



**课程报告**

课程名称 生产实习

学生学院 自动化学院

专业班级 15级物联网工程四班

学 号 3115001475

学生姓名 林 国 志

指导老师 孙为军 黄永慧 钟灵 王春茹

2018年9月

**目录**

[1 设计原则 1](#_Toc9502_WPSOffice_Level1)

[1.1功能性设计 1](#_Toc13046_WPSOffice_Level2)

[1.2安全性设计 2](#_Toc9502_WPSOffice_Level2)

[2 系统设计 2](#_Toc14665_WPSOffice_Level1)

[2.1系统构成拓扑图 2](#_Toc14665_WPSOffice_Level2)

[2.2 vlan划分 2](#_Toc6287_WPSOffice_Level2)

[2.2.1概述 2](#_Toc13046_WPSOffice_Level3)

[2.2.2原理与部署 3](#_Toc9502_WPSOffice_Level3)

[2.3 trunk中继 4](#_Toc21594_WPSOffice_Level2)

[2.3.1背景 4](#_Toc14665_WPSOffice_Level3)

[2.3.2原理 4](#_Toc6287_WPSOffice_Level3)

[2.4三层交换机 4](#_Toc19795_WPSOffice_Level2)

[2.4.1背景 4](#_Toc21594_WPSOffice_Level3)

[2.4.2代码部署 5](#_Toc19795_WPSOffice_Level3)

[2.5局域网通信 6](#_Toc29130_WPSOffice_Level2)

[2.5.1 概述 6](#_Toc24001_WPSOffice_Level3)

[2.5.2 NAT地址翻转 6](#_Toc14508_WPSOffice_Level3)

[3 项目成果 8](#_Toc6287_WPSOffice_Level1)

[4 心得体会 8](#_Toc21594_WPSOffice_Level1)

[5 致谢 8](#_Toc19795_WPSOffice_Level1)

**中小型校园网的安全设计与部署**

林国志 指导老师：陈鑫杰

（广东工业大学自动化学院物联网工程15级4班 ）

**摘 要：**本项目以网络和安全为出发点，通过合理的规划和代码部署，搭建一个能与外网联通的校园网系统。该项目运用了包括设备安全管理、路由协议、交换技术、安全策略等大量的实际知识点。

**关键词：**校园网 安全设计 安全访问

**Safety Design and Deployment of Small and Medium-sized Campus Network**

**Abstract:** This project takes network and security as the starting point, and builds a campus network system that can connect with external network through reasonable planning and code deployment.This project USES a lot of practical knowledge, including equipment security management, routing protocol, switching technology, security policy and so on.

**Key words:** Campus network Safety design Security access

# 1 设计原则

**1.1功能性设计**

1. 校园网内各主机之间能相互通信，并且能访问外网；
2. 根据不同部门的不同需求，将上网流量划分开来，互不干扰；
3. 满足各种流媒体的无障碍传输，保证校园网各种应用畅通无阻。

**1.2安全性设计**

（1）能够实现广播域隔离以防止广播“风暴”并实现局域网内部安全互访；

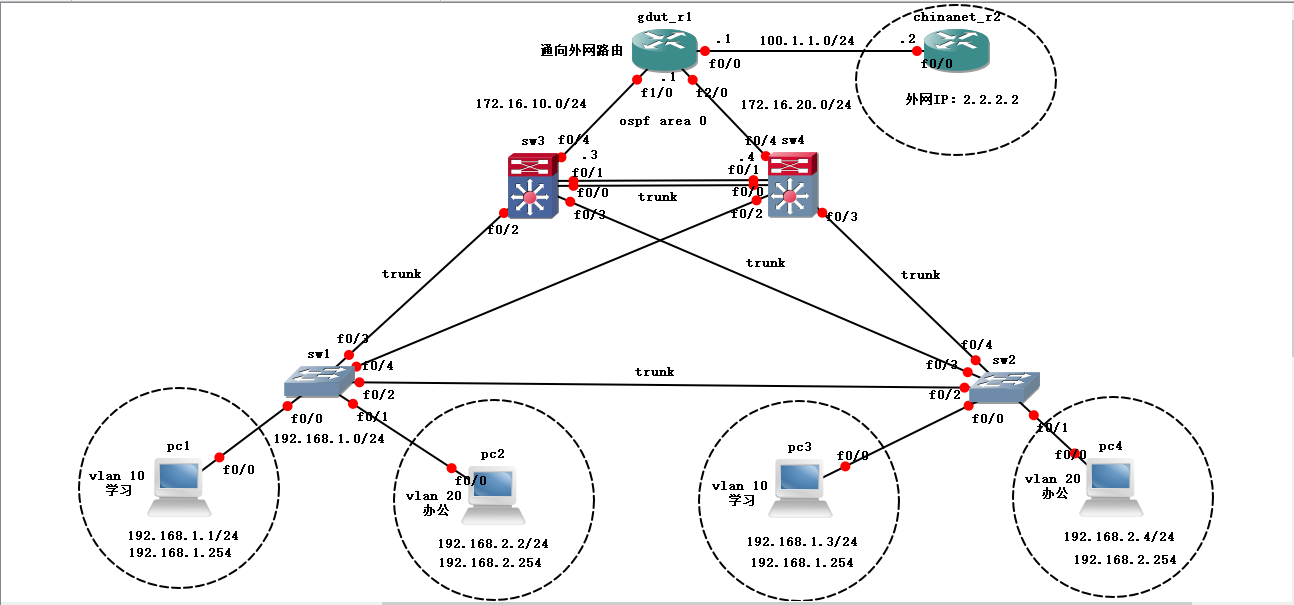
（2）能实现多出口环境下的路径选择，当主路径出现故障后，流量能够自动切换到备用路径，防止单点故障，提高链路的容错率；

（3）能够实现访问控制，非授权用户只能访问特定的网络资源，保证内网的安全。

# 2 系统设计

**2.1系统构成拓扑图**

根据设计的理念，搭建该校园网系统的拓扑图，如下：



**2.2 vlan划分**

2.2.1概述

Virtual LAN，虚拟局域网，可以用于实现广播域隔离并且实现局域网内部安全互访。

VLAN是一个2层接口组成的集合，它具有以下特性：

（1）每个VLAN可包含多个2层口，其中可以有Access接口，也可以有Trunk接口。

（2）每个Access接口只能属于一个VLAN（默认是VLAN1），它只能转发属于同一个VLAN的帧。

（3）Trunk接口可同时属于多个VLAN（默认是所有VLAN），它可以转发属于不同VLAN的帧。

（4）每个VLAN用一个整数标识，称为VLAN ID，取值范围为1~1007（有些交换机的取值范围可以更大）。

（5）初始时，交换机已经定义了一个ID为1的VLAN，所有物理接口默认属于这个VLAN。

（6）属于同一个VLAN的接口可以相互通信，属于不同VLAN的接口间不能通信。

2.2.2原理与部署

查看VLAN

SW1#show vlan-switch brief //查看交换机本地VLAN信息

（默认交换机有1，1002-1005几个vlan，所有接口默认处于VLAN1）

创建VLAN

SW1#vlan database //进入VLAN数据库

SW1(vlan)#vlan 10 name XZ //创建VLAN并给名字

SW1(vlan)#vlan 20 name SJ

SW1(vlan)#exit //保存并退出

将接口放入特定的VLAN

SW1(config)#int range f0/0

SW1(config-if-range)#switchport mode access //设置为主机访问接口

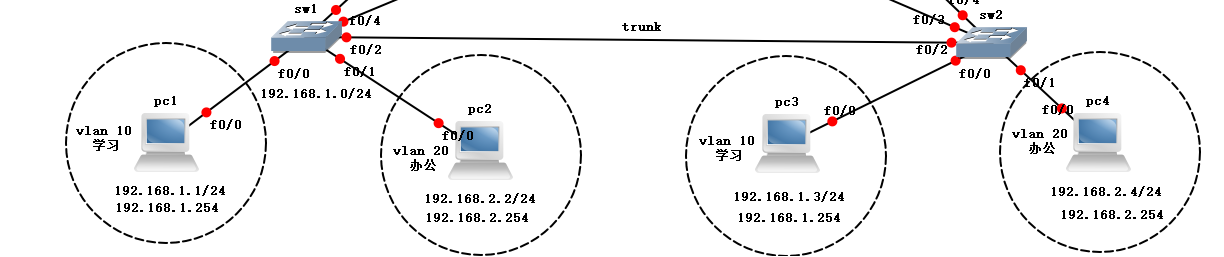
SW1(config-if-range)#switchport access vlan 10 //划入具体的VLAN

SW1(config)#int f0/1

SW1(config-if)#switchport mode access

SW1(config-if)#switchport access vlan 20

如下图所示，将pc1和pc3划入vlan 10，将pc2和pc4划入vlan 20，这样就将学习和办公的主机群相互隔离开来，如果数据包没有携带三层交换机给予的vlan标记，那么不同的vlan之间是不能传递数据包的，即无法通信。这样的优点在于，假若该局域网某个vlan内的主机遭受广播“风暴”的干扰，那么该局域网的其他vlan内的主机是不受影响的。这样的设计思路符合安全策略，即使一个vlan受到网络攻击而崩溃，也不至于导致整个局域网全盘崩溃。



**2.3 trunk中继**

2.3.1背景

通过vlan技术我们能够有效地防范广播“风暴”的诸多影响，但实际上我们又得解决另一个问题：每个VLAN对应一个网线/链路/接口，这样比较消耗交换机的接口资源，即N个VLAN 需要N根网线。当局域网内的主机群十分庞大的时候，交换机数量也比较多，采用VLAN技术，我们将要付出很大的代价，这是不实际的。所以谈到VLAN技术，我们也得提及另一个技术--trunk。

2.3.2原理

Trunk技术的出现能有效地解决这个问题，即使有N个VLAN使用一根网线也足以，这是因为trunk技术可以同过打标签的方式承载不同VLAN的流量，不同的VLAN流量在同一根网线内传递也不会相互冲突。代码部署如下：

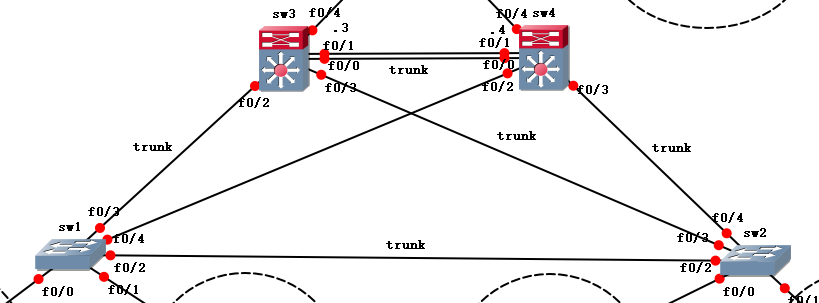
SW2(config)#in f0/2

SW2(config-if)#switchport trunk encapsulation dot1q //定义封装标准

SW2(config-if)#switchport mode trunk //开启TRUNK

SW2#show interfaces trunk //查看TRUNK信息

SW1(config)#default int f0/10 //清除接口配置

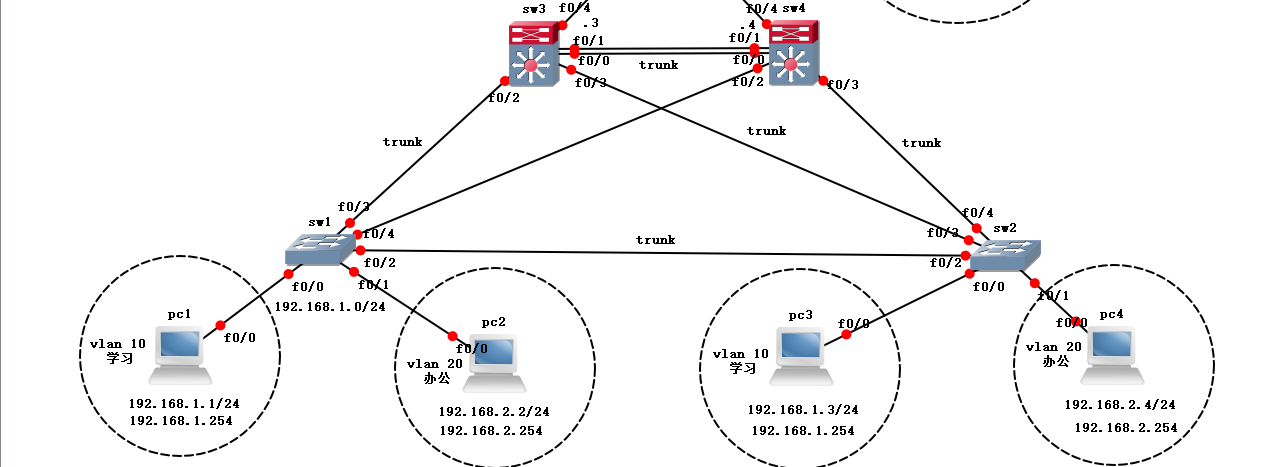


从上图可以看出，在各个交换机之间都部署了trunk技术，既保证了通信之间的顺畅，又大大节省了成本。

**2.4三层交换机**

2.4.1背景

上面已经提到，出于安全和管理方便的考虑，主要是为了减小广播风暴的危害，使用VLAN技术把局域网按功能或地域等因素划成一个个小的局域网，而各个不同VLAN间要经过路由器才能完成通信，这将导致大量的网际互访,单纯地使用二层交换机是不能实现网际互访的。但是如果单纯使用路由器的话,由于接口数量有限和路由转发速度慢,将限制网络的速度和网络规模,所以我们可以采用具有路由功能的快速转发的三层交换机。



以上图为例，sw1和sw2是二层交换机，sw3和sw4是三层交换机，若vlan 10 的pc1想和vlan 20 的pc2通信，仅通过二层交换机sw2是无法实现的，必须要通过具有路由功能的三层交换机sw3或sw4才可实现。顺便一提，sw4是备用交换机，是用来防止出现单点故障的，若sw3不幸发生故障，数据流会通过sw4进行转发，以保障网络畅通。

2.4.2代码部署

主机配置：

配置网关

方法一：

no ip routing

ip default-gateway 192.168.20.254

方法二：

Ip route 0.0.0.0 0.0.0.0 192.168.10.254

路由器配置：sw3->sw1

sw3(config)#ip routing //开启路由功能

sw3(config)#int f0/0

Sw3(config-if)#switchport mode trunk

Sw3(config)#int vlan 10

Sw3(config-subif)#ip address 192.168.10.254 255.255.255.0

Sw3(config-subif)#exit

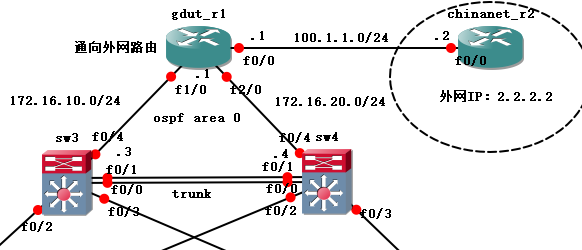
Sw3(config)#int vlan 20

Sw3(config-subif)#ip address 192.168.20.254 255.255.255.0

**2.5局域网通信**

2.5.1 概述

一个校园网系统如果仅仅实现内部通信，却不能与外网联通，我们将不能从万维网上获取信息资源，这样是不能满足需求的，所以我们需要把校园网这个局域网接入外网，以满足上网需要。



如图，为了能与外网通信，我们要设置一个通向外网的出口路由，可事情并没有那么简单，要想实现网络互访，这里得涉及到NAT地址翻转技术。

2.5.2 NAT地址翻转

NAT（Network Address Translation），网络地址翻转：将私有IP地址转换为公有IP地址，NAT一定放在校园网总出口路由。

1. 引入NAT原因：

　（1）ipv4地址严重不够用 ；

　（2）开发了私有IP：

　　10开头的、172.16-172.31开头的、192.168.开头 ；

　3）要求私有IP只能在内网使用，公网上不允许出现私有IP ；

　4）私有IP可以在不同的内网可以重复使用。

2、NAT分类：

　（1）静态NAT：一对一转换，适用于发布内网服务器，称为端口映射(服务器) ；

　（2）动态NAT：多对一转换，但不能同时转换（摒弃） ；

　（3）PAT：多对一转换，多个私有IP同时使用1个公网ip的技术（主流）；。

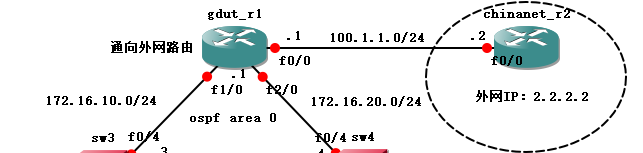
3、NAT原理：

　（1）NAT要求路由器设置内外网端口；

　（2）内网到外网的数据转换源IP ；

　（3）外网到内网的数据转换目标IP 。

4、动态NAT部署



①编写ACL匹配上网流量

access-list 1 permit 192.168.0.0 0.0.0.255

②编写NAT地址池

ip nat pool DAT 100.1.1.0 100.1.1.24 netmask 255.255.255.0

③定义内外接口

R1(config)#int f0/0

R1(config-if)#ip nat inside //内网

R1(config-if)#int f1/0

R1(config-if)#ip nat outside //外网

④执行NAT

ip nat inside source list 1 pool DAT //将内网IP翻转为外网IP

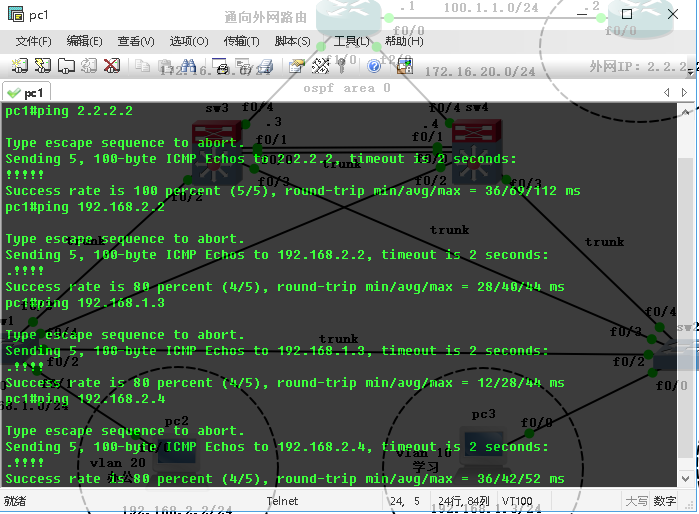
R1#show ip nat translations //查看NAT翻转表

R1#show ip nat statistics //查看NAT状态

R1#debug ip nat //调试NAT翻转

注意，编写ACL（Access Control Lis，t访问控制列表）上网匹配流量是为了保证内网的安全性，使得非授权用户只能访问特定的网络资源，从而达到对访问进行控制的目的。简而言之，ACL可以过滤网络中的流量，是控制访问的一种网络技术手段，可以提高校园网的安全性。

# 3 项目成果

以主机pc1来检验项目成果，分别ping外网地址2.2.2.2、主机pc2和pc3以及pc4的地址，从上图可以看出，都能成功ping通，说明该局域网的通信是没有问题的，也证明该项目成功了。

# 4 心得体会

短短几天，边学习边做项目，日子过得很紧凑，充实而不乏味。这几天真的学到了很多东西，因为给我们讲课的陈老师教学非常认真，善于举例，总能把理论知识与实际生活相结合，他的课趣味性十足，启发性很高，令人印象深刻。从基本的网络协议栈到网络上的各种“明争暗斗”，以各种生活实际案例揭露了网络环境上的尔虞我诈，令我涨了见识，开阔了视野，也更加了解了这个社会的真实，我受益良多。虽然在搭建校园网系统的过程中，我经常犯错，但解决这些问题后，对这些理论知识理解得更深刻了，也非常了解一个局域网的构成，积累了很多宝贵的经验，感觉这些天学有所值。

# 5 致谢

本论文是在导师孙为军、黄永慧、钟灵、王春茹、陈鑫杰的悉心指导下完成的,在论文的选题、撰写和定稿过程中,各位老师给我提出了许多宝贵的意见,而且很耐心的指出需要改进的地方以及微小的错误。各位老师兢兢业业的工作作风、严谨务实的教学风范、耐心的教导方式,给了我莫大的启迪和帮助。在此谨向各位老师表示衷心的感谢和诚挚的敬意!

最后对曾给予我鼓励和帮助的所有同学、朋友一并表示深深的感谢!