计算机网络实验手册

目录

1 实验总体介绍

1.1 实验总体介绍

1.1.1 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。

1.1.2 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；

1.1.3 实验组网介绍

1.1.3.1 组网图例

PC机 or 服务器

接入交换机

汇聚交换机

AP

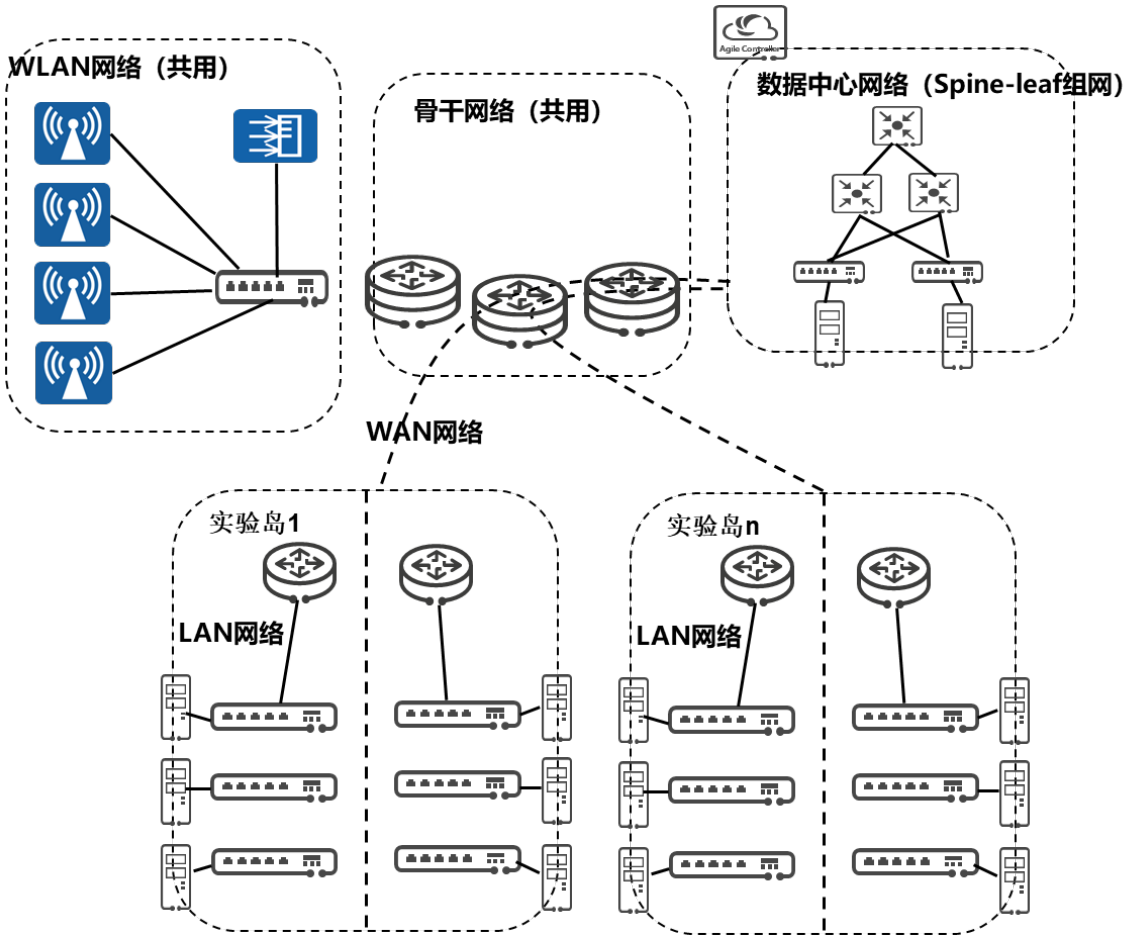
WLAN-AC

接入路由器

核心路由器

控制器

1.1.3.2 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，实验设备包括三层交换机 3 台，路由器 1 台。

图1-1 实验一 基础配置组网图

图1-2 实验二 以太网组网图

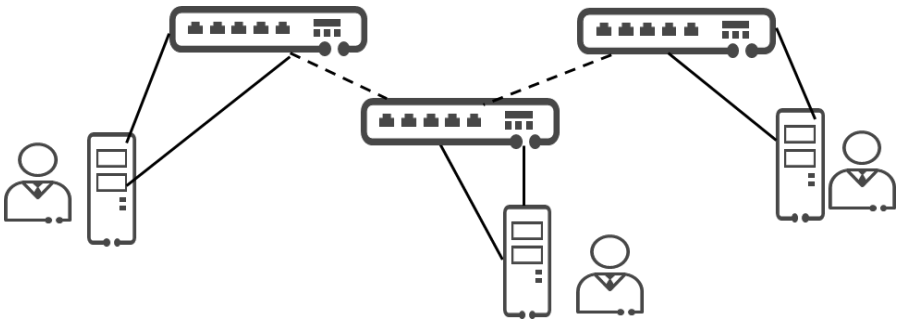


图1-3 实验二 IP 与路由组网图

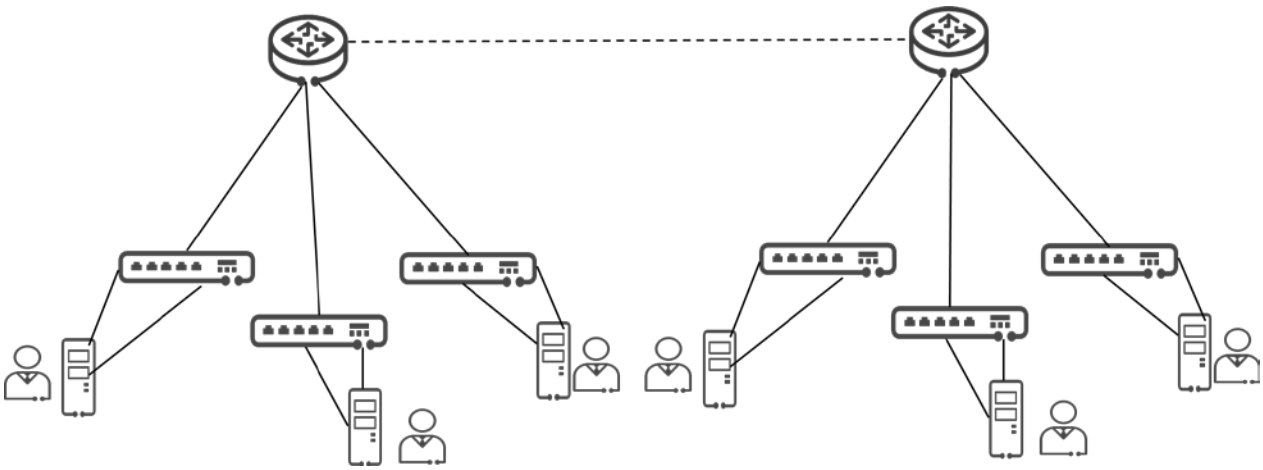


图1-4 实验三 广域网实验组网图

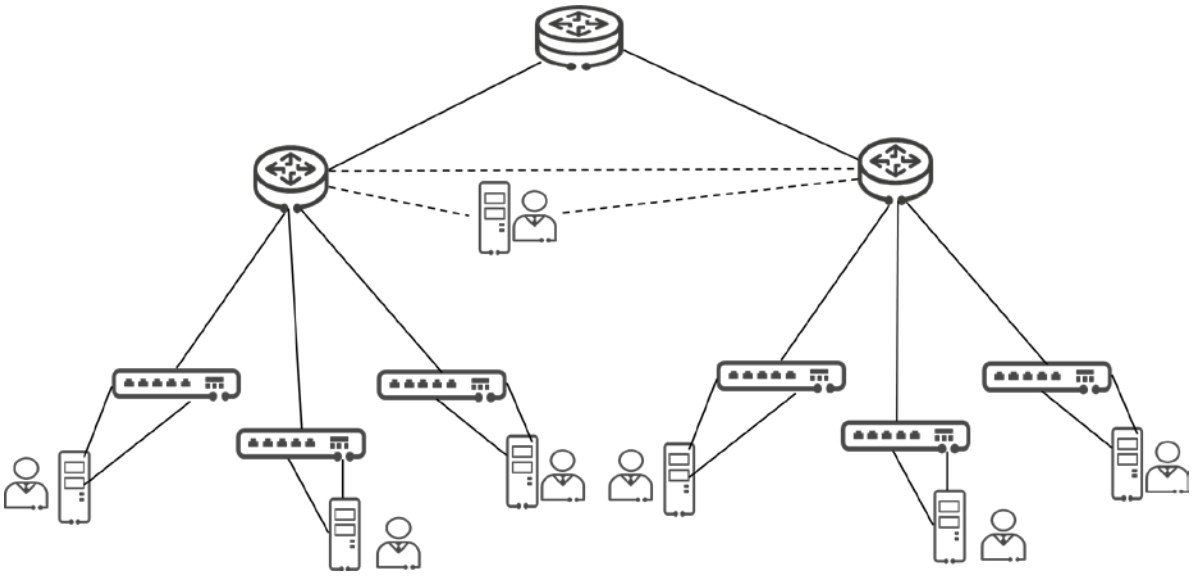
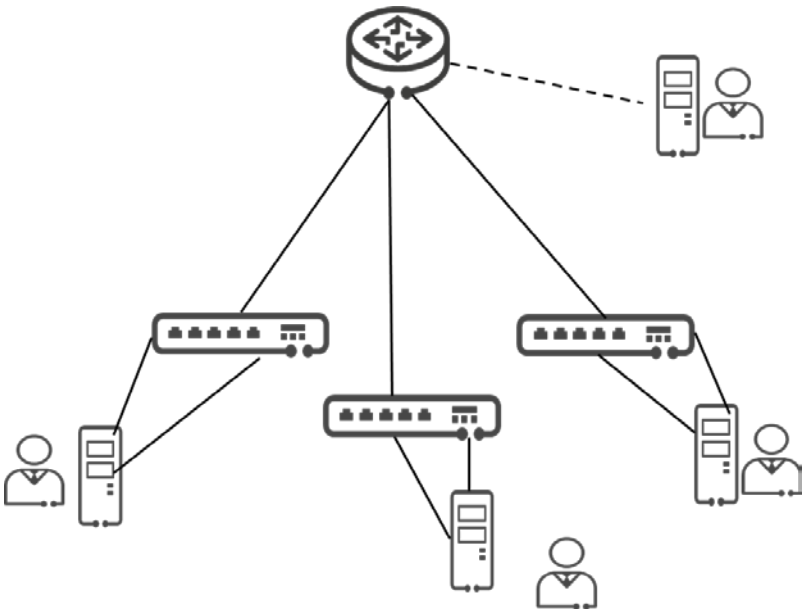


图1-5 实验四 安全配置组网图



1.1.4 实验资源

设备名称、型号与版本的对应关系如下：

表1-1 实验设备详细信息

设备名称	关键功能	建议设备型号	软件版本
岛内交换机	二三层，支持OSPF	S5730LI	V200R019C10
岛内路由器	支持OSPF/NAT/MPLS/IPsec/安全	AR657/AR6140	V300R019C10

1.1.5 实验工具

表1-2 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	实验室提供	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 /mobaxterm/ SecureCRT…	设备管理工具，可仿真console口和telnet/ssh等登录设备 Mac os可使用mobaxterm
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

1.1.6 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。

2 实验任务 1： 基础管理

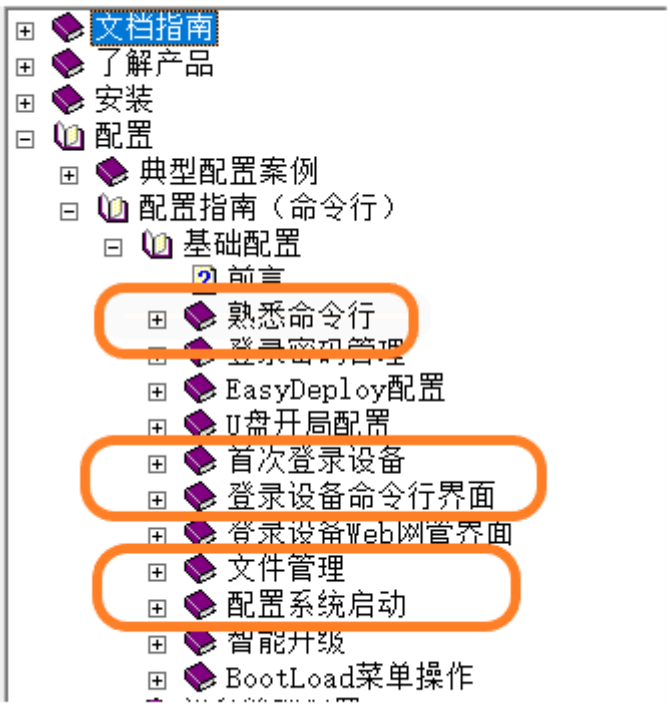
2.1 实验介绍

2.1.1 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。

2.1.2 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

2.2 首次登录设备

2.2.1 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

2.2.2 通过 Console 口首次登录设备

2.2.2.1 实验任务

通过 Console 口 登录设备。

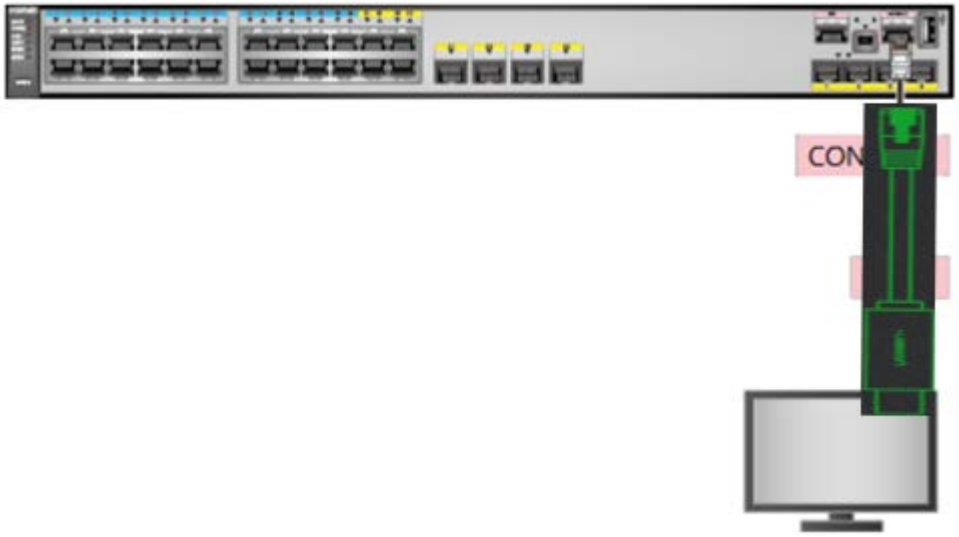
在配置通过 Console 口登录设备之前，需要完成以下前置条件：

- 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。

2.2.2.2 实验组网



-

2.2.2.3 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

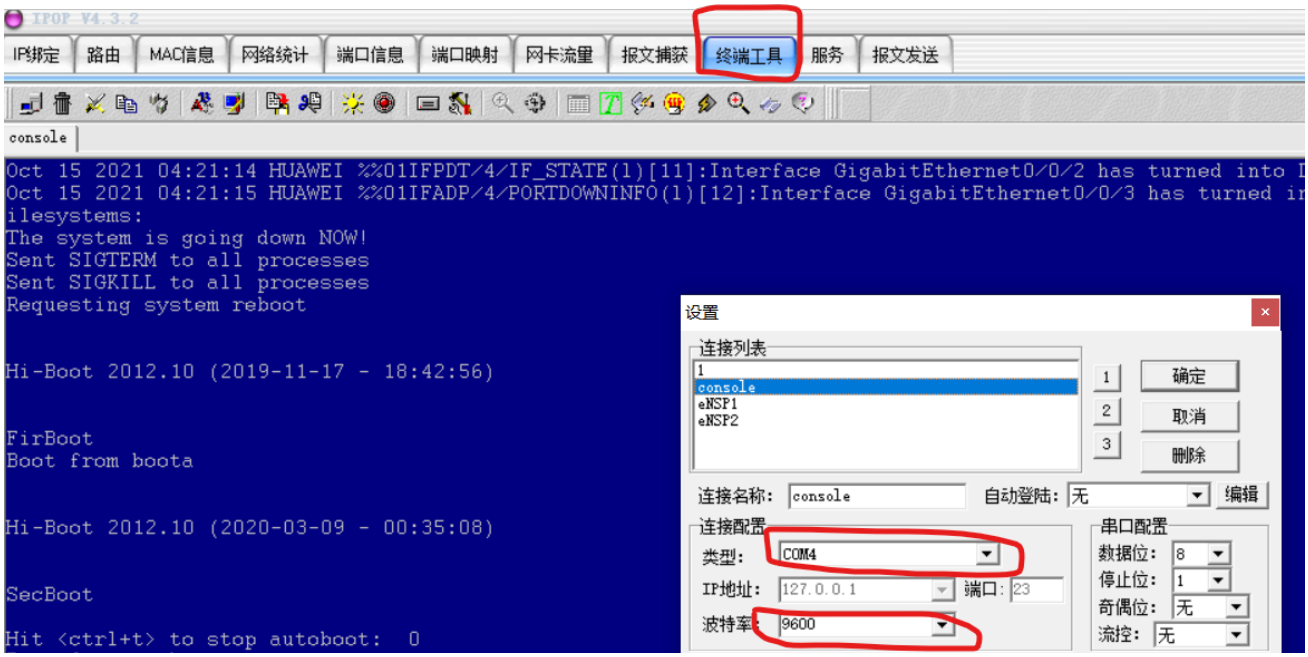
2. 在 PC 上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。

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 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



3. 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

```
User interface con isavailable
Please Press ENTER.
Login authentication
Username:admin
Password:
```

2.2.2.4 实验验证

登录 console 管理设备

2.3 系统常用配置

2.3.1 帮助功能和命令自动补全

2.3.1.1 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。

2.3.1.2 实验任务

掌握命令行帮助功能

2.3.1.3 实验组网

同 2.2.2

2.3.1.4 操作步骤

2.3.1.4.1 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

    ...
```

2）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。

2.3.1.4.2 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
```

2) 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。

2.3.1.5 实验验证

NA

2.3.2 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。

2.3.2.1 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

2.3.2.2 实验任务

查看设备当前运行版本。

2.3.2.3 实验组网

同 2.2.2

2.3.2.4 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

2.3.2.5 实验验证

验证显示的版本信息是否符合预期。

2.3.3 进入视图

2.3.3.1 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。

常用视图名称	进入视图	视图功能
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-GigabitEthernet*X/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。

2.3.3.2 实验任务

理解属性视图概念。完成进入 system 视图实验。

2.3.3.3 实验组网

同 2.2.2

2.3.3.4 操作步骤

```
<HUAWEI> system-view
Enter system view, return user view with Ctrl+Z.
[HUAWEI]
```

2.3.3.5 实验验证

NA

2.3.4 修改设备名称

2.3.4.1 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。

2.3.4.2 实验任务

设置接入交换机设备名称。

2.3.4.3 实验组网

同 2.2.2

2.3.4.4 操作步骤

```
<HUAWEI> system-view
[HUAWEI] sysname 123456
[123456]
```

2.3.4.5 实验验证

验证系统名是否已经修改为学号 123456。

2.3.5 查看当前视图配置

2.3.5.1 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

2.3.5.2 实验任务

查看当前视图生效配置。

2.3.5.3 实验组网

同 2.2.2

2.3.5.4 操作步骤

```
<123456> system-view
[123456]display this
#
sysname 123456
#
```

2.3.5.5 实验验证

查看到系统视图下已经配置命令 sysname 123456

2.3.6 删除已有配置

2.3.6.1 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>
```

2.3.6.2 实验任务

删除设备名配置。

2.3.6.3 实验组网

同 2.2.2

2.3.6.4 操作步骤

```
<123456> system-view
[123456]undo sysname
[Huawei]
```

2.3.6.5 实验验证

查看到设备名已经变为 huawei

2.4 保存恢复配置

2.4.1 任务介绍

2.4.2 保存设备配置

2.4.2.1 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

2.4.2.2 实验任务

保存配置文件，文件名为学号.cfg。

2.4.2.3 实验组网

同 2.2.2

2.4.2.4 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.
```

2.4.2.5 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
#
```

2.4.3 备份设备配置

2.4.3.1 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。

2.4.3.2 实验任务

本实验采用备份文件到存储器方式完成。

2.4.3.3 实验组网

同 2.2.2，需要 PC 机通过网线接入到管理网口。

2.4.3.4 操作步骤

2.4.3.4.1 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
```

2.4.3.5 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

2.4.4 恢复设备配置

2.4.4.1 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。

2.4.4.2 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。

2.4.4.3 实验组网

同 2.2.2

2.4.4.4 操作步骤

缺省情况下从存储器恢复配置文件即可

2.4.4.4.1 从存储器恢复配置文件

恢复配置文件

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

2.4.4.4.2 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.
```

2.4.4.4.3 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。

2.4.4.5 实验验证

查看配置文件是否为自己的配置。

```
<123456> display saved-configuration
#
 sysname 123456
...
#
```

3 实验任务 2： 以太交换

3.1 实验介绍

3.1.1 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。

3.1.2 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。

3.2 广播转发

3.2.1 说明

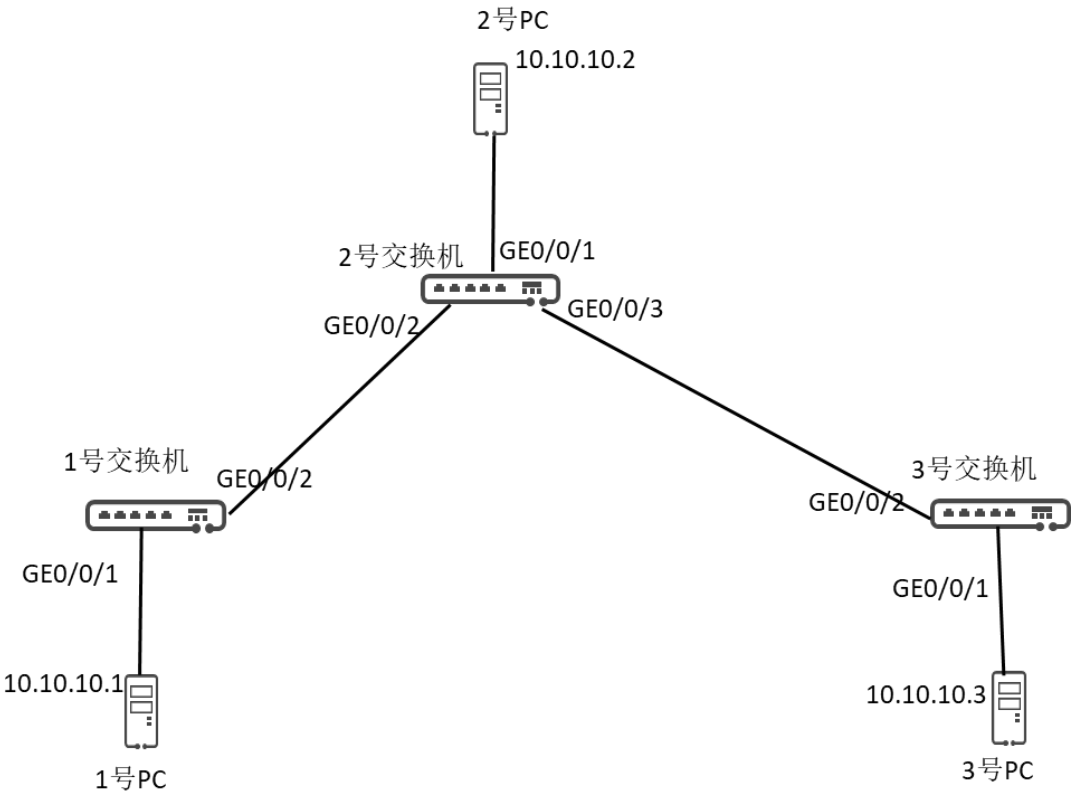
交换机发货接口缺省 VLAN 为 1，此时交换机相当于是一个 Hub，所有接口是互通的。

3.2.2 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。

3.2.3 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。



3.2.4 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
```

3.2.4.1 实验验证

1) 交换机 MAC 学习符合预期
2) PC 机间能够 ping 通

3.3 VLAN 隔离/互通

3.3.1 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。

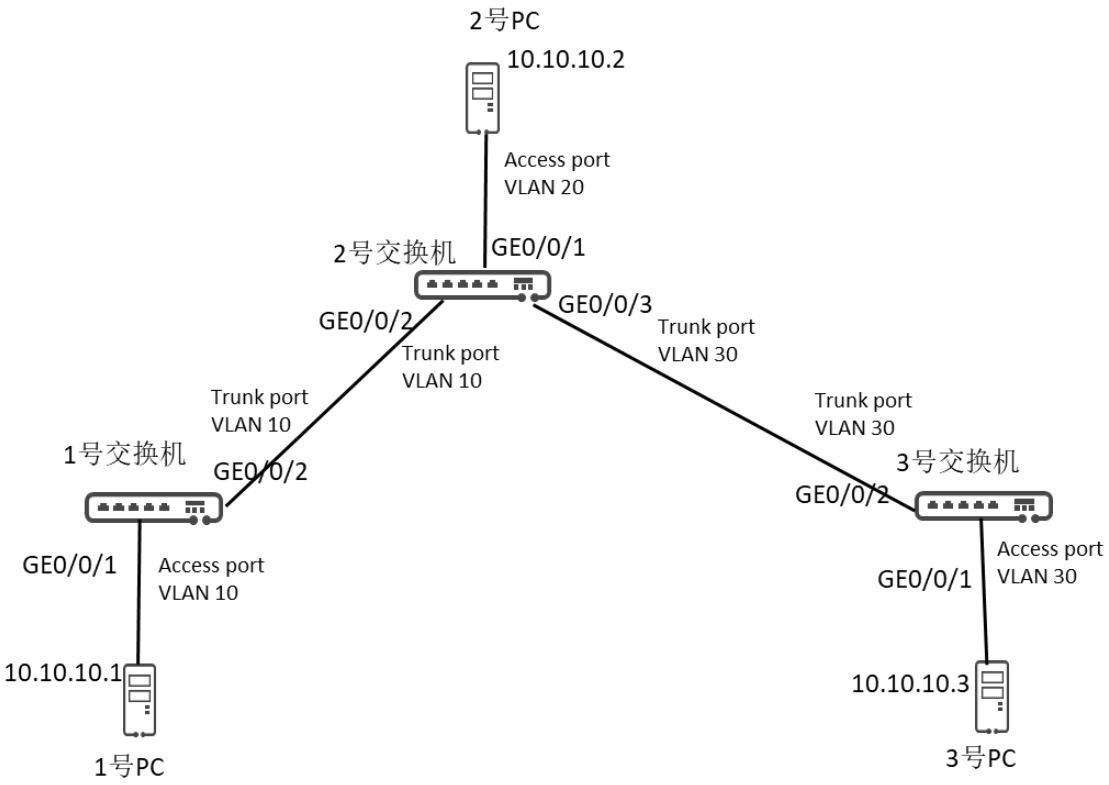
3.3.2 实验任务

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；

3.3.3 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。



3.3.4 操作步骤

3.3.4.1 VLAN 隔离

3.3.4.1.1 实验验证目标

PC_1 与 PC_3 使用不同的 VLAN 隔离，不能互通

3.3.4.1.2 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
```

2) 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

3) 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

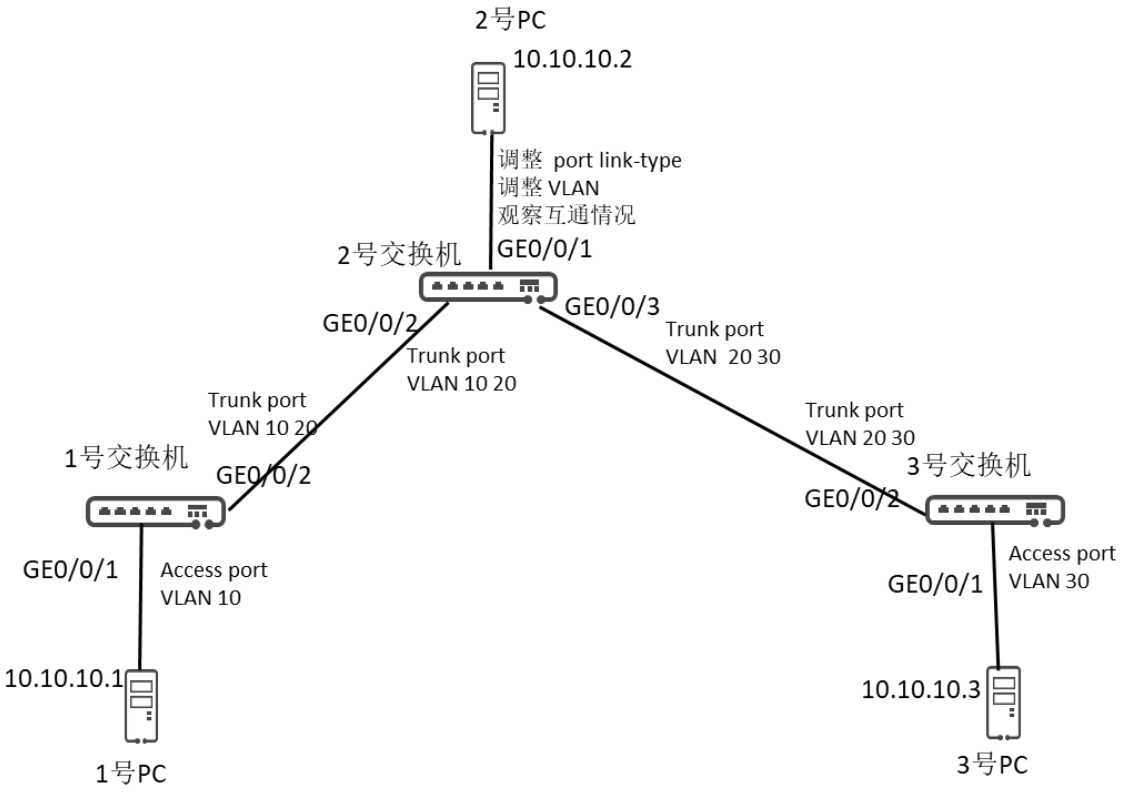
4) 查看 VLAN 配置结果

```
[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
```

3.3.5 VLAN 互通

3.3.5.1.1 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



3.3.6 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

4 实验任务 3： IPv4 与路由

4.1 实验介绍

4.1.1 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：

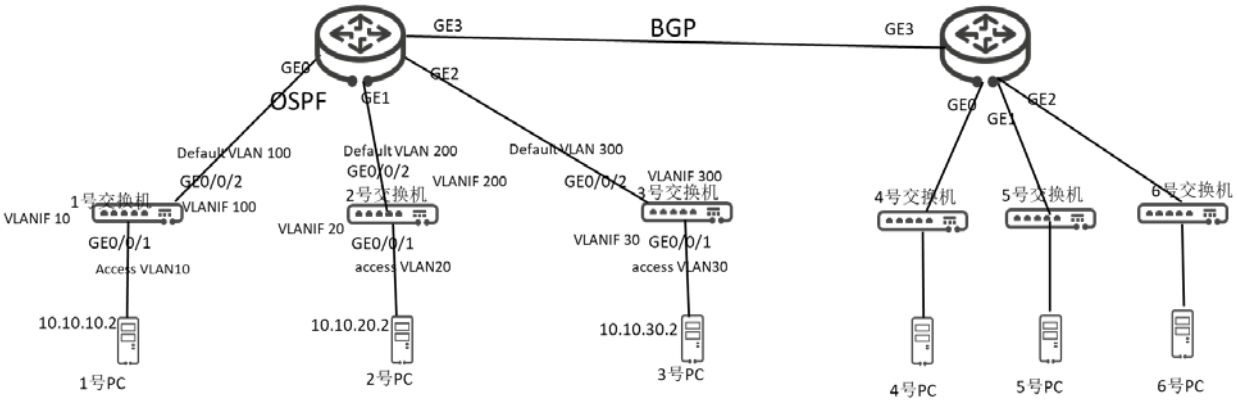
Mooc 可以参考《HCIA-Datacom V1.0 华为认证数通工程师在线课程》中 “网络层协议及 IP 编址”、“IP 路由基础”、“OSPF 基础”、“网络地址转换”章节。

4.1.2 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

4.1.3 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。



4.2 IPv4 地址配置

4.2.1 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；

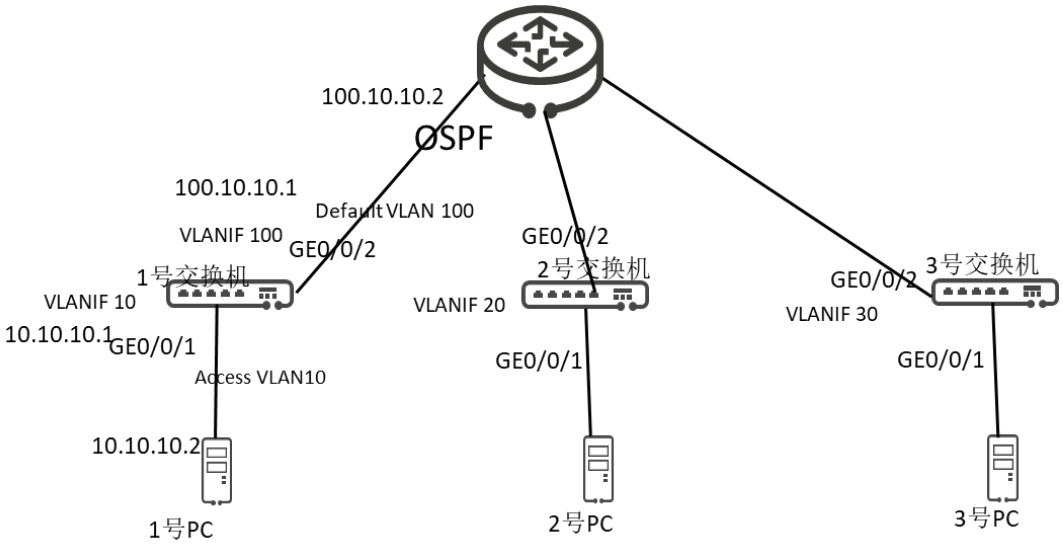
2）交换机至 AR 间接口地址配置为 100.10.10.1, AR 接口地址配置为 100.10.10.2

4.2.2 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

4.2.3 实验组网



Save xxx.cfg

离开实验室 admintemp.cfg 设置为启动文件

4.2.4 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-Vlanif100] ip address 100.10.10.1 24
[Switch_1-Vlanif100] quit


# 配置 AR 路由器，路由器可以直接在物理口配置 IP 地址，不需要配置 VLAN
[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

4.2.5 实验验证

1) IP 地址配置成功后，可以通过 display ip interface brief 查看其状态

```
<LSW1>display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
The number of interface that is UP in Physical is 4
The number of interface that is DOWN in Physical is 2
The number of interface that is UP in Protocol is 4
The number of interface that is DOWN in Protocol is 2

Interface                         IP Address/Mask      Physical
Protocol
LoopBack0                         1.1.1.1/32           up         up(s)
MEth0/0/1                         unassigned           down       down
NULL0                             unassigned           up         up(s)
Vlanif1                           unassigned           down       down
Vlanif10                          10.10.10.1/24        up         up
Vlanif100                         100.10.10.1/24       up         up
```

2) 各 PC 机能够 ping 通 网关，例如 PC1 能 ping 通 10.10.10.1

3) 交换机上 能够 ping 通 直连的路由器接口地址，例如交换机 1 能 ping 通 100.10.10.2

4.3 DHCP 配置

4.3.1 说明

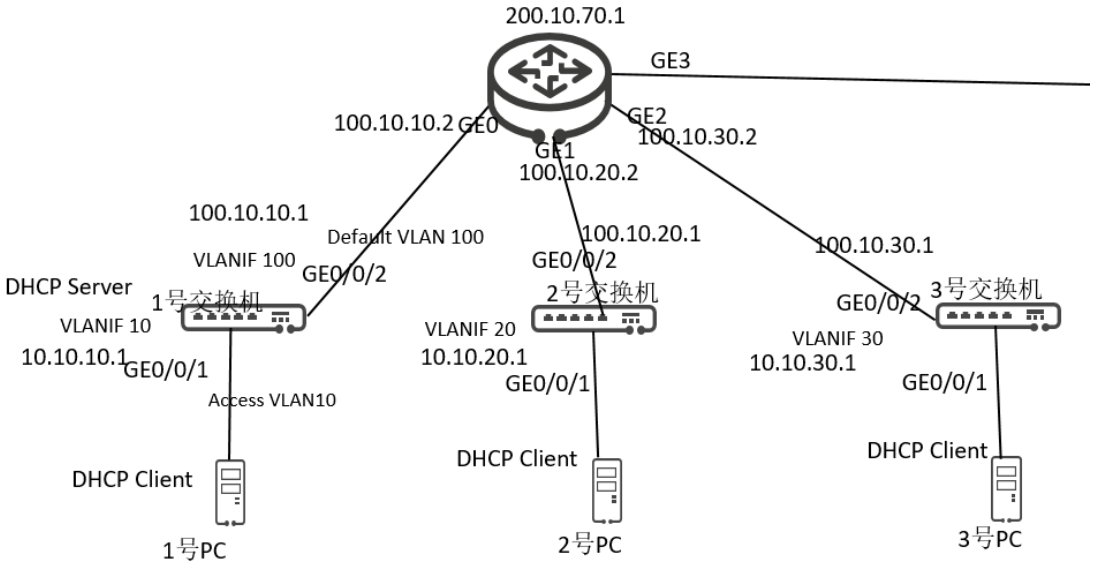
PC 机可以通过 DHCP 获取 IP 地址，便于部署，现网一般采用此种方式进行 IP 地址分配管理。现网通常使用专用 DHCP server 管理 IP 地址，本实验采用在交换机上部署 DHCP server 方式。

4.3.2 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

4.3.3 实验组网



4.3.4 操作步骤

1) 使能 DHCP Server.

```
[Switch_1] dhcp enable
```

2) 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

#选择本 VLANIF 接口网段作为 DHCP server 分配的 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

4.3.5 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
 ------------------------------------------------------------------------
--------------
```

2) 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

   若 PC 机已经通过 DHCP 获取到 IP 地址，可以通过 ipconfig /release，ipconfig /renew 重新获取 IP 地址，用 wireshak 抓取 DHCP 报文交换过程。

3) PC 机上查看分配到的 IP 地址，网关地址，DNS 地址等

4) PC 机能 ping 通交换机网关地址

4.4 静态路由配置

4.4.1 说明

静态路由在不同网络环境中有不同的目的：

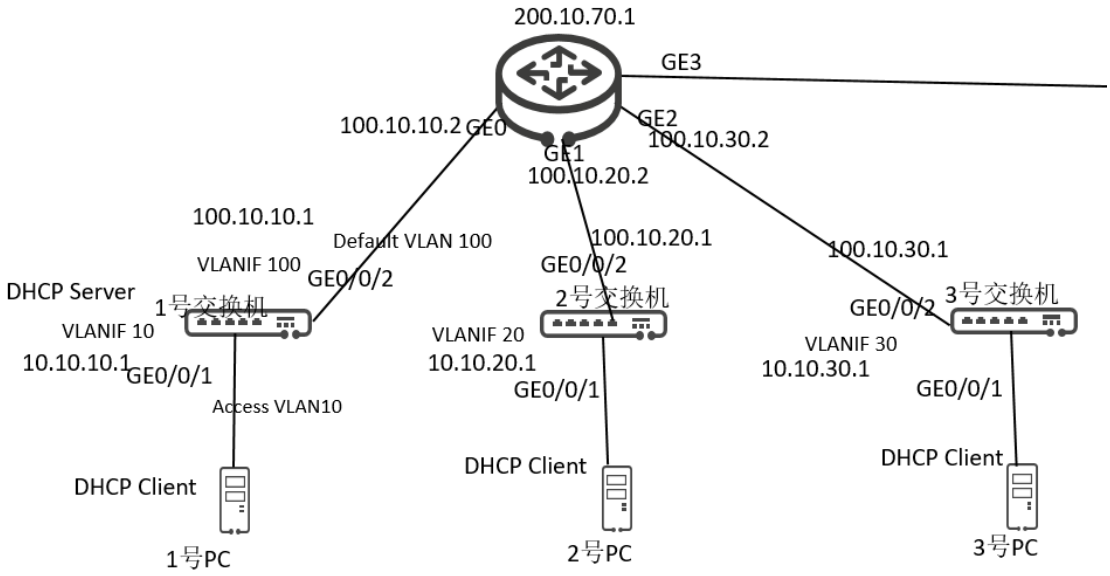
1) 当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。
2) 在复杂网络环境中，配置静态路由可以改进网络的性能，并可为重要的应用保证带宽。

在现网中，经常采用静态路由方式配置缺省路由。

4.4.2 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。

4.4.3 实验组网



4.4.4 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-》AR 路由器 200.10.70.1 地址 icmp request 路由过程:

2) PC 机通过默认网关知道至 200.10.70.1 路由，不需要增加配置。

3) 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-》PC 机 10.10.10.254 的 icmp reply 路由过程:

4) 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
```

5) 交换机 至 10.10.10.0 网段，通过直连路由知道从 VLANIF10 转发，不需要增加配置

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

4.4.5 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?

4.5 OSPF 配置

4.5.1 说明

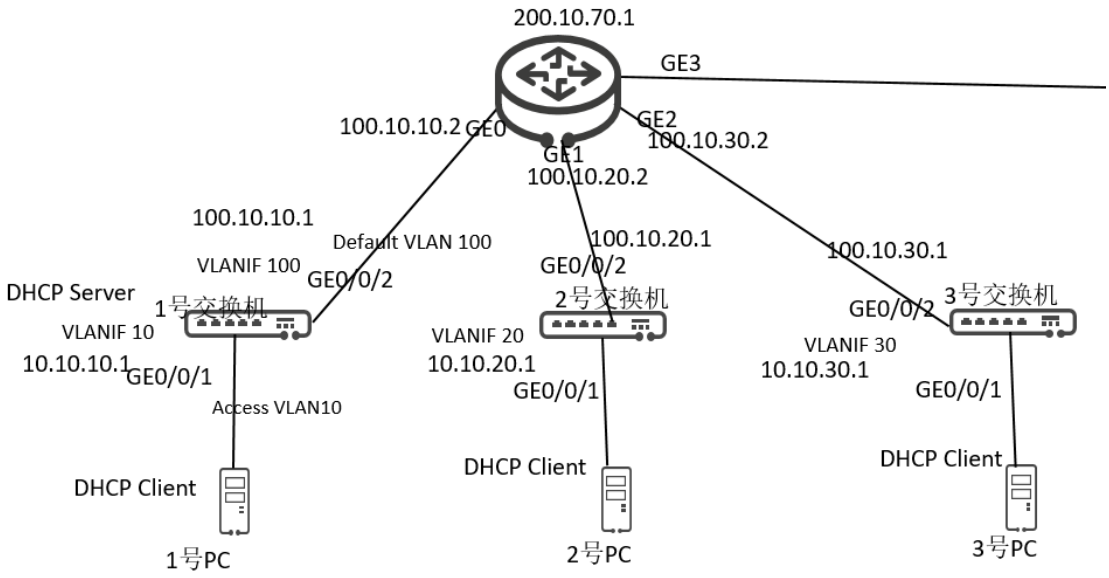
OSPF 是园区网络中应用最广泛的路由协议。

4.5.2 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

4.5.3 实验组网



4.5.4 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。Router-id 网络里唯一，不能冲突

```
[Switch_1]interface loopback 0
[Switch_1-Loopback0] ip address 200.10.10.1 255.255.255.255
```

#启动 OSPF 服务

[Switch_1] ospf 1 router-id 200.10.10.1 //1 的作用是进程号，路由器内部使用，用于为 VPN 网络分别不同的独立进程

#配置 OSPF area，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，并把这个的接口链路状态发布出去.注意反掩码

```
[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，可以选择一种使用：

A）用 network 方式发布出去，1 类 LSA(Router LSA，stubnet)

```
[Switch_1-ospf-1-area-0.0.0.0] network 10.10.10.0 0.0.0.255
```

B）用 import direct 路由方式发布出去。这是引入外部路由方式，5 类 LSA（AS external LSA）。可以引入多种外部路由，比如 direct/RIP/BGP/ISIS 等

```
[Switch_1-ospf-1-area-0.0.0.0] quit
[Switch_1-ospf-1]import-route direct
```

2） AR1 上启用 OSPF

#配置 ospf router-id ，作为 OSPF 路由器标识。注意反掩码

```
[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
```

#与交换机间接口上使能 OSPF，并把这个接口的链路状态发布出去。

```
[AR_1-ospf-1] area 0
[AR_1-ospf-1-area-0.0.0.0] network 100.10.10.0 0.0.0.255  //for switch1
[AR_1-ospf-1-area-0.0.0.0] network 100.10.20.0 0.0.0.255  //for switch2
[AR_1-ospf-1-area-0.0.0.0] network 100.10.30.0 0.0.0.255  //for 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

4.5.5 实验验证

1） 查看 OSPF 是否建立，状态是否为 Full 状态

```
<Switch_1> display ospf peer
<LSW1>display ospf peer

      OSPF Process 1 with Router ID 1.1.1.1
             Neighbors

 Area 0.0.0.0 interface 100.10.10.1(Vlanif100)'s neighbors
 Router ID: 200.10.70.1          Address: 100.10.10.2
   State: Full  Mode:Nbr is  Master  Priority: 1
   DR: 100.10.10.2  BDR: 100.10.10.1  MTU: 0
```

```
  Dead timer due in 40  sec
  Retrans timer interval: 5
  Neighbor is up for 00:01:52
  Authentication Sequence: [ 0 ]
```

2) 查看各设备上路由

```
<Switch_1> display ospf routing
<Switch_1> display ip routing
```

3) PC 机能够互相 ping 通

4.6 BGP 配置(高阶)

4.6.1 说明

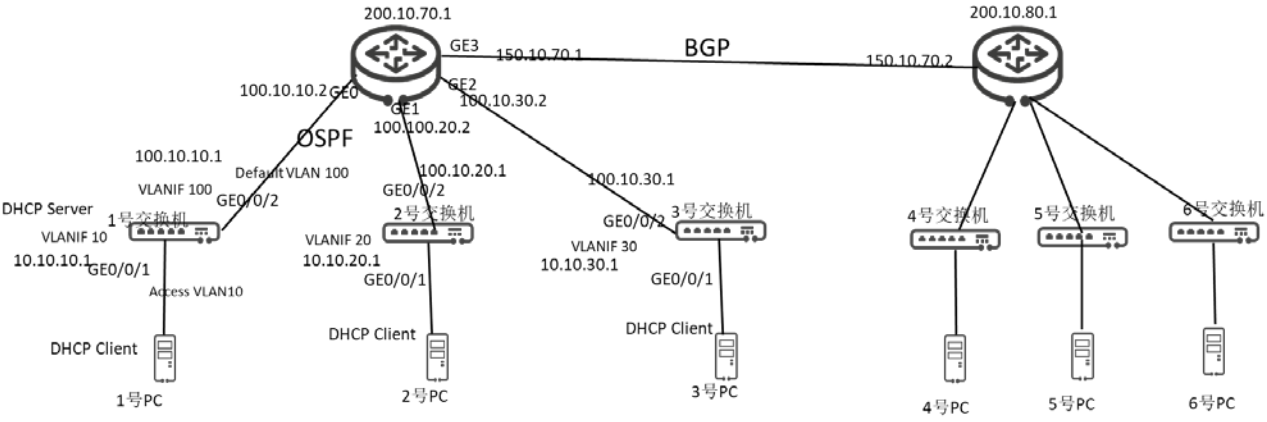
同一岛内 2 个小组 OSPF 配置完成后，可以在 2 个 AR 路由器间配置 BGP 协议发布路由。

4.6.2 实验任务

1）验证 BGP 协议

2）两个组内的 PC 机能够相互 ping 通

4.6.3 实验组网



4.6.4 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
```

2) 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
```

3) AR1 OSPF 引入 BGP 路由

```
[AR_1] ospf
[AR_1-ospf-1] import-route bgp
```

4) 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
```

5) AR2 配置

```
[AR_2] ospf
[AR_2-ospf-1] import-route bgp
```

4.6.5 实验验证

1）查看各设备路由情况

```
display ip routing-table
```

2）PC 间 ping 情况

4.7 NAT

4.7.1 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。

4.7.2 实验任务

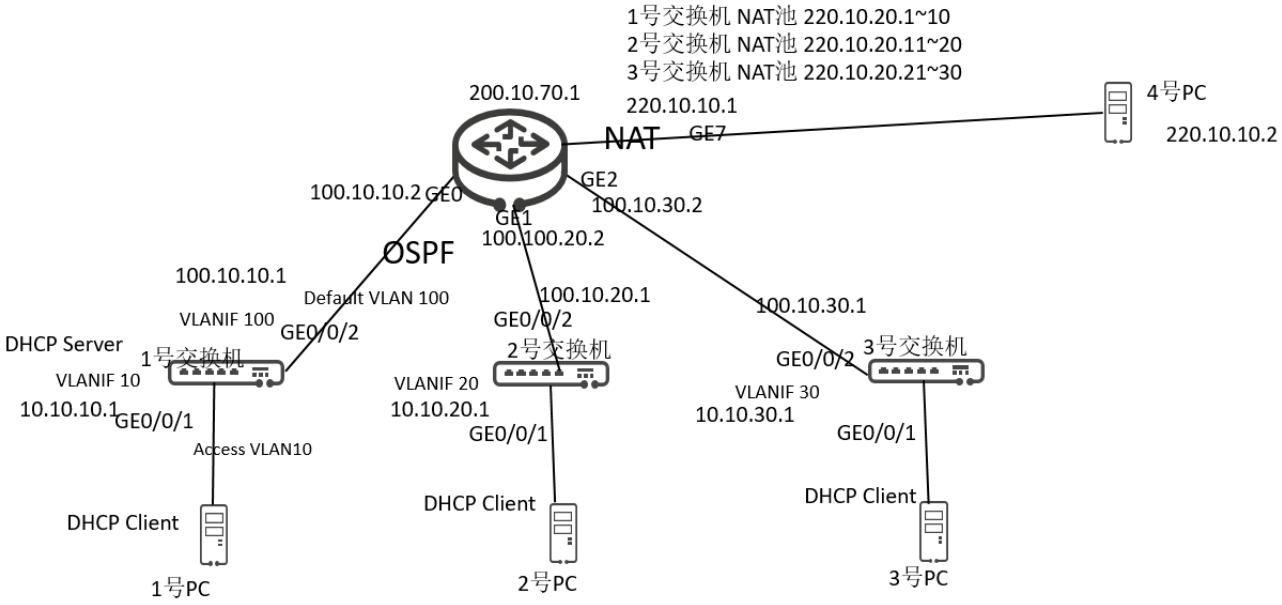
1） AR 上 3 台交换机使用不同的 NAT 地址池

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。

4.7.3 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。



4.7.4 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
```

2） 配置 NAT

#设置 NAT 转换的地址池(公网)

[AR_1] nat address-group 1 220.10.20.1 220.10.20.10 //1 号交换机下挂 PC 机的地址池

#设置 ACL 规则，根据源 IP 地址，将 1 号 PC 的 packets 进行 NAT 转换

#访问 ACL 控制列表

[AR_1] acl 2001 //2001 为内部编号，作为后面引用的索引。

[AR_1-acl-basic-2001] rule 5 permit source 10.10.10.0 0.0.0.255 //注意反掩码
[AR_1-acl-basic-2001] quit

#在出接口匹配 ACL 规则，使用 NAT 地址池进行转换

```
[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 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 //2 号交换机下挂 PC 机的地址池

```
[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
```

4.7.5 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，是否已经变为 NAT 地址池地址。

2） 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     : 220.10.10.2
  Type Code IcmpId   : 0   8   41931
  NAT-Info
    New SrcAddr      : 220.10.20.1
    New DestAddr     : ----
New IcmpId       : 10243
```

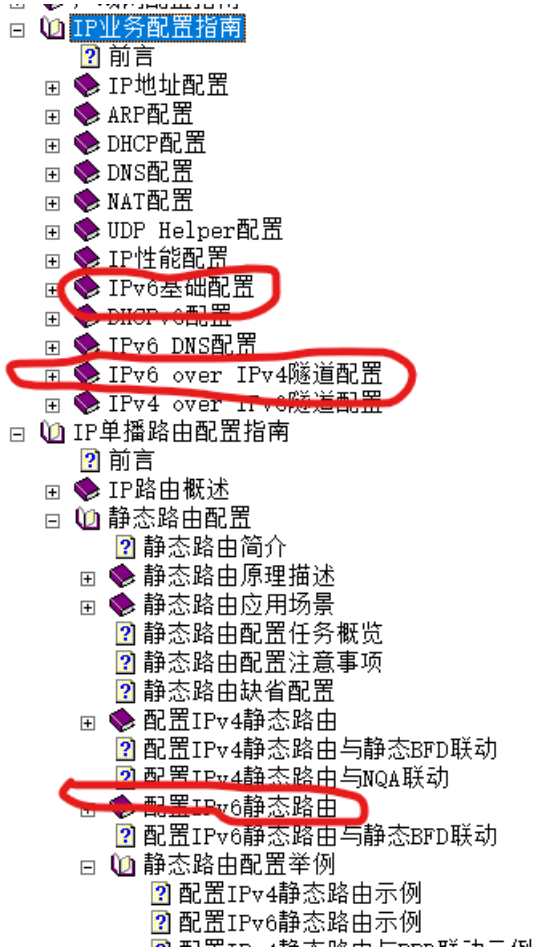
5 实验任务 4： IPv6 与路由

5.1 实验介绍

5.1.1 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：



5.1.2 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

5.2 IPv6 地址配置

5.2.1 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

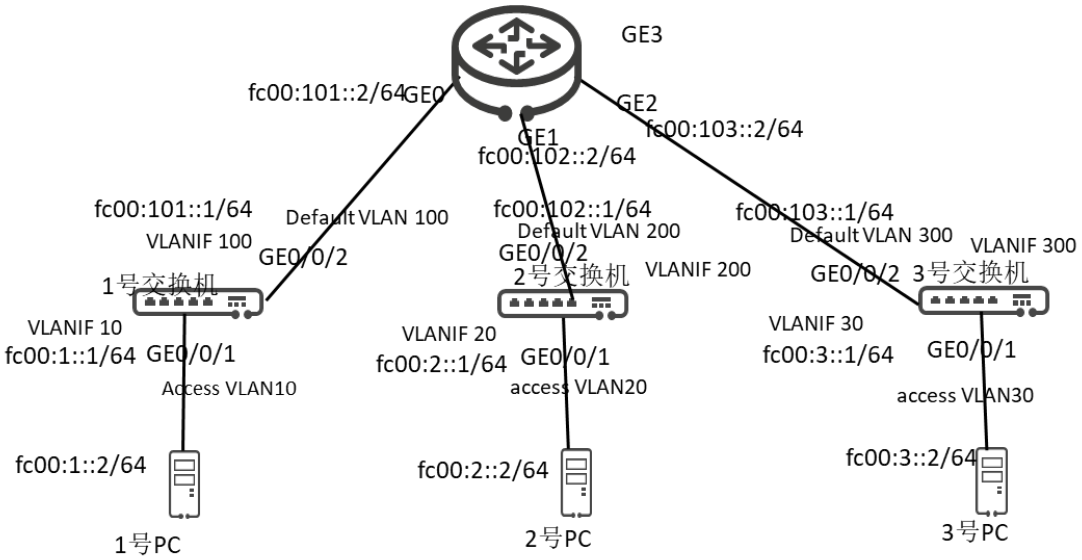
5.2.1.1 实验任务

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

5.2.2 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。



5.2.3 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

5.2.4 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

5.3 IPv6 静态路由

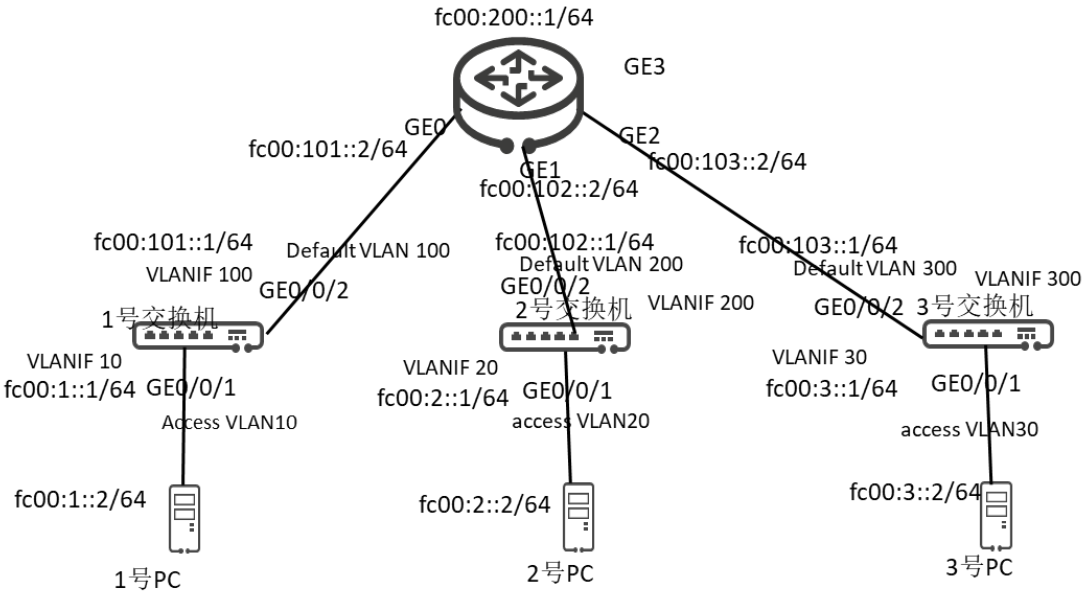
5.3.1 说明

IPv6 静态路由与 IPv4 静态路由模型很类似，参考配置即可。

5.3.2 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。

5.3.3 实验组网



5.3.4 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
```

2) 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
```

3) 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
```

5.3.5 实验验证

1) PC 机能够 ping 通 fc00:200::1

5.4 IPv4/IPv6 过渡(高阶)

5.4.1 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。

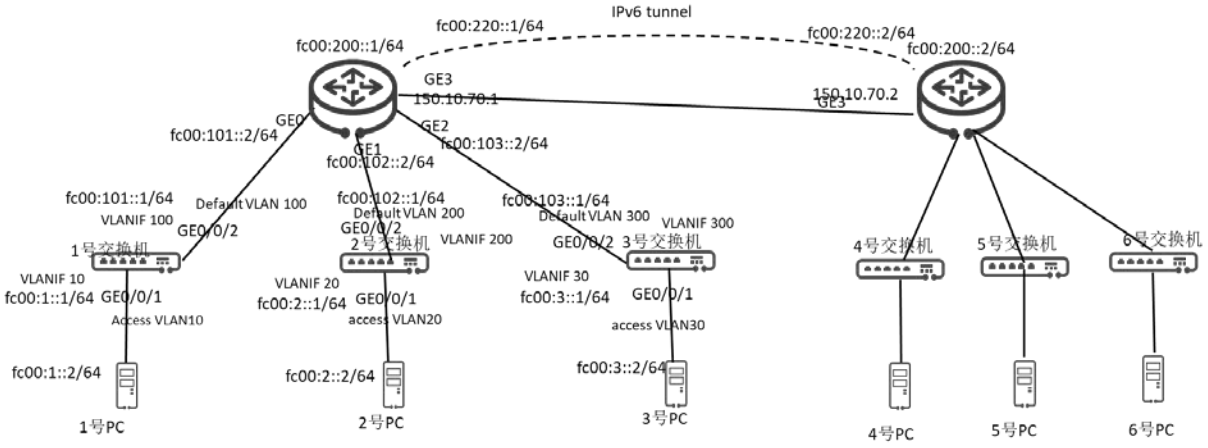
IPv6 过渡技术有多种，本实验验证 IPv6 over IPv4 隧道技术中的手工隧道技术

5.4.2 实验任务

完成岛内两组 IPv6 组网间的 IPv6 over IPv4 隧道。

5.4.3 实验组网

岛内两组 AR 间启用 IPv6 over IPv4 隧道。



5.4.4 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
```

2) 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
```

3) AR2 路由器增加 Ipv6 隧道, 入隧道路由

类似配置，这里不做描述

4) 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
```

5.4.5 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

6 实验任务 5：VPN(高阶)

6.1 实验介绍

6.1.1 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：

6.1.2 实验目的

- 掌握 IPsec VPN 原理和配置。
- 掌握 BGP/MPLS VPN 的原理和配置

6.2 IPSec VPN 配置(高阶)

6.2.1 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。

6.2.2 实验任务

1）岛内两小组 AR 路由器与互相建立 IPSecVPN

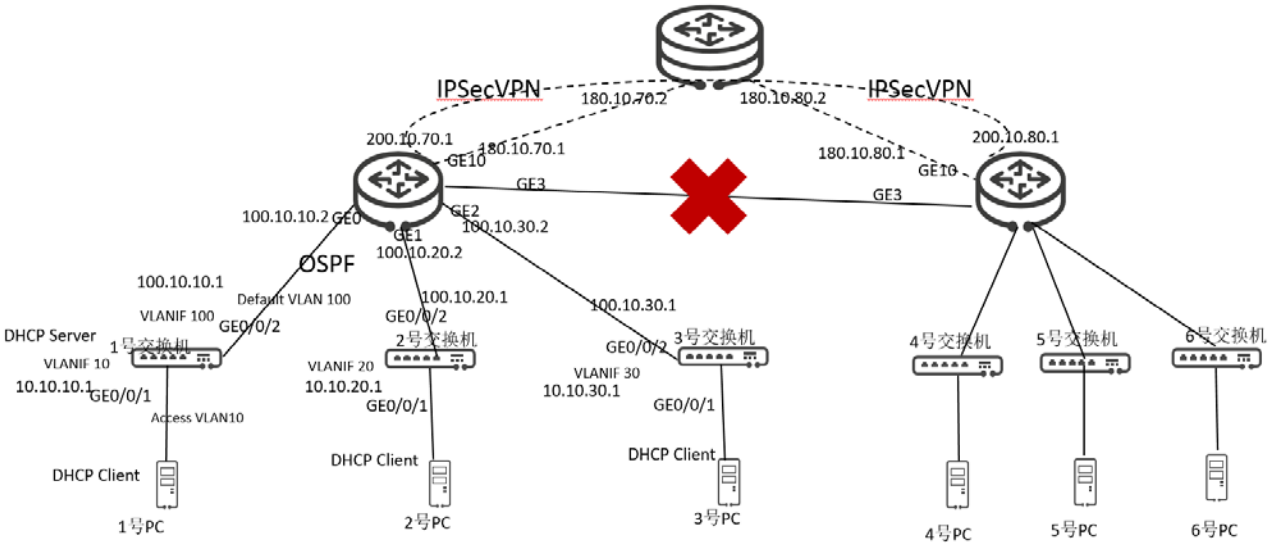
核心路由器 接口地址、路由器配置已经完成，各组不需要参与。

2）各 PC 间能够互通

3）从转发原理中理解 IPSec VPN 的配置模型

6.2.3 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



6.2.4 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
```

2）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
```

3）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
```

4）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

5）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
```

6）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
```

6.2.5 实验验证

1）验证 IPSecVPN 是否建立成功。

```
display ipsec sa
```

2）验证两个小组间 PC 机能够互通。

6.3 BGP/MPLS VPN(高阶+)

6.3.1 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。

6.3.2 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。

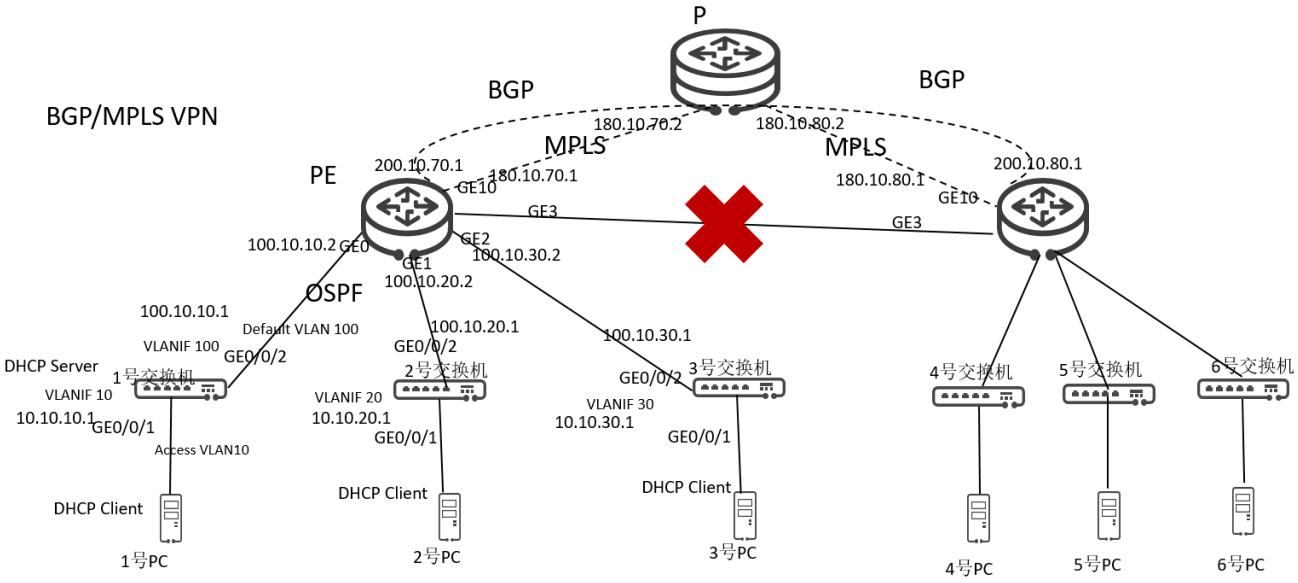
2）岛内交换机作为 CE 设备，与 PE 间发布内网路由

3）两组 PC 能够互通

4）从转发原理中理解 BGP/MPLS VPN 的模型

6.3.3 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



6.3.4 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
```

2） 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
```

3） 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
```

4） 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
```

5）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
```

6）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
```

7）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
```

6.3.5 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。

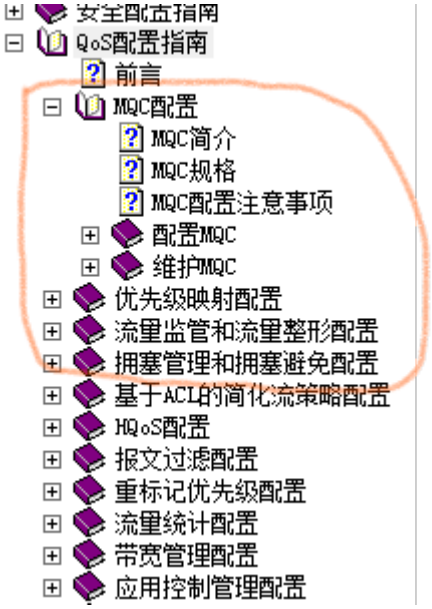
7 实验任务 6：Qos 配置

7.1 实验介绍

7.1.1 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：



7.1.2 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。

7.2 MQC 原理和配置方法

7.2.1 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。

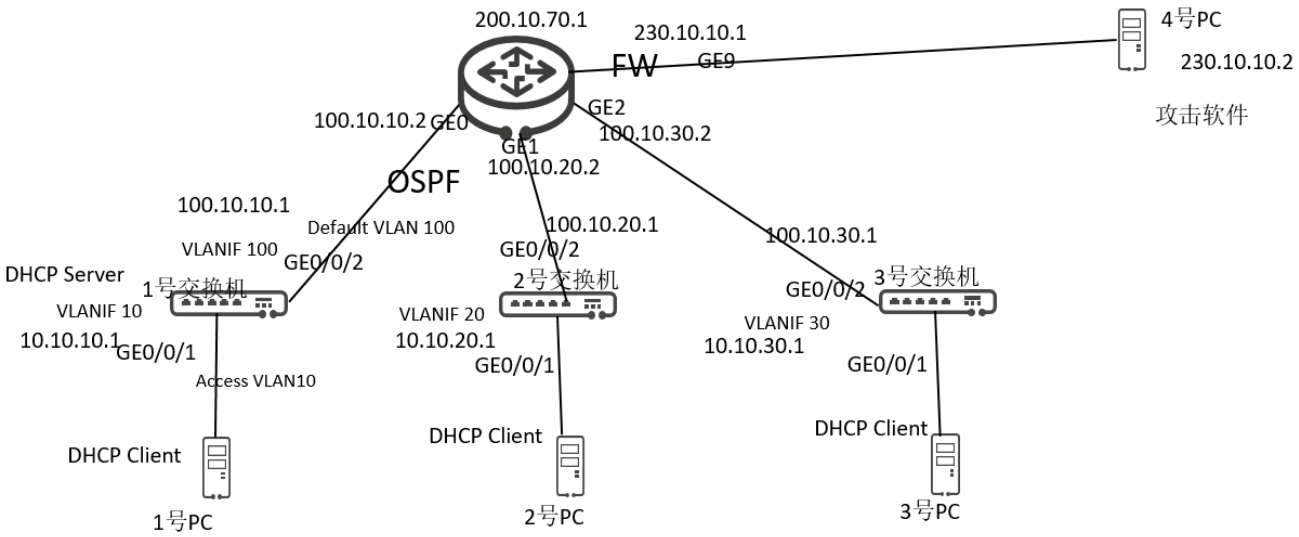
随着网络中 QoS 业务的不断丰富，在网络规划时若要实现对不同流量（如不同业务或不同用户）的差分服务，会使部署比较复杂。MQC 的出现，使用户能对网络中的流量进行精细化处理，用户可以更加便捷的针对自己的需求对网络中的流量提供不同的服务，完善了网络的服务能力。

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

7.2.2 实验任务

使用 MQC，统计各位同学的报文发送个数。

7.2.3 实验组网



7.2.4 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

a) 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
```

b) 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
```

2) 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
```

3) 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
```

4) 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
```

7.2.5 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/
```

7.3 流量监管和流量整形

7.3.1 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

7.3.2 实验任务

调整每台 PC 允许的最大带宽，观察流量限制情况

7.3.3 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。

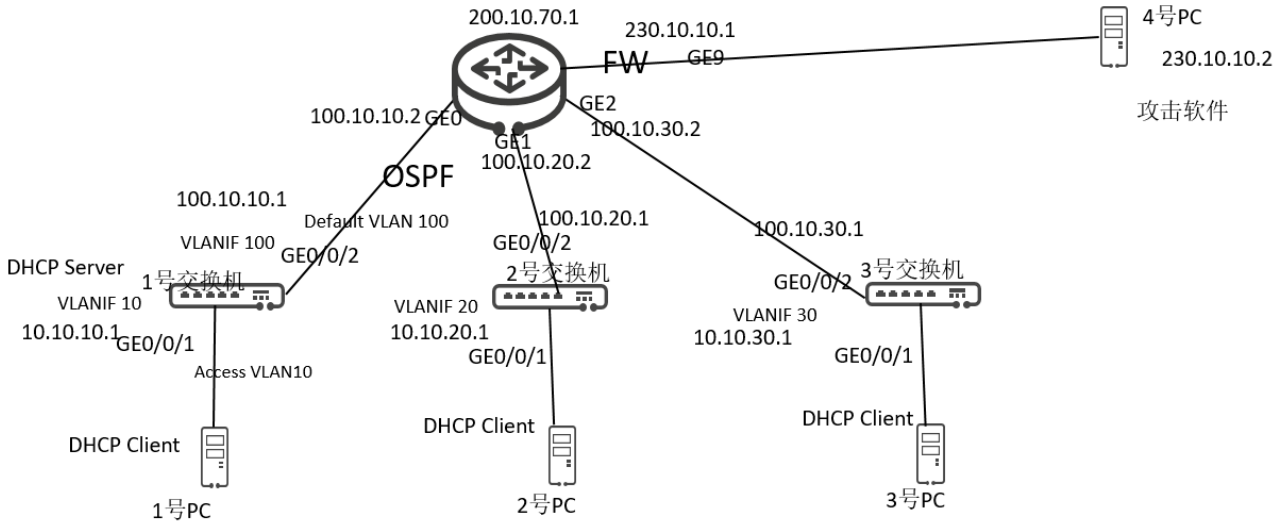


图7-1 物理环境组网

7.3.4 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

a) 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
```

b) 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
```

2) 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
```

3) 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
```

4) 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
```

7.3.5 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
```

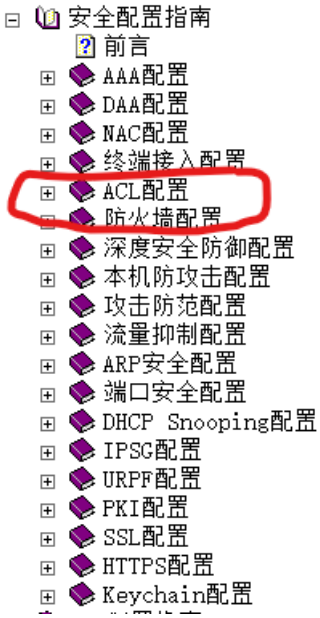
8 实验任务 7：IP 安全配置

8.1 实验介绍

8.1.1 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：



8.1.2 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。

8.2 ACL 配置

8.2.1 基于 IP 地址 ACL 配置

8.2.1.1 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。

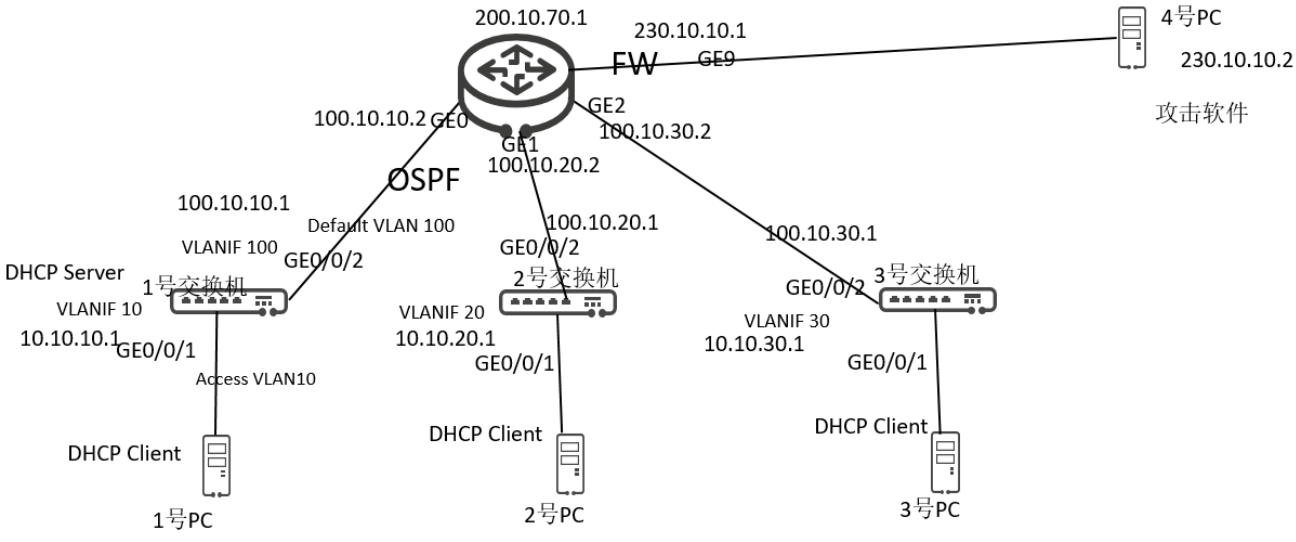
ACL 本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用 ACL 的业务模块的处理策略来允许或阻止该报文通过。

8.2.1.2 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

8.2.1.3 实验组网



8.2.1.4 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，：

C） 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
```

D）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
```

8.2.1.5 实验验证

2） 验证 PC 间是否能够 ping 通

3） 验证 10.10.20.1 是否能够 ping 通

8.3 防火墙配置(高阶)

8.3.1 内外网隔离

8.3.1.1 说明

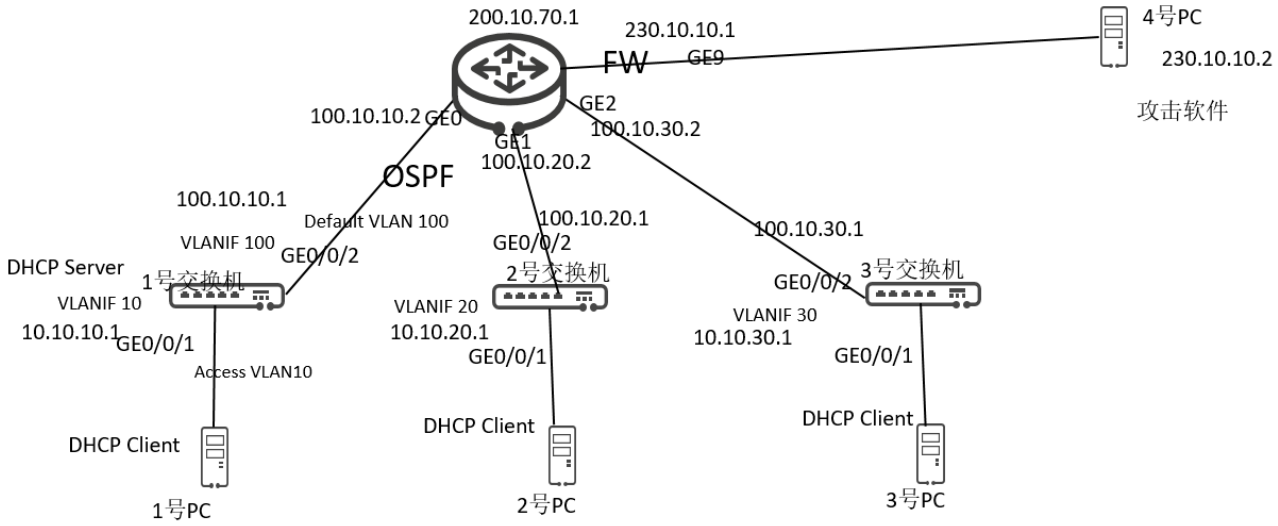
防火墙（Firewall）是一种隔离技术，使内网和外网分开，可以防止外部网络用户以非法手段通过外部网络进入内部网络，保护内网免受外部非法用户的侵入。

8.3.1.2 实验任务

配置防火墙业务，防范外网对内网环境的攻击

8.3.1.3 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。



8.3.1.4 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

2）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
```

3）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
```

8.3.1.5 实验验证

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

8.3.2 攻击防范

8.3.2.1 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。

8.3.2.2 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

8.3.2.3 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

9 实验任务 8：WLAN 配置

9.1 实验介绍

9.1.1 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：

9.1.2 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

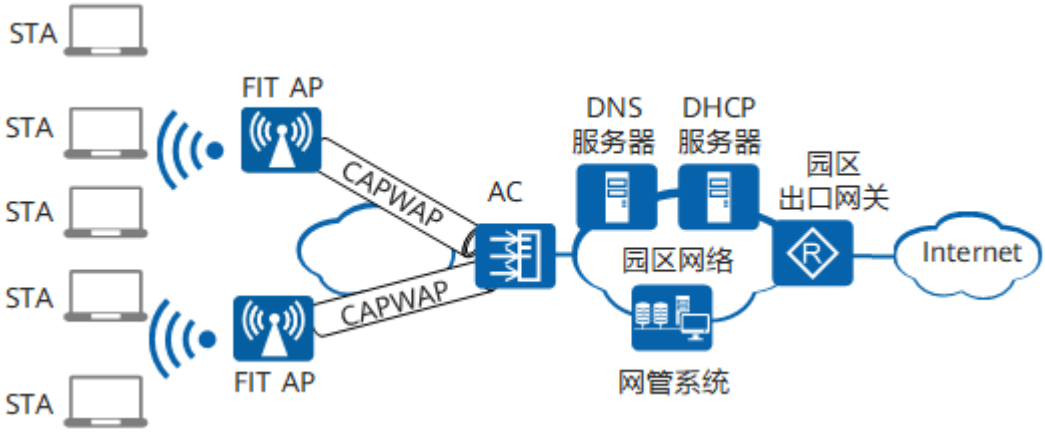
9.2 WLAN 网络架构&AP 接入网络

9.2.1 WLAN 网络架构

9.2.1.1 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。

9.2.2 AP 接入网络

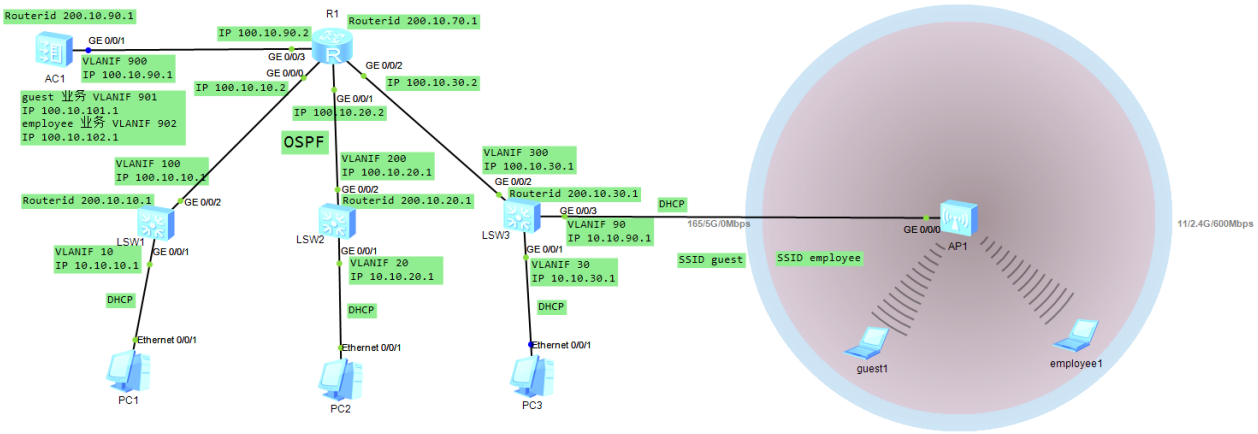
9.2.2.1 说明

本实验完成 FIT AP 接入网络过程

9.2.2.2 实验任务

AP 通过 CAPWAP 隧道接入 AC：

9.2.2.3 实验组网



9.2.2.4 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

2) 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
  #
```

3) 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
```

9.2.2.5 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

9.3 终端接入网络

9.3.1 终端接入网络

9.3.1.1 说明

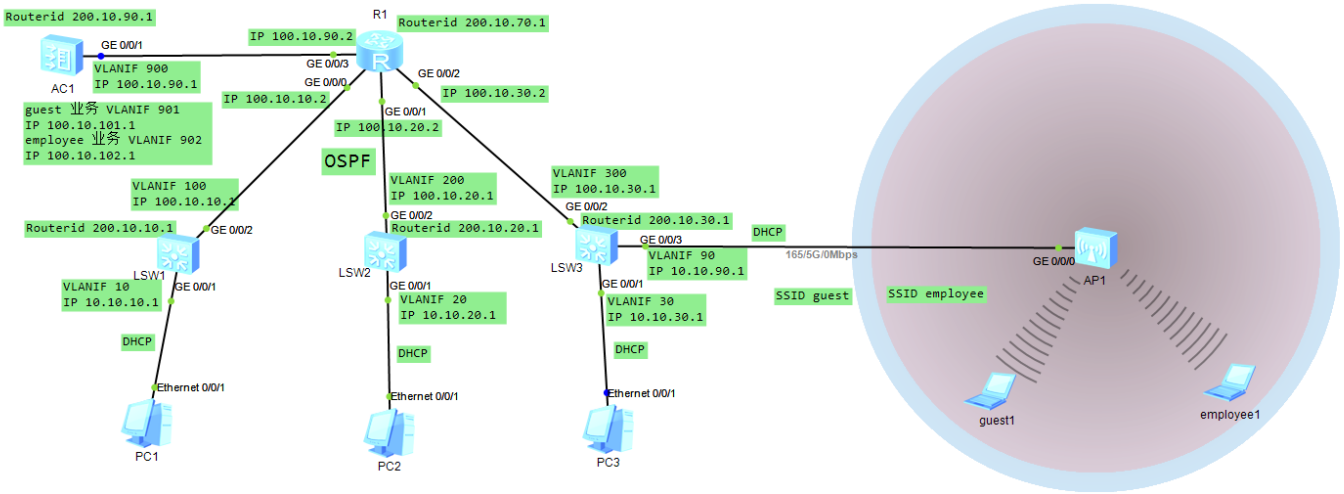
网络中会部署多个 SSID，提供不同服务。同时为了保证接入安全，需要配置不同的安全策略。

9.3.1.2 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。

9.3.1.3 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。



9.3.1.4 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
```

2）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
```

3）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
#
```

4）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
```

9.3.1.5 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
```

2) Guest1 PC 能够访问 1 号 PC

3) Guset1 PC 能够访问 employee1 PC

10 综合实验：校园园区网搭建（高阶+）

10.1 实验介绍

10.1.1 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。

10.1.2 实验目的

- 综合运用网络技术，实践网络工程能力

10.2 校园园区网搭建

10.2.1 实验介绍

10.2.1.1 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。

10.2.1.2 实验任务

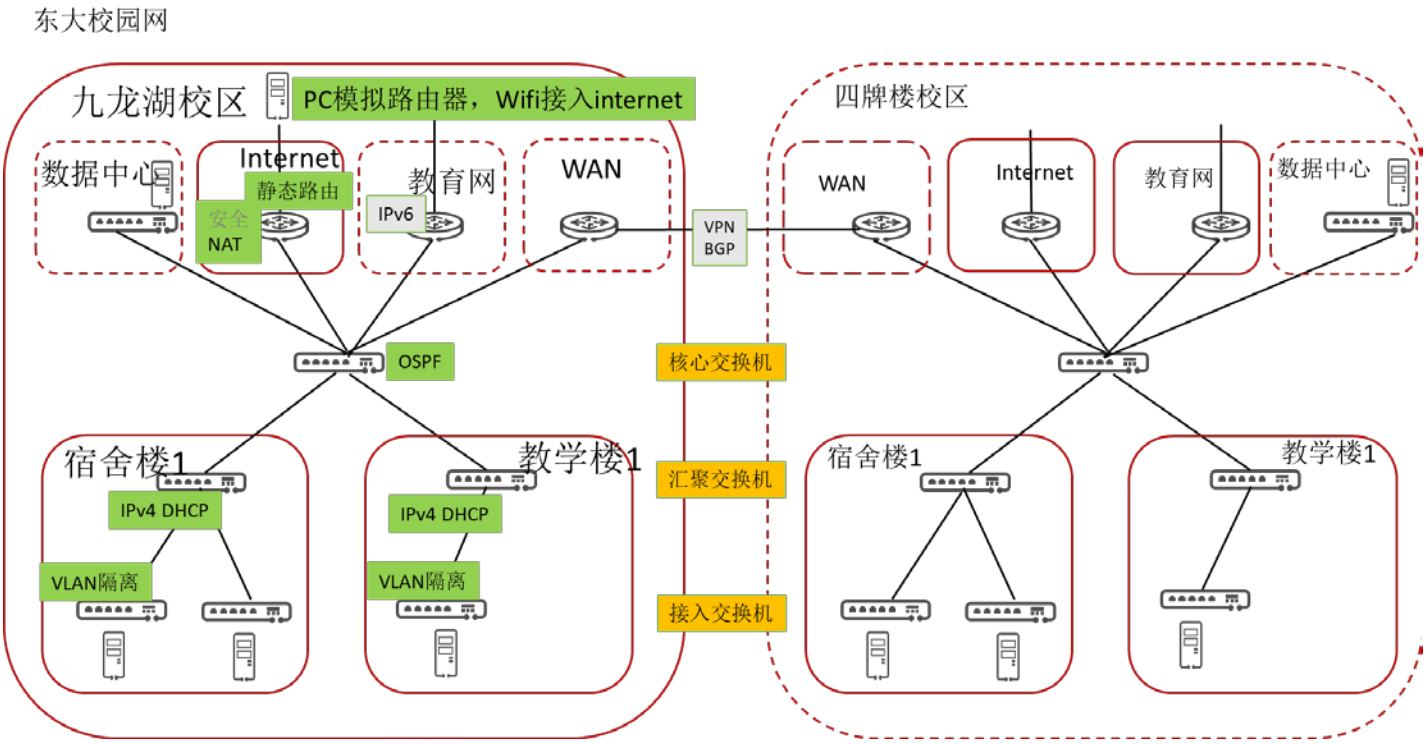
需要同学们规划一张网络，要求：

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

10.2.1.3 实验组网



实线范围内 绿色部分是需要实验的部分

10.2.1.4 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)

10.2.1.5 实验验证

1) 各区域 PC 能够互 ping 通
2) 可访问 Internet

11 实验环境使用建议

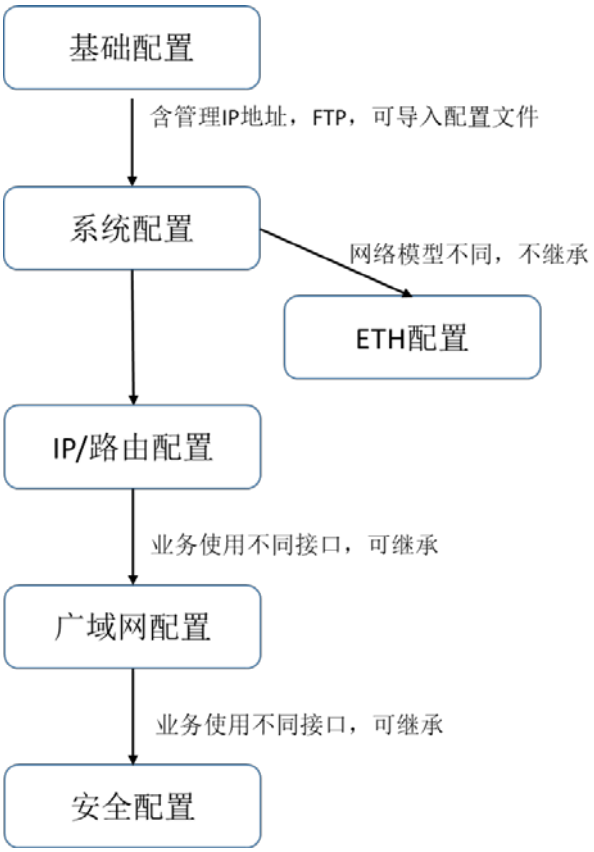
11.1 说明

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。

11.2 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。

2）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

11.3 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

11.3.1 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
```

2）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
```

11.3.2 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

11.3.3 恢复配置文件

3）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
```

4）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

5）重新启动，变更启动的配置

<Huawei>reboot fast

6）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

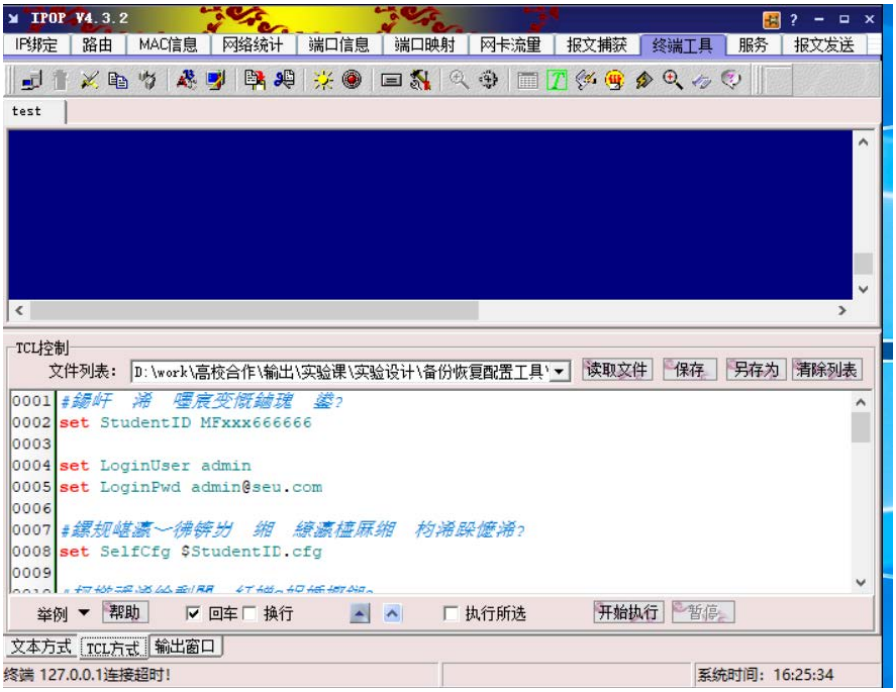
Startup patch package: null

Next startup patch package: null

Startup voice-files: null

Next startup voice-files: null

11.3.4 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