷职业认证体系	229
参考文献	231

实验 1 单臂路由

【实验名称】

单臂路由。

【实验目的】

利用路由器的单臂路由功能实现 VLAN 间路由。

【背景描述】

为减小广播包对网络的影响，网络管理员在公司内部网络中进行了 VLAN 的划分。在实现 VLAN 间路由上，为节约成本充分并且利用现有设备，网络管理员计划利用路由器的单臂路由功能实现 VLAN 间路由。

【需求分析】

通过划分 VLAN 减小广播域的范围，为了节约成本并且充分利用现有设备，在路由器上配置单臂路由实现 VLAN 间路由。

【实验拓扑】

实验的拓扑图，如图 1-1 所示。

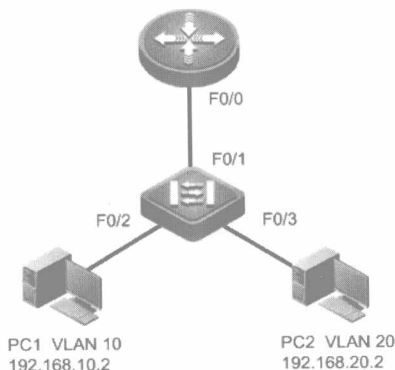


图 1-1

【实验设备】

路由器（软件版本为 RGNOS 10.1.00 及以上版本）1 台。

交换机（软件版本为 RGNOS10.1.00 及以上版本）1 台。

PC 机 2 台。

【预备知识】

交换机转发原理、交换机基本配置、单臂路由原理。

【实验原理】

VLAN 间的主机通信为不同网段间的通信，需要通过三层设备对数据进行路由转发才可以

实现，在路由器上对物理接口划分子接口并封装 802.1Q 协议，使每一个子接口都充当一个 VLAN 网段中主机的网关，利用路由器的三层路由功能可以实现不同 VLAN 间的通信。

【实验步骤】

步骤 1 在路由器上配置子接口并封装 802.1q。

```
Router#configure terminal
Router(config)#interface fastEthernet 0/0
Router(config-if)#no shutdown
Router(config-if)#interface fastethernet 0/0.1
! 创建并进入路由器子接口
Router(config-subif)#description vlan10
! 对子接口进行描述
Router(config-subif)#encapsulation dot1q 10
! 对子接口封装 801.2q 协议，并定义 VID 为 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
! 为子接口配置 IP 地址
Router(config-subif)#no shutdown
Router(config-subif)#exit
Router(config)#interface fastethernet 0/0.2
Router(config-subif)#description vlan20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#no shutdown
Router(config-subif)#end
```

步骤 2 在交换机上定义 Trunk。

```
Switch#configure terminal
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
! 将与路由器相连的端口配置为 Trunk 口。
Switch(config-if)#exit
```

步骤 3 在交换机上划分 VLAN。

```
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#end
```

步骤 4 测试网络连通性。

按上图连接拓扑，给主机配置相应 VLAN 的 IP 地址。从 VLAN10 中的 PC1 ping VLAN20 中的 PC2，由于路由器的单臂路由功能实现了 VLAN 间路由，测试结果如下所示：

```
C:\Documents and Settings\shil>ping 192.168.20.2
```

```
Pinging 192.168.20.2 with 32 bytes of data:
```

```
Reply from 192.168.20.2: bytes=32 time<1ms TTL=63
```

```
Reply from 192.168.20.2: bytes=32 time<1ms TTL=63
```

```
Reply from 192.168.20.2: bytes=32 time<1ms TTL=63
```

```
Reply from 192.168.20.2: bytes=32 time<1ms TTL=63
```

```
Ping statistics for 192.168.20.2:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

从上述测试结果可以看到，通过在路由器上配置单臂路由，实现了不同 VLAN 之间的主机通信。

【注意事项】

交换机上和路由器相连的端口需配置为 Trunk。

【参考配置】

```
Router#show running-config
```

```
Building configuration...
```

```
Current configuration : 668 bytes
```

```
!
```

```
!
```

```
enable secret 5 $1$db44$8x67vy78Dz5pq1xD
```

```
!
```

```
interface FastEthernet 0/0
```

```
duplex auto
```

```
speed auto
```

```
!
```

```
interface FastEthernet 0/0.1
```

```
encapsulation dot1Q 10
```

```
ip address 192.168.10.1 255.255.255.0
```

```
description vlan10
```

```
!
```

```
interface FastEthernet 0/0.2
```

```
encapsulation dot1Q 20
```

```
ip address 192.168.20.1 255.255.255.0
```

```
description vlan20
```

```
!
```

```
interface FastEthernet 0/1
```

```
duplex auto
```

```
speed auto
```

```
!  
line con 0  
line aux 0  
line vty 0 4  
  login  
!  
End
```

Switch#show running-config

System software version : 1.68 Build Apr 25 2007 Release

Building configuration...

Current configuration : 289 bytes

```
!  
!  
hostname Switch  
vlan 1  
!  
vlan 10  
!  
vlan 20  
!  
interface fastEthernet 0/1  
  switchport mode trunk  
!  
interface fastEthernet 0/2  
  switchport access vlan 10  
!  
interface fastEthernet 0/3  
  switchport access vlan 20  
!  
End
```

实验 2 使用 SVI 实现 VLAN 间路由

【实验名称】

使用 SVI 实现 VLAN 间路由。

【实验目的】

利用三层交换机实现 VLAN 间路由。

【背景描述】

为减小广播包对网络的影响，网络管理员在公司内部网络中进行了 VLAN 的划分。完成 VLAN 的划分后，发现不同 VLAN 之间无法互相访问。

【需求分析】

可以通过配置三层交换机的 SVI 接口实现 VLAN 间的路由。

【实验拓扑】

实验的拓扑图，如图 2-1 所示。

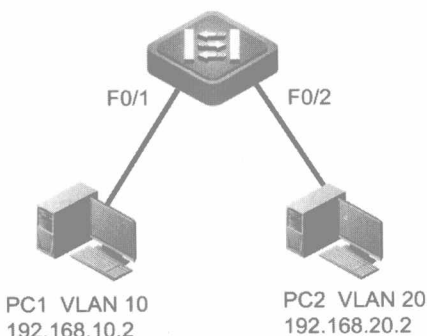


图 2-1

【实验设备】

三层交换机（软件版本为 RGNOS10.1.00 及以上版本）1 台。

PC 机 2 台。

【预备知识】

交换机转发原理、交换机基本配置、三层交换机路由功能。

【实验原理】

VLAN 间的主机通信为不同网段间的通信，需要通过三层设备对数据进行路由转发才可以实现，通过在三层交换机上为各 VLAN 配置 SVI 接口，利用三层交换机的路由功能可以实现 VLAN 间的路由。

【实验步骤】

步骤 1 在三层交换机上创建 VLAN。

```
Switch#configure terminal
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#exit
```

步骤 2 在三层交换机上将端口划分到相应 VLAN。

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
```

步骤 3 在三层交换机上给 VLAN 配置 IP 地址。

```
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.10.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#interface vlan 20
Switch(config-if)#ip address 192.168.20.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

步骤 4 验证测试。

按拓扑中所示配置 PC 并连线，从 VLAN10 中的 PC1 ping VLAN20 中的 PC2，结果如下所示：

```
C:\Documents and Settings\shil>ping 192.168.20.2
Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.20.2: bytes=32 time<1ms TTL=64
Reply from 192.168.20.2: bytes=32 time<1ms TTL=64
Reply from 192.168.20.2: bytes=32 time<1ms TTL=64
Reply from 192.168.20.2: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.20.2:

    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

从上述测试结果可以看到通过在三层交换机上配置 SVI 接口实现了不同 VLAN 之间的主机通信。

【注意事项】

VLAN 中 PC 的 IP 地址需要和三层交换机上相应 VLAN 的 IP 地址在同一网段，并且主机

网关配置为三层交换机上相应 VLAN 的 IP 地址。

【参考配置】

Switch#show running-config

Building configuration...

Current configuration : 1370 bytes

```
!  
vlan 1  
!  
vlan 10  
!  
vlan 20  
!  
!  
enable secret 5 $1$khi7$zBty5tE6xwvCw3Dv  
!  
interface FastEthernet 0/1  
    switchport access vlan 10  
!  
interface FastEthernet 0/2  
    switchport access vlan 20  
!  
interface FastEthernet 0/3  
!  
interface FastEthernet 0/4  
!  
interface FastEthernet 0/5  
!  
interface FastEthernet 0/6  
!  
interface FastEthernet 0/7  
!  
interface FastEthernet 0/8  
!  
interface FastEthernet 0/9  
!  
interface FastEthernet 0/10  
!  
interface FastEthernet 0/11  
!  
interface FastEthernet 0/12  
!
```



```
interface FastEthernet 0/13
!
interface FastEthernet 0/14
!
interface FastEthernet 0/15
!
interface FastEthernet 0/16
!
interface FastEthernet 0/17
!
interface FastEthernet 0/18
!
interface FastEthernet 0/19
!
interface FastEthernet 0/20
!
interface FastEthernet 0/21
!
interface FastEthernet 0/22
!
interface FastEthernet 0/23
!
interface FastEthernet 0/24
!
interface GigabitEthernet 0/25
!
interface GigabitEthernet 0/26
!
interface GigabitEthernet 0/27
!
interface GigabitEthernet 0/28
!
interface VLAN 10
  ip address 192.168.10.1 255.255.255.0
!
interface VLAN 20
  ip address 192.168.20.1 255.255.255.0
!
line con 0
line vty 0 4
  login
!
!
End
```