**计算机网络实验手册**

目录

[1 实验总体介绍 7](#_Toc121152118)

[1.1 实验总体介绍 7](#_Toc121152119)

[1.1.1 关于本实验 7](#_Toc121152120)

[1.1.2 实验目的 7](#_Toc121152121)

[1.1.3 实验组网介绍 7](#_Toc121152122)

[1.1.4 实验资源 11](#_Toc121152123)

[1.1.5 实验工具 11](#_Toc121152124)

[1.1.6 实验实例化 12](#_Toc121152125)

[2 实验任务1： 基础管理 13](#_Toc121152126)

[2.1 实验介绍 13](#_Toc121152127)

[2.1.1 关于本实验 13](#_Toc121152128)

[2.1.2 实验目的 14](#_Toc121152129)

[2.2 首次登录设备 14](#_Toc121152130)

[2.2.1 说明 14](#_Toc121152131)

[2.2.2 通过Console口首次登录设备 14](#_Toc121152132)

[2.3 系统常用配置 17](#_Toc121152133)

[2.3.1 帮助功能和命令自动补全 17](#_Toc121152134)

[2.3.2 查看系统信息 18](#_Toc121152135)

[2.3.3 进入视图 19](#_Toc121152136)

[2.3.4 修改设备名称 20](#_Toc121152137)

[2.3.5 查看当前视图配置 21](#_Toc121152138)

[2.3.6 删除已有配置 22](#_Toc121152139)

[2.4 保存恢复配置 23](#_Toc121152140)

[2.4.1 任务介绍 23](#_Toc121152141)

[2.4.2 保存设备配置 23](#_Toc121152142)

[2.4.3 备份设备配置 24](#_Toc121152143)

[2.4.4 恢复设备配置 25](#_Toc121152144)

[3 实验任务2： 以太交换 27](#_Toc121152145)

[3.1 实验介绍 27](#_Toc121152146)

[3.1.1 关于本实验 27](#_Toc121152147)

[3.1.2 实验目的 27](#_Toc121152148)

[3.2 广播转发 28](#_Toc121152149)

[3.2.1 说明 28](#_Toc121152150)

[3.2.2 实验任务 28](#_Toc121152151)

[3.2.3 实验组网 28](#_Toc121152152)

[3.2.4 操作步骤 28](#_Toc121152153)

[3.3 VLAN隔离/互通 29](#_Toc121152154)

[3.3.1 说明 29](#_Toc121152155)

[3.3.2 实验任务 29](#_Toc121152156)

[3.3.3 实验组网 29](#_Toc121152157)

[3.3.4 操作步骤 30](#_Toc121152158)

[3.3.5 VLAN 互通 31](#_Toc121152159)

[3.3.6 实验验证 32](#_Toc121152160)

[4 实验任务3： IPv4与路由 32](#_Toc121152161)

[4.1 实验介绍 32](#_Toc121152162)

[4.1.1 关于本实验 32](#_Toc121152163)

[4.1.2 实验目的 33](#_Toc121152164)

[4.1.3 组网说明 34](#_Toc121152165)

[4.2 IPv4地址配置 34](#_Toc121152166)

[4.2.1 说明 34](#_Toc121152167)

[4.2.2 实验任务 34](#_Toc121152168)

[4.2.3 实验组网 35](#_Toc121152169)

[4.2.4 操作步骤 35](#_Toc121152170)

[4.2.5 实验验证 36](#_Toc121152171)

[4.3 DHCP 配置 36](#_Toc121152172)

[4.3.1 说明 36](#_Toc121152173)

[4.3.2 实验任务 36](#_Toc121152174)

[4.3.3 实验组网 36](#_Toc121152175)

[4.3.4 操作步骤 36](#_Toc121152176)

[4.3.5 实验验证 37](#_Toc121152177)

[4.4 静态路由配置 38](#_Toc121152178)

[4.4.1 说明 38](#_Toc121152179)

[4.4.2 实验任务 38](#_Toc121152180)

[4.4.3 实验组网 38](#_Toc121152181)

[4.4.4 操作步骤 39](#_Toc121152182)

[4.4.5 实验验证 39](#_Toc121152183)

[4.5 OSPF 配置 39](#_Toc121152184)

[4.5.1 说明 39](#_Toc121152185)

[4.5.2 实验任务 39](#_Toc121152186)

[4.5.3 实验组网 40](#_Toc121152187)

[4.5.4 操作步骤 40](#_Toc121152188)

[4.5.5 实验验证 41](#_Toc121152189)

[4.6 BGP 配置(高阶) 41](#_Toc121152190)

[4.6.1 说明 41](#_Toc121152191)

[4.6.2 实验任务 41](#_Toc121152192)

[4.6.3 实验组网 41](#_Toc121152193)

[4.6.4 操作步骤 42](#_Toc121152194)

[4.6.5 实验验证 42](#_Toc121152195)

[4.7 NAT 43](#_Toc121152196)

[4.7.1 说明 43](#_Toc121152197)

[4.7.2 实验任务 43](#_Toc121152198)

[4.7.3 实验组网 43](#_Toc121152199)

[4.7.4 操作步骤 43](#_Toc121152200)

[4.7.5 实验验证 44](#_Toc121152201)

[5 实验任务4： IPv6与路由 45](#_Toc121152202)

[5.1 实验介绍 45](#_Toc121152203)

[5.1.1 关于本实验 45](#_Toc121152204)

[5.1.2 实验目的 46](#_Toc121152205)

[5.2 IPv6地址配置 46](#_Toc121152206)

[5.2.1 说明 46](#_Toc121152207)

[5.2.2 实验组网 47](#_Toc121152208)

[5.2.3 操作步骤 47](#_Toc121152209)

[5.2.4 实验验证 48](#_Toc121152210)

[5.3 IPv6静态路由 48](#_Toc121152211)

[5.3.1 说明 48](#_Toc121152212)

[5.3.2 实验任务 48](#_Toc121152213)

[5.3.3 实验组网 48](#_Toc121152214)

[5.3.4 操作步骤 48](#_Toc121152215)

[5.3.5 实验验证 49](#_Toc121152216)

[5.4 IPv4/IPv6过渡(高阶) 49](#_Toc121152217)

[5.4.1 说明 49](#_Toc121152218)

[5.4.2 实验任务 49](#_Toc121152219)

[5.4.3 实验组网 49](#_Toc121152220)

[5.4.4 操作步骤 50](#_Toc121152221)

[5.4.5 实验验证 50](#_Toc121152222)

[6 实验任务5：VPN(高阶) 51](#_Toc121152223)

[6.1 实验介绍 51](#_Toc121152224)

[6.1.1 关于本实验 51](#_Toc121152225)

[6.1.2 实验目的 51](#_Toc121152226)

[6.2 IPSec VPN配置(高阶) 52](#_Toc121152227)

[6.2.1 说明 52](#_Toc121152228)

[6.2.2 实验任务 52](#_Toc121152229)

[6.2.3 实验组网 52](#_Toc121152230)

[6.2.4 操作步骤 53](#_Toc121152231)

[6.2.5 实验验证 54](#_Toc121152232)

[6.3 BGP/MPLS VPN(高阶+) 54](#_Toc121152233)

[6.3.1 说明 54](#_Toc121152234)

[6.3.2 实验任务 54](#_Toc121152235)

[6.3.3 实验组网 54](#_Toc121152236)

[6.3.4 操作步骤 55](#_Toc121152237)

[6.3.5 实验验证 57](#_Toc121152238)

[7 实验任务6：Qos配置 58](#_Toc121152239)

[7.1 实验介绍 58](#_Toc121152240)

[7.1.1 关于本实验 58](#_Toc121152241)

[7.1.2 实验目的 58](#_Toc121152242)

[7.2 MQC原理和配置方法 59](#_Toc121152243)

[7.2.1 说明 59](#_Toc121152244)

[7.2.2 实验任务 59](#_Toc121152245)

[7.2.3 实验组网 59](#_Toc121152246)

[7.2.4 操作步骤 59](#_Toc121152247)

[7.2.5 实验验证 60](#_Toc121152248)

[7.3 流量监管和流量整形 61](#_Toc121152249)

[7.3.1 说明 61](#_Toc121152250)

[7.3.2 实验任务 62](#_Toc121152251)

[7.3.3 实验组网 62](#_Toc121152252)

[7.3.4 操作步骤 62](#_Toc121152253)

[7.3.5 实验验证 63](#_Toc121152254)

[8 实验任务7：IP安全配置 64](#_Toc121152255)

[8.1 实验介绍 64](#_Toc121152256)

[8.1.1 关于本实验 64](#_Toc121152257)

[8.1.2 实验目的 65](#_Toc121152258)

[8.2 ACL配置 65](#_Toc121152259)

[8.2.1 基于IP地址ACL配置 65](#_Toc121152260)

[8.3 防火墙配置(高阶) 67](#_Toc121152261)

[8.3.1 内外网隔离 67](#_Toc121152262)

[8.3.2 攻击防范 69](#_Toc121152263)

[9 实验任务8：WLAN配置 69](#_Toc121152264)

[9.1 实验介绍 69](#_Toc121152265)

[9.1.1 关于本实验 69](#_Toc121152266)

[9.1.2 实验目的 70](#_Toc121152267)

[9.2 WLAN网络架构&AP接入网络 70](#_Toc121152268)

[9.2.1 WLAN网络架构 70](#_Toc121152269)

[9.2.2 AP接入网络 71](#_Toc121152270)

[9.3 终端接入网络 73](#_Toc121152271)

[9.3.1 终端接入网络 73](#_Toc121152272)

[10 综合实验：校园园区网搭建（高阶+） 76](#_Toc121152273)

[10.1 实验介绍 76](#_Toc121152274)

[10.1.1 关于本实验 76](#_Toc121152275)

[10.1.2 实验目的 76](#_Toc121152276)

[10.2 校园园区网搭建 77](#_Toc121152277)

[10.2.1 实验介绍 77](#_Toc121152278)

[11 实验环境使用建议 79](#_Toc121152279)

[11.1 说明 79](#_Toc121152280)

[11.2 各个实验配置基础关系 79](#_Toc121152281)

[11.3 多批次同学共用设备 81](#_Toc121152282)

[11.3.1 保存配置至交换机Flash 81](#_Toc121152283)

[11.3.2 FTP 下载配置文件至PC机/PC 机上传配置文件 82](#_Toc121152284)

[11.3.3 恢复配置文件 82](#_Toc121152285)

[11.3.4 TCL脚本工具 83](#_Toc121152286)

# 实验总体介绍

## 实验总体介绍

### 关于本实验

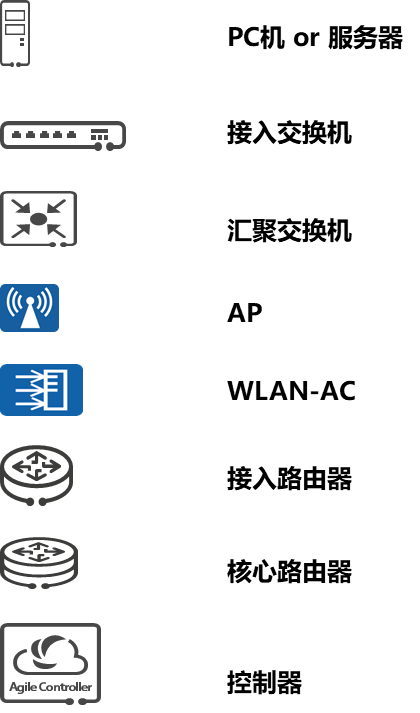
本实验面向高校学习计算机网络的相关学生，内容包括交换机、路由器的基础操作，以太网交换机技术、路由协议原理、广域网技术等基础实验，以及网络应用相关高阶实验组成。

### 实验目的

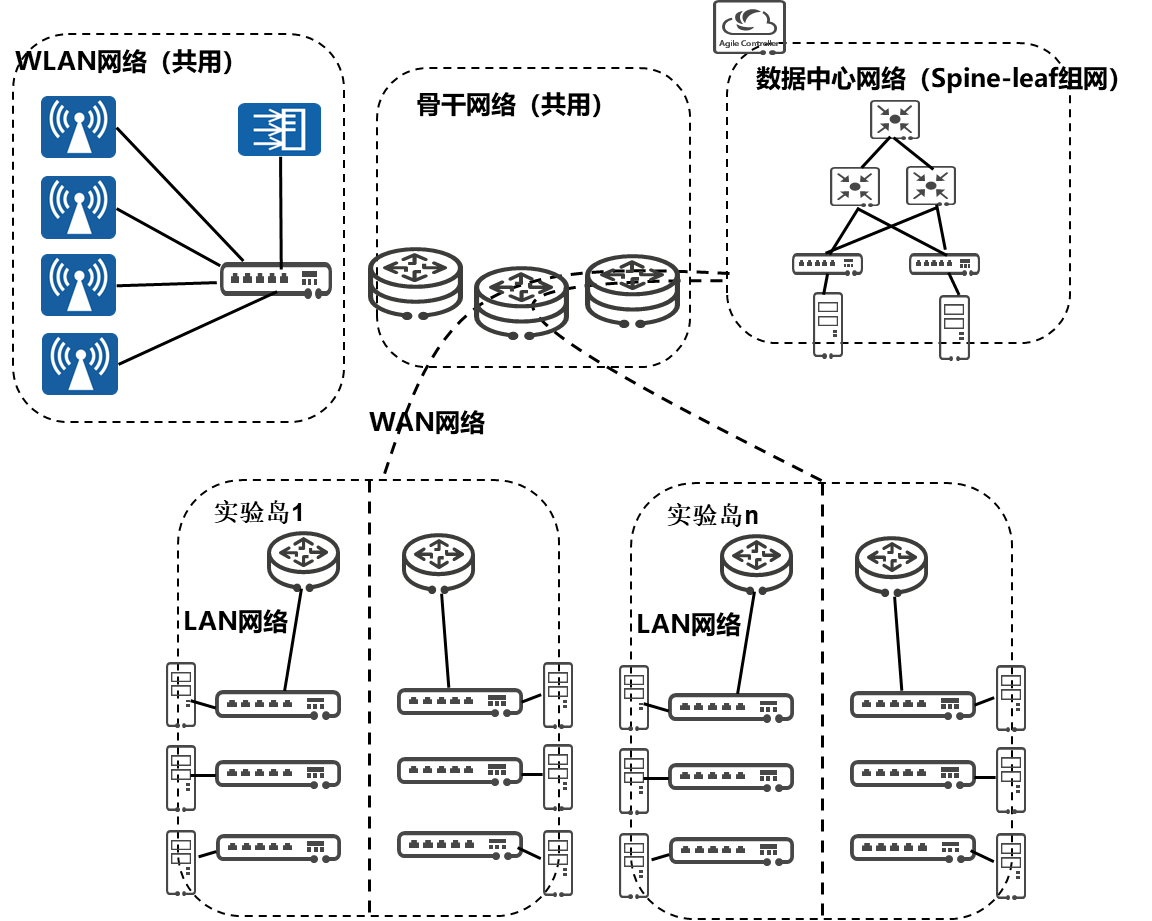
* 掌握交换路由基础知识；
* 掌握简单企业广域网部署；
* 掌握简单安全配置；
* 应用网络数据信息提供业务服务；

### 实验组网介绍

#### 组网图例



#### 组网图

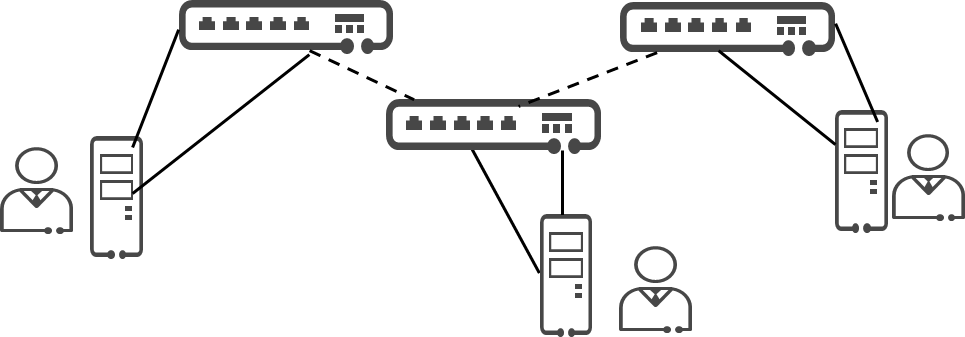


建议实验环境部署如下：按实验岛方式部署基础实验环境，为学生提供相对独立的操作空间。每个实验岛为6名学生提供实验环境。每岛分为2个实验小组，每组环境提供给3个学生同时上机操作，实验设备包括交换机交换机3台，路由器1台。

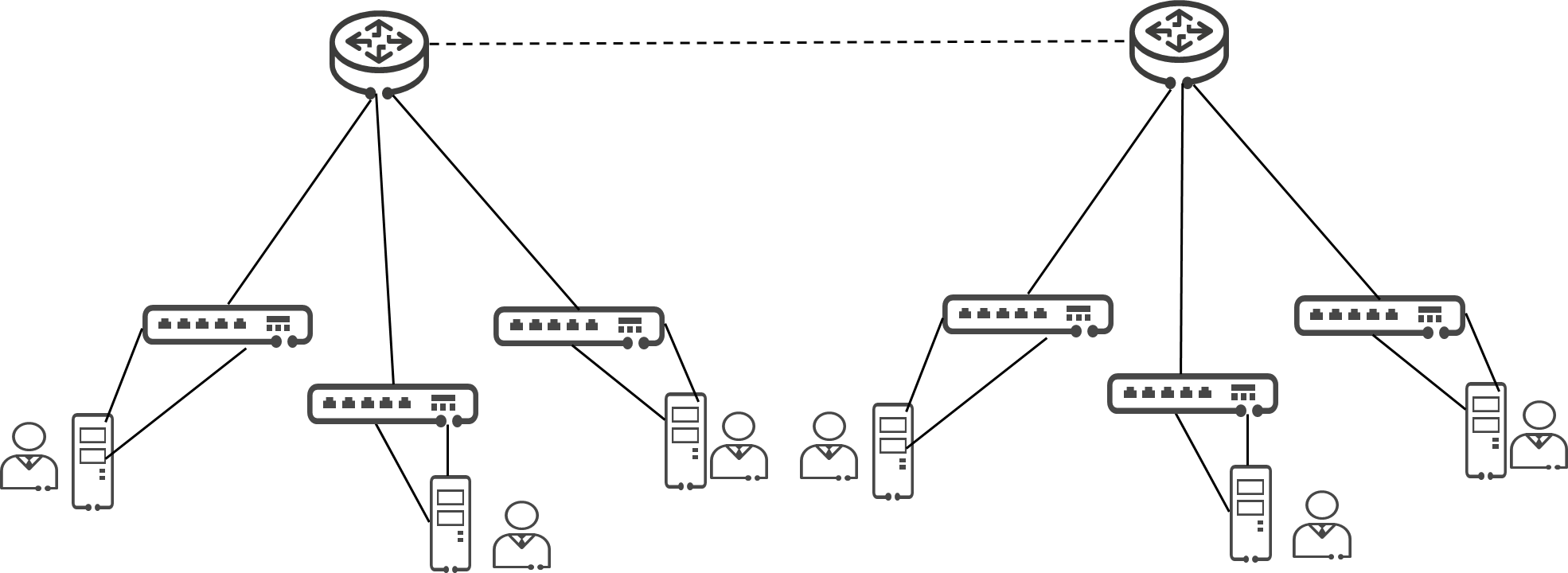
实验一 基础配置组网图



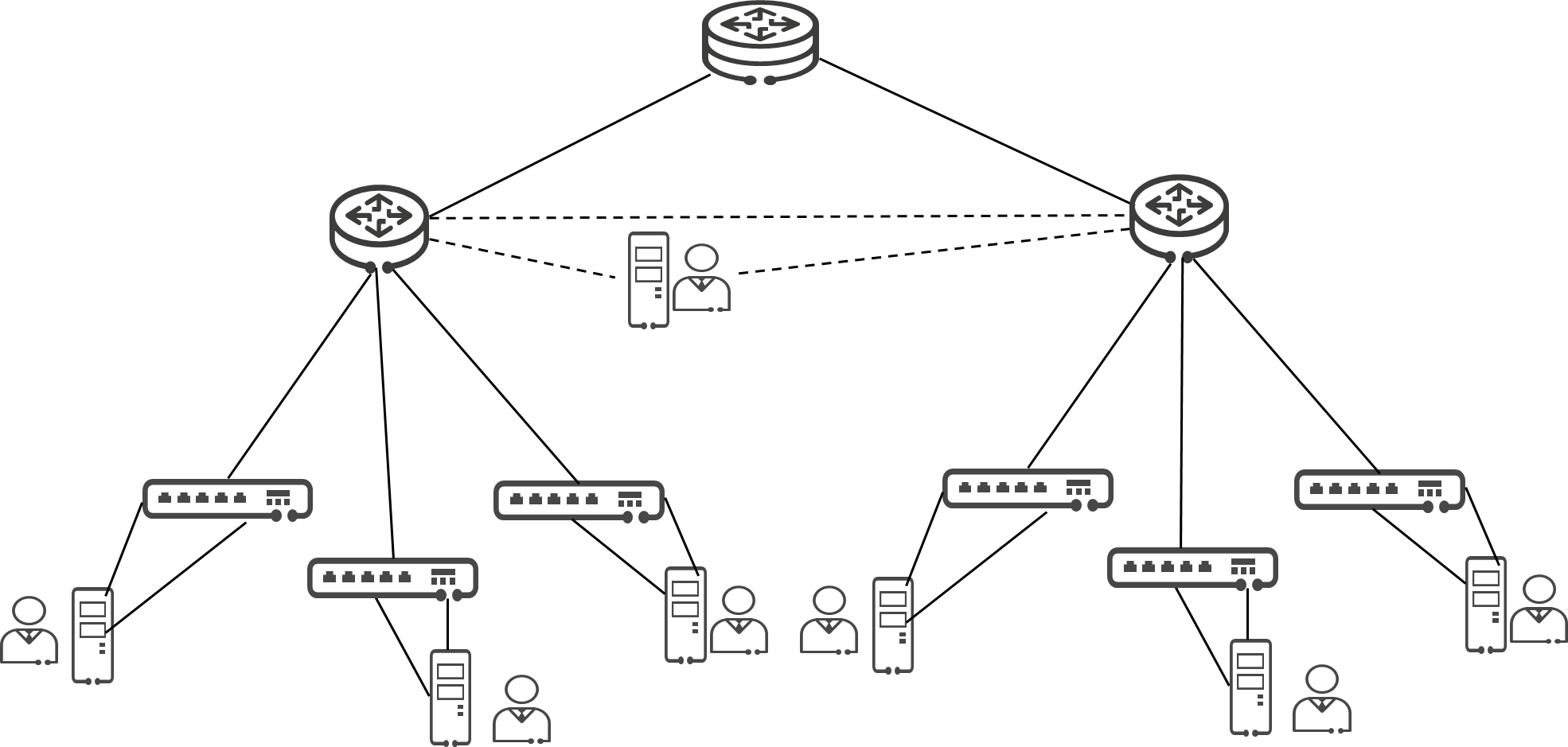
实验二 以太网组网图



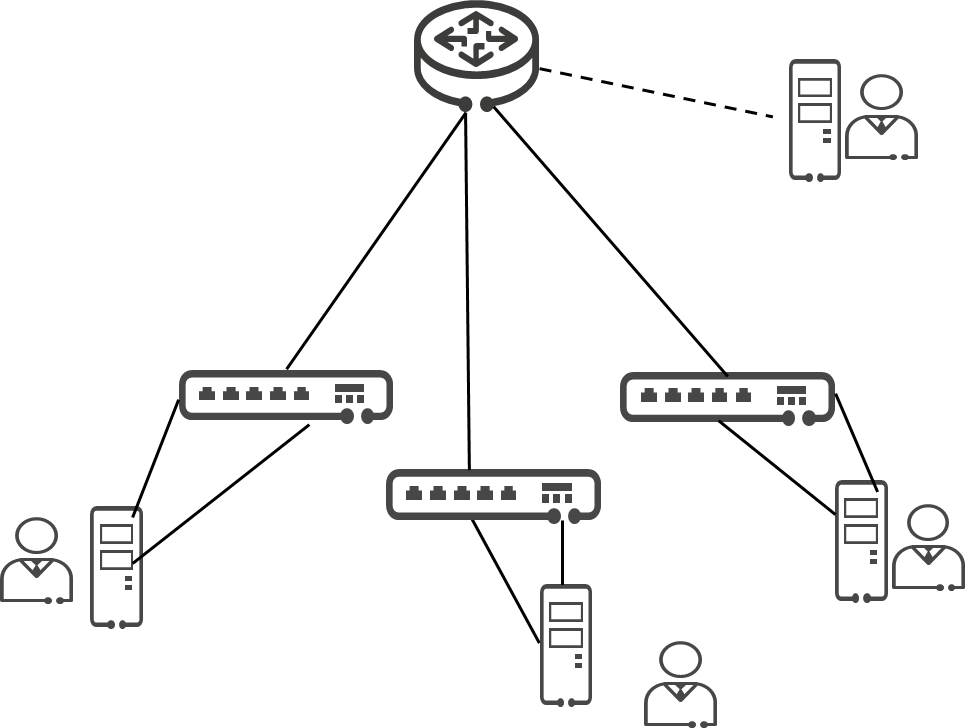
实验二 IP与路由组网图



实验三 广域网实验组网图



实验四 安全配置组网图



### 实验资源

设备名称、型号与版本的对应关系如下：

实验设备详细信息

|  |  |  |
| --- | --- | --- |
| 设备名称 | 设备型号 | 软件版本 |
| 岛内交换机 | S5730LI/S5330LI | V200R019C10 |
| 岛内路由器 | AR657/AR6140 | V300R019C10 |
|  |  |  |

### 实验工具

实验工具详细信息

|  |  |  |
| --- | --- | --- |
| 名称 | 获取途径 | 用途 |
| PC机 | 需同学们自带笔记本电脑。建议使用Windows10 笔记本电脑。苹果Mac实验用例未经过验证 | 使用串口转换器管理设备  使用ETH网口连接网络 |
| USB转console控制线 | 学校提供 | USB口转换为console，连接管理设备。需安装驱动 |
| 设备管理工具 | IPOP4.1/SecureCRT/mobaxterm… | 设备管理工具，可仿真console口和telnet/ssh等登录设备 |
| wireshark | https://www.wireshark.org/ | 抓包分析工具 |
| MOOC | HCIA Mooc 《HCIA-Datacom V1.0 华为认证数通工程师在线课程》  https://talent.huaweiuniversity.com/portal/courses/HuaweiX+EBGTC00000546/about | MOOC教学，需要注册账号 |
| 交换机产品文档 | https://support.huawei.com/enterprise/zh/doc/EDOC1100126575?idPath=24030814%7C21782164%7C21782167%7C22318564%7C6691579### | 交换机配置参考 |
| 路由器产品文档 | https://support.huawei.com/enterprise/zh/doc/EDOC1100087045?idPath=24030814%7C21432787%7C23708834%7C250680707### | 路由器配置参考 |
| eNSP | https://forum.huawei.com/enterprise/zh/thread-573181.html | 华为数通设备模拟器，在上机前模拟使用。建议第三章及以后章节提前模拟 |

### 实验实例化

本次实验部分配置可使用学号实例化，例如设备名称，IP地址。

1. 设备名称，每位同学一台交换机，交换机配置为自己的学号。
2. 设备上各接口IP地址。本实验用例地址仅做参考，各组在实验时IP地址自行规划。原则上组内IP地址不冲突即可。

# 实验任务1： 基础管理

## 实验介绍

### 关于本实验

本实验完成接入交换机的基础管理。其它设备如路由器配置方式类似，不重复实验。

所以的实验组网都采用PC机直连交换机console口方式完成。

实验参考相应的产品文档，本实验可参考章节如下：



Mooc 可以参考《HCIA-Datacom V1.0 华为认证数通工程师在线课程》中 “华为VRP系统”章节。

### 实验目的

掌握Console口/telnet登录方法；

掌握设备系统参数的配置方法，包括查看系统信息，帮助命令，设备名称、系统时间。

配置设备的管理IP地址

掌握保存、恢复配置文件的方法

掌握重启设备的方法

## 首次登录设备

### 说明

要对一台新出厂的设备进行业务配置，通常需要本地登录设备。本地登录以后，完成设备名称、管理IP地址和系统时间等系统基本配置，并配置Telnet或STelnet协议实现远程登录。

设备支持的首次登录方式有：

•Console口登录，使用CLI命令行方式管理设备

•Web网管登录，使用web 图形化方式管理设备

本次实验完成console 口登录设备

### 通过Console口首次登录设备

#### 实验任务

通过Console口 登录设备。

在配置通过Console口登录设备之前，需要完成以下前置条件：

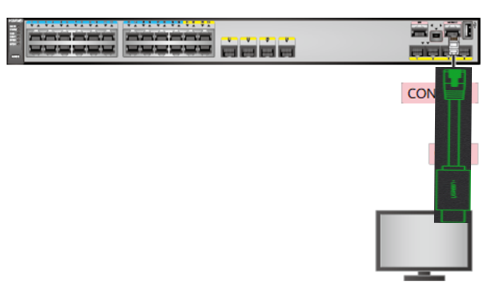
* 设备正常上电，此时设备sys灯会显示绿灯。
* 准备好USB转Console控制线缆。根据线缆类型，PC机上安装好驱动程序。

插入线缆后，在设备管理器会看到新增 USB-to-Serial 端口。



* 准备好终端仿真软件。

#### 实验组网

* 

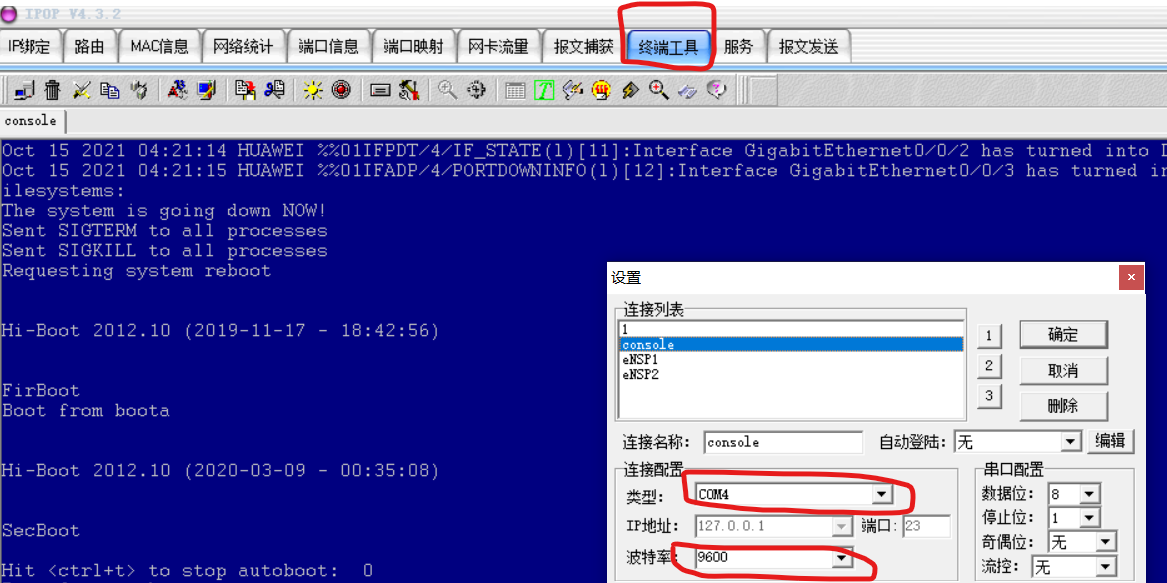
#### 操作步骤

1. 将Console通信电缆的USB口插入PC机的USB口中，再将RJ-45插头端插入设备的Console口中
2. 在PC上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。

设置终端软件的通信参数需与设备的缺省值保持一致，设置终端软件的通信参数如[表1](mk:@MSITStore:D:\work\高校合作\输出\素材\S2720,%20S5700,%20S6700%20V200R020C00%20产品文档.chm::/dc/dc_cfg_first_1004.html#ZH-CN_TASK_0177100089__table990516335152)所示。

|  |  |
| --- | --- |
| **表1** 设备缺省值 | |
| **参数** | **缺省值** |
| 传输速率 | **9600bit/s** |
| 流控方式 | 不进行流控 |
| 校验方式 | 不进行校验 |
| 停止位 | 1 |
| 数据位 | 8 |

以IPOP 为例，设置如下：其中COM4 选择为设备管理器中新增的那个端口



1. 终端界面会出现如下显示信息，提示输入用户名密码。（以下显示信息仅为示意）

本实验管理员缺省用户名是 [admin；密码需咨询实验老师](mailto:admin/admin@seu.com)

User interface con isavailable

Please Press ENTER.

Login authentication

Username:admin

Password:

#### 实验验证

登录console管理设备

## 系统常用配置

### 帮助功能和命令自动补全

#### 说明

在线帮助通过键入“?”来获取，在命令行输入过程中，用户可以随时键入“?”以获得在线帮助。命令行在线帮助可分为完全帮助和部分帮助。

#### 实验任务

掌握命令行帮助功能

#### 实验组网

同2.2.2

#### 操作步骤

##### 完全帮助

当用户输入命令时，可以使用命令行的完全帮助获取全部关键字和参数的提示。下面给出几种完全帮助的实例供参考：

1. 在任一命令视图下，键入“?”获取该命令视图下所有的命令及其简单描述。举例如下：

<HUAWEI> ?

User view commands:

backup Backup electronic elabel

cd Change current directory

...

1. 键入一条命令的部分关键字，后接以空格分隔的“?”，如果该位置为关键字，则列出全部关键字及其简单描述。举例如下：

<HUAWEI> system-view

[HUAWEI] user-interface vty 0 4

[HUAWEI-ui-vty0-4] authentication-mode ?

aaa AAA authentication, and this authentication mode is recommended

none Login without checking

password Authentication through the password of a user terminal interface

其中“aaa”和“password”是关键字，“AAA authentication”和“Authentication through the password of a user terminal interface”是对关键字的描述。

##### 部分帮助

1. 键入一条命令，后接一字符串紧接“?”，列出命令以该字符串开头的所有关键字。举例如下：

<HUAWEI> display b?

bpdu bridge

buffer

1. 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。

#### 实验验证

NA

### 查看系统信息

执行 **display version** 命令，查看设备的软件版本与硬件信息。

#### 说明

通过查看设备当前的版本信息，可以判断设备是否需要升级或者升级是否成功

#### 实验任务

查看设备当前运行版本。

#### 实验组网

同2.2.2

#### 操作步骤

<HUAWEI>display version

Huawei Versatile Routing Platform Software

VRP (R) software, Version 5.170 (S5735 V200R019C10SPC500)

Copyright (C) 2000-2020 HUAWEI TECH Co., Ltd.

HUAWEI S5735-L24T4S-A Routing Switch uptime is 0 week, 0 day, 4 hours, 3 minutes

ES5D2T28S022 0(Master) : uptime is 0 week, 0 day, 4 hours, 2 minutes

DDR Memory Size : 1024 M bytes

FLASH Total Memory Size : 512 M bytes

FLASH Available Memory Size : 306 M bytes

Pcb Version : VER.D

BootROM(1st) Version : 0000.0121

BootROM(2nd) Version : 0000.0200

BootLoad Version : 0213.0000

CPLD Version : 0106

Software Version : VRP (R) Software, Version 5.170 (V200R019C10SPC500)

FLASH Version : 0000.0000

命令回显信息中包含了VRP版本，设备型号和启动时间等信息

#### 实验验证

验证显示的版本信息是否符合预期。

### 进入视图

#### 说明

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，华为交换机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。

常用视图名称如下：

| **常用视图名称** | **进入视图** | **视图功能** |
| --- | --- | --- |
| 用户视图 | 用户从终端成功登录至设备即进入用户视图，在屏幕上显示：  <HUAWEI> | 在用户视图下，用户可以完成查看运行状态和统计信息等功能。 |
| 系统视图 | 在用户视图下，输入命令**system-view**后回车，进入系统视图。  <HUAWEI> **system-view**  Enter system view, return user view with Ctrl+Z.  [HUAWEI] | 在系统视图下，用户可以配置系统参数以及通过该视图进入其他的功能配置视图。 |
| 接口视图 | 使用**interface**命令并指定接口类型及接口编号可以进入相应的接口视图。  [HUAWEI] **interface gigabitethernet** X/Y/Z  [HUAWEI-GigabitEthernetX/Y/Z]  X/Y/Z为需要配置的接口的编号，分别对应“堆叠ID/子卡号/接口序号”。  上述举例中GigabitEthernet接口仅为示意。 | 配置接口参数的视图称为接口视图。在该视图下可以配置接口相关的物理属性、链路层特性及IP地址等重要参数。 |

#### 实验任务

理解属性视图概念。完成进入system视图实验。

#### 实验组网

同2.2.2

#### 操作步骤

<HUAWEI> system-view

Enter system view, return user view with Ctrl+Z.

[HUAWEI]

#### 实验验证

NA

### 修改设备名称

#### 说明

设备发货缺省设备名为HUAWEI。配置设备时，为了便于区分，往往给设备定义不同的名称。在现网部署中一般会指明设备处于的位置，比如大楼-楼层-接入点等。

在本实验中，我们以学生学号作为设备名称。

#### 实验任务

设置接入交换机设备名称。

#### 实验组网

同2.2.2

#### 操作步骤

<HUAWEI> system-view

[HUAWEI] sysname 123456

[123456]

#### 实验验证

验证系统名是否已经修改为学号123456。

### 查看当前视图配置

#### 说明

在视图下，使用display this命令，可以查看已经配置的命令。例如可以查看系统视图，接口视图下命令

#### 实验任务

查看当前视图生效配置。

#### 实验组网

同2.2.2

#### 操作步骤

<123456> system-view

[123456]display this

#

sysname 123456

#

#### 实验验证

查看到系统视图下已经配置命令 sysname 123456

### 删除已有配置

#### 说明

若希望删除视图下已经配置的命令，可以在该视图下使用undo 命令，删除掉该命令。有两点要注意：

1. 若几条命令有相互依赖关系，则需要先删除后配置的命令，接触依赖后才能删除前面配置的命令
2. 一般情况下 可以用undo [想删除的完整命令] 。部分命令由于其参数具有唯一性，可以不输入参数就能删除。这类命令一般情况下可以直接修改最后的参数。例如，删除设备名

[123456]undo sysname 123456

^

会提示123456 有错误。此时可以用? 帮助，只需要使用undo sysname 即可

[123456]undo sysname ?

<cr>

#### 实验任务

删除设备名配置。

#### 实验组网

同2.2.2

#### 操作步骤

<123456> system-view

[123456]undo sysname

[Huawei]

#### 实验验证

查看到设备名已经变为huawei

## 保存恢复配置

### 任务介绍

### 保存设备配置

#### 说明

用户通过命令行可以修改设备的当前配置，而这些配置是暂时的，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。

save命令用来保存当前配置信息到系统默认的存储路径中

display current-configuration 命令用来查看当前设备内存中生效的配置。

display startup 命令用来查看设备启动时使用哪个配置文件

#### 实验任务

保存配置文件，文件名为学号.cfg。

#### 实验组网

同2.2.2

#### 操作步骤

<HUAWEI> save 123456.cfg

The current configuration will be written to flash:/ 123456.cfg.

Are you sure to continue?[Y/N]y

Now saving the current configuration to the slot 0.

Info: Save the configuration successfully.

#### 实验验证

查看配置文件是否被保存成功。

<123456> dir

Directory of flash:/

Idx Attr Size(Byte) Date Time(LMT) FileName

0 -rw- 981 Oct 19 2021 09:23:19 123456.cfg

1 drw- - Oct 19 2021 09:20:23 dhcp

2 -rw- 121,802 May 26 2014 09:20:58 portalpage.zip

3 -rw- 2,263 Oct 19 2021 09:20:12 statemach.efs

4 -rw- 828,482 May 26 2014 09:20:58 sslvpn.zip

5 -rw- 352 Oct 19 2021 09:23:20 private-data.txt

1,090,732 KB total (784,448 KB free)

查看配置文件内容：

<12345>more 123456.cfg

#

sysname 12345

#

### 备份设备配置

#### 说明

为防止设备意外损坏，导致配置文件无法恢复，有多种方法进行备份配置文件：

* 直接屏幕拷贝。
* 备份配置文件到存储器中。
* 通过FTP、TFTP、FTPS、SFTP和SCP备份配置文件。
* 通过执行命令行进行备份。
* 通过执行命令行实时备份当前配置

可能出现多个同学共用设备情况，每个同学配置不同，需要将配置文件备份，用于下次恢复使用。

需要同学每次实验完成后，都完成配置文件的备份工作。

#### 实验任务

本实验采用备份文件到存储器方式完成。

#### 实验组网

同2.2.2，需要PC机通过网线接入到管理网口。

#### 操作步骤

##### 备份文件到存储器方式

该步骤主要便于用户在设备的flash中及时备份当前配置文件。在设备启动之后，使用如下命令在设备的flash中备份配置文件。

<123456> save 123456.cfg

<HUAWEI> copy 123456.cfg 123456bk.cfg

#### 实验验证

确认**123456**.cfg和**123456bk**.cfg的文件大小是否一致。如果文件大小一致则认为备份成功

### 恢复设备配置

#### 说明

不同学生更换使用设备时，可以通过以下两种方法进行配置文件恢复：

* 从存储器恢复配置文件。
* 通过FTP、TFTP、FTPS、SFTP和SCP恢复配置文件。

本实验使用存储器方式恢复配置文件。

#### 实验任务

123456同学使用上一个同学654321的环境，将配置文件替换为自己的配置文件。

#### 实验组网

同2.2.2

#### 操作步骤

缺省情况下从存储器恢复配置文件即可

##### 从存储器恢复配置文件

恢复配置文件

<huawei> copy flash:/123456.cfg flash:/123456bk.cfg

##### 设置重启配置文件：

执行命令startup saved-configuration configuration-file，指定系统下次启动时使用的配置文件。

<654321> startup saved-configuration 123456.cfg

Info: Succeeded in setting the configuration for booting system.

##### 重启设备：

在用户视图下，执行命令reboot fast，实现对设备的重新启动。

指定fast，表示快速重启设备，不会提示是否保存配置文件。

#### 实验验证

查看配置文件是否为自己的配置。

<123456> display saved-configuration

#

sysname 123456

...

#

# 实验任务2： 以太交换

## 实验介绍

### 关于本实验

本实验完成接入交换机的ETH配置，用于理解ETH的转发原理。

实验参考相应的产品文档，本实验可参考章节如下：



Mooc 可以参考《HCIA-Datacom V1.0 华为认证数通工程师在线课程》中 “以太交换基础”、“VLAN原理与配置”章节。

### 实验目的

* 掌握二层转发相关流程
* 掌握VLAN的部署和配置流程。

## 广播转发

### 说明

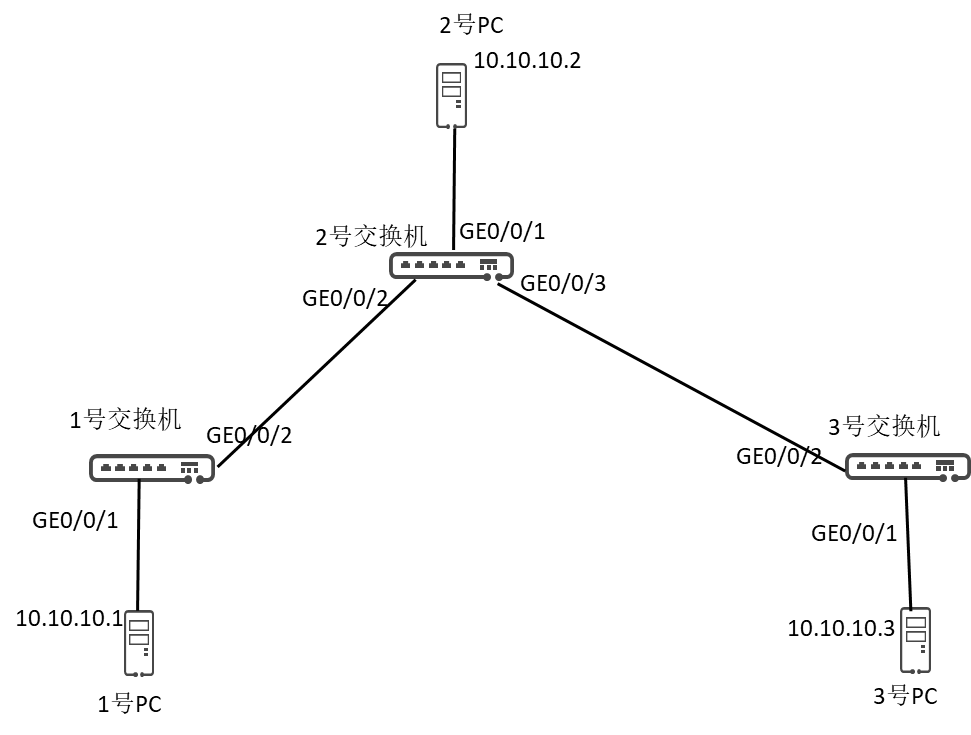
交换机发货接口缺省VLAN为1，此时交换机相当于是一个Hub，所有接口是互通的。

### 实验任务

学习以太网转发流程，理解MAC学习过程以及转发过程。

### 实验组网

同一个小组3位同学配合做实验，连线关系如下图，PC机配置如下IP地址，IP地址都在同一广播域中。



### 操作步骤

1. 3台PC间 ping 测试互通
2. 登录到交换机上，查看MAC地址学习过程，关注学习到的MAC对应的端口/VLAN 情况

display mac-address

#### 实验验证

1. 交换机MAC学习符合预期
2. PC机间能够ping通

## VLAN隔离/互通

### 说明

配置VLAN，隔离广播域。可以通过调整Trunk 接口上的VLAN，观察各设备上MAC学习情况，理解交换机转发过程。

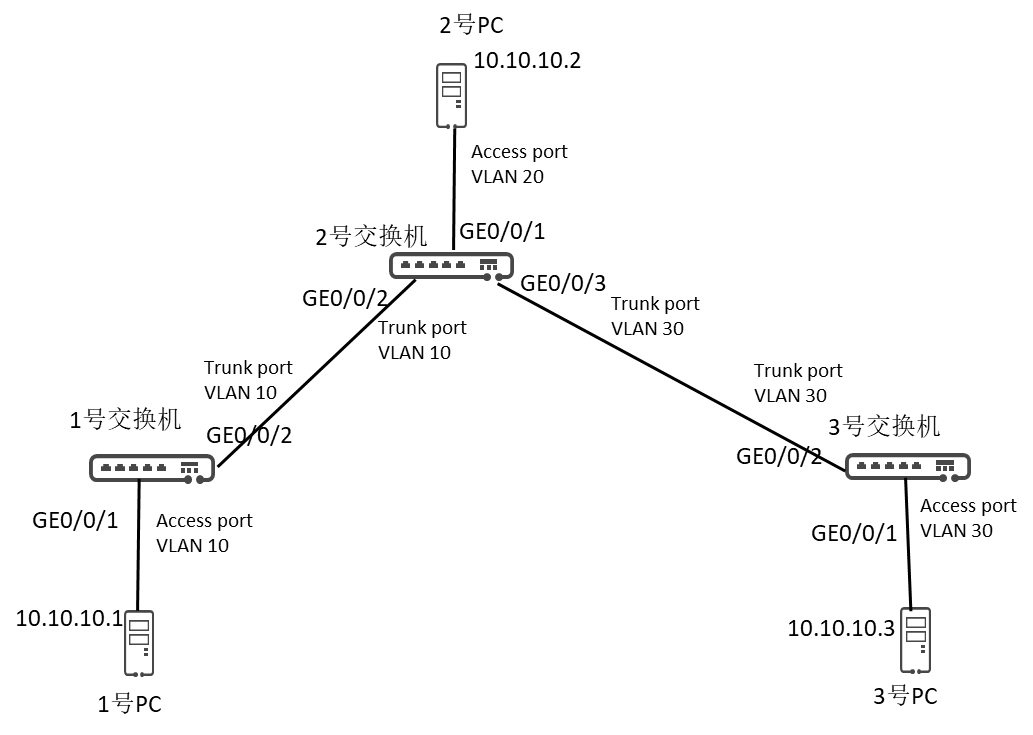
### 实验任务

各同学配置不同接入VLAN。交换机间接口配置Trunk VLAN。

理解VLAN概念以及其与接口的关系；

### 实验组网

同一个小组3位同学配合做实验，连线关系如下图，PC机配置如下IP地址，在各端口分别配置如下VLAN。



### 操作步骤

#### VLAN 隔离

##### 实验验证目标

PC1 与PC3 使用不同的VLAN隔离，不能互通

##### 实验配置

1. 1号交换机配置

# 接入端口VLAN配置为 VLAN 10，Trunk 口配置 10 VLAN.举例如下：

#交换机上全局开启VLAN资源，batch可以创建多个

[Switch\_1] vlan batch 10 20 30

#接PC机接口设置为access接口，并配置缺省VLAN

[Switch\_1] interface gigabitethernet 0/0/1 //进入接口视图

[Switch\_1-GigabitEthernet0/0/1] port link-type access //配置access类型

[Switch\_1-GigabitEthernet0/0/1] port default vlan 10 //配置缺省VLAN，VLAN 10 与这个端口关联了

#接2号交换机接口 设置为Trunk接口，并配允许通过的VLAN

[Switch\_1] interface gigabitethernet 0/0/2

[Switch\_1-GigabitEthernet0/0/2] port link-type trunk //配置trunk类型

[Switch\_1-GigabitEthernet0/0/2] port trunk allow-pass vlan 10//允许接口上VLAN 10 通过，VLAN 10 与这个端口关联了

[Switch\_1-GigabitEthernet0/0/2] quit

1. 2号交换机配置

#接入端口VLAN配置为 VLAN 20，Trunk 口配置 20 VLAN

配置类似，这里不做具体描述

1. 3号交换机配置

# 接入端口VLAN配置为 VLAN 30，Trunk 口配置 30 VLAN

配置类似，这里不做具体描述

1. 查看VLAN配置结果

[123456-GigabitEthernet0/0/2]display vlan

The total number of VLANs is: 2

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

U: Up; D: Down; TG: Tagged; UT: Untagged;

MP: Vlan-mapping; ST: Vlan-stacking;

#: ProtocolTransparent-vlan; \*: Management-vlan;

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

VID Type Ports

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

1 common UT:GE0/0/2(D) GE0/0/3(D) GE0/0/4(D) GE0/0/5(D)

GE0/0/6(D) GE0/0/7(D) GE0/0/8(D) GE0/0/9(D)

GE0/0/10(D) GE0/0/11(D) GE0/0/12(D) GE0/0/13(D)

GE0/0/14(D) GE0/0/15(D) GE0/0/16(D) GE0/0/17(D)

GE0/0/18(D) GE0/0/19(D) GE0/0/20(D) GE0/0/21(D)

GE0/0/22(D) GE0/0/23(D) GE0/0/24(D) GE0/0/25(D)

GE0/0/26(D) GE0/0/27(D) GE0/0/28(D)

10 common UT:GE0/0/1(D) //access 接口，Untagged

TG:GE0/0/2(D) // trunk 接口，Tagged

VID Status Property MAC-LRN Statistics Description

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

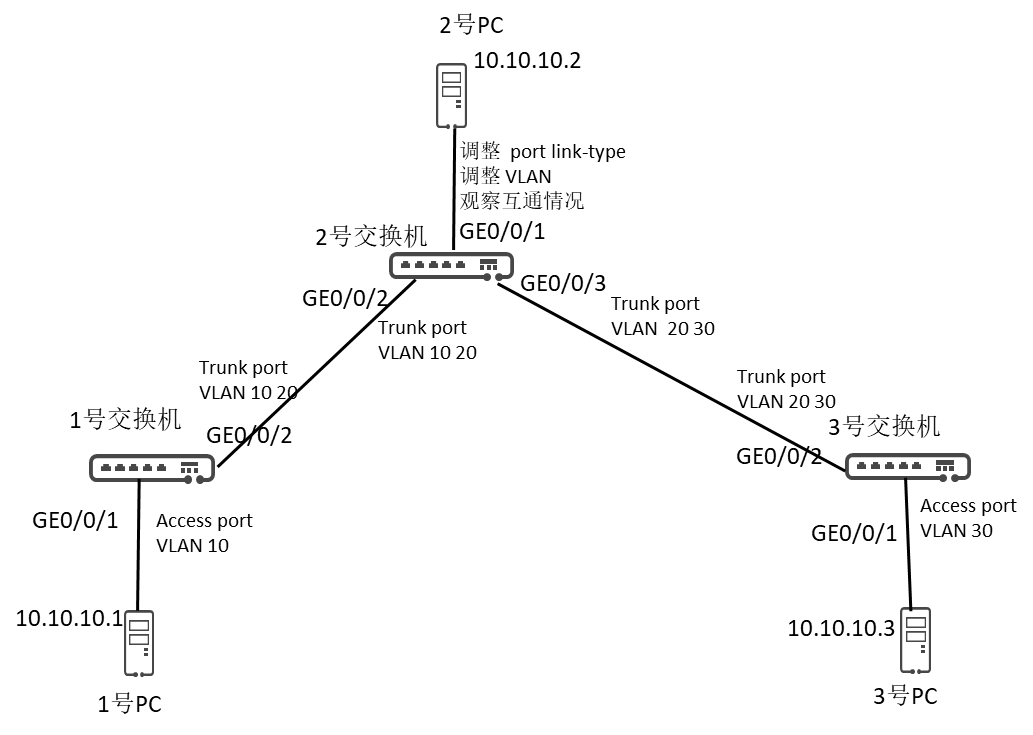
1 enable default enable disable VLAN 0001

10 enable default enable disable VLAN 0010

### VLAN 互通

##### 实验验证目标

在上个测试项中，变更2号交换机 access VLAN 配置，分别变化为VLAN 10 和VLAN30，测试PC1和PC2是否可以互通，PC2和PC3是否可以互通



### 实验验证

1. 验证各种情况下 PC间互通情况
2. 验证各种情况下交换机MAC学习情况。观察交换机上学习到哪些MAC地址，学习在哪个VLAN中，哪个端口上
3. 可以变更Trunk 口VLAN，观察MAC学习情况

# 实验任务3： IPv4与路由

## 实验介绍

### 关于本实验

本实验完成IPv4地址相关配置，完成路由协议部署。

交换机和路由器三层配置有所区别：

交换机中一般是采用VLANIF方式承载3层业务， AR路由器一般采用物理端口或者子接口方式承载3层业务。本实验中两种设备上IP业务配置的接口方式会有所不同。

实验参考相应的产品文档，本实验可参考章节如下：



Mooc 可以参考《HCIA-Datacom V1.0 华为认证数通工程师在线课程》中 “网络层协议及IP编址”、“IP路由基础”、“OSPF基础”、“网络地址转换”章节。

### 实验目的

掌握IPv4地址以及部署方式

掌握基础路由支持

掌握OSPF的部署和配置流程；

掌握BGP基本配置(高阶)

掌握NAT基本原理与配置

### 组网说明

路由实验分几部分，IPv4/路由配置比较复杂，涉及配置比较多，需要在每个实验用例后保存配置，下个用例沿用此配置。



## IPv4地址配置

### 说明

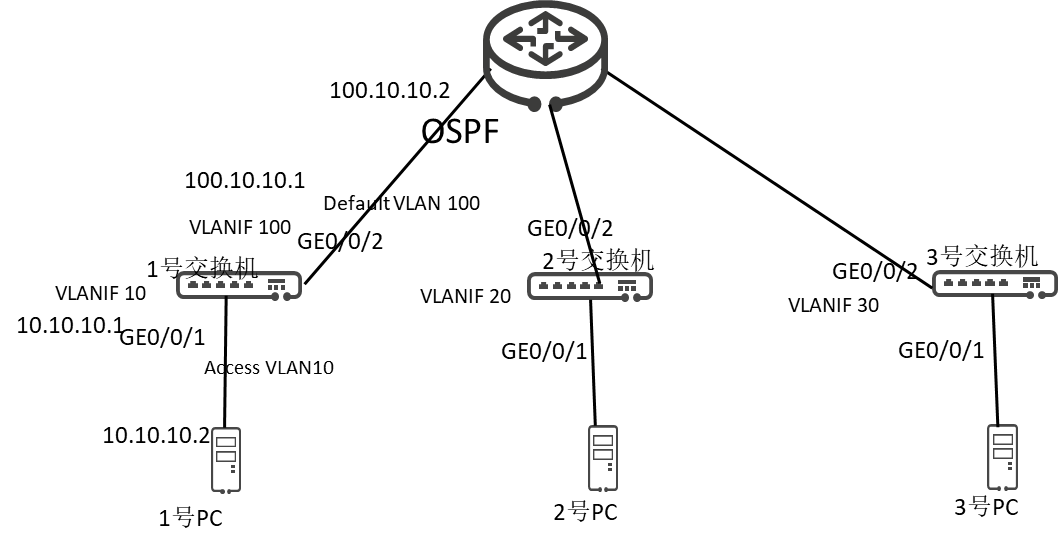
以1号同学为例：

1. PC机地址配置为10.10.10.2，对应的接入交换机VLANIF接口地址配置为10.10.10.1；
2. 交换机至AR间接口地址配置为 100.100.10.1, AR 接口地址配置为100.100.10.2

### 实验任务

1. 配置交换机与PC机间的接口IP地址
2. 配置交换机与AR间的接口IP地址

### 实验组网



### 操作步骤

# 配置Switch 1，交换机需要通过VLANIF 配置IP地址

#与PC连接的端口，首先设置二层

[Switch\_1] vlan batch 10 100

[Switch\_1] interface gigabitethernet 0/0/1

[Switch\_1-GigabitEthernet0/0/1] port link-type access

[Switch\_1-GigabitEthernet0/0/1] port default vlan 10

[Switch\_1-GigabitEthernet0/0/1] quit

#对应的VLAN上启用三层

[Switch\_1] interface vlanif 10

[Switch\_1-Vlanif10] ip address 10.10.10.1 24

[Switch\_1-Vlanif10] quit

#与路由器连接的端口，首先设置二层

[Switch\_1] interface gigabitethernet 0/0/2

[Switch\_1-GigabitEthernet0/0/2] port link-type access

[Switch\_1-GigabitEthernet0/0/2] port default vlan 100

[Switch\_1-GigabitEthernet0/0/2] quit

#对应的VLAN上启用三层

[Switch\_1] interface vlanif 100

[Switch\_1-Vlanif10] ip address 100.10.10.1 24

[Switch\_1-Vlanif10] quit

# 配置AR路由器，路由器可以直接在物理口配置IP地址

[AR\_1] interface gigabitethernet 0/0/0

[AR\_1-GigabitEthernet0/0/0] **undo portswitch** //与AR 型号相关，本实验使用AR下行接口缺省是二层口，需要转换为3层口。

[AR\_1-GigabitEthernet0/0/0] ip address 100.10.10.2 24

其它交换机/AR根据分配的IP地址/VLAN做配置，配置类似，这里不做具体描述

### 实验验证

1. PC机能够ping 通 10.10.10.1
2. 交换机上 能够ping 通 100.10.10.2

## DHCP 配置

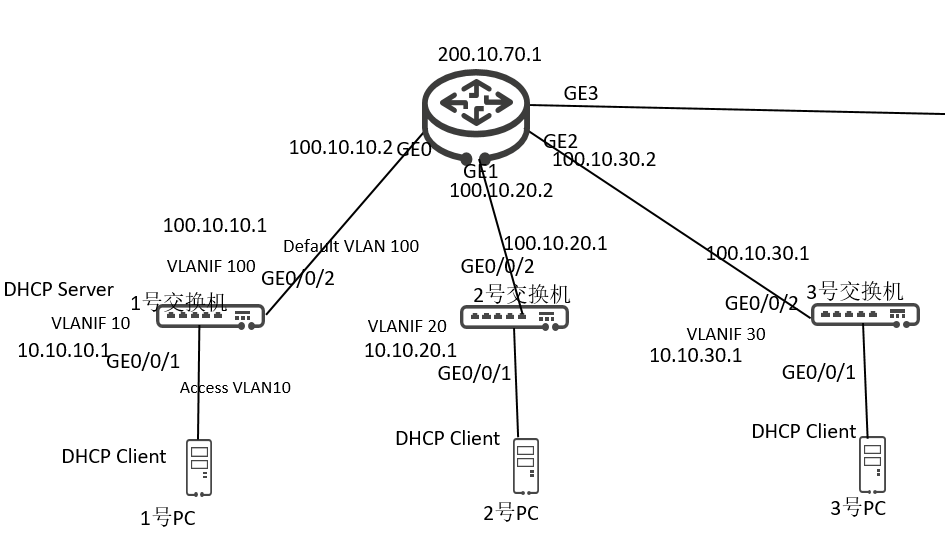
### 说明

PC机可以通过DHCP 获取IP地址，便于部署，现网一般采用此种方式进行IP地址分配管理。现网通常使用专用DHCP server 管理IP地址，本实验采用在交换机上部署DHCP server方式。

### 实验任务

1. 配置交换机启用DHCP server
2. PC机抓取DHCP 报文，观察交互流程

### 实验组网



### 操作步骤

1. 使能DHCP Server.

[Switch\_1] dhcp enable

1. 配置DHCP 地址池相关信息

在3.3.2 已经配置了接口IP地址，在此配置基础上增加地址池配置：

[Switch\_1] interface vlanif 10

#选择接口网段作为IP地址池网段

[Switch\_1-Vlanif10] dhcp select interface

#可选，设置DHCP分配的网关地址。

[Switch\_1-Vlanif10] dhcp server gateway-list 10.10.10.1 //不配置时会自动选择该接口的ip 地址作为网关地址。ensp不支持该命令

#设置DHCP分配的DNS服务器地址。

[Switch\_1-Vlanif10] dhcp server dns-list 114.114.114.114 //可尝试修改dns server地址，抓包/PC机ipconfig 可见.

其它交换机配置类似，这里不做具体描述

### 实验验证

1. 查看DHCP 地址池信息

[Switch\_1]display ip pool interface vlanif10

Pool-name : Vlanif10

Pool-No : 0

Lease : 1 Days 0 Hours 0 Minutes

Domain-name : example.com

DNS-server0 : 114.114.114.114

NBNS-server0 : -

Netbios-type : -

Position : Interface

Status : Unlocked

Gateway-0 : 10.10.10.1

Network : 10.10.10.0

Mask : 255.255.255.0

VPN instance : --

Logging : Disable

Conflicted address recycle interval: -

Address Statistic: Total :253 Used :1

Idle :252 Expired :0

Conflict :0 Disabled :0

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

Network section

Start End Total Used Idle(Expired) Conflict Disabled

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

10.10.10.1 10.10.10.254 253 1 252(0) 0 0

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

1. PC机上抓包查看DHCP 报文交互流程，查看DHCP 报文中分配的IP地址，网关地址，DNS地址
2. PC机上查看分配到的IP地址，网关地址，DNS地址等

## 静态路由配置

### 说明

静态路由在不同网络环境中有不同的目的：

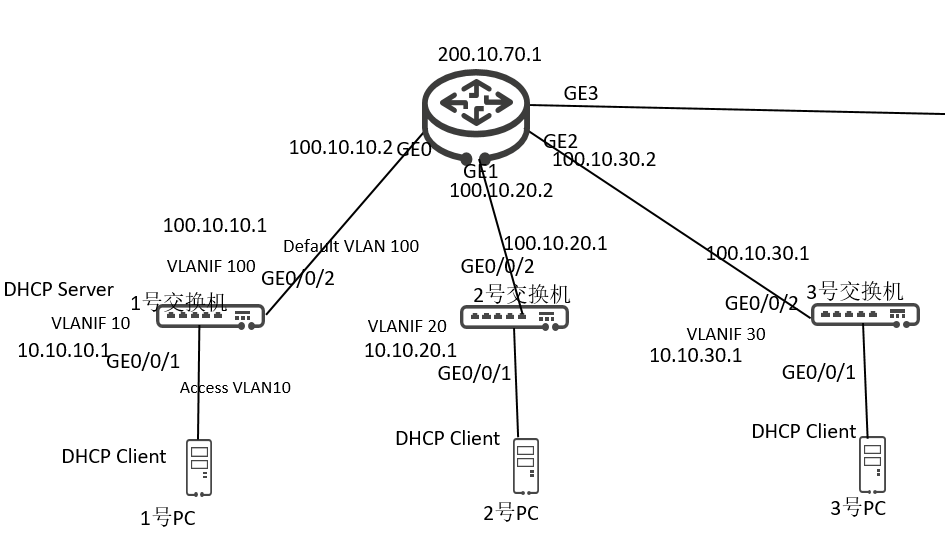
1. 当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。
2. 在复杂网络环境中，配置静态路由可以改进网络的性能，并可为重要的应用保证带宽。

在现网中，经常采用静态路由方式配置缺省路由。

### 实验任务

在AR 路由器上配置200.10.70.1 这个地址，这个地址不通过路由协议发布。通过配置静态路由方式，PC机能够ping通此IP地址。

### 实验组网



### 操作步骤

交换机上相关IP配置沿用4.3 配置.

1. AR 路由器增加一个IP地址 200.10.70.1

#使用loopback接口来承载IP地址

[AR\_1]interface loopback 0

[AR\_1\_Loopbak0] ip address 200.10.70.1 255.255.255.255

#PC-》200.10.70.1 icmp request 路由过程

1. PC机通过缺省网关知道至200.10.70.1 路由，不需要增加配置
2. 交换机上配置至AR路由器200.10.70.1的路由。

#配置 200.10.70.1 的静态路由。注意三个参数 IP地址 + 掩码 + 下一跳地址

[Switch\_1] ip route-static 200.10.70.1 255.255.255.255 100.10.10.2

#AR路由器-》10.10.10.254 PC机的 icmp reply 路由过程

1. AR路由器 配置至 10.10.10.0网段的静态路由

[AR\_1] ip route-static 10.10.10.0 255.255.255.0 100.10.10.1

1. 交换机 至 10.10.10.0网段，通过直连路由知道从VLANIF10转发

其它交换机/AR 根据分配的IP地址，配置类似，这里不做具体描述

### 实验验证

1. PC机能够ping 通 200.10.70.1
2. 理解静态路由配置中，下一跳地址的作用。例如在本实验中，交换机配置的下一跳地址为何是100.10.10.2 而不是100.10.10.1？

## OSPF 配置

### 说明

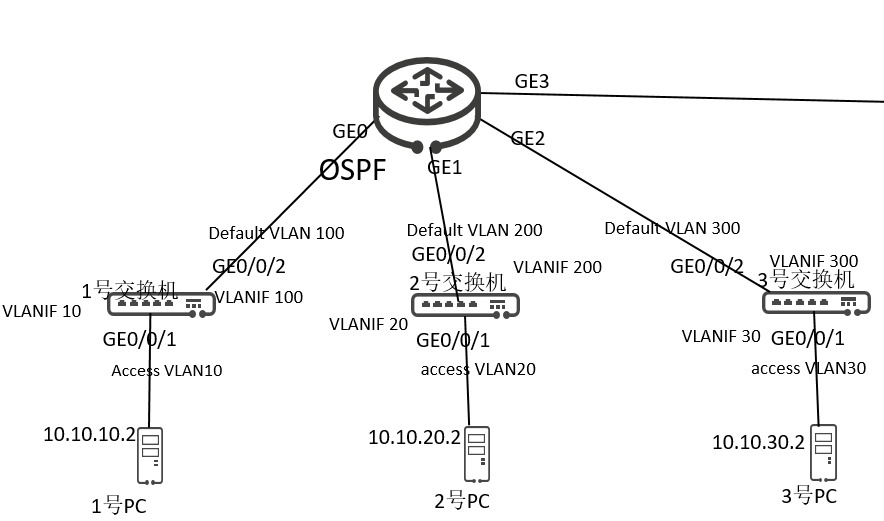
OSPF 是园区网络中应用最广泛的路由协议。

### 实验任务

AR 与 3台交换机启用OSPF路由协议。

3台PC机能够互通ping通

### 实验组网



### 操作步骤

1. 交换机上启用OSPF并发布路由

#配置ospf router-id ，作为OSPF 路由器标识。

[Switch\_1]interface loopback 0

[Switch\_1\_Loopbak0] ip address 200.10.10.1 255.255.255.255

[Switch\_1] ospf 1 router-id 200.10.10.1 //2号交换机用 200.10.20.1

#本实验仅部署area 0

[Switch\_1-ospf-1] area 0

#与路由器间接口上使能OSPF，并把这个网段路由发布出去

[Switch\_1-ospf-1-area-0.0.0.0] network 100.10.10.0 0.0.0.255

# 至PC机网段，可以有两种方式：

1. 用import direct 路由方式发布出去。这是引入外部路由方式

[Switch\_1-ospf-1-area-0.0.0.0] quit

[Switch\_1-ospf-1]import-route direct

1. 用network 方式发布出去，不推荐

[Switch\_1-ospf-1-area-0.0.0.0] network 10.10.10.0 0.0.0.255

1. AR1上启用OSPF

#配置ospf router-id ，作为OSPF 路由器标识。

[AR\_1]interface loopback 0

[AR\_1\_Loopbak0] ip address 200.10.70.1 255.255.255.255

[AR\_1] ospf 1 router-id 200.10.70.1

#OSPF 设置network 的接口

[AR\_1-ospf-1] area 0

[AR\_1-ospf-1-area-0.0.0.0] network 100.10.10.0 0.0.0.255 //To switch1

[AR\_1-ospf-1-area-0.0.0.0] network 100.10.20.0 0.0.0.255 //To switch2

[AR\_1-ospf-1-area-0.0.0.0] network 100.10.30.0 0.0.0.255 //To switch3

[AR\_1-ospf-1-area-0.0.0.0] quit

其它的交换机/AR根据分配的IP地址，做配置类似，这里不做具体描述

### 实验验证

1. 查看OSPF是否建立

<Switch\_1> display ospf peer

1. 查看各设备上路由

<Switch\_1> display ospf routing

<Switch\_1> display ip routing

1. PC机能够互相ping通

## BGP 配置(高阶)

### 说明

同一岛内2个小组OSPF 配置完成后，可以在2个AR路由器间配置BGP协议发布路由。

### 实验任务

1. 验证BGP协议
2. 两个组内的PC机能够相互ping通

### 实验组网



### 操作步骤

1. 配置 AR间接口IP地址

[AR\_1] interface gigabitethernet 0/0/3

[AR\_1-GigabitEthernet0/0/0] ip address 150.10.70.1 24

[AR\_2] interface gigabitethernet 0/0/3

[AR\_2-GigabitEthernet0/0/0] ip address 150.10.70.2 24

1. AR1 BGP 配置

#标识自己

[AR\_1] bgp 65107 // 自治系统号

[AR\_1-bgp] router-id 200.10.70.1

#找到对方路由器

[AR\_1-bgp] peer 150.10.70.2 as-number 65108 //对端IP地址，对端自治系统号

#引入路由，对外发布。路由协议可以引入多种其他的路由协议，比如static静态路由，direct直连路由,ospf路由等。可以根据现网应用情况选择。

[AR\_1-bgp] ipv4-family unicast

[AR\_1-bgp-af-ipv4] import-route direct //引入直连路由

[AR\_1-bgp-af-ipv4] import-route ospf 1 //引入OSPF路由

[AR\_1-bgp] quit

1. AR1 OSPF 引入BGP 路由

[AR\_1] ospf

[AR\_1-ospf-1] import-route bgp

1. AR2 配置

[AR\_2] bgp 65108

[AR\_2-bgp] router-id 200.10.70.2

[AR\_2-bgp] peer 150.10.70.1 as-number 65107

[AR\_2-bgp] ipv4-family unicast

[AR\_2-bgp-af-ipv4] import-route direct //引入直连路由

[AR\_2-bgp-af-ipv4] import-route ospf 1 //引入OSPF路由

[AR\_2-bgp] quit

1. AR2 配置

[AR\_2] ospf

[AR\_2-ospf-1] import-route bgp

### 实验验证

1. 查看各设备路由情况

display ip routing-table

1. PC间ping情况

## NAT

### 说明

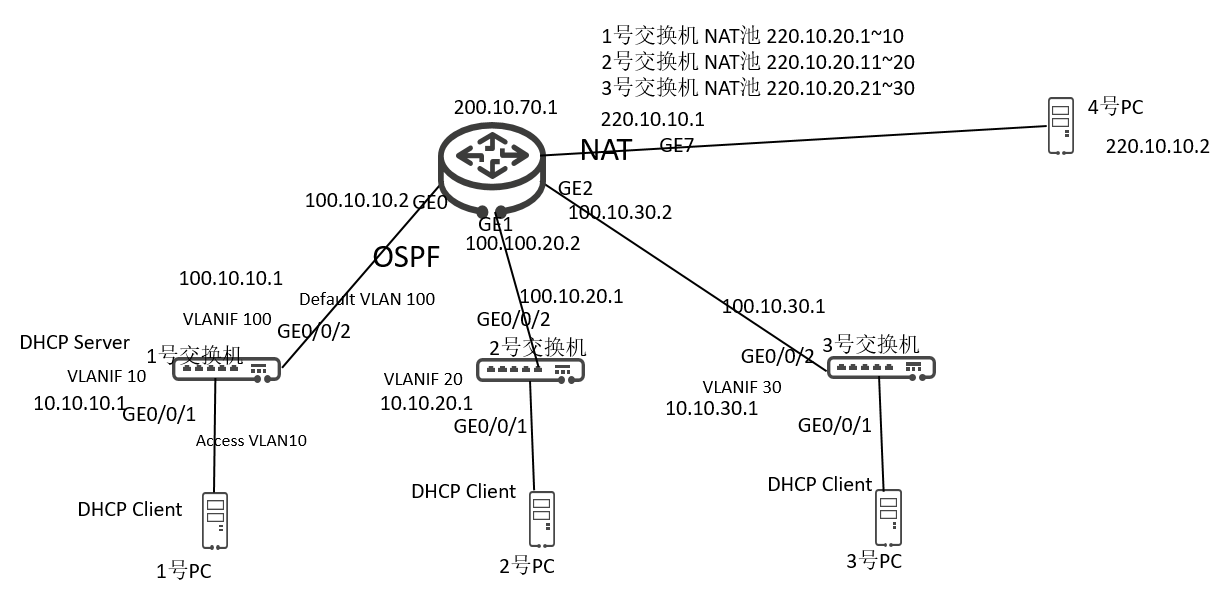
随着Internet的发展和网络应用的增多，IPv4地址枯竭已成为制约网络发展的瓶颈。当内网的主机要访问外网时，通过NAT技术可以将其私网地址转换为公网地址，可以实现多个私网用户共用一个公网地址来访问外部网络，这样既可保证网络互通，又节省了公网地址。

### 实验任务

1. AR 上 3台交换机使用不同的NAT地址池
2. 1/2/3 号PC 使用内网 地址，ping 220.10.10.2 地址
3. 在4号PC上抓包，查看ping 报文源地址。

### 实验组网

岛内3位同学一组，AR WAN侧端口与4号PC机相连，4号PC机模拟广域网。



### 操作步骤

1. 配置AR 与4号PC间接口地址，PC机需要静态配置地址，并设置网关

[AR\_1] interface gigabitethernet 0/0/7

[AR\_1-GigabitEthernet0/0/7] undo portswitch

[AR\_1-GigabitEthernet0/0/7] ip address 220.10.10.1 24

1. 配置NAT

#设置NAT转换的地址池(公网)

[AR\_1] nat address-group 1 220.10.20.1 220.10.20.2 //1号交换机下挂所有PC机的地址池

#通过设置规则，将1号PC 的packets 匹配到NAT转换的出口上

#访问控制列表

[AR\_1] acl 2001

[AR\_1-acl-basic-2001] rule 5 permit source 10.10.10.0 0.0.0.255

[AR\_1-acl-basic-2001] quit

[AR\_1] interface gigabitethernet 0/0/7

[AR\_1-GigabitEthernet0/0/7] nat outbound 2001 address-group 1

[AR\_1-GigabitEthernet0/0/7] quit

[AR\_1] nat address-group 2 220.10.20.11 220.10.20.20 //2号交换机下挂所有PC机的地址池

[AR\_1] acl 2002

[AR\_1-acl-basic-2002] rule 5 permit source 10.10.20.0 0.0.0.255

[AR\_1-acl-basic-2002] quit

[AR\_1] interface gigabitethernet 0/0/7

[AR\_1-GigabitEthernet0/0/7] nat outbound 2002 address-group 2

[AR\_1-GigabitEthernet0/0/7] quit

[AR\_1] nat address-group 3 220.10.20.21 220.10.20.30 //3号交换机地址池

[AR\_1] acl 2003

[AR\_1-acl-basic-2003] rule 5 permit source 10.10.30.0 0.0.0.255

[AR\_1-acl-basic-2001] quit

[AR\_1] interface gigabitethernet 0/0/7

[AR\_1-GigabitEthernet0/0/7] nat outbound 2003 address-group 3

[AR\_1-GigabitEthernet0/0/7] quit

### 实验验证

1. 验证pc 机是否可以ping 通 220.10.10.2。

4号PC上抓包，观察从1/2/3 号PC上过来的icmp报文源地址是否符合预期

1. display nat session all，查看 私网、公网 的mapping关系，例如

[AR4-GigabitEthernet0/0/1]disp nat session all

NAT Session Table Information:

Protocol : ICMP(1)

SrcAddr Vpn : 10.10.10.254

DestAddr Vpn : 200.10.40.2

Type Code IcmpId : 0 8 41931

NAT-Info

New SrcAddr : 210.1.1.5

New DestAddr : ----

New IcmpId : 10243

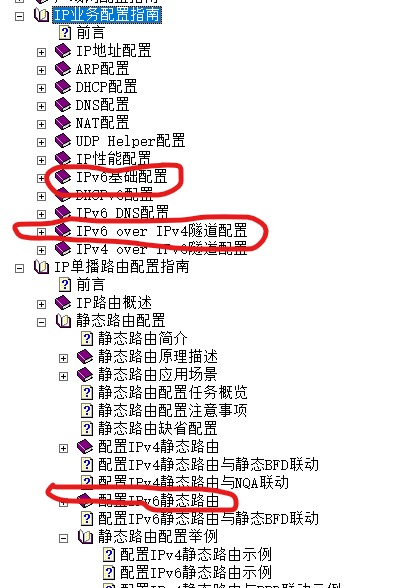
# 实验任务4： IPv6与路由

## 实验介绍

### 关于本实验

本实验重点帮助同学理解IPv6地址以及转发，以及IPv4/IPv6过渡技术；IPv6 路由协议与IPv4模型很相似，本实验不再重点配置，有兴趣的同学可以参考相关配置手册自行验证。

实验参考相应的产品文档，本实验可参考章节如下：



### 实验目的

掌握IPv6地址

掌握IPv6基础路由转发

掌握IPv4/IPv6过渡隧道技术

## IPv6地址配置

### 说明

以1号同学为例：

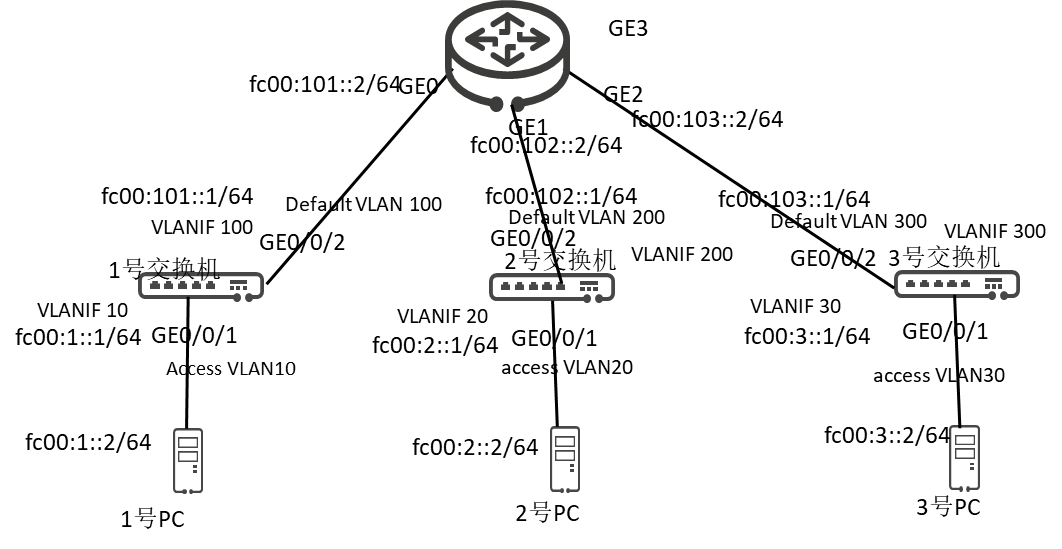
1. PC机地址配置为fc00:1::2/64，对应的接入交换机VLANIF接口地址配置为fc00:1::1/64；
2. 交换机至AR间接口地址配置为 fc00:101::1/64, AR 接口地址配置为fc00:101::2/64

#### 实验任务

1. 配置交换机与PC机间的接口IPv6地址
2. 配置交换机与AR间的接口IPv6地址

### 实验组网

交换机、路由器 都支持IPv4/IPv6 双栈部署，本实验组网可以继续沿用IPv4组网。



### 操作步骤

# 配置Switch 1。

[Switch\_1] ipv6 //整机使能ipv6

[Switch\_1] interface vlanif 10

[Switch\_1-Vlanif10] ipv6 enable //接口使能ipv6

[Switch\_1-Vlanif10] ipv6 address fc00:1::1/64

[Switch\_1-Vlanif10] quit

[Switch\_1] interface vlanif 100

[Switch\_1-Vlanif10] ipv6 enable //接口使能ipv6

[Switch\_1-Vlanif10] ipv6 address fc00:101::1/64

[Switch\_1-Vlanif10] quit

其它的交换机配置类似，这里不做具体描述

# 配置AR1

[AR\_1] ipv6 //整机使能ipv6

[AR\_1] interface gigabitethernet 0/0/0

[AR\_1-GigabitEthernet0/0/0] undo portswitch

[AR\_1-GigabitEthernet0/0/0] ipv6 enable

[AR\_1-GigabitEthernet0/0/0] ipv6 address fc00:101::2/64

AR其它接口配置类似，这里不做具体描述

### 实验验证

1. PC机能够ping通 fc00:101::1
2. 交换机上 能够ping ipv6通 fc00:101::2

## IPv6静态路由

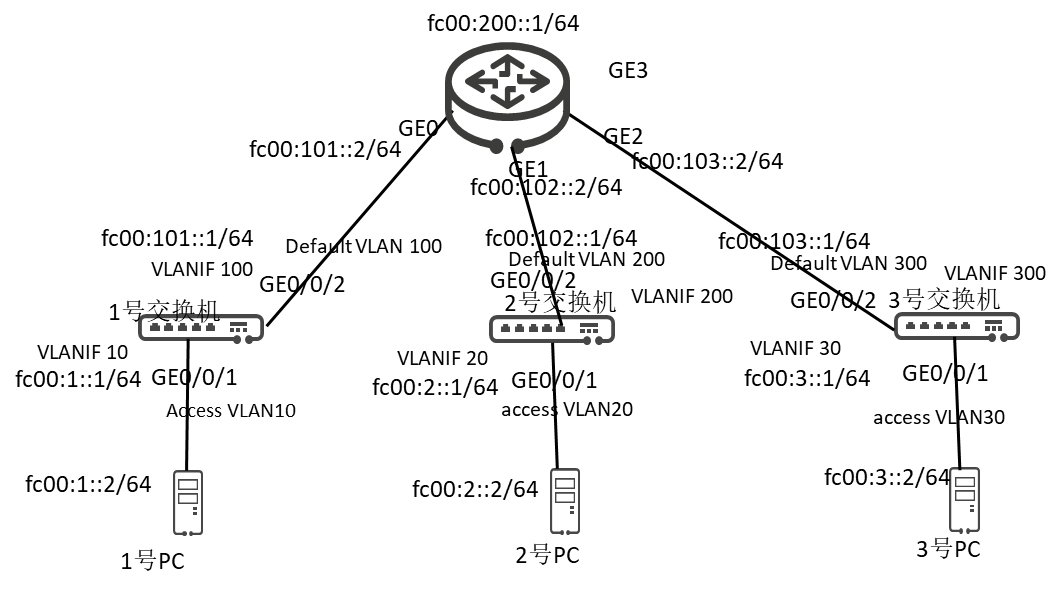
### 说明

IPv6 静态路由与IPv4 静态路由模型很类似，参考配置即可。

### 实验任务

在AR 路由器上配置fc00:200::1/64 这个地址，这个地址不通过路由协议发布。通过配置静态路由方式，PC机能够ping通此地址。

### 实验组网



### 操作步骤

交换机上相关IP配置沿用5.2 配置.

1. AR 路由器增加一个IP地址 fc00:200::1/64

[AR\_1]interface loopback 0

[AR\_1\_Loopbak0] ipv6 enable

[AR\_1\_Loopbak0] ipv6 address fc00:200::1/64

1. 交换机上配置 fc00:200::1 的静态路由

[Switch\_1] ipv6 route-static fc00:200::1 64 vlanif100 fc00:101::2

1. AR路由器上配置至 fc00:1::1/64网段的静态路由

[AR\_1] ipv6 route-static fc00:1::1 64 gigabitethernet 0/0/0 fc00:101::1

### 实验验证

1. PC机能够ping 通 fc00:200::1

## IPv4/IPv6过渡(高阶)

### 说明

由于IPv4地址的枯竭和IPv6的先进性，IPv4过渡为IPv6势在必行。因为IPv6与IPv4的不兼容性，所以需要对原有的IPv4设备进行替换。但是如果贸然将IPv4设备大量替换所需成本会非常巨大，且现网运行的业务也会中断，显然并不可行。所以，IPv4向IPv6过渡是一个渐进的过程。

在过渡初期，IPv4网络已经大量部署，而IPv6网络只是散落在各地的“孤岛”，IPv6 over IPv4隧道就是通过隧道技术，使IPv6报文在IPv4网络中传输，实现IPv6网络之间的孤岛互连。

IPv6 过渡技术有多种，本实验验证IPv6 over IPv4隧道技术中的手工隧道技术

### 实验任务

完成岛内两组IPv6组网间的IPv6 over IPv4隧道。

### 实验组网

岛内两组AR间启用IPv6 over IPv4隧道。



### 操作步骤

交换机上相关IP配置沿用5.3 配置.AR间接口地址参见4.6

1. AR1 路由器增加Ipv6 隧道

# 配置协议类型为IPv6-IPv4。

[AR\_1] interface tunnel 0/0/1

[AR\_1-Tunnel0/0/1] tunnel-protocol ipv6-ipv4

# 配置隧道接口的IPv6地址、源接口、目的地址。

[AR\_1-Tunnel0/0/1] ipv6 enable

[AR\_1-Tunnel0/0/1] ipv6 address fc00:220::1/64

[AR\_1-Tunnel0/0/1] source gigabitethernet 0/0/3

[AR\_1-Tunnel0/0/1] destination 150.10.70.2

[AR\_1-Tunnel0/0/1] quit

1. AR1 路由器配置 路由入IPv6 隧道

[AR\_1] ipv6 route-static fc00:4::64 tunnel0/0/1

[AR\_1] ipv6 route-static fc00:5::64 tunnel0/0/1

[AR\_1] ipv6 route-static fc00:6::64 tunnel0/0/1

1. AR2 路由器增加Ipv6 隧道, 入隧道路由

类似配置，这里不做描述

1. 交换机1上配置 fc00:200::1 的静态路由

[Switch\_1] ipv6 route-static fc00:200::1 64 vlanif100 fc00:101::2

[Switch\_1] ipv6 route-static fc00:4::1 64 vlanif100 fc00:101::2

[Switch\_1] ipv6 route-static fc00:5::1 64 vlanif100 fc00:101::2

[Switch\_1] ipv6 route-static fc00:6::1 64 vlanif100 fc00:101::2

### 实验验证

1. Switch1 上能ping通 4交换机 fc00:4::1 地址，命令为ping ipv6 fc00:4::1
2. PC机1能够ping 通 fc00:4::2 地址

# 实验任务5：VPN(高阶)

## 实验介绍

### 关于本实验

同一个机构若存在多个分支，如学校多校区，企业多分支，需要网络互通，从经济性考虑，一般会租用运营商网络。从安全意义上考虑，要在运营商网络中保密隔离，此时通常使用VPN技术。

目前有两种比较常用的VPN技术，一种是IPSecVPN，另一种是BGP/MPLS VPN。IPSec VPN的运营主体一般是机构的网管，而MPLS VPN的运营主体一般是运营商。

实验参考相应的产品文档，本实验可参考章节如下：



### 实验目的

掌握IPsec VPN原理和配置。

掌握BGP/MPLS VPN的原理和配置

## IPSec VPN配置(高阶)

### 说明

IPSec VPN提供安全加密并且穿透运营商网络，其特点是经济但可靠性低于MPLS VPN。

IPSec VPN 有两种主要的部署方式：

* + 1. 中小型分支网络，各分支通过IPSec VPN与公司内网连接。例如办事处接入总部内网
    2. 个人通过IPSec VPN拨号软件接入 公司内网，例如疫情下的远程办公

本实验中只验证第一种部署方式。

### 实验任务

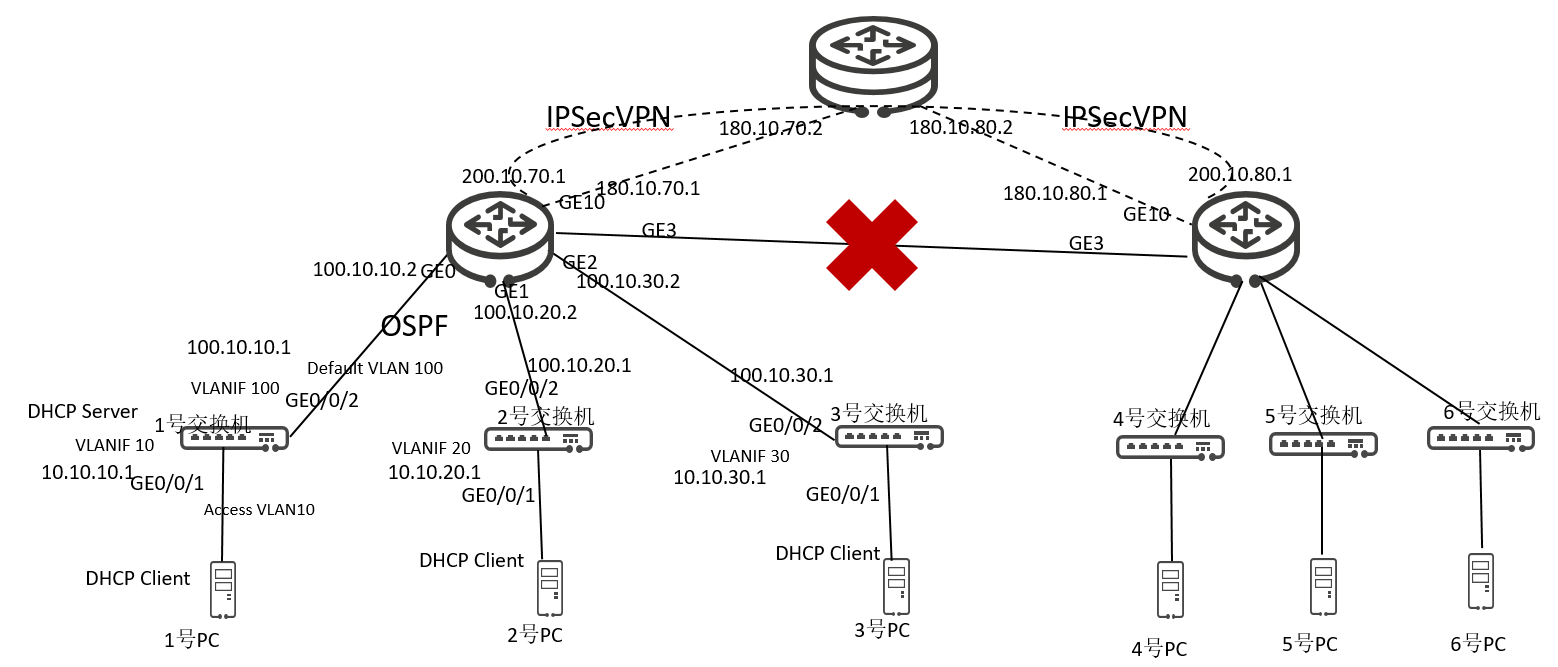
1. 岛内两小组AR路由器与互相建立IPSecVPN

核心路由器 接口地址、路由器配置已经完成，各组不需要参与。

1. 各PC 间能够互通
2. 从转发原理中理解IPSec VPN 的配置模型

### 实验组网

1. 岛内3位同学一组，AR 路由器做Spoke 节点与核心路由器建立 IPSecVPN.
2. 去掉 3.3.6 BGP用例中的 GE3的连线



### 操作步骤

配置实例中仅列出了AR1相关配置，AR2相关配置类似

1. 配置AR1 与广域路由器接口地址

[AR\_1] interface gigabitethernet 0/0/10

[AR\_1-GigabitEthernet0/0/10]ip address 180.10.70.1 24

1. 配置静态路由，下一跳路由器接口地址是 180.10.70.2

[AR\_1] ip route-static 10.10.0.0 255.255.0.0 180.10.70.2

[AR\_1] ip route-static 180.10.80.0 255.255.0.0 180.10.70.2

1. 配置ACL，定义由组1子网去 其它子网数据流。

[AR\_1] acl number 3101

[AR\_1-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 10.0.0.0 0.255.255.255

[AR\_1-acl-adv-3101] quit

1. 配置IPSec安全提议。

[AR\_1] ipsec proposal tran1

[AR\_1-ipsec-proposal-tran1] esp authentication-algorithm sha2-256

[AR\_1-ipsec-proposal-tran1] esp encryption-algorithm aes-128

[AR\_1-ipsec-proposal-tran1] quit

分别在RouterA和RouterB上创建安全策略

1. 配置配置手工方式安全策略。

[AR\_1] ipsec policy map1 10 manual

[AR\_1-ipsec-policy-manual-map1-10] security acl 3101

[AR\_1-ipsec-policy-manual-map1-10] proposal tran1

[AR\_1-ipsec-policy-manual-map1-10] tunnel remote 180.10.80.1

[AR\_1-ipsec-policy-manual-map1-10] tunnel local 180.10.70.1

[AR\_1-ipsec-policy-manual-map1-10] sa spi outbound esp 12345

[AR\_1-ipsec-policy-manual-map1-10] sa spi inbound esp 54321

[AR\_1-ipsec-policy-manual-map1-10] sa string-key outbound esp cipher huawei

[AR\_1-ipsec-policy-manual-map1-10] sa string-key inbound esp cipher huawei

[AR\_1-ipsec-policy-manual-map1-10] quit

1. 在AR\_1的接口上引用安全策略组。

[AR\_1] interface gigabitethernet 1/0/0

[AR\_1-GigabitEthernet1/0/0] ipsec policy map1

[AR\_1-GigabitEthernet1/0/0] quit

### 实验验证

1. 验证IPSecVPN 是否建立成功。

display ipsec sa

1. 验证两个小组间PC机能够互通。

## BGP/MPLS VPN(高阶+)

### 说明

MPLS VPN 是运营商给机构分支提供专线业务，可靠性很高的同时费用也很高，一般应用于银行、大型企业等。

MPLS VPN 有两种主要的部署方式：

* + 1. L2 VPN部署。此方式要求机构网管有比较强的管理能力，其特点是可以二层互通，适用于特定的场景。
    2. L3 VPN 部署。此部署方式需要机构网管与运营商共同管理路由，BGP/MPLS VPN是目前比较主流的部署方式。

本实验中只验证第二种部署方式。

### 实验任务

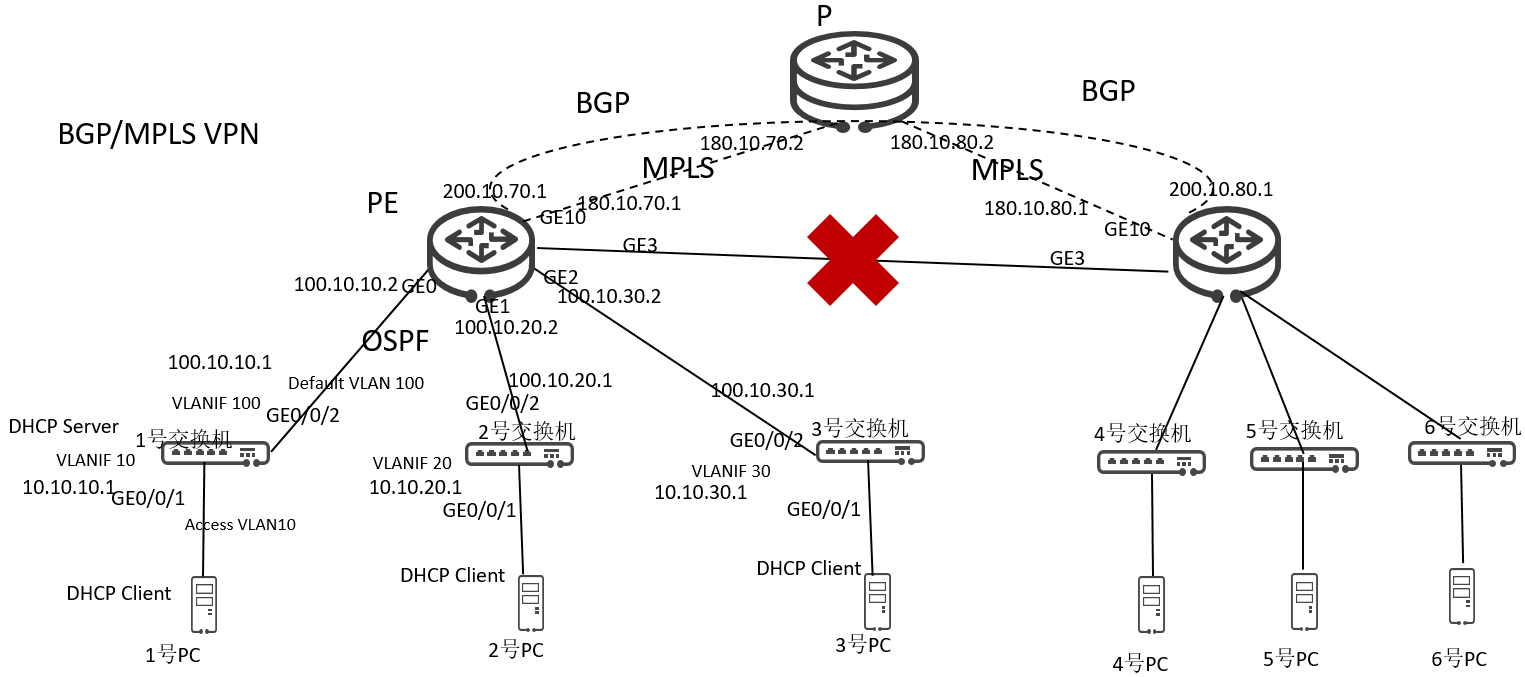
1. 岛内两小组AR路由器作为PE设备，核心路由器作为P设备，建立BGP/MPLS VPN。

核心路由器 接口地址、路由器配置已经完成，各组不需要参与。

1. 岛内交换机作为CE设备，与PE间发布内网路由
2. 两组PC 能够互通
3. 从转发原理中理解BGP/MPLS VPN 的模型

### 实验组网

1. 岛内3位同学一组，AR 路由器做PE节点，与交换机间接口启用VPN.
2. 去掉 3.3.6 BGP用例中的 GE3的连线
3. 核心路由器做P设备，与AR路由器间启用MPLS



### 操作步骤

配置实例中仅列出了AR1相关配置，AR2相关配置类似。P设备统一提前配置好

1. 配置AR1 与核心路由器接口地址

[AR\_1] interface gigabitethernet 0/0/10

[AR\_1-GigabitEthernet0/0/10]ip address 180.10.70.1 24

1. AR1 与核心路由器间OSPF发布路由

[AR\_1] ospf 1

[AR\_1-ospf-1] area 0

[AR\_1-ospf-1-area-0.0.0.0] network 180.10.70.0 0.0.0.255

[AR\_1-ospf-1-area-0.0.0.0] quit

[AR\_1-ospf-1] quit

1. AR1与核心路由器间启用mpls ldp

[AR\_1] mpls lsr-id 200.10.70.1

[AR\_1] mpls

[AR\_1] mpls ldp

[AR\_1] interface gigabitethernet 0/0/10

[AR\_1-GigabitEthernet0/0/10]mpls

[AR\_1-GigabitEthernet0/0/10]mpls ldp

此时 查看ldp session 能够看到已经建立

[AR\_1] display mpls ldp session

1. 在AR1设备上配置VPN实例，将CE接入PE

[AR\_1] ip vpn-instance vpna

[AR\_1-vpn-instance-vpna] ipv4-family

[AR\_1-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1 //AR2需差异配置 200:1

[AR\_1-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both

[AR\_1-vpn-instance-vpna-af-ipv4] quit

[AR\_1-vpn-instance-vpna] quit

[AR\_1] interface gigabitethernet 0/0/0 //GE1/GE2 也加入vpna

[AR\_1-GigabitEthernet0/0/0] ip binding vpn-instance vpna

[AR\_1-GigabitEthernet0/0/0] ip address 100.10.10.2 24

[AR\_1-GigabitEthernet0/0/0] quit

此时 查看vpn情况， 能够看到已经创建

[AR\_1] display ip vpn-instance verbose

1. AR1 与交换机间OSPF发布路由

[AR\_1] ospf 2 vpn-instance vpna

[AR\_1-ospf-1] area 0

[AR\_1-ospf-1-area-0.0.0.0] network 100.10.10.0 0.0.0.255

[AR\_1-ospf-1-area-0.0.0.0]import-route bgp //引入BGP路由

[AR\_1-ospf-1-area-0.0.0.0] quit

[AR\_1-ospf-1] quit

1. AR1、AR2之间建立MP-IBGP对等体关系。

[AR\_1] bgp 100

[AR\_1-bgp] peer 200.10.80.1 as-number 100

[AR\_1-bgp] peer 200.10.80.1 connect-interface loopback 0

[AR\_1-bgp] ipv4-family vpnv4

[AR\_1-bgp-af-vpnv4] peer 200.10.80.1 enable

[AR\_1-bgp-af-vpnv4] quit

[AR\_1-bgp] quit

此时 查看bgp情况， 能够看到已经创建

[AR\_1] display bgp vpnv4 vpn-instance vpna peer

1. VPN 引入CE路由。

[AR\_1] bgp 100

[AR\_1-bgp] ipv4-family vpn-instance vpna

[AR\_1-bgp-vpna] peer 10.1.1.1 as-number 65410

[AR\_1-bgp-vpna] import-route ospf 2

[AR\_1-bgp-vpna] quit

此时 查看vpn 路由器情况， 能够看到路由已经发布

[AR\_1] display ip routing-table vpn-instance vpna

### 实验验证

1. 验证BGP/MPLS VPN是否建立成功。
2. 验证两个小组间PC机能够互通。

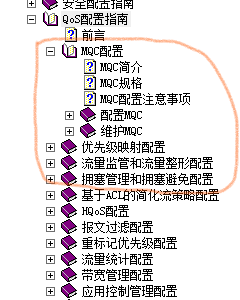
# 实验任务6：Qos配置

## 实验介绍

### 关于本实验

服务质量QoS（Quality of Service）用于评估服务方满足客户服务需求的能力。通过配置QoS，对企业的网络流量进行调控，避免并管理网络拥塞，减少报文的丢失率，同时也可以为企业用户提供专用带宽或者为不同的业务（语音、视频、数据等）提供差分服务。

实验参考相应的产品文档，本实验可参考章节如下：



### 实验目的

掌握MQC原理和配置方法

掌握流量监管原理和配置方法。

## MQC原理和配置方法

### 说明

模块化QoS命令行MQC（Modular QoS Command-Line Interface）是指通过将具有某类共同特征的报文划分为一类，并为同一类报文提供相同的服务，也可以对不同类的报文提供不同的服务。

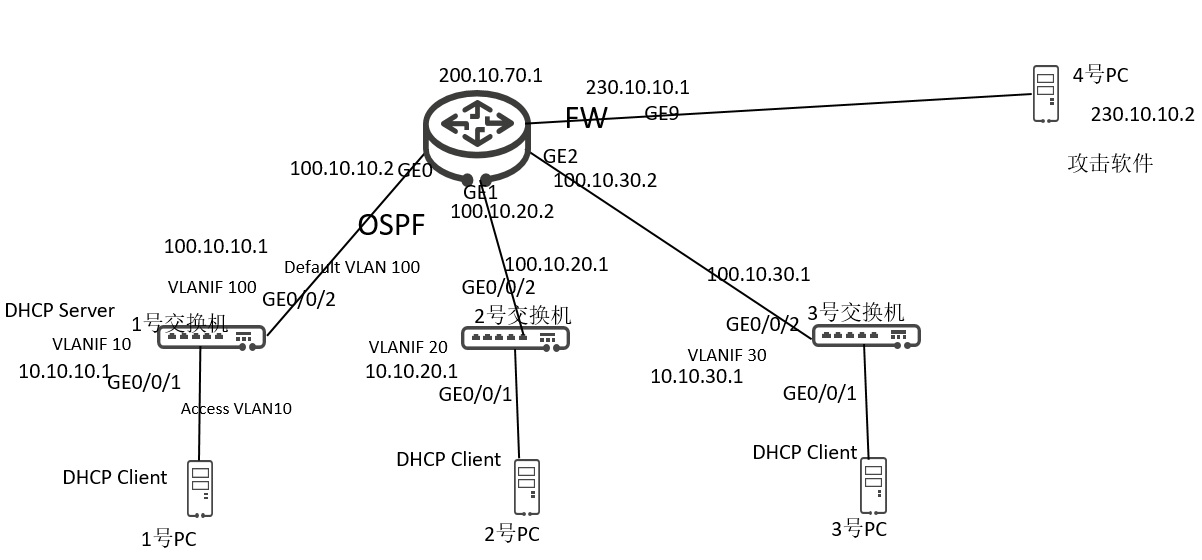
随着网络中QoS业务的不断丰富，在网络规划时若要实现对不同流量（如不同业务或不同用户）的差分服务，会使部署比较复杂。MQC的出现，使用户能对网络中的流量进行精细化处理，用户可以更加便捷的针对自己的需求对网络中的流量提供不同的服务，完善了网络的服务能力。

MQC包含三个要素：流分类（traffic classifier）、流行为（traffic behavior）和流策略（traffic policy）。

### 实验任务

使用MQC，统计各位同学的报文发送个数。

### 实验组网



### 操作步骤

物理实验室环境在交换机、路由器上都可以完成此功能。

eNSP仿真只能在路由器上完成该功能，并且**路由器需要选择AR2240**.

本实验配置以物理环境上１号交换机配置举例。其它环境配置类似：

1. 创建流分类
   1. 配置匹配PC1 的ACL，假设PC1 地址为10.10.10.253

[Switch\_1] acl 3001

[Switch\_1-acl- adv-3001] rule permit ip source 10.10.10.253 0

* 1. 创建流分类

# 创建流分类c\_pc1，匹配acl 3001，目的地址是pc2的报文。

[Switch\_1] traffic classifier c\_pc1

[Switch\_1-classifier-c\_pc1] if-match acl 3001

[Switch\_1-classifier-c\_pc1] quit

1. 配置流行为：

# 创建流行为b\_pc2，动作为statistic，即统计匹配指定规则的报文。

[Switch\_1] traffic behavior b\_statis

[Switch\_1-behavior-b\_statis] statistic enable

[Switch\_1-behavior-b\_statis] quit

1. 配置流策略

# 创建流策略p\_pc1\_statis，绑定流分类c\_pc1和流行为b\_statis。

[Switch\_1] traffic policy p\_pc1\_statis

[Switch\_1-trafficpolicy-p\_pc1­\_statis] classifier c\_pc1 behavior b\_statis

[Switch\_1-trafficpolicy-p\_pc1\_statis] quit

1. 应用流策略

# 在接口GE0/0/1的入方向应用流策略p1。

[Switch\_1] interface gigabitethernet 0/0/1

[Switch\_1-GigabitEthernet0/0/1] traffic-policy p\_pc1\_statis inbound

[Switch\_1-GigabitEthernet0/0/1] quit

### 实验验证

1. PC间ping 报文时，查看统计计数

disp traffic policy statistics interface GigabitEthernet 0/0/1 inbound

Interface: GigabitEthernet0/0/1

Traffic policy inbound: pc1-statis

Rule number: 1

Current status: OK!

Item Sum(Packets/Bytes) Rate(pps/bps)

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

Matched 10/ 1/

980 184

+--Passed 10/ 1/

980 184

+--Dropped 0/ 0/

0 0

+--Filter 0/ 0/

0 0

+--CAR 0/ 0/

0 0

+--Queue Matched 0/ 0/

0 0

+--Enqueued 0/ 0/

0 0

+--Discarded 0/ 0/

0 0

+--Car 0/ 0/

## 流量监管和流量整形

### 说明

流量监管和流量整形通过监督进入网络的流量速率，用来限制流量及其资源的使用，保证更好的为用户提供服务。

如果报文的发送速率大于接收速率，或者下游设备的接口速率小于上游设备的接口速率，就会引起网络拥塞。如果不限制用户发送的业务流量，大量用户不断突发的业务数据会使网络更加拥挤。为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，必须对用户的业务流量加以限制。

流量监管和流量整形就是一种通过对流量规格的监督，来限制流量及其资源使用的流控策略。

1） 流量监管

流量监管TP（Traffic Policing）就是对流量进行控制，通过监督进入网络的流量速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，从而保护网络资源和用户的利益。

2） 流量整形

流量整形TS（Traffic Shaping）是一种主动调整流量输出速率的措施。当下游设备的入接口速率小于上游设备的出接口速率或发生突发流量时，下游设备入接口处可能出现流量拥塞的情况，此时用户可以通过在上游设备的接口出方向配置流量整形，将上游不规整的流量进行削峰填谷，输出一条比较平整的流量，从而解决下游设备的拥塞问题。

流量整形与流量监管的主要区别在于，流量整形对原本要被丢弃的报文进行缓存，当令牌桶有足够的令牌时，再均匀的向外发送这些被缓存的报文。流量整形与流量监管的另一区别是，整形可能会增加延迟，而监管几乎不引入额外的延迟。

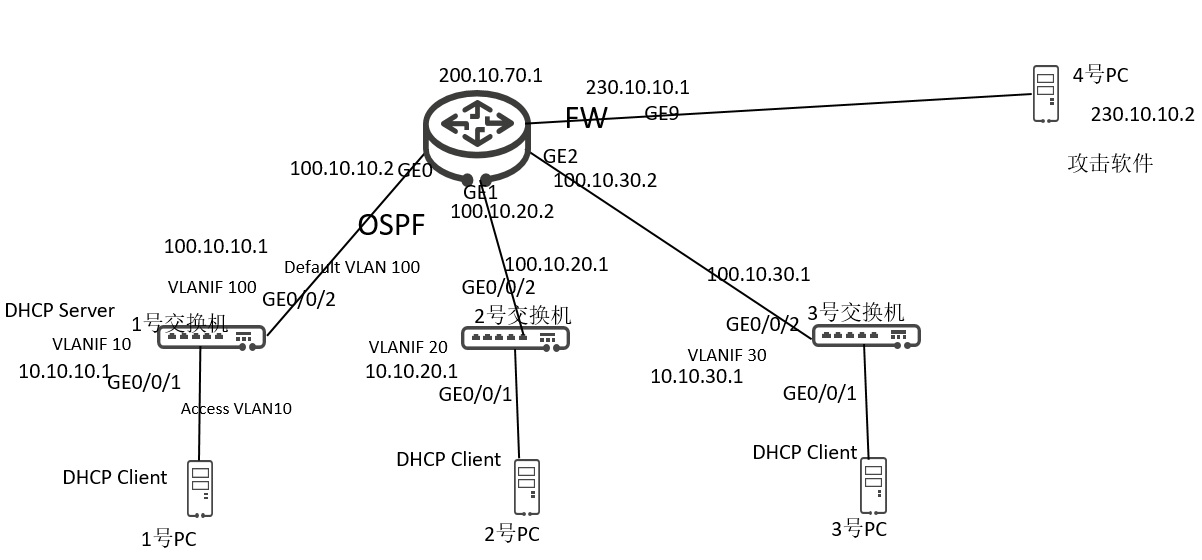
本实验只实现流量监管

### 实验任务

调整每台PC 允许的最大带宽，观察流量限制情况

### 实验组网

岛内3位同学一组，AR WAN侧GE8端口与4号PC机相连，4号PC机模拟外网的网络攻击。



物理环境组网

### 操作步骤

物理实验室环境在交换机、路由器上都可以完成此功能。

eNSP仿真交换机不支持，只能在路由器上完成该功能，并且**路由器需要选择AR2240**.

本实验配置以物理环境上１号交换机配置举例。其它环境配置类似：

1. 创建流分类，匹配PC机发送的流量
2. 配置匹配PC1 的ACL，假设PC1 地址为10.10.10.253

[Switch\_1] acl 3001

[Switch\_1-acl- adv-3001] rule permit ip source 10.10.10.253 0

1. 创建流分类

# 创建流分类c\_pc1，匹配acl 3001，目的地址是pc2的报文。

[Switch\_1] traffic classifier c\_pc1

[Switch\_1-classifier-c\_pc1] if-match acl 3001

[Switch\_1-classifier-c\_pc1] quit

1. 配置流行为：

# 创建流行为b\_car，动作为限速，即超过一定带宽报文会被丢弃。

[Switch\_1] traffic behavior b\_car

[Switch\_1-behavior-b\_statis] car cir 8 // 配置cir速率为8k

[Switch\_1-behavior-b\_statis] statistic enable //可选，配置后可以查看统计信息

[Switch\_1-behavior-b\_statis] quit

1. 配置流策略

# 创建流策略p\_pc1\_car，绑定流分类c\_pc1和流行为b\_car。

[Switch\_1] traffic policy p\_pc1\_car

[Switch\_1-trafficpolicy-p\_pc1­\_statis] classifier c\_pc1 behavior b\_car

[Switch\_1-trafficpolicy-p\_pc1\_statis] quit

1. 应用流策略

# 在接口GE0/0/1的入方向应用流策略p1。

[Switch\_1] interface gigabitethernet 0/0/1

[Switch\_1-GigabitEthernet0/0/1] traffic-policy p\_pc1\_car inbound

[Switch\_1-GigabitEthernet0/0/1] quit

### 实验验证

1. PC1 ping PC2，icmp 报文长度设置为1400。调整流行为car 的值，观察是否会出现限速情况
2. 若behavior 下使能过statistic，则可以查看流策略的命中信息

<Switch\_1>disp traffic policy statistics interface g 0/0/1 inbound

Interface: GigabitEthernet0/0/1

Traffic policy inbound: p\_pc1\_car

Rule number: 2

Current status: OK!

Item Sum(Packets/Bytes) Rate(pps/bps)

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

Matched 2,203/ 1/

3,223,190 7,912

+--Passed 1,056/ 1/

1,517,496 4,216

+--Dropped 1,147/ 1/

1,705,694 3,688

+--Filter 0/ 0/

0 0

+--CAR 1,147/ 1/

1,705,694 3,688

+--Queue Matched 0/ 0/

0 0

+--Enqueued 0/ 0/

0 0

+--Discarded 0/ 0/

0 0

+--Car 2,203/ 1/

3,223,190 7,912

+--Green packets 1,056/ 1/

1,517,496 4,216

+--Yellow packets 0/ 0/

0 0

+--Red packets 1,147/ 1/

1,705,694 3,688

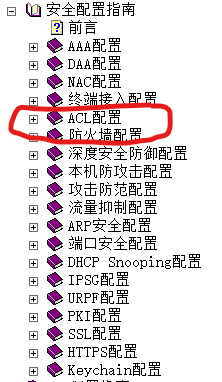
# 实验任务7：IP安全配置

## 实验介绍

### 关于本实验

安全涉及领域范围很广，本实验选择其中两个点做实验：ACL 访问控制和防火墙功能

实验参考相应的产品文档，本实验可参考章节如下：



### 实验目的

掌握ACL 原理和配置方法

掌握防火墙原理和配置方法

本实验暂不做深度安全防御如IPS、URL过滤等，有兴趣同学可以自行实验。

## ACL配置

### 基于IP地址ACL配置

#### 说明

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。

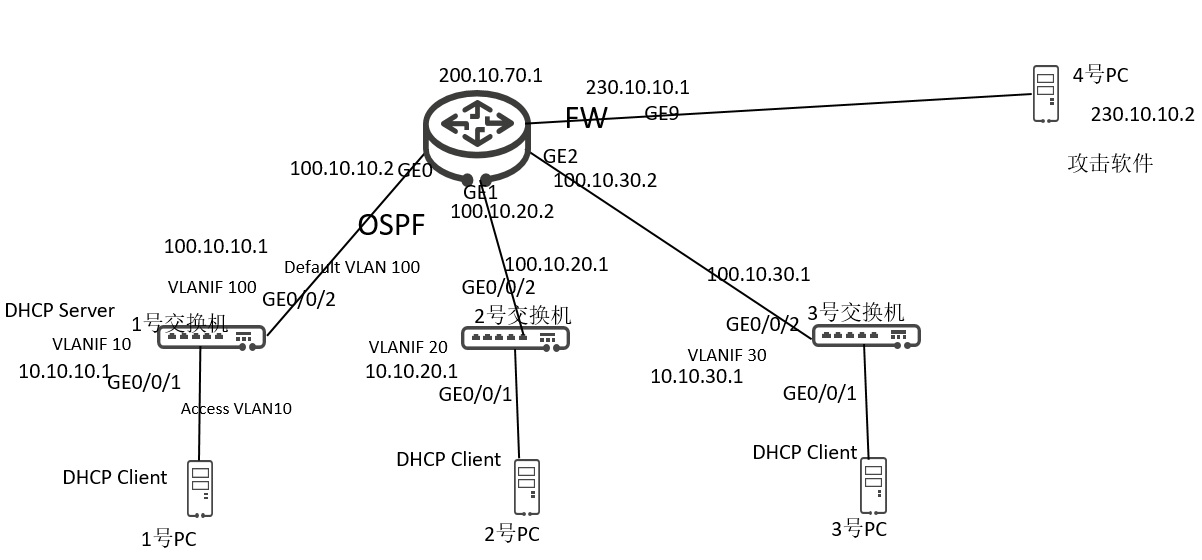
ACL本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用ACL的业务模块的处理策略来允许或阻止该报文通过。

#### 实验任务

在4.5 OSPF路由学习完全的基础上，基于ACL的流量过滤功能：

1. 1号PC 能访问10.10.20.1，不能访问　2号PC
2. 2号PC 能访问 10.10.30.1，不能访问 3号PC
3. 3号PC 能访问 10.10.10.1，不能访问 1号PC

#### 实验组网



#### 操作步骤

以１号交换机配置举例，假设查询２号PC地址为10.10.20.1，：

1. 配置禁止访问目的地址　10.10.20.1　的规则

[Switch\_1] acl 3001

[Switch\_1-acl- adv-3001] rule permit ip destination 10.10.20.1 0

1. 创建流策略

配置流分类 ：

# 创建流分类c\_pc2，匹配acl 3001，目的地址是pc2的报文。

[Switch\_1] traffic classifier c\_pc2

[Switch\_1-classifier-c\_pc2] if-match acl 3001

[Switch\_1-classifier-c\_pc2] quit

配置流行为：

# 创建流行为b\_pc2，动作为deny，即丢弃匹配指定规则的报文。

[Switch\_1] traffic behavior b\_pc2

[Switch\_1-behavior-b\_pc2] deny

[Switch\_1-behavior-b\_pc2] quit

配置流策略

# 创建流策略p\_pc2，绑定流分类c\_pc2和流行为b\_pc2。

[Switch\_1] traffic policy p\_pc2

[Switch\_1-trafficpolicy-p\_pc2] classifier c\_pc2 behavior b\_pc2

[Switch\_1-trafficpolicy-p\_pc2] quit

应用流策略

# 在接口GE0/0/1的入方向应用流策略p1。

[Switch\_1] interface gigabitethernet 0/0/1

[Switch\_1-GigabitEthernet0/0/1] traffic-policy p\_pc2 inbound

[Switch\_1-GigabitEthernet0/0/1] quit

#### 实验验证

1. 验证PC间是否能够ping 通
2. 验证 10.10.20.1 是否能够ping 通

## 防火墙配置(高阶)

### 内外网隔离

#### 说明

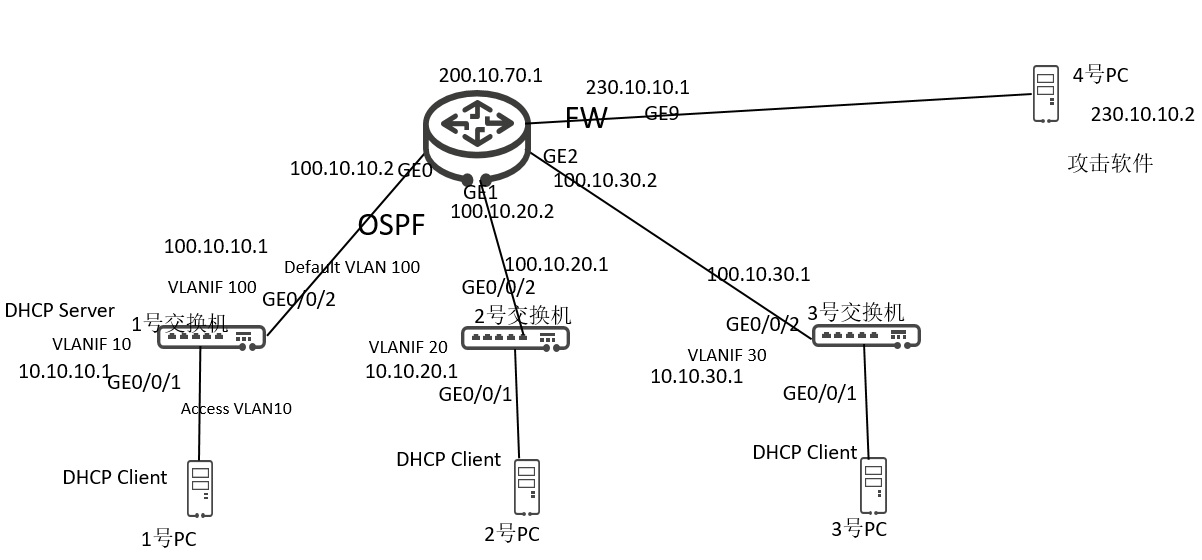
防火墙（Firewall）是一种隔离技术，使内网和外网分开，可以防止外部网络用户以非法手段通过外部网络进入内部网络，保护内网免受外部非法用户的侵入。

#### 实验任务

配置防火墙业务，防范外网对内网环境的攻击

#### 实验组网

岛内3位同学一组，AR WAN侧GE8端口与4号PC机相连，4号PC机模拟外网的网络攻击。



#### 操作步骤

1. 配置AR 与4号PC间接口地址

[AR\_1] interface gigabitethernet 0/0/9

[AR\_1-GigabitEthernet0/0/9] ip address 230.10.10.1 24

PC机配置IP地址 230.10.10.2，网关230.10.10.1

1. 配置安全区域和安全域间。

[AR\_1] firewall zone trust

[AR\_1-zone-trust] priority 14

[AR\_1-zone-trust] quit

[AR\_1] firewall zone untrust

[AR\_1-zone-untrust] priority 1

[AR\_1-zone-untrust] quit

[AR\_1] firewall interzone trust untrust

[AR\_1-interzone-trust-untrust] firewall enable

[AR\_1-interzone-trust-untrust] quit

1. 配置安全区域和安全域间。

[Huawei] interface gigabitethernet 0/0/0 // 1号交换机区域

[Huawei-GigabitEthernet0/0/0] zone trust

[Huawei-GigabitEthernet0/0/0] quit

[Huawei] interface gigabitethernet 0/0/1 // 2号交换机区域

[Huawei-GigabitEthernet0/0/1] zone trust

[Huawei-GigabitEthernet0/0/1] quit

[Huawei] interface gigabitethernet 0/0/2 // 3号交换机区域

[Huawei-GigabitEthernet0/0/2] zone trust

[Huawei-GigabitEthernet0/0/2] quit

[Huawei] interface gigabitethernet 0/0/9 // 外网非信任区域

[Huawei-GigabitEthernet0/0/9] zone untrust

[Huawei-GigabitEthernet0/0/9] quit

#### 实验验证

1. 1~3 号PC能够访问 4号PC，4号PC无法访问 1~3号PC
2. 4号PC 攻击软件 攻击 1号PC
3. FW 能够防范4号PC的攻击，在1号PC 抓包未发现攻击报文。

### 攻击防范

#### 说明

攻击防范是防火墙中一种重要的网络安全功能。它可以检测出多种类型的网络攻击行为，并能够采取相应的措施保护内部网络免受恶意攻击，以保证内部网络及系统的正常运行。

#### 实验任务

配置防火墙攻击防范，防范拒绝服务型攻击、扫描窥探攻击和畸形报文攻击等各种外网攻击

#### 实验组网

岛内3位同学一组，AR WAN侧GE8端口与4号PC机相连，4号PC机模拟外网的网络攻击。

相关FW配置沿用 7.3.1 配置

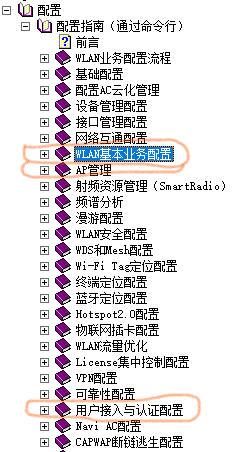
# 实验任务8：WLAN配置

## 实验介绍

### 关于本实验

本实验完成AP接入AC，终端接入至WLAN网络。

实验参考相应的产品文档，本实验参考无线接入控制器(AC和FIT AP) V200R021C00 产品文档，可参考章节如下：



### 实验目的

掌握WLAN组网模型和配置方法

掌握AP接入AC配置方法

掌握终端安全接入配置方案

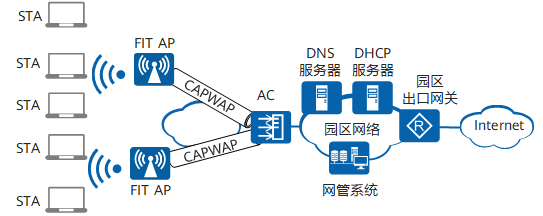
## WLAN网络架构&AP接入网络

### WLAN网络架构

#### 说明

WLAN网络架构分有线侧和无线侧两部分，有线侧是指AP上行到Internet的网络使用以太网协议。无线侧是指STA到AP之间的网络使用802.11协议。无线侧接入的WLAN网络架构为集中式架构。

集中式架构又分为瘦接入点（FIT AP）架构和敏捷分布Wi-Fi方案架构。本实验只介绍FIT AP接入方式。



所有无线接入功能由AP和AC共同完成：

•AC集中处理所有的安全、控制和管理功能，例如移动管理、身份验证、VLAN划分、射频资源管理和数据包转发等。

•FIT AP完成无线射频接入功能，例如无线信号发射与探测响应、数据加密解密、数据传输确认等。

•AP和AC之间采用CAPWAP协议进行通讯，AP与AC间可以跨越二层网络或三层网络。

用户接入无线网络的过程分两步：

1.FIT AP与AC建立CAPWAP隧道，详细内容请参见AP接入网络过程。

2.STA与FIT AP的关联过程，详细内容请参见STA接入过程。

### AP接入网络

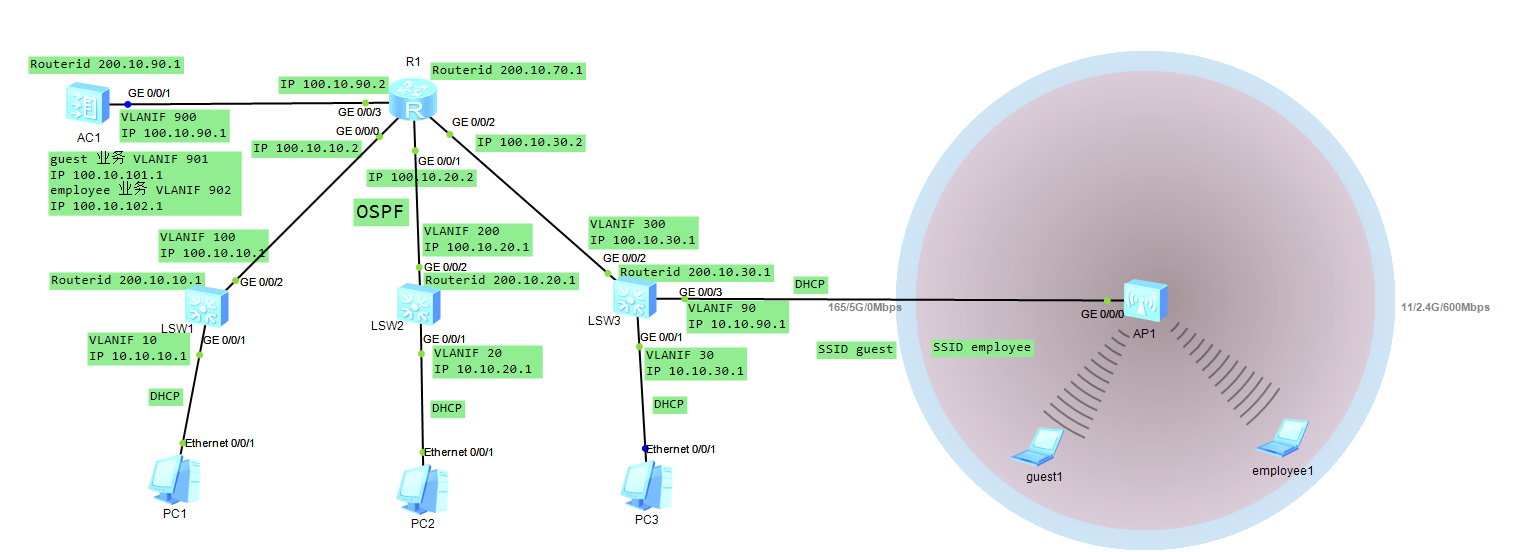
#### 说明

本实验完成FIT AP 接入网络过程

#### 实验任务

AP 通过CAPWAP隧道接入AC：

#### 实验组网



#### 操作步骤

以１号交换机配置举例，假设查询２号PC地址为10.10.20.1：

1. 配置AC 接入至网络中

#配置AC 与AR1 间接口地址。

AC 与交换机类似，需要采用VLANIF配置三层接口

#配置AC 与AR1 间启用OSPF

AC 与交换机类似

1. 配置AP 接入至网络中

以AP 接在LSW3，LSW3 作为L3交换机为例：

# LSW3 配置AP接入的VLANIF 接口

# LSW3 配置DHCP 服务，为AP分配IP地址，并告知AP接入AC的地址

#

interface Vlanif90

ip address 10.10.90.1 255.255.255.0

dhcp select interface

dhcp server option 43 sub-option 2 ip-address **100.10.90.1** //通过DHCP option告知AP 接入AC的地址

#

1. 配置AP上线

#配置capwap 隧道,允许AP与其建立capwap隧道

[AC]capwap source interface vlanif 200

#配置AP 接入控制策略

[AC] wlan //系统试图下进入WLAN 视图

[AC-wlan-view] ap auth-mode mac-auth // AC上对AP接入认证，缺省使用AP mac进行认证

#找到AP mac地址，配置允许接入的AP白名单

查看ap 上线失败，会发现接入失败的AP信息

[AC6605-wlan-view]disp ap online-fail-record all

Info: This operation may take a few seconds. Please wait for a moment.done.

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

MAC Last fail time Reason

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

**00e0-fcb1-1a80** 2022-04-29/08:43:15 Not in MAC whitelist

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

配置允许该AP接入到网络中

[AC6605-wlan-view]ap-mac 00e0-fcb1-1a80

#### 实验验证

1. AP 能够接入至AC中

<AC6605>disp ap all

Info: This operation may take a few seconds. Please wait for a moment.done.

Total AP information:

nor : normal [1]

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

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

ID MAC Name Group IP Type State ST

A Uptime

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

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

0 00e0-fcb1-1a80 00e0-fcb1-1a80 default 10.10.90.254 AP4030TN nor 0

11M:32S

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

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

Total: 1

## 终端接入网络

### 终端接入网络

#### 说明

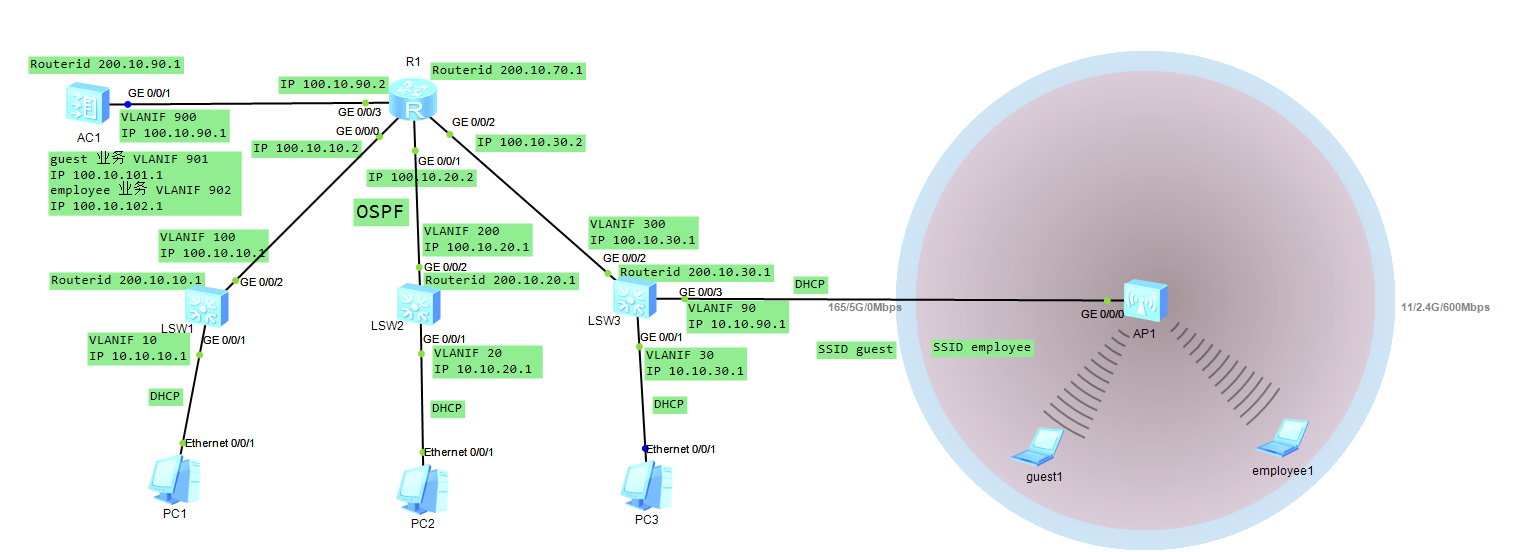
网络中会部署多个SSID，提供不同服务。同时为了保证接入安全，需要配置不同的安全策略。

#### 实验任务

部署2个SSID，分别为访客、员工提供业务。举例中以配置WPA2+PSK+AES的安全策略为例，密码分别为“a1234567”和“b1234567”，实际配置中请根据实际情况，配置符合实际要求的安全策略。

#### 实验组网

岛内3位同学一组，AR WAN侧GE8端口与4号PC机相连，4号PC机模拟外网的网络攻击。



#### 操作步骤

1. 创建SSID模板

# 创建名为“guest”和“employee”的SSID模板，并分别配置SSID名称为“guest”和“employee”。

[AC-wlan-view] ssid-profile name guest

[AC-wlan-ssid-prof-guest] ssid guest

[AC-wlan-ssid-prof-guest] quit

[AC-wlan-view] ssid-profile name employee

[AC-wlan-ssid-prof-employee] ssid employee

[AC-wlan-ssid-prof-employee] quit

1. 创建安全策略

#配置WPA2+PSK+AES的安全策略

[AC-wlan-view] security-profile name guest

[AC-wlan-sec-prof-guest] security wpa2 psk pass-phrase a1234567 aes

[AC-wlan-sec-prof-guest] quit

[AC-wlan-view] security-profile name employee

[AC-wlan-sec-prof-employee] security wpa2 psk pass-phrase b1234567 aes

[AC-wlan-sec-prof-employee] quit

1. 创建VAP模板

# 创建名为“guest”和“employee”的VAP模板，配置业务数据转发模式、业务VLAN，并且引用安全模板和SSID模板

[AC-wlan-view] vap-profile name guest

[AC-wlan-vap-prof-guest] forward-mode tunnel

[AC-wlan-vap-prof-guest] service-vlan vlan-id 901 //guest 业务VLAN 901,从guest SSID上线的用户，数据报文会加上这个VLAN，通过capwap隧道到达AC。AC侧需要能够处理此VLAN

[AC-wlan-vap-prof-guest] security-profile guest

[AC-wlan-vap-prof-guest] ssid-profile guest

[AC-wlan-vap-prof-guest] quit

[AC-wlan-view] vap-profile name employee

[AC-wlan-vap-prof-employee] forward-mode tunnel

[AC-wlan-vap-prof-employee] service-vlan vlan-id 902 // employee业务VLAN 902

[AC-wlan-vap-prof-employee] security-profile employee

[AC-wlan-vap-prof-employee] ssid-profile employee

[AC-wlan-vap-prof-employee] quit

#AC 上配置业务VLAN

[AC6605]vlan batch 901 902

#创建vlanif 901/902 接口。需要注意，GE0/0/1接口同时绑定多个VLAN，需要变更link-type 为Trunk

interface GigabitEthernet0/0/1

port link-type trunk

port trunk pvid vlan 900

port trunk allow-pass vlan 900 to 902

#

#guest ssid接入用户的vlan

interface Vlanif901

ip address 100.10.101.1 255.255.255.0

dhcp select interface

# employee ssid接入用户的vlan

interface Vlanif902

ip address 100.10.102.1 255.255.255.0

dhcp select interface

#

1. AP引用VAP模板

# 配置AP组引用VAP模板，AP上所有射频使用VAP模板的配置。

[AC-wlan-view] ap-group name default

[AC-wlan-ap-group-default] vap-profile guest wlan 1 radio all

[AC-wlan-ap-group-default] vap-profile employee wlan 2 radio all

[AC-wlan-ap-group-default] quit

#### 实验验证

1. Guset1 PC 、employee1 PC 都能上线

<AC6605>display station all

Rf/WLAN: Radio ID/WLAN ID

Rx/Tx: link receive rate/link transmit rate(Mbps)

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

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

STA MAC AP ID Ap name Rf/WLAN Band Type Rx/Tx RSSI VLAN

IP address SSID

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

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

5489-989f-20b4 0 00e0-fcb1-1a80 0/2 2.4G - -/- - 902

100.10.102.214 employee

5489-98e0-6ff9 0 00e0-fcb1-1a80 0/1 2.4G - -/- - 901

100.10.101.178 guest

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

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

Total: 2 2.4G: 2 5G: 0

1. Guest1 PC能够访问 1号PC
2. Guset1 PC 能够访问 employee1 PC

# 综合实验：校园园区网搭建（高阶+）

## 实验介绍

### 关于本实验

使用已经学习到的网络技术，组合构建一张校园园区网络。

### 实验目的

综合运用网络技术，实践网络工程能力

## 校园园区网搭建

### 实验介绍

#### 说明

模拟搭建东大校园网，网络包括九龙湖校区和四牌楼校区。校区内园区网络包括宿舍区、教学区，出口区域包括Internet区域、WAN区域(校区间互通，暂不模拟)、教育网(IPv6,暂不模拟)，DC区域(暂不模拟)。

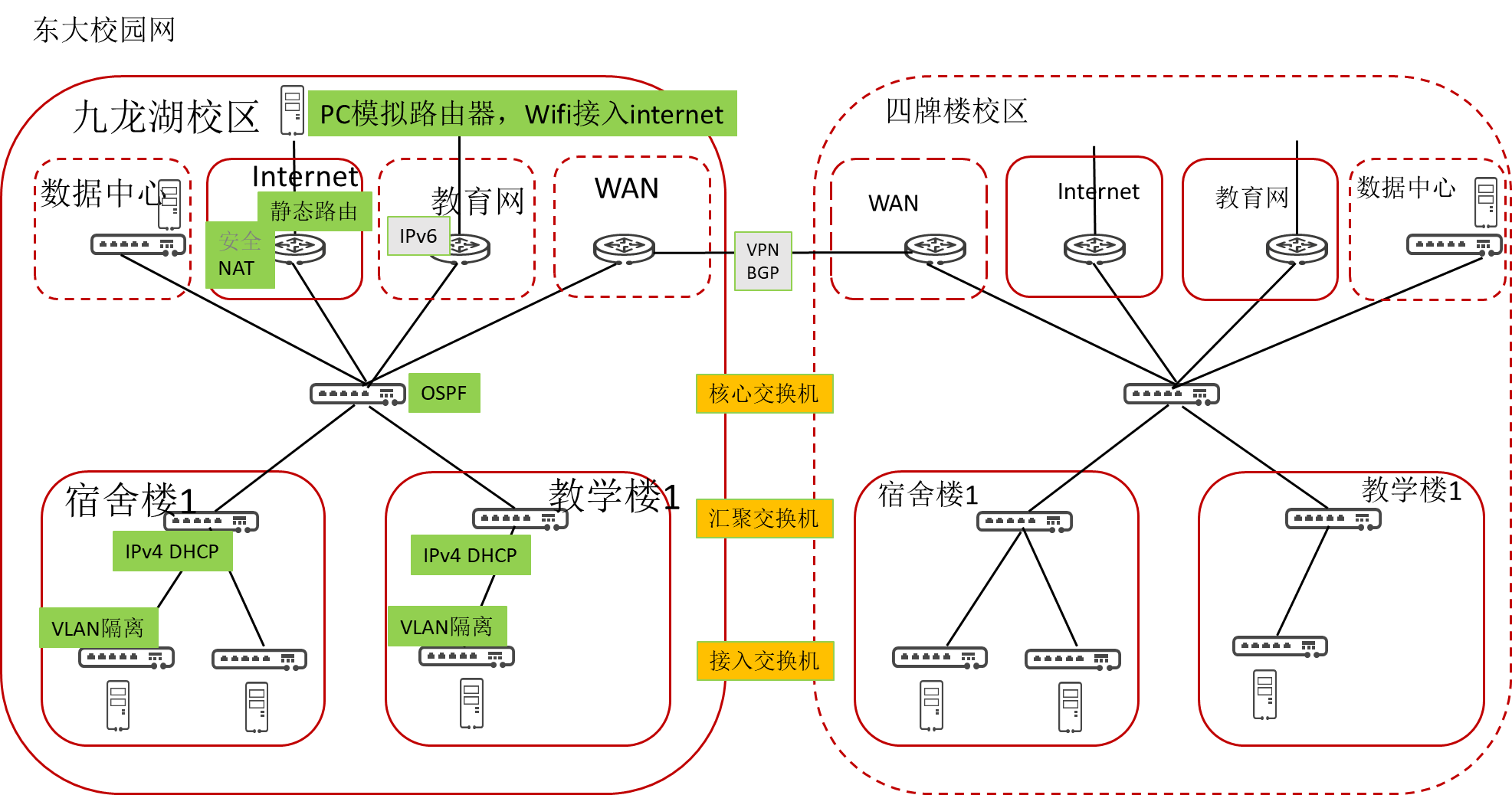
实验采用联合分组方式进行。

#### 实验任务

需要同学们规划一张网络，要求：

1. 宿舍区、教学区PC都可以接入网络，含IPv4
2. 宿舍区、教学区需要规划VLAN，避免广播域过大。实验中可以每台接入交换机1VLAN。
3. IP网关部署在大楼的汇聚交换机上
4. 汇聚/核心/Internet 间 采用OSPF发布路由
5. 路由器至Internet 静态路由
6. Internet 需要部署NAT
7. 需要通过校园网Wifi接入Internet，参考： https://cloud.tencent.com/developer/article/1678119

#### 实验组网



实线范围内 绿色部分是需要实验的部分

#### 部署思路

1. 规划VLAN，隔离接入交换机，接入交换机不能在汇聚交换机二层互通
2. 规划私网IP地址，校园网内唯一。部署DHCP，DNS地址与校园网DNS地址保持一致
3. 路由协议设计：围绕核心交换机OSPF，Internet 出口部署静态路由，并在OSPF中引入缺省路由(配置 default-route-advertise)。
4. Internet出口部署NAT，安全(暂不实现)
5. WAN VPN建立以及校区间路由发布(暂不实现)
6. 教育网IPv6 双栈部署(暂不实现)
7. DC 网络模拟(暂不实现)

#### 实验验证

1. 各区域PC能够互ping 通
2. 可访问Internet

# 实验环境使用建议

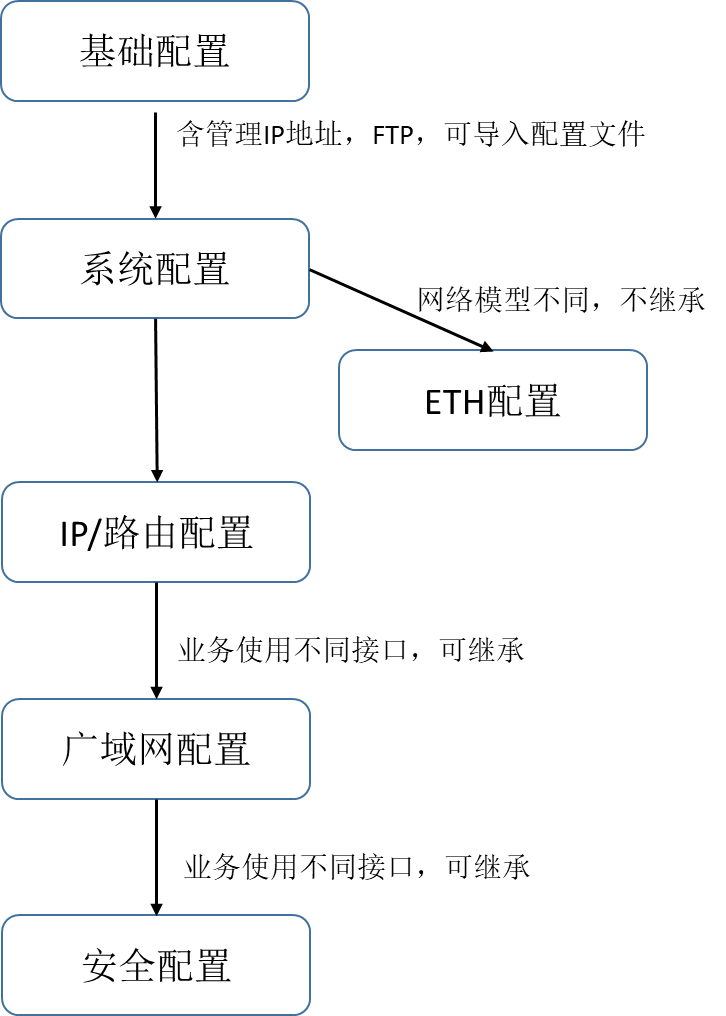
## 说明

实验在开展过程中，会出现

1. 2个课时无法完成一个实验用例情况
2. 多个用例配置沿用情况
3. 多个班级共用设备情况

因此在实验过程中，需要保存备份配置文件。待自己继续实验室时恢复使用。保存恢复配置参见2.5 章节。

## 各个实验配置基础关系



各实验设备首先 保存一个基础配置，含管理IP地址，FTP，公共管理账号。

* 1. 各实验阶段中，ETH 配置由于组网模型不一样，与下面配置文件不一样，可以单独保存配置，与下面用例独立开。

#

sysname switch-1-1 //1号岛 1号交换机

#

user-interface password complexity-check disable //交换机支持，AR不支持

#

ftp server enable

#

telnet server enable

#

aaa

undo user-password complexity-check

local-user admin password irreversible-cipher admin@nju.com

local-user admin service-type telnet terminal ftp

local-user admin ftp-directory flash:

undo local-aaa-user password policy administrator

#

interface MEth0/0/1

ip address 192.10.10.1 255.255.255.0 //根据岛位置分配地址

#

user-interface con 0

authentication-mode aaa

#

此配置备份在flash中，命名为adminbk.zip。若出现配置问题，可以使用此文件恢复初始配置。

* 1. 后续 IP与路由、IPv6与路由、企业广域网、IP安全配置4个实验 可以逐步开展，使用相同的配置文件。需要注意的是，这几个实验中广域相关的接口要根据用例描述进行，尽量不要变更，避免出现业务冲突

## 多批次同学共用设备

* 1. 各实验设备首先 保存一个基础配置，含管理IP地址，FTP 使能，公共账号。此配置备份在设备flash中，PC上。后续同学配置都是在此基础上增量开展。
  2. 各同学创建自己的设备账号，以此账号管理设备。AR设备小组3人共用，选择一位同学管理。
  3. 各同学实验课结束时，在设备flash中保存自己的配置文件，并备份为xxxbk.cfg，作为下次实验恢复使用。保险起见，在PC机上也通过FTP备份一次
  4. 下次另外的同学实验课时，使用公共账号登录设备，使用flash中自己上次备份的配置文件启动设备。
  5. 若备份文件被误删，则从PC机上通过FTP重新加载配置文件
  6. 若公共用户名被破坏，则只能通过串口登录设备，重新恢复基础配置，加载自己的配置文件

示例：

每位同学有唯一命名的配置文件，规定为学号.cfg. 例如张三同学学号为 MG21230088，则位置文件名称为MG21230088.cfg

### 保存配置至交换机Flash

* 1. 每次实验课完成后，张三同学保存配置文件：

<Huawei> save MG21230088.cfg

Are you sure to save the configuration to xxxxx.cfg? (y/n)[n]:y

It will take several minutes to save configuration file, please wait.......

Configuration file had been saved successfully

Note: The configuration file will take effect after being activated

* 1. 查看flash 中已经保存了此配置文件

<Huawei>dir \*.cfg

Directory of flash:/

Idx Attr Size(Byte) Date Time(LMT) FileName

0 -rw- 981 Nov 05 2021 10:47:07 MG21230088.cfg

### FTP 下载配置文件至PC机/PC 机上传配置文件

交换机/路由器 已经开启FTP server，若未开启，参见实验手册 2.5.3.4.2 章节

当前实验PC机已经能够ping 通交换机VLANIF 接口地址，则可以直接用ftp 连接此地址。

例如 ftp 10.10.10.1

可以用get 下载配置文件MG21230088.cfg，用put 上传MG21230088.cfg

### 恢复配置文件

* 1. 新进入实验课后，张三同学复制一份文件。

<Huawei>copy MG21230088.cfg MG21230088run.cfg

Copy flash:/xxxxx.cfg to flash:/xxxxxrun.cfg? (y/n)[n]:y

100% complete

Info: Copied file flash:/ MG21230088.cfg to flash:/ MG21230088run.cfg...Done

* 1. 设置启动自己的配置文件。

<Huawei>startup saved-configuration MG21230088run.cfg

This operation will take several minutes, please wait....

Info: Succeeded in setting the file for booting system

<Huawei>disp startup

MainBoard:

Startup system software: null

Next startup system software: null

Backup system software for next startup: null

Startup saved-configuration file: flash:/vrpcfg.zip

Next startup saved-configuration file: flash:/ MG21230088run.cfg

Startup license file: null

Next startup license file: null

Startup patch package: null

Next startup patch package: null

Startup voice-files: null

Next startup voice-files: null

* 1. 重新启动，变更启动的配置

<Huawei>reboot fast

* 1. 启动完成后，可以看到已经使用MG21230088run.cfg 配置文件

<Huawei>display startup

MainBoard:

Startup system software: null

Next startup system software: null

Backup system software for next startup: null

Startup saved-configuration file: flash:/ MG21230088run.cfg

Next startup saved-configuration file: flash:/ MG21230088run.cfg

Startup license file: null

Next startup license file: null

Startup patch package: null

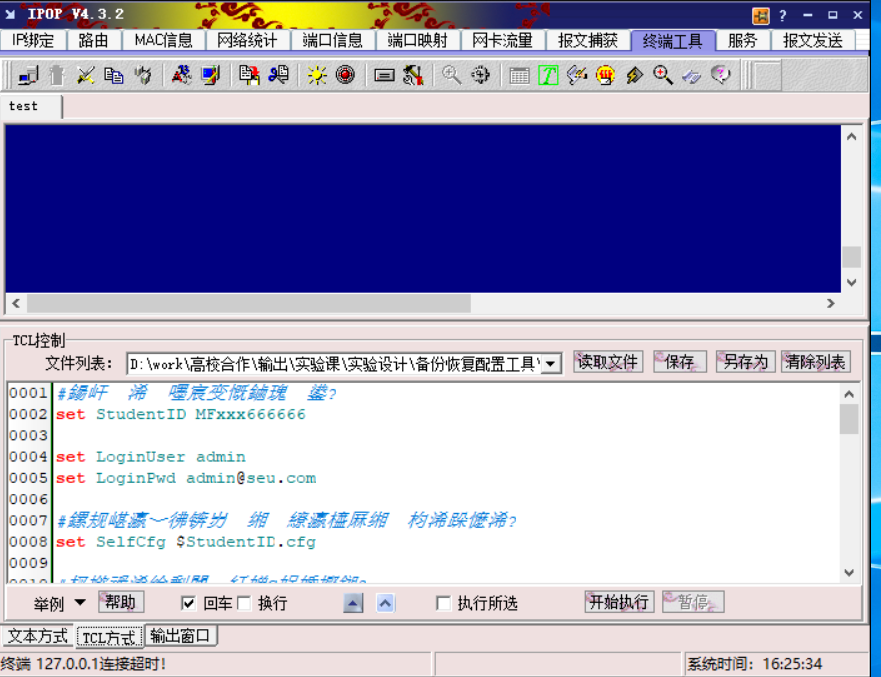
Next startup patch package: null

Startup voice-files: null

Next startup voice-files: null

### TCL脚本工具





1. 终端工具->T快捷栏->TCL方式->读取文件
2. 开始实验前，运行EnterLab.tcl
   * 缺省配置上设置自己的配置文件，重启
3. 结束实验离开前，运行LeaveLab.tcl
   * 保存自己的配置文件，并重启为缺省配置

注意：！！！使用前需要将这两个文件中学号改为自己的学号

