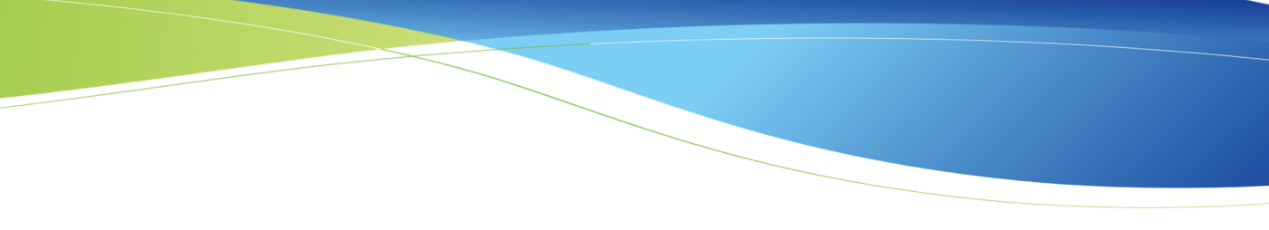


深信服网络基础实验手册

——思科模拟器

**文档版本** 02

**发布日期**  2025.2.11

深信服科技股份有限公司

**思科IOS平台操作说明**

**Cisco IOS 基础**

Cisco IOS（Cisco Internetwork Operating System，思科网际操作系统）简单的说就是一套运行在 Cisco 网络设备上的操作系统，就像 Windows 是 PC 的操作系统。针对 IOS 的配置通常是通过命令行界面

（Command Line Interface，CLI）进行，因此掌握各种常用的 IOS 命令是从事数据网络建设的基础。当我们按照上一个小节讲述的方法搭建好配置环境后，即可通过终端管理软件登陆到网络设备上，而登录

进入后看到的界面，就是 IOS 的 CLI。

# 一、Cisco IOS 配置模式

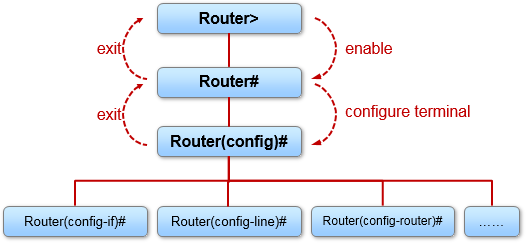


图 1-11 Cisco IOS 配置模式

IOS 定义了各种各样的配置模式（如图 1-11 所示），要想对设备的某个模块进行配置，就要进入相 应的配置模式。配置模式的设定使得命令更加模块化和层次化，而且也避免了误操作。当我们登陆一台设备的IOS 命令行时，可能看到是“Router>”这样的指示符，Router 是设备的名称，这是可 以自定义的，而“>”这个符号则表示你当前处于“用户模式”，在用户模式下我们只能够做一些基本的查看 及验证命令。在用户模式下使用“enable”命令，你会发现“Router>”变成了“Router#”，这表示

你已经进入“特权模式”，在这个模式下可以执行更多的命令。而继续使用“configure terminal”命令， 则可进入“全局模式”，在该模式下可以对设备的全局特性或功能做一些调试，例如修改设备名称， 定义特权密码，或者开启、关闭某个服务等。而在全局模式下使用“interface”关键字加上某个接口， 例如 interface serial 0/0，则会进入到 serial0/0 这个接口的配置模式下，就可以针对该接口进行相应的配置，而且此时所做的配置只会影响这个接口。使用“exit”命令可以返回上一个模式。

# 二、IOS 的命令及关键字

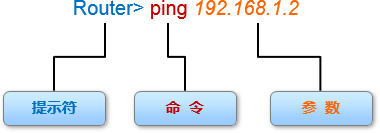


图 1-12 命 令

一条典型的 IOS 命令如上图所示，“ping”是关键字，“192.168.1.2”是参数，这条命令用于探测本地到 192.168.1.2 的连通性。再与“hostname R1”这条命令中，“hostname”是关键字， “R1”是参数，这条命令被配置后设备的名称就变成了 R1。当然要注意的是特定的命令需要在正确的配置模式下完成输入才能生效，否则就有可能会报错。

# 三、使用 IOS 的帮助功能

初学 IOS 的时候，你可能会感觉非常吃力，因为有太多的命令需要去记，其实不用着急，许多命令和关键字都是在重复使用中自然而然就记住了，而且 IOS 强大的帮助功能也使我们上手更容易。

## 命令提示及补全

当我们要输入一个关键字，但你却又忘记了这个关键字的全称而只是记得开头的几个字符，这时可以在键入头几个字符后按”? ”号：

R1(config)#ho?

hostname

上面的例子中，我想给设备改个名字，但是只记得关键字的开头是 ho，于是我输入”ho? ”， 系统会自动弹出 ho 开头的所有关键字。另外，如果输入一个关键字后，后续的关键字或者参数我们不知道要再键入什么信息了，亦可在键入该关键字后，输入空格，再输入”? ”号：

R1(config)#hostname ?

WORD This system's network name

上面的例子中，我们输入了 hostname，但是 hostname 后面该输入啥，我忘了，于是我使用问号，即可得到提示。

另外，IOS 还有命令补齐功能，也就是在你输入一个关键字的开头几个字符后，使用

“[tab]”键（大小写切换键上面的那个键），系统会自动将命令补齐，例如下面的例子：

R1(config)#ho[tab]

R1(config)#hostname

我输入 ho 后接着按 Tab 键，系统自动将关键字补齐为 hostname。当然这里要求当前配置模式下 ho 开头的就这一个关键字。补充一点，其实 IOS 所有的命令，都可以采用简化的书写方式，只要不会引发歧义，例如“hostname hello”这条命令，等同于“ho hello ”，

也就是说关键字只输入了”ho”这两个字符，这大大提升了我们的配置效率，当然采用这种

输入方式的前提是，输入的关键字不能有歧义，”ho”开头的不能存在 2 个或以上的关键字， 如果存在，那就多输入几个字符，例如“host hello”。

## 命令语法检查

当输入的命令有错误时，系统会弹出相应的报错： 示例 1：

R1(config)#router ospf

% Incomplete command. ! 命令不完整

命令没输完就按了回车，router ospf 后面还有参数。示例 2：

R1(config)#router ospd 1

^

% Invalid input detected at ‘^’ marker. !! 箭头所指字符无法识别，可能输入有误

示例 3：

R1(config)#s

% Ambiguous command: “s“ !! 未知的输入

s 开头的关键字太多，只输入了一个字符，系统表示不知道你想输入啥。

## 常用快捷键

快捷键：

-Tab 填写命令或关键字的剩下部分。

-Ctrl-U 删除一整行

-Ctrl-Z 退出配置模式并返回到执行模式

-向下箭头 用于在前面用过的命令的列表中向前滚动

-向上箭头 用于在前面用过的命令的列表中向后滚动

-Ctrl-Shift-6 用于中断诸如 ping 或 traceroute 之类的 IOS 进程

-Ctrl-C 放弃当前命令并退出配置模式

目录

[实验一：熟悉设备操作，学习ARP使用 9](#_Toc25016)

[一、实验介绍 9](#_Toc13146)

[1、关于本实验 9](#_Toc20195)

[2、实验目的 9](#_Toc10098)

[3、实验组网介绍 9](#_Toc18162)

[4、实验背景 9](#_Toc11476)

[二、实验任务配置 9](#_Toc11832)

[1、配置思路 9](#_Toc20576)

[2、配置步骤 9](#_Toc30875)

[三、实验介绍 14](#_Toc3780)

[1、关于本实验 14](#_Toc12011)

[2、配置步骤 14](#_Toc14594)

[实验二：静态路由实验 15](#_Toc25549)

[一、实验介绍 15](#_Toc11817)

[1、关于本实验 15](#_Toc15627)

[2、实验目的 15](#_Toc7155)

[3、实验组网介绍 15](#_Toc7237)

[4、实验背景 15](#_Toc17692)

[二、实验任务配置 16](#_Toc2654)

[1、配置思路 16](#_Toc947)

[2、配置步骤 16](#_Toc25367)

[实验三：OSPF路由协议基础实验 23](#_Toc11955)

[一、实验介绍 23](#_Toc27315)

[1、关于本实验 23](#_Toc1447)

[2、实验目的 23](#_Toc1440)

[3、实验组网介绍 23](#_Toc6693)

[4、实验背景 23](#_Toc19060)

[二、实验任务配置 24](#_Toc11873)

[1、配置思路 24](#_Toc10429)

[2、配置步骤 24](#_Toc31023)

[3、结果验证 27](#_Toc29563)

[实验四：以太网基础与VLAN配置实验 28](#_Toc802)

[一、实验介绍 28](#_Toc21562)

[1、关于本实验 28](#_Toc11702)

[2、实验目的 28](#_Toc5158)

[3、实验组网介绍 28](#_Toc15517)

[4、实验背景 28](#_Toc21134)

[二、实验任务配置 29](#_Toc15021)

[1、配置思路 29](#_Toc15534)

[2、配置步骤 29](#_Toc7934)

[结果验证 31](#_Toc14533)

[实验五：实现VLAN间通信 32](#_Toc31801)

[一、实验介绍 32](#_Toc18100)

[1、关于本实验 32](#_Toc4907)

[2、实验目的 32](#_Toc10941)

[3、实验组网介绍 33](#_Toc11027)

[4、实验背景 33](#_Toc23325)

[二、实验任务配置 34](#_Toc25930)

[1、配置思路 34](#_Toc12181)

[2. 配置步骤 34](#_Toc12079)

[实验六：DHCP基础配置实验 36](#_Toc2592)

[一、实验介绍 36](#_Toc19587)

[1、关于本实验 36](#_Toc10851)

[2、实验目的 36](#_Toc1435)

[3、实验组网介绍 37](#_Toc10653)

[4、实验背景 37](#_Toc8199)

[二、实验任务配置 37](#_Toc19237)

[1、配置思路 37](#_Toc15785)

[2、配置步骤 37](#_Toc28081)

[实验七：生成树基础实验 39](#_Toc23889)

[一、实验介绍 39](#_Toc3067)

[1、关于本实验 39](#_Toc20816)

[2、实验目的 39](#_Toc28551)

[3、实验组网介绍 39](#_Toc25516)

[4、实验背景 40](#_Toc3731)

[二、实验任务配置 40](#_Toc23760)

[1、配置思路 40](#_Toc5745)

[2、配置步骤 40](#_Toc2293)

[实验八：以太网链路聚合实验 45](#_Toc28132)

[一、实验介绍 45](#_Toc31125)

[1、关于本实验 45](#_Toc5943)

[2、实验目的 45](#_Toc27554)

[3、实验组网介绍 45](#_Toc22559)

[4、实验背景 45](#_Toc16478)

[二、实验任务配置 46](#_Toc32175)

[1、配置思路 46](#_Toc9731)

[2、配置步骤 46](#_Toc1250)

[实验九：访问控制列表配置 50](#_Toc13982)

[一、实验介绍 50](#_Toc29837)

[1、关于本实验 50](#_Toc18120)

[2、实验目的 50](#_Toc23471)

[3、实验组网介绍 50](#_Toc11042)

[4、实验背景 50](#_Toc16253)

[二、实验任务配置 51](#_Toc12996)

[1、配置思路 51](#_Toc24222)

[2、配置步骤 51](#_Toc17909)

[实验十：网络地址转换配置实验 52](#_Toc7023)

[一、实验介绍 52](#_Toc21488)

[1、关于本实验 52](#_Toc11598)

[2、实验目的 52](#_Toc20353)

[3、实验组网介绍 53](#_Toc31026)

[4、实验背景 53](#_Toc14771)

[二、实验任务配置 54](#_Toc13345)

[1、配置思路 54](#_Toc29430)

[2、配置步骤 54](#_Toc17989)

[3、结果验证 57](#_Toc3680)

**实验一：熟悉设备操作，学习ARP使用**

**一、实验介绍**

**1、关于本实验**

本实验通过配置思科设备，了解并熟悉路由器交换机系统的基本操作。

**2、实验目的**

* 理解命令行视图的含义以及进入离开命令行视图的方法
* 掌握一些常见的命令
* 掌握使用命令行在线帮助的方法
* 掌握如何撤销命令
* 掌握如何使用命令行快捷键
* 掌握设备部署和基础配置
* 掌握ARP，PING等命令的使用

**3、实验组网介绍**

略

**4、实验背景**

Router是一台全新无配置的路由器，PC通过串口线缆连接到Router的Console Port，需要对Router进行一些初始化操作。

**二、实验任务配置**

**1、配置思路**

1.1完成设备命名、路由器接口IP地址等基础配置

1.2保存设备配置

**2、配置步骤**

**步骤1 使用模拟器拖拽对应设备**

**步骤2 通过Console方式登录到Router的CLI**

略。模拟器使用CLI的方式即可

**步骤3 查看设备基本信息**

# 查看设备版本信息

Router>show version

Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2007 by Cisco Systems, Inc.

Compiled Wed 18-Jul-07 06:21 by pt\_rel\_team

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

Copyright (c) 2000 by cisco Systems, Inc.

System returned to ROM by power-on

System image file is "c2800nm-advipservicesk9-mz.124-15.T1.bin"

This product contains cryptographic features and is subject to United

States and local country laws governing import, export, transfer and

use. Delivery of Cisco cryptographic products does not imply

third-party authority to import, export, distribute or use encryption.

Importers, exporters, distributors and users are responsible for

compliance with U.S. and local country laws. By using this product you

agree to comply with applicable laws and regulations. If you are unable

to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to

export@cisco.com.

cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

Processor board ID JAD05190MTZ (4292891495)

M860 processor: part number 0, mask 49

2 FastEthernet/IEEE 802.3 interface(s)

239K bytes of NVRAM.

62720K bytes of processor board System flash (Read/Write)

Configuration register is 0x21025

**步骤4 完成设备基本配置**

# 修改Router的名字为Sangfor-Router

Router>enable

Router#

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#

*此时设备已经从用户视图进入到了特权视图，又进入到全局视图。*

Router(config)#hostname Sangfor-Router

Sangfor-Router(config)#

*此时设备名称已经修改为Sangfor-Router。*

思科设备提供丰富的功能，相应的也提供了多样的配置和查询命令。为便于用户使用这些命令，思科设备按功能分类将命令分别注册在不同的命令行视图下。配置某一功能时，需首先进入对应的命令行视图，然后执行相应的命令进行配置。

# 进入接口配置接口的IP地址

[Sangfor-Router(config)#int *//输入TAB补全命令*

Sangfor-Router(config)#interface *//“interface”是唯一可选的关键字*

Sangfor-Router(config)#interface fastEthernet *//“fastEthernet”是唯一可选的关键字*

Sangfor-Router(config)#interface fastEthernet 0/1 *//“0/1”是唯一可选的关键字*

Sangfor-Router(config-if)#ip address 192.168.1.1 255.255.255.0

Sangfor-Router(config-if)#

输入命令的某个关键字的前几个字母，按下<tab>键，可以显示出完整的关键字，前提是这几个字母可以唯一标示出该关键字，否则，连续按下<tab>键，可出现不同的关键字，用户可以从中选择所需要的关键字。如：

“inter”+TAB，因为当前视图下以inter开头的命令只有interface，则命令直接补全为interface，连续按多次TAB也不会变化。

此时已经进入到了接口fastEthernet 0/1的视图

Sangfor-Router(config-if)#i?

ip ipv6

当用户输入命令时，如果只记得此命令关键字的开头一个或几个字符，可以使用部分帮助获取以该字符串开头的所有关键字的提示。如：

在fastEthernet 0/1接口视图下，输入“i”+“?”，则会显示当前视图下所有“i”开头的命令的可选项，此时可以用TAB键补全，也可以手动补全。其中，“ip”，“ipv6”等为关键字。

Sangfor-Router(config-if)#exit

Sangfor-Router(config)#exit

Sangfor-Router#

%SYS-5-CONFIG\_I: Configured from console by console

Sangfor-Router#

Sangfor-Router#exit

exit 命令用来从当前视图退回到较低级别视图，如果是用户视图，则退出系统。

# 此时发现接口IP地址配置错误，需要将该地址配置到interface fastEthernet接口

Sangfor-Router(config)#int fastEthernet 0/1

Sangfor-Router(config-if)#no ip address

需要先删除fastEthernet的IP地址配置，否则会产生地址冲突无法配置。

在命令前加no关键字，即为no命令行。no命令行一般用来恢复缺省情况、禁用某个功能或者删除某项配置。几乎每条配置命令都有对应的no命令行。

# 查看设备当前配置（需要退到特权模式）

[Sangfor-Router]display current-configuration

Sangfor-Router#show running-config

Building configuration...

Current configuration : 458 bytes

!

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

!

hostname Sangfor-Router

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

interface FastEthernet0/0

no ip address

duplex auto

speed auto

shutdown

!

interface FastEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

!

!

!

!

!

!

!

line con 0

line vty 0 4

login

!

!

!

end

当执行某一命令后，如果显示的信息超过一屏时，系统会自动暂停输出信息，以方便用户查看。此时在显示信息的最底部会出现“---- More ----”的字样，此时可以通过：

（1）键入<Ctrl+C>或<Ctrl+Z>，停止显示或命令执行。

（2）键入空格键，继续显示下一屏信息。

（3）键入回车键，继续显示下一行信息。

**步骤5 保存设备当前配置**

# exit返回到特权视图

# 保存配置

Sangfor-Router#write

Building configuration...

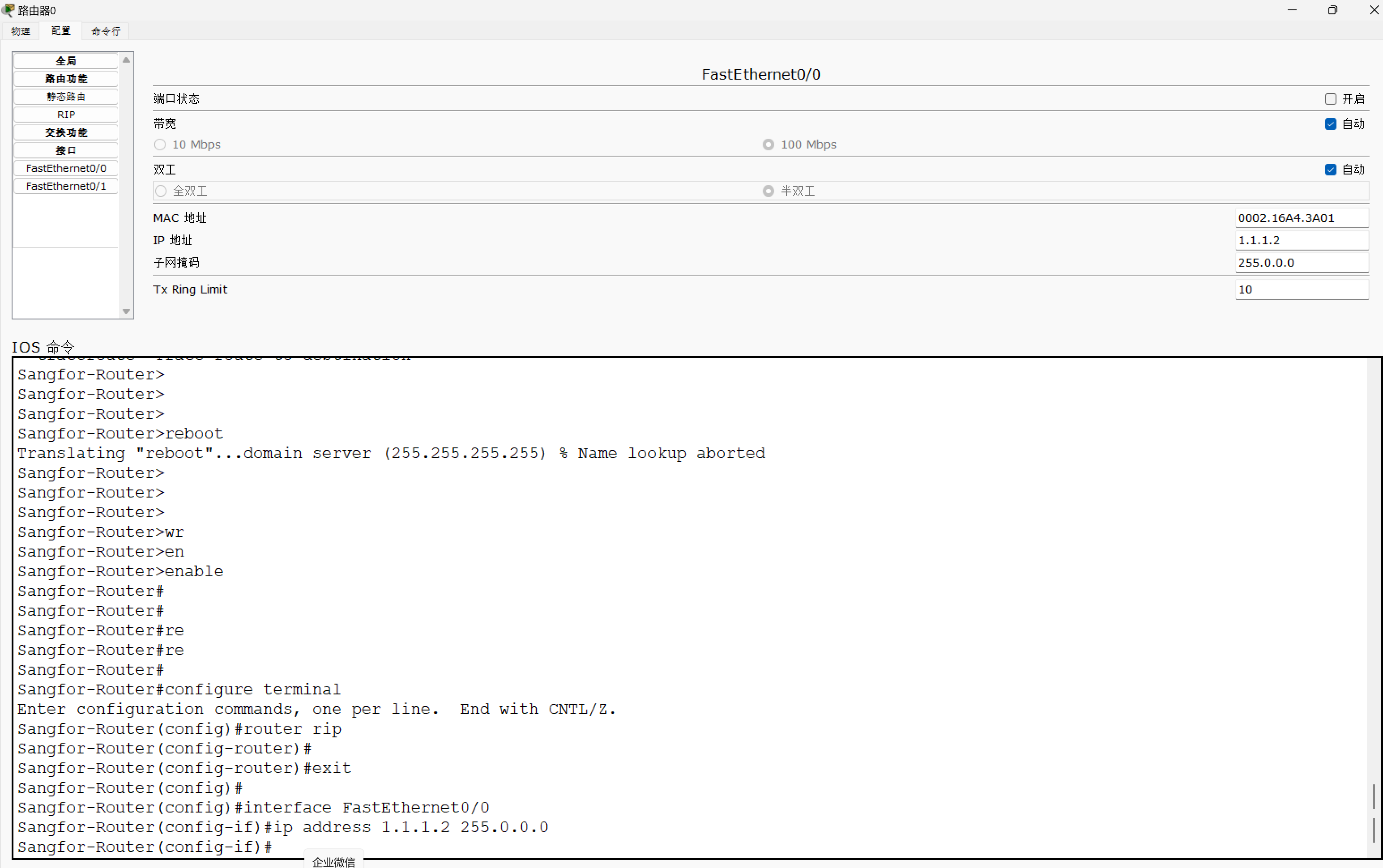
[OK]

Sangfor-Router#

当前配置已经成功保存！

用户通过命令行可以修改设备的当前配置，而这些配置未被保存的，如果要使当前配置在系统下次重启时仍然有效，在重启设备前，需要将当前配置保存到配置文件中。可以通过wirte直接保存到默认路径并覆盖原有的配置文件，

**步骤6 使用设备图形化页面完成配置**



点击对应选项，填入参数，可以直接使用图形化工具的方式完成配置

**三、实验介绍**

**1、关于本实验**

本实验通过操作自己电脑，了解并熟悉PING和ARP的基本操作。

**2、配置步骤**

步骤一：使用管理员模式打开CMD

步骤二：输入arp -d清除arp表

步骤三：输入arp -a查看arp表，可看到现在arp表是空的，只有组播地址

步骤四：输入ping+IP地址的方式，与组内同学进行通信，如ping 192.168.1.1

步骤五：输入arp -a查看arp表，可看到现在arp表已经有你刚才ping过的记录

**实验二：静态路由实验**

**一、实验介绍**

**1、关于本实验**

IPv4（Internet Protocol Version 4）是TCP/IP协议族中最为核心的协议之一。它工作在TCP/IP参考模型的网际互联层，该层与OSI参考模型的网络层相对应。网络层提供了无连接数据传输服务，即网络在发送分组时不需要先建立连接，每一个分组（也就是IP数据报文）独立发送。

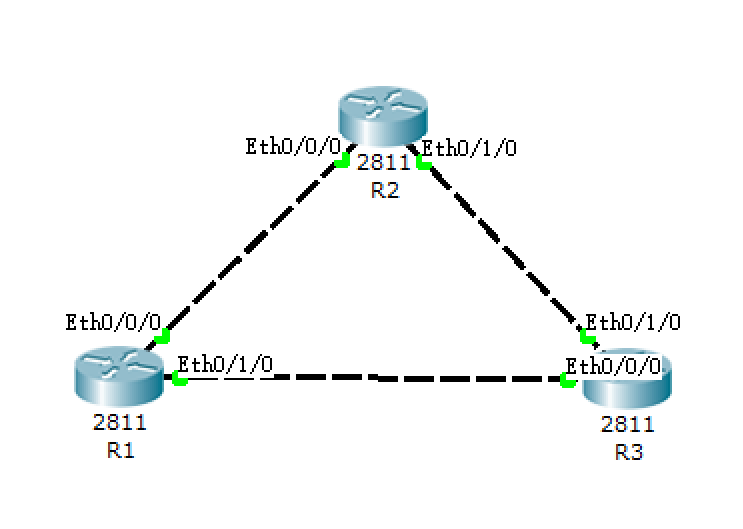
路由是数据通信网络中最基本的要素。路由信息就是指导IP报文发送的路径信息，路由的过程就是报文转发的过程。

本实验将通过IPv4地址以及IPv4静态路由的配置，帮助学员理解路由转发的基本原理。

**2、实验目的**

* 掌握接口IPv4地址的配置方法
* 理解直连路由的产生原则
* 掌握静态路由的配置方法并理解其生效的条件
* 掌握并理解特殊静态路由的配置方法与应用场景

**3、实验组网介绍（需要预先添加路由接口）**



IPv4编址及IPv4路由基础实验拓扑

**4、实验背景**

R1、R2、R3都是各自网络的网关设备，现在需要通过相应的配置，来实现这些网络之间的互联互通。

## 二、实验任务配置

**1、配置思路**

1.1配置路由器上各接口的IP地址

1.2配置静态路由来实现互联互通

**2、配置步骤**

**步骤1 设备基础配置**

# 设备命名

略。

**步骤2 查看路由器当前接口IP地址配置与路由表**

# 查看路由器上的接口状态，仅以R1为例

R1>show ip interface brief

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 unassigned YES unset up down

FastEthernet0/1 unassigned YES unset up down

Ethernet0/0/0 unassigned YES unset up up

Ethernet0/1/0 unassigned YES unset up up

Ethernet0/2/0 unassigned YES unset up down

Ethernet0/3/0 unassigned YES unset up down

Vlan1 unassigned YES unset administratively down down

show ip interface brief命令用来查看接口与IP相关的简要信息，包括IP地址、子网掩码、物理状态和协议状态以及处于不同状态的接口数目等。

当前R1上的Ethernet0/0/1和Ethernet0/0/3接口由于尚未配置IP地址，所以IP Address/Mask字段为unassigned状态，Protocol字段为down状态，Physical字段为up状态。

# 查看路由器上的路由表情况，仅以R1为例

R1>show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

**步骤3 配置路由物理接口的IP地址**

# 按照下表配置路由器的物理接口的IP地址

|  |  |  |
| --- | --- | --- |
| **路由器** | **接口** | **IP Address/Mask** |
| R1 | Ethernet0/0/0 | 10.0.12.1/24 |
| Ethernet0/0/1 | 10.0.13.1/24 |
| R2 | Ethernet0/0/0 | 10.0.12.2/24 |
| Ethernet0/0/1 | 10.0.23.2/24 |
| R3 | Ethernet0/0/0 | 10.0.13.3/24 |
| Ethernet0/0/1 | 10.0.23.3/24 |

设备物理接口IP

R1(config)#interface Ethernet0/0/0

R1(config-if)#ip address 10.0.12.1 255.255.255.0

R1(config-if)#exit

R1(config)#interface Ethernet0/1/0

R1(config-if)#ip address 10.0.13.1 255.255.255.0

R2(config)#interface Ethernet0/0/0

R2(config-if)#ip address 10.0.12.2 255.255.255.0

R2(config-if)#exit

R2(config)#interface Ethernet0/1/0

R2(config-if)#ip address 10.0.23.2 255.255.255.0

R3(config)#interface Ethernet0/0/0

R3(config-if)#ip address 10.0.13.3 255.255.255.0

R3(config-if)#exit

R3(config)#interface Ethernet0/1/0

R3(config-if)#ip address 10.0.23.3 255.255.255.0

# 使用ping工具测试联通性

R1#ping 10.0.12.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.12.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/7 ms

R1#ping 10.0.13.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.13.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/8 ms

# 查看R1的路由表

R1#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 2 subnets

C 10.0.12.0 is directly connected, Ethernet0/0/0

C 10.0.13.0 is directly connected, Ethernet0/1/0

可以看到，在接口IP地址配置完成之后，针对每个接口自动生成了一条直连路由。

**步骤4 添加不同网段的PC**

# 按照下表配置路由器的物理接口的IP地址

|  |  |  |
| --- | --- | --- |
| **路由器** | **接口** | **IP Address/Mask** |
| R1 | Ethernet0/0/3 | 10.0.1.254/24 |
| R2 | Ethernet0/0/3 | 10.0.2.254/24 |
| R3 | Ethernet0/0/3 | 10.0.3.254/24 |

使用3台PC连接对应的G0/0/3口，并配置IP地址为10.0.1.1，10.0.2.1，10.0.3.1，网关则使用路由器接口的IP地址。

**步骤5 配置静态路由**

# 在R1上配置到达R2和R3的PC的路由条目

R1(config)#ip route 10.0.2.0 255.255.255.0 10.0.12.2

R1(config)#ip route 10.0.3.0 255.255.255.0 10.0.13.3

# 查看R1的路由表

R1#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 5 subnets

C 10.0.1.0 is directly connected, Ethernet0/3/0

S 10.0.2.0 [1/0] via 10.0.12.2

S 10.0.3.0 [1/0] via 10.0.13.3

C 10.0.12.0 is directly connected, Ethernet0/0/0

C 10.0.13.0 is directly connected, Ethernet0/1/0

配置的静态路由被加入到了IP路由表中

# 测试联通性

使用R1下边的PC还是无法PING通R2的PC，因为此时R2上没有到R1的PC的路由

# 在R2上添加到达R1的PC的路由

R2(config)#ip route 10.0.1.0 255.255.255.0 10.0.12.1

# 测试联通性

此时R1的PC已经可以和R2的PC实现互通。

# 完成剩余路由条目的配置

略，自行脑补

# 自行测试路由器的PC接口之间的联通性

**步骤6 配置R1->R3->R2作为R1的PC到R2的PC接口的备份路径**

# 配置R1和R2上的静态路由

R1(config)#ip route 10.0.2.0 255.255.255.0 10.0.13.3 100

R2(config)#ip route 10.0.1.0 255.255.255.0 10.0.23.3 100

# 查看R1和R2上的路由表

此时配置的preference为100的静态路由没有被加载到路由表中。

# 关闭R1和R2之间的链路对应的接口（GigabitEthernet0/0/0），使得优先级高的路由失效。

R1(config)#interface ethernet 0/0/0

R1(config-if)#shutdown

%LINK-5-CHANGED: Interface Ethernet0/0/0, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0, changed state to down

# 查看R1和R2的路由表，随着高优先级路由失效，低优先级路由被激活

R1#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 4 subnets

C 10.0.1.0 is directly connected, Ethernet0/3/0

**S 10.0.2.0 [100/0] via 10.0.13.3**

S 10.0.3.0 [1/0] via 10.0.13.3

C 10.0.13.0 is directly connected, Ethernet0/1/0

此时由于链路断开，原先的静态路由失效，低优先级的静态路由被激活。

# 检查联通性

使用ping命令检查连通性

**步骤7 通过默认路由实现R3的PC接口和R1的PC接口互联互通**

# 在R3上删除到10.0.1.0的静态路由，配置默认路由

R3(config)#no ip route 10.0.1.0 255.255.255.0 10.0.13.1

R3(config)#ip route 0.0.0.0 0.0.0.0 10.0.13.1

# 查看R1的路由条目

R3#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 10.0.23.2 to network 0.0.0.0

10.0.0.0/24 is subnetted, 3 subnets

C 10.0.3.0 is directly connected, Ethernet0/3/0

C 10.0.13.0 is directly connected, Ethernet0/0/0

C 10.0.23.0 is directly connected, Ethernet0/1/0

**S\* 0.0.0.0/0 [1/0] via 10.0.13.1**

默认路由已经被激活

# 测试R1的PC接口到R2的PC接口的联通性

此时R1的PC接口到R2的PC接口之间可以互联互通。

**实验三：OSPF路由协议基础实验**

**一、实验介绍**

**1、关于本实验**

开放式最短路径优先OSPF（Open Shortest Path First）是IETF组织开发的一个基于链路状态的内部网关协议（Interior Gateway Protocol）。目前针对IPv4协议使用的是OSPF Version 2（RFC2328）；OSPF作为基于链路状态的协议，OSPF具有以下优点：

* OSPF采用组播形式收发报文，这样可以减少对其它不运行OSPF路由器的影响。
* OSPF支持无类型域间选路（CIDR）。
* OSPF支持对等价路由进行负载分担。

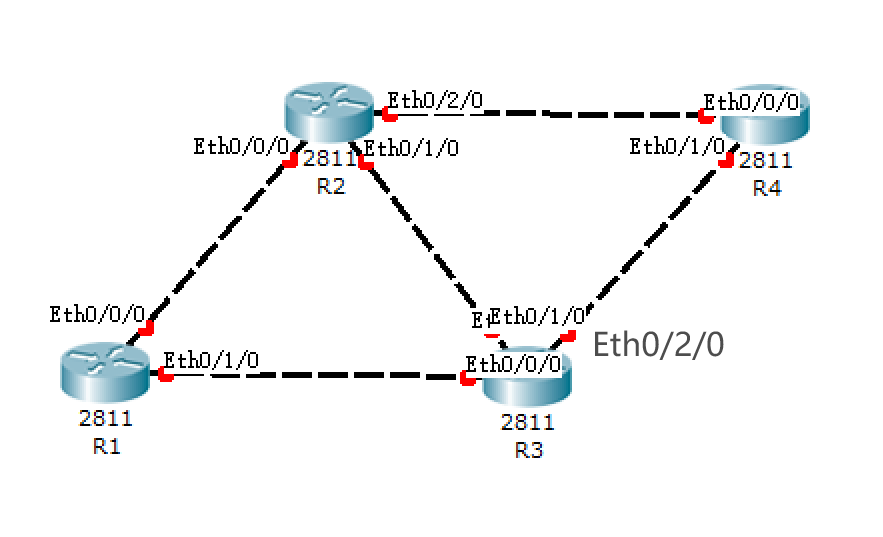
由于OSPF具有以上优势，使得OSPF作为优秀的内部网关协议被快速接收并广泛使用

本实验将通过配置单区域OSPF，帮助大家理解OSPF基本配置与原理。

**2、实验目的**

* 掌握OSPF的基本配置命令
* 掌握如何查看OSPF的运行状态
* 掌握如何通过Cost控制OSPF的选路
* 掌握OSPF发布默认路由的方法

**3、实验组网介绍**



OSPF路由协议基础实验拓扑

**4、实验背景**

R1、R2、R3、R4都是各自网络的网关设备，现在需要通过OSPF动态路由协议，来实现这些网络之间的互联互通。

**二、实验任务配置**

**1、配置思路**

（1）创建设备上的OSPF进程并使能接口上的OSPF功能

（2）通过OSPF发布默认路由

**2、配置步骤**

**步骤1 设备基础配置**

# 按照实验一的步骤1、2、3、4完成路由器的命名、物理接口

的IP地址配置，路由器之间互联IP全部以10.0.[RXRY].RX和10.0.[RXRY].RY

**并在R1和R4上使用Eth0/0/3口连接一台PC，网段为10.0.1.0和10.0.4.0**

**步骤2 完成OSPF基本配置**

# 创建OSPF进程

R1(config)#router ospf 1

R1(config-router)#

创建OSPF进程是配置与OSPF协议有关参数的首要步骤。OSPF支持多进程，在同一台设备上可以运行多个不同的OSPF进程，它们之间互不影响，彼此独立。不同OSPF进程之间的路由交互相当于不同路由协议之间的路由交互。可以在创建OSPF进程时指定进程号。

R1(config-router)#network 10.0.1.0 0.0.0.255 area 0

R1(config-router)#network 10.0.12.0 0.0.0.255 area 0

R1(config-router)#network 10.0.13.0 0.0.0.255 area 0

network network-address wildcard-mask area 0用来指定运行OSPF协议的接口。满足下面两个条件，OSPF协议才能在接口上运行：

（1）接口的IP地址掩码长度≥network命令中的掩码长度。OSPF使用反掩码，例如0.0.0.255表示掩码长度24位。

（2）接口的IP地址必须在network命令指定的网段范围之内。

此时三个接口都被使能，同时使能时指定接口属于区域0。

R2(config-router)#network 10.0.12.0 0.0.0.255 area 0

R2(config-router)#network 10.0.23.0 0.0.0.255 area 0

R2(config-router)#network 10.0.24.0 0.0.0.255 area 0

[R3][R4]略

[R4]注意宣告10.0.4.0网段

**步骤3 查看OSPF状态**

# 查看OSPF邻居（以R1为例）

R1#show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface

10.0.34.3 1 FULL/BDR 00:00:33 10.0.13.3 Ethernet0/1/0

10.0.24.2 1 FULL/BDR 00:00:32 10.0.12.2 Ethernet0/0/0

show ip ospf peer命令用来显示OSPF中各区域邻居的信息。包括邻居所属的区域、邻居Router ID、邻居状态、接口等信息。

# 查看IP路由表中由OSPF学习到的路由

R1#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 7 subnets

C 10.0.1.0 is directly connected, Ethernet0/3/0

**O 10.0.4.0 [110/30] via 10.0.12.2, 00:00:53, Ethernet0/0/0**

**[110/30] via 10.0.13.3, 00:00:22, Ethernet0/1/0**

C 10.0.12.0 is directly connected, Ethernet0/0/0

C 10.0.13.0 is directly connected, Ethernet0/1/0

**O 10.0.23.0 [110/20] via 10.0.12.2, 00:01:59, Ethernet0/0/0**

**[110/20] via 10.0.13.3, 00:01:16, Ethernet0/1/0**

O 10.0.24.0 [110/20] via 10.0.12.2, 00:01:59, Ethernet0/0/0

O 10.0.34.0 [110/20] via 10.0.13.3, 00:01:16, Ethernet0/1/0

可以看到，OSPF会自动对等价路由进行负载分担，生成两条相同优先级的路由同时写入路由表中。

**步骤4 假设R1为所有网络的出口，所以在R1上向OSPF宣告默认路由**

# 在R1上模拟配置一条默认路由，并宣告

R1(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.1

R1(config)#router ospf 1

R1(config-router)#default-information originate

default-information originate命令用来将默认路由通告到普通OSPF区域，本机路由表中必须有激活的非本OSPF默认路由时才向其他路由器发布默认路由。

# 查看其余路由器上的IP路由表

R3#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 10.0.13.1 to network 0.0.0.0

10.0.0.0/24 is subnetted, 7 subnets

O 10.0.1.0 [110/20] via 10.0.13.1, 00:09:29, Ethernet0/0/0

O 10.0.4.0 [110/20] via 10.0.34.4, 00:08:37, Ethernet0/2/0

O 10.0.12.0 [110/20] via 10.0.13.1, 00:09:29, Ethernet0/0/0

[110/20] via 10.0.23.2, 00:08:58, Ethernet0/1/0

C 10.0.13.0 is directly connected, Ethernet0/0/0

C 10.0.23.0 is directly connected, Ethernet0/1/0

O 10.0.24.0 [110/20] via 10.0.23.2, 00:08:58, Ethernet0/1/0

[110/20] via 10.0.34.4, 00:08:37, Ethernet0/2/0

C 10.0.34.0 is directly connected, Ethernet0/2/0

**O\*E2 0.0.0.0/0 [110/1] via 10.0.13.1, 00:02:23, Ethernet0/0/0**

R2与R3、R4上已经学习到相应的默认路由。

**3、结果验证**

（1）通过ping功能检查两台PC设备和各接口之间的联通性。

（2）通过关闭接口模拟链路故障，查看路由表的变化。

**实验四：以太网基础与VLAN配置实验**

**一、实验介绍**

**1、关于本实验**

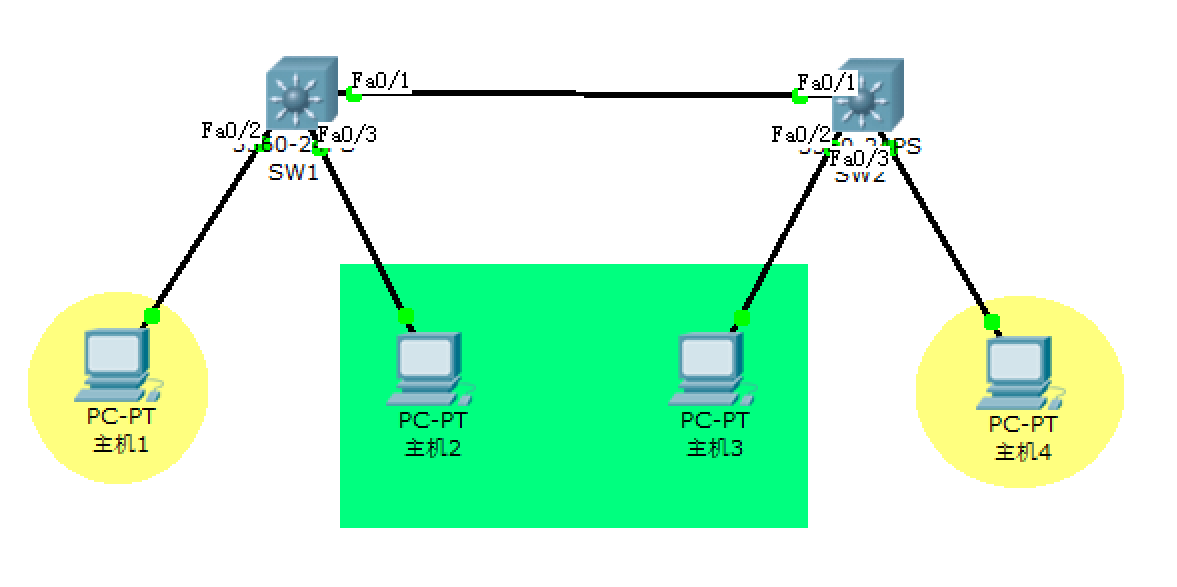
以太网是一种基于CSMA/CD（Carrier Sense Multiple Access/Collision Detection）的共享通讯介质的数据网络通讯技术。当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至造成网络不可用等问题。通过交换机实现LAN互连虽然可以解决冲突严重的问题，但仍然不能隔离广播报文和提升网络质量。

在这种情况下出现了VLAN技术，这种技术可以把一个LAN划分成多个逻辑的VLAN，每个VLAN是一个广播域，VLAN内的主机间通信就和在一个LAN内一样，而VLAN间则不能直接互通，这样，广播报文就被限制在一个VLAN内。

**2、实验目的**

* 掌握VLAN的创建方法
* 掌握Access、Trunk类型接口的配置方法
* 掌握基于接口划分VLAN的配置方法
* 掌握MAC地址表及VLAN信息的查看方式

**3、实验组网介绍**



VLAN配置实验拓扑

**4、实验背景**

某公司根据业务需求，需要对其二层网络进行VLAN划分。PC2和PC3为VLAN 10，PC1和PC4为VLAN 20。

如实验拓扑图所示，可以在SW1和SW2交换机上配置基于接口划分VLAN，把业务相同的用户连接的接口划分到同一VLAN。

**二、实验任务配置**

**1、配置思路**

（1）创建VLAN

（2）配置交换机基于接口划分VLAN

**2、配置步骤**

**步骤1 配置S1和S2设备名称**

# 设备命名

略。

**步骤2 配置PC设备的IP地址**

# 略，但要注意，同一VLAN应配置为同一网段

# 在交换机S1和S2上创建VLAN 3

SW1(config)#vlan 10

SW1(config-vlan)#exit

SW1(config)#vlan 20

[S2]略

2. 配置交换机S1和S2与PC互联的接口为Access接口，并按图将接口划入对应的VLAN

S1(config)#interface FastEthernet0/2

S1(config-if)#switchport access vlan 10

S1(config-if)#exit

S1(config)#interface FastEthernet0/3

S1(config-if)#switchport access vlan 20

S1(config-if)#exit

# 配置交换机S1和S2的互联接口为Trunk接口，并仅允许VLAN 10、20通过，心情不好的话，也可以允许全部VLAN通过

S1(config)#interface FastEthernet0/1

S1(config-if)#

S1(config-if)#switchport mode access

switchport trunk allowed vlan all命令用来配置Trunk类型接口加入的VLAN。模拟器默认全允许。

S1(config-if)#switchport trunk allowed vlan 10

S1(config-if)#switchport trunk allowed vlan all

no switchport trunk allowed vlan 1命令用来删除Trunk类型接口加入的VLAN。

VLAN 1默认就在允许通过列表中，若无实际业务用途，出于安全考虑，一般要将它删除。（可选）

**步骤3 查看配置信息**

# 查看交换机的VLAN信息

S1#show vlan

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/4, Fa0/5, Fa0/6, Fa0/7

Fa0/8, Fa0/9, Fa0/10, Fa0/11

Fa0/12, Fa0/13, Fa0/14, Fa0/15

Fa0/16, Fa0/17, Fa0/18, Fa0/19

Fa0/20, Fa0/21, Fa0/22, Fa0/23

Fa0/24, Gig0/1, Gig0/2

10 10 active Fa0/2

20 20 active Fa0/3

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2

---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

1 enet 100001 1500 - - - - - 0 0

10 enet 100010 1500 - - - - - 0 0

20 enet 100020 1500 - - - - - 0 0

1002 fddi 101002 1500 - - - - - 0 0

1003 tr 101003 1500 - - - - - 0 0

1004 fdnet 101004 1500 - - - ieee - 0 0

1005 trnet 101005 1500 - - - ibm - 0 0

Remote SPAN VLANs

------------------------------------------------------------------------------

Primary Secondary Type Ports

------- --------- ----------------- ------------------------------------------

show vlan命令用来查看VLAN的相关信息。思科交换机中，1002以后的VLAN为保留VLAN，无需关心具体作用。

# 查看交换机的MAC表信息

S1#show mac-address-table

Mac Address Table

-------------------------------------------

Vlan Mac Address Type Ports

---- ----------- -------- -----

1 00d0.ff34.e101 DYNAMIC Fa0/1

**结果验证**

检测设备连通性，验证VLAN配置结果

1、在PC1上执行Ping命令，使得PC1可以Ping通PC4。

2、在PC3上执行Ping命令，使得PC3可以Ping通PC2。

3、在PC3上执行Ping命令，无法Ping通PC1和PC4。

4、在S1和S2上通过display mac-address，查看交换机的MAC地址表，并查看接口、MAC地址、PC的对应关系。

**实验五：实现VLAN间通信**

**一、实验介绍**

**1、关于本实验**

划分VLAN后，不同VLAN的用户间不能二层互访，这样能起到隔离广播的作用。但实际应用中，不同VLAN的用户又常有互访的需求，此时就需要实现不同VLAN的用户互访，简称VLAN间互访。

现如今局域网内，常用的技术为VLANIF接口

Dot1q子接口仅做了解对比，着重熟悉路由器与三层交换机的区别。

Dot1q子接口：子接口也是一种三层的逻辑接口。跟VLANIF接口一样，在子接口上配置Dot1q功能和IP地址后，设备也会添加相应的MAC表项并置位三层转发标志位，进而实现VLAN间的三层互通。Dot1q子接口适用于通过一个三层以太网接口下接多个VLAN网络的环境。

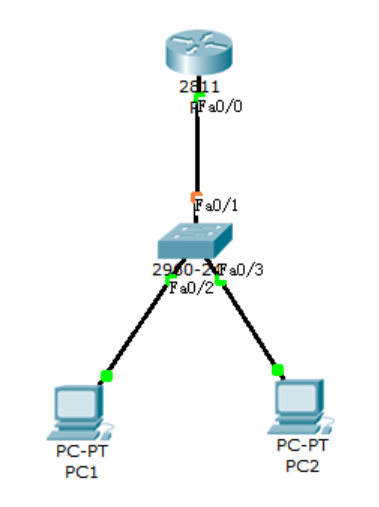
VLANIF接口：VLANIF接口是一种三层的逻辑接口。在VLANIF接口上配置IP地址后，设备会在MAC地址表中添加VLANIF接口的MAC地址+VID表项，并且为表项的三层转发标志位置位。当报文的目的MAC地址匹配该表项后，会进行三层转发，进而实现VLAN间的三层互通。

本实验将通过这两种方式来实现VLAN间互访需求，帮助学员进一步理解跨VLAN互访的原理。

**2、实验目的**

* 掌握通过配置Dot1q子接口方法实现VLAN间互访
* 掌握通过配置VLANIF接口方法实现VLAN间互访
* 深入理解VLAN间互相访问的转发流程

1. **实验组网介绍**



实现VLAN间通信实验拓扑

（1）PC1和PC2，IP地址分别为192.168.2.1/24和192.168.3.1/24。

（2）PC1和PC2的网关地址分别为192.168.2.254和192.168.3.254。

（3）在SW1上将Ethernet0/0/2和Ethernet0/0/3分别划入VLAN2和VLAN3。

（4）在R1上配置子接口，地址分别为192.168.2.254和192.168.3.254，做PC的网关。

（5）将R1替换为L3SW（三层交换机），配置VLAN子接口，将IP地址迁移到VLAN子接口上。

**4、实验背景**

PC1和PC2处于不同的VLAN，现要求通过VLANIF接口和Dot1q子接口的两种方式，分别实现PC1和PC2之间的互访需求。

**二、实验任务配置**

**1、配置思路**

（1）配置Dot1q子接口方法实现VLAN间互访

（2）配置VLANIF接口方法实现VLAN间互访

**2. 配置步骤**

**步骤1 配置S1和R1设备名称和配置PC设备的IP地址**

# 设备命名

略。

**步骤2 在S1上对R2和R3进行VLAN划分**

SW1(config)#vlan 2

SW1(config-vlan)#exit

SW1(config)#vlan 3

SW1(config-vlan)#exit

SW1(config)#interface FastEthernet0/2

SW1(config-if)#switchport access vlan 2

SW1(config-if)#exit

SW1(config)#interface FastEthernet0/3

SW1(config-if)#switchport access vlan 3

SW1(config-if)#exit

**步骤3 通过Dot1q子接口实现VLAN间互访**

# 配置S1上的Trunk接口

SW1(config)#interface fastEthernet 0/1

SW1(config-if)#switchport mode trunk

SW1(config-if)#switchport trunk allowed vlan all

因为VLAN间互访数据要由R1来VLAN，所以S1和R1之间的链路要允许VLAN2和VLAN3通过，思科交换机trunk接口默认允许所有vlan通过，这里直接配置使用vlan all。

# 在R1上创建并配置Dot1q子接口

[R1]interface GigabitEthernet 0/0/0.2

创建并进入子接口视图。2代表子接口的编号，一般建议子接口编号与VLAN ID相同，方便记忆。

R1(config)#int fastEthernet 0/0.2

%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

R1(config-subif)#encapsulation dot1Q 2

encapsulation dot1Q vlan-id命令用来配置子接口Dot1q的VLAN ID。

以此配置为例：当fastEthernet 0/0接口收到带有VLAN 2标签的数据之后，会交由2号子接口进行VLAN操作并做后续处理。从2号子接口发出的数据也会带上VLAN 2的标签。

R1(config-subif)#ip address 192.168.2.254 255.255.255.0

R1(config-subif)#exit

R1(config)#int fastEthernet 0/0.3

R1(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up

R1(config-subif)#encapsulation dot1Q 3

R1(config-subif)#ip address 192.168.3.254 255.255.255.0

R1(config-subif)#exit

# PC上检测VLAN间互访联通性

略。

*此时VLAN2和VLAN3之间已经可以正常的互访。*

**步骤4 通过VLANIF接口实现VLAN间互访**

# 使用三层交换机对路由器进行替换

略。

# 配置L3SW上和SW1互联的接口为Trunk

略。

# 在L3SW上创建相应的VLAN和VLANIF接口

L3SW(config)#vlan 2

L3SW(config-vlan)#exit

L3SW(config)#vlan 3

L3SW(config-vlan)#exit

interface vlanif vlan-id命令用来创建VLANIF接口并进入VLANIF接口视图。只有先通过命令创建VLAN后，才能执行interface vlanif命令创建VLANIF接口。

L3SW(config)#interface vlan 2

L3SW(config-if)#ip address 192.168.2.254 255.255.255.0

L3SW(config-if)#interface vlan 3

L3SW(config-if)#ip address 192.168.3.254 255.255.255.0

# 检测VLAN间互访联通性

此时VLAN2和VLAN3之间已经可以正常的互访。

**实验六：DHCP基础配置实验**

**一、实验介绍**

**1、关于本实验**

动态主机配置协议DHCP（Dynamic Host Configuration Protocol）是一种用于集中对用户IP地址进行动态管理和配置的技术。即使规模较小的网络，通过DHCP也可以使后续增加网络设备变得简单快捷。

DHCP协议由RFC 2131定义，采用客户端/服务器通信模式，由客户端（DHCP Client）向服务器（DHCP Server）提出配置申请，服务器返回为客户端分配的配置信息。

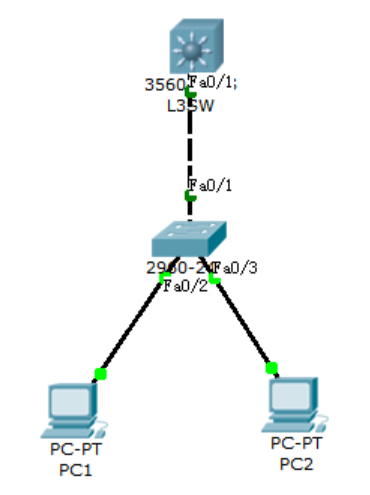
DHCP可以提供两种地址分配机制，网络管理员可以根据网络需求为不同的主机选择不同的分配策略。

* 动态分配机制：通过DHCP为主机分配一个有使用期限（这个使用期限通常叫做租期）的IP地址。这种分配机制适用于主机需要临时接入网络或者空闲地址数小于网络主机总数且主机不需要永久连接网络的场景。
* 静态分配机制：网络管理员通过DHCP为指定的主机分配固定的IP地址。相比手工静态配置IP地址，通过DHCP方式静态分配机制避免人工配置发生错误，方便管理员统一维护管理。

**2、实验目的**

* 掌握DHCP接口地址池的配置方法
* 掌握DHCP全局地址池的配置方法
* 掌握通过DHCP分配静态IP地址的方法

**3、实验组网介绍**



DHCP配置实验拓扑

（1）PC1和PC2模拟客户端，作为DHCP Client。

（2）L3SW作为DHCP Server为PC1和PC2分配IP地址。

**4、实验背景**

某企业为了减少IP地址维护的工作量，增加IP地址的利用率，准备在网络内部部署DHCP协议。

**二、实验任务配置**

**1、配置思路**

（1）配置DHCP 服务器

（2）配置DHCP客户端

**2、配置步骤**

**步骤1 基本配置**

略，参考上一个实验

**步骤2 配置全局地址池**

# 配置全局地址池，为PC1分配IP地址

L3SW(config)#ip dhcp pool sangfor

L3SW(dhcp-config)# network 192.168.2.0 255.255.255.0

L3SW(dhcp-config)# ip dhcp excluded-address 192.168.2.254

ip dhcp pool sangfor 命令用来创建一个名字为sangfor的地址池。

由于 192.168.2.254 已经被网关使用，因此该地址必须排除在 DHCP 地址池之外。

L3SW(dhcp-config)# default-router 192.168.2.254

L3SW(dhcp-config)# dns-server 8.8.8.8

default-router 命令用来为DHCP Client配置出口网关地址。R3在获取地址之后，会生成一条默认路由，下一跳地址为192.168.2.254。

# 配置全局地址池，为PC2分配IP地址

略

***此时可以尝试修改PC的地址分配方式，并查看自动分配地址的功能是否生效。***

*然后可以使用ipconfig命令查看PC1和PC2的地址，并测试连通性。*

**实验七：生成树基础实验**

## 一、实验介绍

**1、关于本实验**

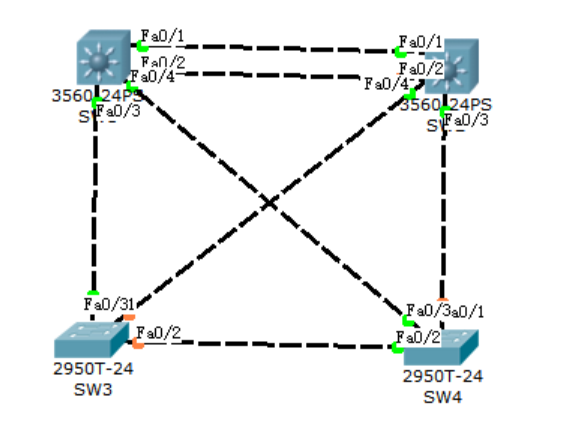
以太网交换网络中为了进行链路备份，提高网络可靠性，通常会使用冗余链路。但是使用冗余链路会在交换网络上产生环路，引发广播风暴以及MAC地址表不稳定等故障现象，从而导致用户通信质量较差，甚至通信中断。为解决交换网络中的环路问题，提出了生成树协议STP（Spanning Tree Protocol）。

与众多协议的发展过程一样，生成树协议也是随着网络的发展而不断更新的，从最初的IEEE 802.1D中定义的STP到IEEE 802.1W中定义的快速生成树协议RSTP（Rapid Spanning Tree Protocol），再到最新的IEEE 802.1S中定义的多生成树协议MSTP（Multiple Spanning Tree Protocol）。

**2、实验目的**

* 掌握修改桥优先级，控制根桥选举的方法
* 掌握修改端口开销，控制根端口和指定端口选举的方法
* 掌握边缘端口的配置方法

**3、实验组网介绍**



**生成树基础实验拓扑**

**（此实验由于模拟器的随机性，连接端口号不做强制要求）**

**4、实验背景**

某公司的二层交换网络中，为了提高网络可靠性，故在二层交换网络中增加冗余链路。为了阻止冗余链路可能带来的广播风暴，MAC地址漂移等负面影响，需要在交换机之间部署生成树协议。

## 二、实验任务配置

**1、配置思路**

（1）查看设备的生成树参数

（2）修改桥优先级来控制根桥的选举

（3）修改接口参数来控制端口角色

（4）配置STP边缘端口

**2、配置步骤**

**步骤1 查看状态设备STP运行的状态，确认根桥**

# 查看设备生成树的状态，以SW1为例

# 查看各交换机上接口的生成树状态信息。

SW1#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0003.E4A2.21D8

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0003.E4A2.21D8

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/2 Desg FWD 19 128.2 P2p

Fa0/4 Desg FWD 19 128.4 P2p

Fa0/1 Desg FWD 19 128.1 P2p

Fa0/3 Desg FWD 19 128.3 P2p

显示信息还包括各个接口的状态，在上述输出中已经按ctrl+c结束显示。

SW2#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0003.E4A2.21D8

Cost 19

Port 1(FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0060.5C18.5BB4

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/4 Desg FWD 19 128.4 P2p

Fa0/3 Desg FWD 19 128.3 P2p

Fa0/2 Altn BLK 19 128.2 P2p

Fa0/1 Root FWD 19 128.1 P2p

SW3#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0003.E4A2.21D8

Cost 19

Port 1(FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 00E0.B051.D7D5

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/3 Altn BLK 19 128.3 P2p

Fa0/2 Altn BLK 19 128.2 P2p

Fa0/1 Root FWD 19 128.1 P2p

SW4#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 32769

Address 0003.E4A2.21D8

Cost 19

Port 3(FastEthernet0/3)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 00E0.8F91.62C7

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/1 Altn BLK 19 128.1 P2p

Fa0/2 Desg FWD 19 128.2 P2p

Fa0/3 Root FWD 19 128.3 P2p

# 综合根桥ID信息以及各个交换机上端口的生成树信息，可得当前拓扑中SW1为根桥（因为根交换机上的端口都是指定端口）

注：由于模拟器的随机性，该拓扑仅供参考，不一定与你们自己实验环境中的生成树拓扑相同。

**步骤2 修改设备参数，使得SW2成为根桥，SW1成为备份根桥**

# 修改SW1和SW2的桥优先级

SW2(config)#spanning-tree vlan 1 root primary

由于根桥在网络中的重要性，在根桥选举过程中，通常希望性能高、网络层次高的交换设备会被选举为根桥。但是，性能高、网络层次高的交换设备其优先级不一定高，因此可以通过执行相应命令手动配置其为根桥，以保证该设备成为根桥。spanning-tree vlan 1 root 命令用来配置当前交换设备为指定生成树的根桥或备份根桥。思科交换机需要基于VLAN来配置优先级，如果网络中有多个VLAN，则都要做配置。

* 执行spanning-tree vlan 1 root primary命令指定当前交换设备为根交换设备，则表示该设备在指定生成树中的优先级为0，且优先级不能修改。
* 执行spanning-tree vlan 1 root secondary命令指定当前交换设备在指定生成树中为备份根桥，则表示该设备的优先级数值为4096，且优先级不能修改。

SW1(config)#spanning-tree vlan 1 root secondary

# 在S1上查看当前STP状态

SW1#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 20481

Address 0060.5C18.5BB4

Cost 19

Port 1(FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0003.E4A2.21D8

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/2 Altn BLK 19 128.2 P2p

Fa0/4 Desg FWD 19 128.4 P2p

Fa0/1 Root FWD 19 128.1 P2p

Fa0/3 Desg FWD 19 128.3 P2p

此时自身桥ID与根桥ID相同，且根路径开销为0，说明S1是当前网络的根桥。

# 在所有设备上查看STP状态摘要

SW2#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 20481

Address 0060.5C18.5BB4

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 20481 (priority 20480 sys-id-ext 1)

Address 0060.5C18.5BB4

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/4 Desg FWD 19 128.4 P2p

Fa0/3 Desg FWD 19 128.3 P2p

Fa0/2 Desg FWD 19 128.2 P2p

Fa0/1 Desg FWD 19 128.1 P2p

SW1#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 20481

Address 0060.5C18.5BB4

Cost 19

Port 1(FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0003.E4A2.21D8

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/2 Altn BLK 19 128.2 P2p

Fa0/4 Desg FWD 19 128.4 P2p

Fa0/1 Root FWD 19 128.1 P2p

Fa0/3 Desg FWD 19 128.3 P2p

SW3#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 20481

Address 0060.5C18.5BB4

Cost 19

Port 3(FastEthernet0/3)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 00E0.B051.D7D5

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/3 Root FWD 19 128.3 P2p

Fa0/2 Altn BLK 19 128.2 P2p

Fa0/1 Altn BLK 19 128.1 P2p

SW4#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 20481

Address 0060.5C18.5BB4

Cost 19

Port 1(FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 00E0.8F91.62C7

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/1 Root FWD 19 128.1 P2p

Fa0/2 Desg FWD 19 128.2 P2p

Fa0/3 Altn BLK 19 128.3 P2p

# 综合根桥ID信息以及各个交换机上的端口信息，可得当前拓扑，SW2已经变成根交换机。

**步骤3 修改设备参数，使得SW3的FastEthernet0/1接口成为端口**

# 修改SW3的FastEthernet0/2和FastEthernet0/3的接口cost值，做增加

SW3(config)#interface fastEthernet 0/2

SW3(config-if)#speed 10

SW3(config)#interface fastEthernet 0/3

SW3(config-if)#speed 10

由于模拟器的问题，这里使用降低双工和速度的方式来增加cost

# 查看当前STP状态信息摘要

SW3#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 24577

Address 0001.C732.1172

Cost 38

Port 1(FastEthernet0/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)

Address 0007.ECEE.4C46

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface Role Sts Cost Prio.Nbr Type

---------------- ---- --- --------- -------- --------------------------------

Fa0/1 Root FWD 19 128.1 P2p

Fa0/2 Altn BLK 100 128.2 P2p

Fa0/3 Altn BLK 100 128.3 P2p

在重新学习后，由于从FastEthernet0/2和FastEthernet0/3口的开销突然增大，FastEthernet0/1接口已经协商成为根端口

**步骤4 配置边缘端口**

# SW3的FastEthernet 0/10-0/13确认只会连接终端设备，需要被配置为边缘端口

SW3(config)#interface FastEthernet 0/10

通常，设备的以太网接口数比较多，并且在很多以太网接口下有相同的配置。如果对这些以太网接口进行逐个配置会较为繁琐，且容易输入错误。因此，将需要执行相同配置命令的以太网接口加入到一个临时端口组，在临时端口组配置命令时，系统会自动到临时端口组绑定的所有成员接口下执行这些命令行，完成以太网接口批量配置。

SW3(config-if)#spanning-tree bpduguard enable

spanning-tree bpduguard enable命令用来配置当前端口为边缘端口。这个功能可以帮助防止交换机端口接收或发送BPDU（Bridge Protocol Data Unit）包，这在某些情况下可以避免错误的BPDU包导致网络问题。当前端口配置成边缘端口后，如果收到BPDU报文，交换设备会自动将边缘端口设置为非边缘端口，并重新进行生成树计算。

# **实验八：以太网链路聚合实验**

## 一、实验介绍

**1、关于本实验**

随着网络规模不断扩大，用户对骨干链路的带宽和可靠性提出越来越高的要求。在传统技术中，常用更换高速率的接口板或更换支持高速率接口板的设备的方式来增加带宽，但这种方案需要付出高额的费用，而且不够灵活。

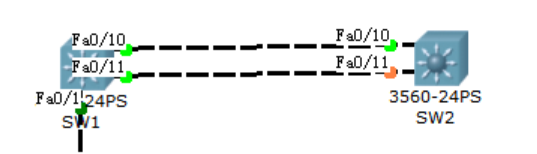
采用链路聚合技术可以在不进行硬件升级的条件下，通过将多个物理接口捆绑为一个逻辑接口，达到增加链路带宽的目的。在实现增大带宽目的的同时，链路聚合采用备份链路的机制，可以有效的提高设备之间链路的可靠性。链路聚合技术主要有以下三个优势：

* 增加带宽：链路聚合接口的最大带宽可以达到各成员接口带宽之和。
* 提高可靠性：当某条活动链路出现故障时，流量可以切换到其他可用的成员链路上，从而提高链路聚合接口的可靠性。
* 负载分担：在一个链路聚合组内，可以实现在各成员活动链路上的负载分担。
* 本实验将通过手工和LACP模式的以太网链路聚合的配置，帮助学员了解以太网链路聚合技术的配置及原理。

**2、实验目的**

* 掌握使用手动模式配置链路聚合的方法
* 掌握使用LACP模式配置链路聚合的方法

**3、实验组网介绍**



以太网链路聚合实验拓扑

**4、实验背景**

在生成树实验中，S1与S2之间的两条链路无法同时处于数据转发的状态。为了充分利用这两条链路的带宽，需要在S1和S2之间配置以太网链路聚合。

## **二、实验任务配置**

**1、配置思路**

（1）配置手工模式链路聚合

（2）配置LACP模式链路聚合

**2、配置步骤**

**步骤1 配置手工链路聚合**

# 创建Port-channel接口

SW1(config)#interface port-channel 1

SW1(config-if)#

interface port-channel命令用来进入已经存在的port-channel接口，或创建并进入port-channel接口。数字“1”代表接口编号，编号范围根据设备情况有所不同。

SW2(config)#interface port-channel 1

SW2(config-if)#

# 设置port-channel接口的聚合模式

SW1(config-if)#channel-protocol lacp

channel-protocol命令用来配置聚合口的工作模式，常用的是LACP模式和手工负载分担模式（手工模式）两种，缺省情况下，port-channel的工作模式为手工负载分担模式。此处SW1上的模式配置仅为示范目的，此处暂不配置，后续在实际生效。

# 将成员接口加入聚合组

SW1(config)#interface fastEthernet 0/10

SW1(config-if)#channel-group 1 mode on

SW1(config)#interface fastEthernet 0/11

SW1(config-if)#channel-group 1 mode on

可进入到成员接口的接口视图下，逐一添加到**port-channel**接口。

将成员接口加入Port-channel时，需要注意以下问题：

* 每个Port-channel接口下最多可以包含32个成员接口。
* Port-channel接口不能嵌套，即Port-channel接口的成员接口不能是Port-channel接口。
* 一个以太网接口只能加入到一个Port-channel接口，如果需要加入其它Port-channel接口，必须先退出原来的Port-channel接口。
* 如果本地设备使用了Port-channel，与成员接口直连的对端接口也必须捆绑为Port-channel接口，两端才能正常通信。
* Port-channel链路两端相连的物理接口的数量、速率、双工方式等必须一致。

# 查看Port-channel接口状态

SW1#show interfaces etherchannel

FastEthernet0/10:

Port state = 1

Channel group = 1 Mode = On Gcchange = -

Port-channel = Po1 GC = - Pseudo port-channel = Po1

Port index = 0 Load = 0x0 Protocol = -

Age of the port in the current state: 00d:00h:03m:27s

FastEthernet0/11:

Port state = 1

Channel group = 1 Mode = On Gcchange = -

Port-channel = Po1 GC = - Pseudo port-channel = Po1

Port index = 0 Load = 0x0 Protocol = -

Age of the port in the current state: 00d:00h:03m:27s

----

Port-channel1:Port-channel1

Age of the Port-channel = 00d:00h:15m:04s

Logical slot/port = 2/1 Number of ports = 2

GC = 0x00000000 HotStandBy port = null

Port state =

Protocol = 3

Port Security = Disabled

Ports in the Port-channel:

Index Load Port EC state No of bits

------+------+------+------------------+-----------

0 00 Fa0/10 On 0

0 00 Fa0/11 On 0

Time since last port bundled: 00d:00h:03m:27s Fa0/11

**步骤2 配置LACP模式的链路聚合**

# 修改聚合模式

SW1(config)#int port-channel 1

SW1(config-if)#channel-protocol lacp

channel-protocol lacp 指定聚合口工作模式为LACP模式。

SW2(config)#int port-channel 1

SW2(config-if)#channel-protocol lacp

# 查看聚合接口状态

**步骤3 测试Port-channel接口的连通性和使用方式。**

Port-channel接口作为一个逻辑接口，使用方式和物理接口几乎是相同的，可以尝试一下对Port-channel接口本身作直接配置，如划分VLAN，开启关闭等操作，如有时间，并尝试把实验四中，两台交换机互联的链路修改为Port-channel接口进行测试。

**步骤4 修改负载分担模式**

# 修改Port-channel接口的负载分担模式为基于目的IP地址

SW1(config)#port-channel load-balance ?

dst-ip Dst IP Addr

dst-mac Dst Mac Addr

src-dst-ip Src XOR Dst IP Addr

src-dst-mac Src XOR Dst Mac Addr

src-ip Src IP Addr

src-mac Src Mac Addr

当需要将Port-channel接口的流量分散到不同的链路上，最后能到达统一目的地时，使用port-channel load-balance命令配置Port-channel接口负载分担模式，以确保出方向的流量在各物理链路间进行合理的负载分担，避免链路阻塞。由于负载分担只对出方向的流量有效，因此链路两端接口的负载分担模式可以不一致，两端互不影响。

# **实验九：访问控制列表配置**

## 一、实验介绍

**1、关于本实验**

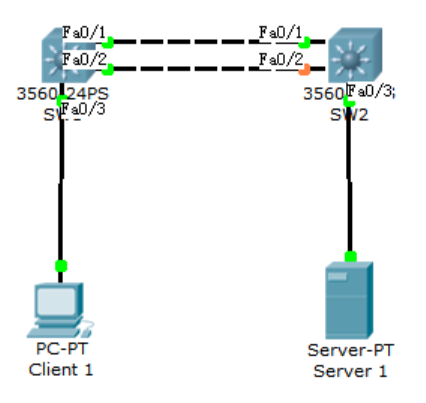
访问控制列表ACL（Access Control List）是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。

ACL本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用ACL的业务模块的处理策略来允许或阻止该报文通过。

**2、实验目的**

* 掌握ACL的配置方法
* 掌握ACL在接口下的应用方法
* 掌握流量过滤的基本方式

**3、实验组网介绍**



ACL配置实验拓扑

**4、实验背景**

如组网图所示，Server 1为服务器，Client 1为客户端，客户端与服务器之间网络可达即可，ACL与二层可达还是三层可达无关。

客户端需要远程访问服务器Server 1的web服务，尝试对其进行限制。

## 二、实验任务配置

**1、配置思路**

（1）配置设备IP地址

（2）配置ACL，匹配特定流量

（3）配置流量过滤，在接口上引用ACL

**2、配置步骤**

**步骤1 配置设备IP地址和web服务**

略，用你喜欢的方式保障Client 1和Server 1网络可达即可（本次采用Client 1：192.168.1.1和Ssever 1：192.168.1.2）

**步骤2 在S1编写ACL访问控制列表，拒绝C1到S1访问的80端口**

SW1(config)#access-list 100 deny tcp 192.168.1.1 0.0.0.0 192.168.1.2 0.0.0.0 eq www

*eq命令用来向ACL端口池添加具体某个端口号。*

*gt命令用来向ACL端口池添加多个端口号，范围是大于某个端口号。*

*lt命令用来向ACL端口池添加多个端口号，范围是小于某个端口号。*

*此处我们应用eq命令封堵HTTP的流量。*

**步骤3 在交换机上应用并查看效果**

在交换机与PC连接的接口上，调用ACL，封堵Client 1到Ssever 1的流量

SW1(config)#int f0/3

SW1(config-if)#no switchport

SW1(config-if)#ip access-group 100 in

*思科交换机需要no switchport先修改为三层接口，才能应用acl策略*

**步骤4 尝试按照不同的方式，编写新的ACL访问控制列表，查看效果**

*如修改ACL提示Error: The ACL is contained by some application(s) and forbidden to be modif，先在接口下取消应用即可。*

# **实验十：网络地址转换配置实验**

## 一、实验介绍

**1、关于本实验**

网络地址转换NAT（Network Address Translation）是将IP数据报文头中的IP地址转换为另一个IP地址的过程。作为减缓IP地址枯竭的一种过渡方案，NAT通过地址重用的方法来满足IP地址的需要，可以在一定程度上缓解IP地址空间枯竭的压力。NAT除了解决IP地址短缺的问题，还带来了两个好处：

* 有效避免来自外网的攻击，可以很大程度上提高网络安全性。
* 控制内网主机访问外网，同时也可以控制外网主机访问内网，解决了内网和外网不能互通的问题。

本实验将通过配置不同场景下的NAT帮助学员理解NAT技术的原理。

**2、实验目的**

* 掌握动态NAT的配置方法
* 掌握Easy IP的配置方法
* 掌握NAT Server的配置方法

**3、实验组网介绍**

##### 

网络地址转换配置实验拓扑

（1）蓝色实线圈内的网络属于企业内部网络，使用私网IPv4地址。红色实线圈内的网络属于互联网。

（2） Private设备模拟客户端，R1作为的网关，同时也是连接公网的出口路由器。

（3）Public设备模拟公网，R2作为运营商路由器，互联网使用SW2做汇聚，SW2无需配置，仅做二层连接。

**4、实验背景**

由于IPv4地址紧缺，企业内部一般使用私网IPv4地址。然而，企业网络用户时常会有访问公网的需求，同时部分企业还会对外提供相应的服务。此时需要配置NAT来实现这些需求。

## 二、实验任务配置

**1、配置思路**

（1）配置动态NAT

（2）配置Easy IP

（3）配置NAT Server

**2、配置步骤**

**步骤1 基本配置**

# 新增设备的接口IP地址和路由配置（其余继承）

|  |  |  |
| --- | --- | --- |
| **设备** | **接口** | **IP Address/Mask** |
| R1 | FastEthernet0/0 | 10.0.12.2/24 |
| FastEthernet0/1 | 202.99.191.1/24 |
| R2 | FastEthernet0/0 | 202.99.191.254/24 |
| FastEthernet0/1 | 202.99.192.254/24 |
| L3SW（使用VLANIF 10做互联，或者使用三层接口） | FastEthernet0/1 | 略 |
| FastEthernet0/2  （VLANIF 10的IP或接口IP） | 10.0.12.1/24 |
| Public Client | Ethernet0 | 202.99.192.1/24  GW：202.99.192.254 |
| Public server | Ethernet0 | 202.99.192.2/24  GW：202.99.192.254 |
| Private Client | Ethernet0 | 192.168.2.100/24  GW：192.168.2.1 |
| Private server | Ethernet0 | 192.168.3.100/24  GW：192.168.3.1 |

# 配置使用OSPF，让R1学习到192.168.2.0和192.168.3.0的地址，实现私网全网互通

略。

**但注意：使用OSPF时，由于202.99段模拟的是公网地址，实际场景中，公网地址和私网地址是无法路由的，所以R1禁止把202.99网段宣告进私网。**

**可在R1上配置默认路由，下一跳地址为R2的 FastEthernet0/0接口地址，然后使用引入默认路由的方式，让L3SW学习到默认路由，且转发均通过R1进行。**

**R2均为直连路由，无需单独配置，且R2是模拟公网路由器，禁止让R2学习到目标地址为192.168段的路由，运营商是不可能给你指一条到你内网私有地址段的路由回来的。这是许多同学经常犯的一个错误**

# 测试当前联通性

此时模拟的公网和私网已经分别生成了相应的路由，公网和私网分别可达，但由于没有打通路由，公网和私网之间并不可达。

**步骤2 假设该公司从电信运营商那里获得了202.99.191.10至202.99.191.20这段公网IP，现需要配置动态NAT，让私网设备使用获取到的公网地址进行互联网的访问。**

# 配置NAT地址池

R1(config)# ip nat pool sangfor 202.99.191.10 202.99.191.20 netmask 255.255.255.0

ip nat pool命令用来配置NAT地址池。Sangfor代表地址池的名字，地址池必须是一段连续的IP地址集合，当内部数据报文通过地址转换到达外部网络时，其源地址将被地址池转换为其他地址。

# 配置ACL

R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255

为了配置简单，此处使用序号为1的acl定义192.168.0.0/16段的地址。

# 配置内外网接口

R1(config)#interface fastEthernet 0/0

R1(config-if)#ip nat inside

R1(config-if)#exit

R1(config)#interface fastEthernet 0/1

R1(config-if)#ip nat outside

思科设备需要手工指定内网接口和外网接口

# 在R1配置动态NAT

R1(config)#ip nat inside source list 1 pool sangfor

ip nat inside命令用来将一个访问控制列表ACL和一个地址池关联起来，符合ACL中规定的地址可以使用地址池进行地址转换，从对应接口下出去的流量，源地址会被转换为地址池中的地址。

# 测试联通性，并查看R1上的NAT会话表

R1#show ip nat translations

Pro Inside global Inside local Outside local Outside global

icmp 202.99.191.10:23 192.168.2.100:23 202.99.192.1:23 202.99.192.1:23

icmp 202.99.191.10:24 192.168.2.100:24 202.99.192.1:24 202.99.192.1:24

icmp 202.99.191.10:25 192.168.2.100:25 202.99.192.1:25 202.99.192.1:25

icmp 202.99.191.10:26 192.168.2.100:26 202.99.192.1:26 202.99.192.1:26

尽管此时公网没有到192.168.0.0段的路由条目，但是由于转换后的源地址为202.99.191.14，Public设备会将数据回复给该地址，R1收到后会根据NAT会话表中的数据重新转换为R1的地址并转发。所以此时私网可以主动发起到公网的访问。这就是我们平时上网的过程。

**步骤3 由于经济条件有限，没有钱购买多余的地址，假设R1的FastEthernet0/1的地址不是固定IP地址（DHCP动态获取或PPPoE拨号获取），那么此时需要配置Easy IP，可以让设备使用接口下配置的地址进行源地址转换，毕竟这个地址闲着也是闲着。**

# 删除上一步骤的配置

R1(config)#no ip nat inside source list 1 pool sangfor

R1(config)#no ip nat pool sangfor 202.99.191.10 202.99.191.20 netmask 255.255.255.0

如果此处删除提示报错，NAT在使用，可检查是否有PING任务在运行，或者等待一会儿再删除。

# 配置Easy IP

R1(config)#ip nat inside source list 1 interface fastEthernet 0/1 overload

# 测试联通性

略，此时Easy IP模式下，被转换成的地址只有接口下配置的地址。此处为202.99.191.1

**步骤4 假设R1要向公网提供网络服务（用web模拟），由于服务器部署在私网内，没有公网IP地址，故需要在R1的出接口上配置NAT Server，让公网设备能通过访问该公司网络出口的地址来访问到私有服务器。**

# 在R1上配置NAT Server

R1(config)#ip nat inside source static tcp 192.168.3.100 80 202.99.191.1 8080

ip nat命令用来定义一个内部服务器的映射表，外部用户可以通过地址和端口转换来访问内部服务器的某项服务。配置内部服务器可以使外部网络主动访问私网中的服务器。当外部网络向内部服务器的外部地址（global-address）发起连接请求时，NAT将该请求的目的地址替换为私网地址（inside-address）后，转发给私网内的服务器。

# Public Client通过访问202.99.191.1的8080端口，以访问内部的web服务器

**3、结果验证**

略。