锐捷职业认证系列丛书

RCNP实验指南：

构建高级的交换网络（BASN）

Building Advanced Switched Networks

主编　方洋　李文宇　张选波
主审　石林

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

RCNP实验指南

构建高级的交换网络（IBASN）

Building Advanced Switched Networks

锐捷职业认证系列丛书

RCNP 实验指南：构建高级的交换网络（BASN）

Building Advanced Switched Networks

主编　方　洋　李文宇　张选波
主审　石　林

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内容简介

本书是锐捷网络有限公司授权出版的针对 RCNP（锐捷认证资深网络工程师）认证中 BASN（构建高级的交换网络）课程推出的实验指南，作为 BASN 课程的实验指导书籍。

本书总共分为 9 章，针对 BASN 学习指南一书中各章节的主要内容提供了多个项目式的实验案例，并在每个案例中给出了针对实现某种特定网络需求或技术的详细配置过程，主要内容包括 VLAN 实验、STP 实验、RSTP 实验、MSTP 实验、VRRP 实验、DHCP 实验、局域网安全实验、802.1x 实验和 WLAN 实验。

本书不仅作为准备参加 BASN 考试并且欲取得 RCNP 认证人员的学习用书，还可以作为网络设计师、网络工程师、系统集成工程师以及任何技术人员在实际构建路由网络中的技术参考用书。

图书在版编目（CIP）数据

RCNP 实验指南：构建高级的交换网络（BASN）/ 方洋，李文宇，张选波主编. —北京：电子工业出版社，2008.7
（锐捷职业认证系列丛书）
ISBN 978-7-121-07040-2

Ⅰ. R… Ⅱ. ①张…②石…③方… 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（2008）第 099602 号

策划编辑：施玉新
责任编辑：施玉新 牛旭东
印　　刷：北京市海淀区四季青印刷厂
装　　订：三河市万和装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱 邮编 100036
开　　本：787×1 092 1/16 印张：19.75 字数：524.5 千字
印　　次：2008 年 7 月第 1 次印刷
印　　数：3 000 册 定价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

锐捷职业认证体系

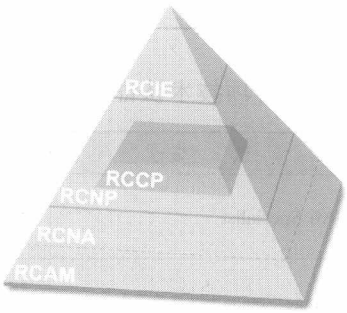
锐捷职业认证是IT领域的一项网络专业技能认证，拥有锐捷职业认证资格的专业人士将具有专业的网络知识和网络技能，并且能为雇用他们的管理者、组织、企业带来巨大的价值和报酬。

锐捷认证体系包括通用技术认证和专项技术认证。通用技术认证包括网络工程方向及网络安全方向，专项技术认证包括IPv6、存储、无线和IP通信方向。其中通用技术认证是目前国内外需求量最大，考取人数最多的认证。

一、锐捷职业认证体系概述

1. 通用技术认证

锐捷在通用技术认证中的网络工程方向提供了五个认证等级，它们所代表的专业水平逐级提升：网络管理员、网络工程师、调试工程师、资深网络工程师和互联网专家：



◆ 网络管理员（RCAM）：锐捷职业认证的第一步首先从网络管理员级别开始，其代表网络技术的入门等级，适用于网络技术的初学者。

◆ 网络工程师（RCNA）：网络工程领域的初级资格认证，获得RCNA资格的人员可以搭建和维护100个以下节点的中小型网络。

◆ 调试工程师（RCCP）：网络工程领域的中级资格认证。获得RCCP资格的人员具备丰富的网络知识和实践操作技能，能够熟练地配置和调试多种网络设备。具有RCCP认证的工程师能够设计和构建超过100个节点的大中型园区网络。

◆ 资深网络工程师（RCNP）：网络工程领域的高级资格认证。获得RCNP认证的人员能够驾驭路由器、交换机、WLAN等产品，熟练地对其各种功能和特性进行配置和调试，并在网络中部署高级的路由选择协议和各种安全特性、冗余机制、优化技术等。具有RCNP认证的工程师能够设计和构建超过500个节点的大中型园区网络。

◆ 互联网专家（RCIE）：网络工程领域的顶级认证。获得RCIE认证的人员作为网络技术领域的专家，不仅具有丰富的网络理论知识和实践操作技能，并能够对网络中出现的故障和疑难问题进行分析及排错。获得RCIE认证的人员将具备实施大型网络中所需要的各种技能。

2. 专项技术认证

锐捷职业认证还提供了多个专项技术认证，以考查相关人员在特定的技术领域方面具备的知识和技能。锐捷专项技术认证包括IPv6、存储、无线和IP通信。通过四门专项认证课程的学习，学习者能够在IPv6、存储、无线及IP通信技术领域具有专家级的知识和技能，并拥有驾驭相关产品的能力。

二、锐捷职业认证和途径

锐捷认证面向的是锐捷合作伙伴、经销商、网络技术专业人士以及对网络技术感兴趣的人

群。要获得职业认证体系中的不同等级的认证，都需要通过一些必需的笔试、Lab 考试以及具备必要的必备资格。

1. 通用技术认证

认证	认证课程	必需的考试	必备资格
RCAM	网络基础 Fundamental	Fundamental	—
RCNA	网络设备互连（IND） Interconnecting Networking Devices	IND Written IND Lab	—
RCCP	网络设备的调试与优化（DOND） Debugging and Optimizing Networking Devices	DOND Written DOND Lab	具有生效的 RCNA 证书
RCNP	构建高级的路由互联网络（BARI） Building Advanced Routing Internetworks	BARI Written BARI Lab	具有生效的 RCNA 或 RCCP 证书
	构建高级的交换网络（BASN） Building Advanced Switched Networks	BASN Written BASN Lab	
	构建优化的互联网络（BOI） Building Optimized Internetworks	BOI Written BOI Lab	
	网络服务架构的设计与实施（DINSA） Designing and Implementing Network Service Architectures	DINSA Written DINSA Lab	
RCIE	—	RCIE Written RCIE Lab	—

2. 专项技术认证

认　证	认证课程	必需的考试
IPv6 Specialist	部署 IPv6 网络 Deploying IPv6 Networks	IPv6 Written IPv6 Lab
Storage Specialist	构建存储网络 Building Storage Networks	Storage Written Storage Lab
WLAN Specialist	无线局域网的设计与实施 Designing and Implementing Wireless LAN	WLAN Written WLAN Lab
IP Communication Specialist	IP 通信技术 IP Communication Technology	IP Communication Written IP Communication Lab

注：对于锐捷专项技术认证，不需要考生预先具有任何认证证书，只需要通过相应的专项技术考试即可。

锐捷网络认证中心

前言

随着网络技术的普及，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。在早期的园区网络中，通常是由集线器（Hub）、二层交换机和相对低性能的路由器等设备构成，主要目的是提供信息节点之间的连接性。但随着信息技术的飞速发展，以及人们对网络的依赖性的增强，早期的园区网络无论从性能、灵活性、可靠性、扩展性以及安全性的角度来讲都已经无法满足需求，所以在园区网络中出现了三层交换技术，以及四层到七层的交换技术。

从分层次的模块化网络结构来看，在当今园区网络中部署最多的网络组件为提供信息节点接入的二层交换机以及提供汇聚和核心转发的三层交换机。并且三层交换机的出现解决了低端路由器的端口密度小、性能差等缺点，使路由选择和高性能的交换结合到一起，为园区网络提供了高性能的、灵活的、可靠的解决方案。对于当今的园区网络来说，单纯具备高性能是不够的，我们还需要考虑到园区网络的可靠性、冗余性、安全性、易部署性等因素。针对这些需求，我们可以在园区网络中部署 VRRP 提高网关的冗余性，使用防止 ARP 技术和 802.1x 等技术提高网络的安全性，以及部署 WLAN 技术从而免去布线所带来的大量工作。

本书由锐捷网络的资深技术专家李文宇、张选波、方洋、石林基于多年的网络工作经验以及对网络技术的深刻理解联合编写而成。在本书的编写过程中，还得到了锐捷网络的其它技术工程师、产品经理杨靖、谷会波、吴龚斌、张勇、程银光、孙含元等的大力支持。这些来自工程一线的工程师都拥有多年的丰富的工程实施经验，为本书的真实性和专业性给予了有力的支持。

本书目标

本书的目标是帮助读者备考 RCNP 认证中的 BASN 考试，以使读者顺利通过 BASN 考试。本书作为 BASN 课程的实验指导书籍，提供了大量的实验案例，并且在每个实验案例中首先针对目前的网络状况或背景进行分析，然后选择恰当的技术去解决这些问题，达到理论和实践相结合的目的。

BASN Lab 考试是需要考生在实际网络设备上进行配置操作的实验考试，本书中所涉及的内容不但包括了 BASN Lab 考试中所需要的所有实际操作技能，而且部分内容还超出了 BASN Lab 考试的大纲。所以，本书的目标不仅是为了帮助读者准备和通过 BASN 考试，而且还可以帮助读者进行技术上的积累，使其能够在实际的工作中恰当地运用这些技术，解决实际网络中遇到的各种问题。

本书读者

本书的读者对象可以为准备参加 BASN 考试的专业人士，以及希望学习如何在网络设备上配置各种路由协议及相关技术的人员。

对于阅读本书的读者，我们推荐其具有 RCNA 认证或具有与 RCNA 同等水平的网络知识，并且具备 BASN 课程的理论知识，以便更好的理解本书中所涉及的内容。

阅读方法

本书将所有内容分为了 9 个章节，每个章节都针对一种路由协议或技术提供了多个实验案例，读者可以选择逐页的阅读方式，也可以灵活的有选择的对某些章节进行阅读。

本书作为 BASN 考试的实验指南，以实践配置为主。读者在学习本书的内容并准备参加 BASN 考试时，推荐结合 BASN 课程的学习指南，以达到理论和实践的融合，这样将使读者在 BASN 的笔试和 Lab 考试中取得更优异的成绩，从而顺利地通过 BASN 考试。

本书结构

本书总共分为 9 个章节为各种路由协议和相关技术提供了实验案例。本书没有对 BASN 课程中相关技术的理论知识进行阐述，这些内容可以在 BASN 学习指南中找到。本书的具体结构如下：

第 1 章　VLAN 实验：本章提供了 VLAN 间通信、Private VLAN 和 Super VLAN 的实验案例。

第 2 章　STP 实验：本章提供了 STP 协议的实验案例，包括配置 STP 优先级、配置 STP 路径开销和端口优先级。

第 3 章　RSTP 实验：本章提供了 RSTP 协议的实验案例。

第 4 章　MSTP 实验：本章提供了 MSTP 协议的实验案例。

第 5 章　VRRP 实验：本章提供了 VRRP 的实验案例，包括配置 VRRP 单备份组、配置 VRRP 多备份组等。

第 6 章　DHCP 实验：本章提供了 DHCP 协议的实验案例，包括配置 DHCP 单地址池、配置 DHCP 多地址池、配置 DHCP 中继代理。

第 7 章　局域网安全实验：本章提供了局域网安全技术的实验案例，包括配置端口安全、配置风暴控制、配置 DHCP 监听、配置 DAI、配置 ACL 等。

第 8 章　AAA 和 RADIUS 实验：本章提供了远程登录和 PPP 链路的 AAA 认证实验。

第 9 章　802. 1x 实验：本章提供了 802. 1x 协议的实验案例，包括配置接入层 802. 1x 和配置分布层 802. 1x。

第 10 章　WLAN 实验：本章提供了 WLAN 技术的实验案例，包括配置 Ad-Hoc 模式无线网络、配置基础结构模式无线网络、配置无线接入点客户端模式、配置 SSID 隐藏等。

本书使用的图标

以下为本书中所使用的图标示例：


接入交换机
固化汇聚交换机
模块化汇聚交换机
核心交换机
二层堆栈交换机
三层堆栈交换机
中低端路由器
高端路由器
Voice多业务路由器
SOHO多业务路由器
IPv6多业务路由器
服务器
单路AP
双路AP
无线网卡1
无线网卡2
无线网桥
无线交换机
带无线网卡的笔记本电脑
室外天线
台式机
笔记本电脑
SAM服务器
认证客户端
黑客1
黑客2
黑客3
打印机
电话
IP电话
磁带库
磁盘阵列
防火墙
VPN网关
IDS入侵检测系统
IPS入侵保护系统

目 录

第 1 章　VLAN 实验

实验 1　配置单臂路由

【实验名称】

配置单臂路由

【实验目的】

使用路由器的单臂路由功能实现 VLAN 间路由

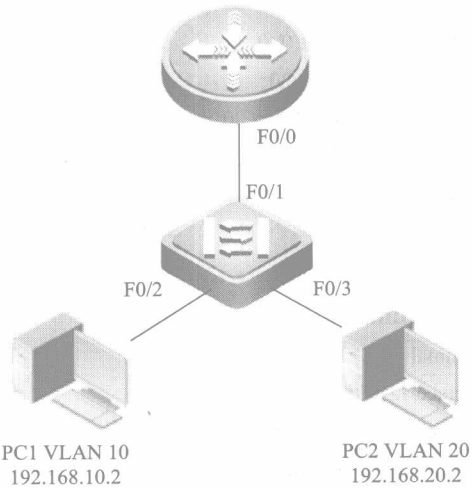
【背景描述】

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。但是网络中没有三层交换机设备，并且路由器上的接口数量有限，在这种情况下要实现 VLAN 间路由。

【需求分析】

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】



【实验设备】

路由器　1 台
交换机　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，利用路由器的路由功能可以实现不同 VLAN 间的通信。

【实验步骤】

第一步：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
```

第二步：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
```

第三步：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
```

第四步：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 配置SVI实现VLAN间路由

【实验名称】

配置SVI实现VLAN间路由

【实验目的】

使用三层交换机实现VLAN间路由

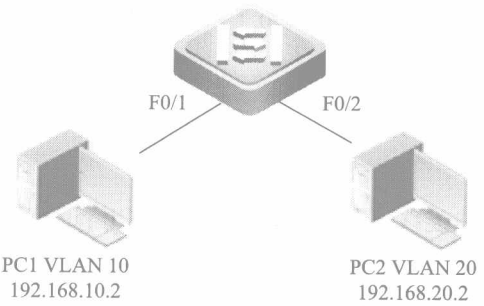
【背景描述】

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】



【实验设备】

三层交换机	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】

第一步：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
```

第二步：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
```

第三步：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
```

第四步：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。