# 电子政务网的设计与项目实施毕业论文

## 目录

## 目录

# 第 1 章　绪论

## 1.1 选题背景

由于企业的业务和网络的需求都在变得日趋复杂，因此，某种特定的网络模型已无法满足企业园区网络在功能和服务方面的需求。设计一个企业园区网无异于设计一个大型综合系统，所以，设计人员必须依据工程方面的一些根本原则，才能确保其设计的网络在可用性，安全性，灵活性和可管理性方面，都能够满足今后的业务和技术需求。为了简化园区网的架构，本文采用了园区网设计方案中的分层模型。这种模型可以提供一个模块化的框架，使网络设计变得更加灵活，实施和排错变得更加轻松。

为了比较系统地对学习过的知识和技能进行再复习，我全心全意地写下了这篇毕业论文。了解过情况的人就会知道，社会对个人的工作经验比较看重，如果只有纸面上的功夫会显得很苍白，所以，本论文将结合荔湾区电子政务外网的改造项目来讲述成功部署园区网络的设计和实施流程。以网络规划和设计的理论为基础，结合本次实习期间所得的项目实施经验，促使自身综合技能的提升，从而拥有更强的竞争力为以后的事业做好铺垫。

## 1.2 内容提要

本文主要包括一下内容：

1.从选题背景出发，讲述了园区网的设计的原则和设计中使用的分层模型，还对园区网的发展趋势做了分析。

2.以荔湾区电子政务外网项目为背景，展示园区网设计的内容，包括需求分析，通信规范，逻辑网络设计和物理网络设计。还通过网络测试实现对项目的验收。

## 1.3 论文结构

全文分为6章，第1章是绪论部分，第2至4章为主体，第5章是结束语，第6章是参考文献。

第1章：绪论。介绍了本论文选题的背景和内容的提要

第2章：园区网设计概述。包括讲述园区网设计中需要遵循的几点原则，还有设计中采用了分层设计的理念。

第3章：荔湾区电子政务外网设计方案。以这个项目的设计为背景展开了几大方面的设计，包括需求分析，通信规范等。其中逻辑网络设计介绍了拓扑，生成树，vlan的规划，路由协议的选择。物理设计介绍了设备的安装规范和选型等内容。

第4章：网络测试。测试网络的连通性和可靠性。

第5，6章分别是结束语和参考文献的索引。

# 第 2 章　园区网设计概述

## 2.1 园区网的设计原则

如果园区架构设计合理的话，那么网络应该是模块化的，是可以快速复原的，而且它的灵活性很强。设计优良的园区架构不仅节约时间，节省成本，而且还可以简化 IT 工程师的工作，并且能够让企业务量显著提高。要设计出具有上述特性的园区网，就要了解一些设计原则和方法：

- **模块化：**根据模块化方式设计出来园区网更容易扩展和修改。当相关人员在对网络进行扩展时，只需为网络添加新的模块即可，而无需从新设计一个新的网络。
- **快速修复：**网络短时间的中断就可能影响大量业务，造成重大损失。设计园区网的理想目标应该是接近 100%的时间里网络都可以正常工作的。也就是实现网络的高可用性。
- **灵活性：**业务上的变化旨在确保企业能够适应市场的发展。随着企业自身业务的发展，企业单位对网络的需求也不断发展。所以要求设计的园区网能够快速适应将来网络的新需求。

## 2.2 园区网设计中的分层模型

和 OSI(开放系统互联)参考模型的目的一样，为了帮助大家理解计算机之间的通信任务，园区网中也采用了分层的做法。由于分层模型中的每一层都只关注一个特性的功能，因此网络设计师就可以更轻松地为每一层选择最为合适的系统和特性。这种模型可以提供一个模块化的框架，使网络设计变得更加灵活，实施和排错变得更加轻松。

园区网架构可以将网络中的模块化区域从根本上氛围三个层面，即接入层，汇聚层和核心层，这三个层面分别具有一下特点：

- **接入层**：用来使用户，服务器或边缘设备能够访问网络。在园区网设计方案中，接入层交换机一般包含为工作站，服务器，打印机，无线接入点等设备提供连接端口的交换机。
- **汇聚层**：位于接入层和核心层之间，充当服务和控制的边界。出于安全性原因对资源访问的控制，出于性能原因对通过核心层流量的控制等都在汇聚层。
- **核心层**：高速的骨干旨在以最快的速度交换数据包。在当代园区网设计方案中，核心骨干必须使用至少万兆的以太网链路来与其它交换机建立连接。由于核心层对于网络连通性来说是最为关键的一层，所以它必须提供最高级别的可用性，并且必须能够最快地适应网络的变化。

当我们将分层模型应用在模块化的园区网设计方案后，网络可以概括为图 2-1 所示示的拓扑。

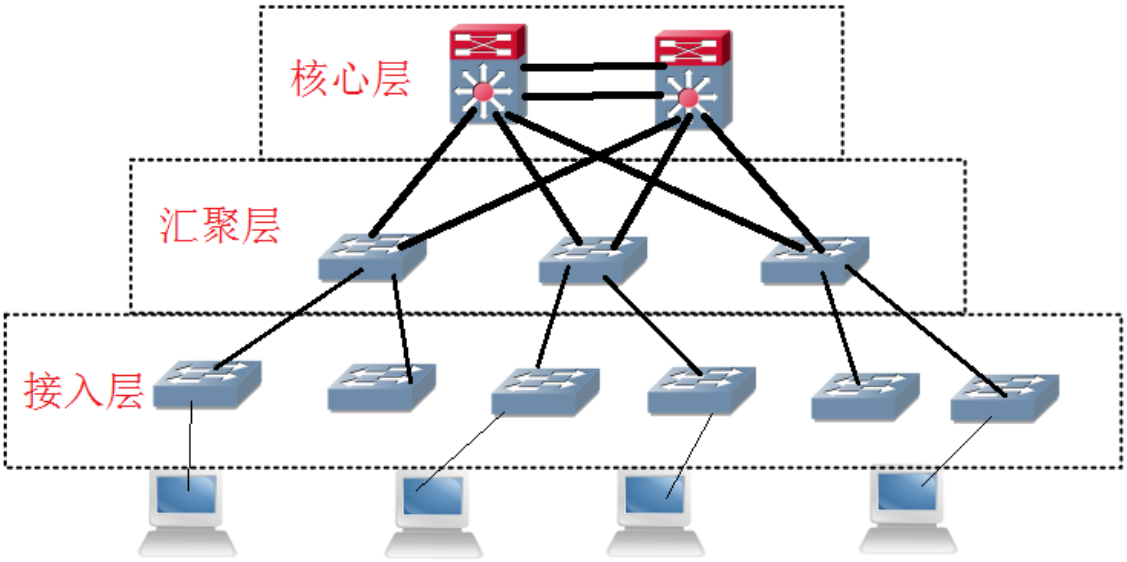


图 2-1 分层模型应用于园区网的示意图

## 2.3 多层交换机对园区网发展趋势的影响

二层交换机根据 MAC 地址进行交换，由于众多的因素，传统的二层交换机受到网络扩展性的限制。第二层交换机会在整个广播域中泛洪未知的单播帧，组播和广播流量，广播域内的所有网络设备都要处理这些不必要的流量，这样就导致了网络拓扑中的二层交换机数量不能太多。三层交换是基于硬件的路由选择，通过提供路由表，

三层交换机克服了二层设备扩展性不足的缺点。

多层交换将二层交换和三层路由选择的功能结合起来了。多层交换机不进能够对园区网络中的通信流量进行线速转发，而且还能够满足第三层的连通性要求。从设计的角度上看，所有企业园区设计方案都在某些地方包含了多层交换机，尤其是在网络的核心层和汇聚层部分。有些企业网的设计方案甚至在接入层上完全使用第三层交换技术，以便未来在各个接入端口上支持第三层网络端口。在以后的几年中，园区网的发展趋势是成为一个由廉价的三层交换机所构成的纯三层环境。

下一章将结合实习期间参与的荔湾区政务外网项目做一个园区网的设计。

# 荔湾区电子政务外网项目设计方案

3 月曾到锐捷网络公司参与广州市荔湾区电子政务外网项目的实施，在项目组里担当了一名售后工程师。实习的时间虽不长，但是我以抱着认真对待工作的态度在工作中获得了不少实战经验，对社会工作有了更深刻的体会，逐步摆脱那种毫无工作经验的学生模样。借此次毕业论文的机会，让我仔细回顾这次项目实施的过程，同时也等于对相关的网络技术进行了一次总复习。

## 3.1 需求分析

荔湾区电子政务外网是属于广州市荔湾区政府的，主要用于区政府下属的部门之间的自动化办公系统和访问互联网。整期工程完成后，将有 300 多个终端设备使用该网络，所以这是一个中型的园区网络。

该项目分两期实施，第一期为迁移一期，是网络割接，共有 90 个点需从原来使用的 MPLS 网络迁移到本项目新建的裸光纤网。第二期为新建二期，在第一期完成的基础上，新增 205 个点。

迁移一期共有 90 个实施点，分别位于广州市荔湾区科技和信息化局，疾控中心，劳动局，区就业中心，卫生监督所等 13 个职能部门。该网络有 6 个汇聚点，分别是荔枝湾，观绿，西华，花地，芳村，流花。核心交换机位于中山七区府 8 楼机房。该园区网的需求包括：

■迁移一期 90 个街道办事处保证每个街道办迁移过程中 IP 不更改，断网时间在半小时内；

■新建二期 205 个街道办事处由于是新建网络，没有断网要求；

■使用该网络的客户都能够登录内部的办公系统和访问互联网。

原有的 MPLS 网络在迁移之前正常使用，等待新建成的裸光纤网通过测试后，再把 90 个点迁移到新的交换机上，从而使用户平稳而快速地切换到新建的光纤网络。

## 3.2 通信规范

各层中的流量模式和流量类型对于打造园区网设计方案来说至关重要。每种类型的流量都代表一种特定的需求，比如带宽和流模式等。网络中的流量类型包括但不限于这些：网络管理，语音，IP 组播，一般数据。通信模式可以分为三类：

■点到点的应用。即大量的网络流量都从一台终端设备通过企业网发往另一台设备。

■客户端/服务器应用。用户访问数据中心服务器组中的应用时。客户端/服务器集群应用有一个 20/80 原则，也就是 20%的流量会留在本地 LAN 网络，而 80%的流量都会离开本地网络并去往中心服务器，Internet 等。

■客户端/企业边缘应用。通俗地说就是上外网，企业内部的终端访问外部的公共服务器。

经过咨询和了解，荔湾区电子政务外网（以后简称政务外网）的通信流量分布符合 20/80 原则，流量类型中，一般数据占据的比较多，而一般数据所占据的带宽属于中低级别。

## 3.3 逻辑网络设计与实施范例

逻辑网络设计工作主要包括：

- 网络结构的设计
- 局域网技术选择与应用
- IP 地址设计和命名规范
- 路由选择协议
- 网络安全

其中，局域网技术的选择主要包括生成树协议和 VLAN。

### 3.3.1 拓扑介绍

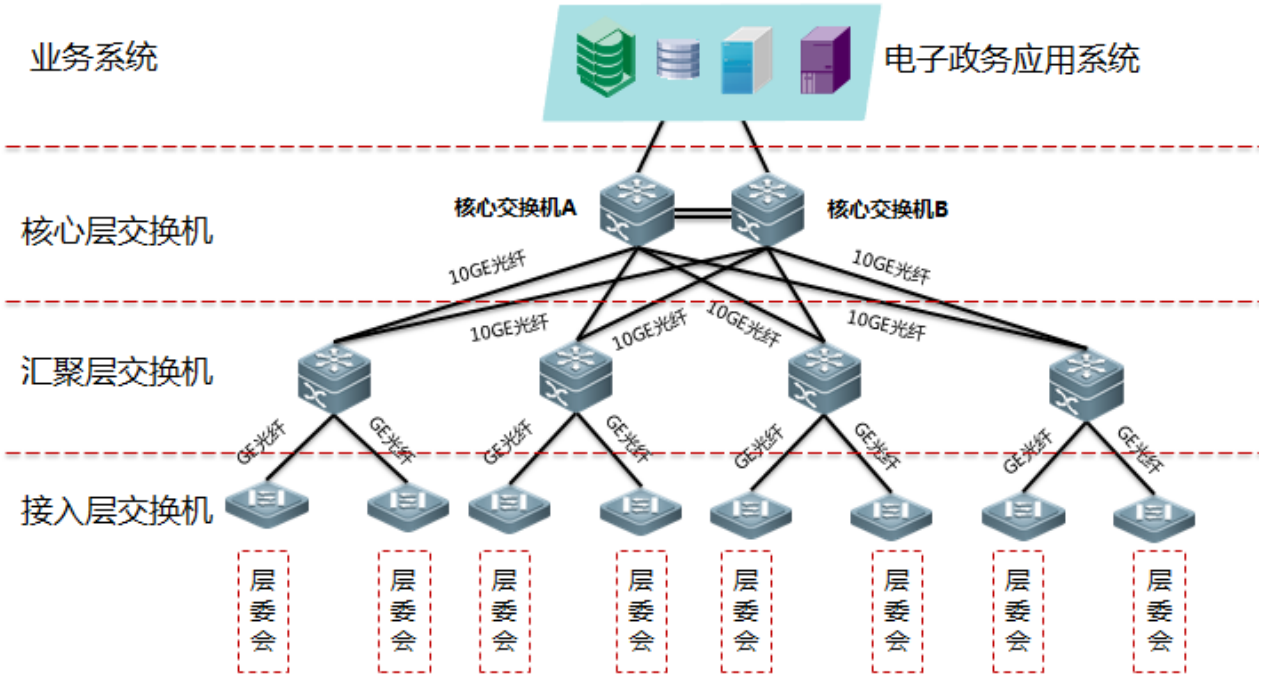


图 3-1 荔湾区电子政务外网拓扑

设计采用了核心、汇聚、接入三层架构设计。核心和汇聚之间使用全万兆光纤链路，双上联，全冗余连接，汇聚与接入之间全千兆光纤链路。构成核心到汇聚万兆双链路骨干，汇聚到接入千兆链路的高性能三层架构网络。各核心交换机和汇聚交换机均配置双电源、双引擎。

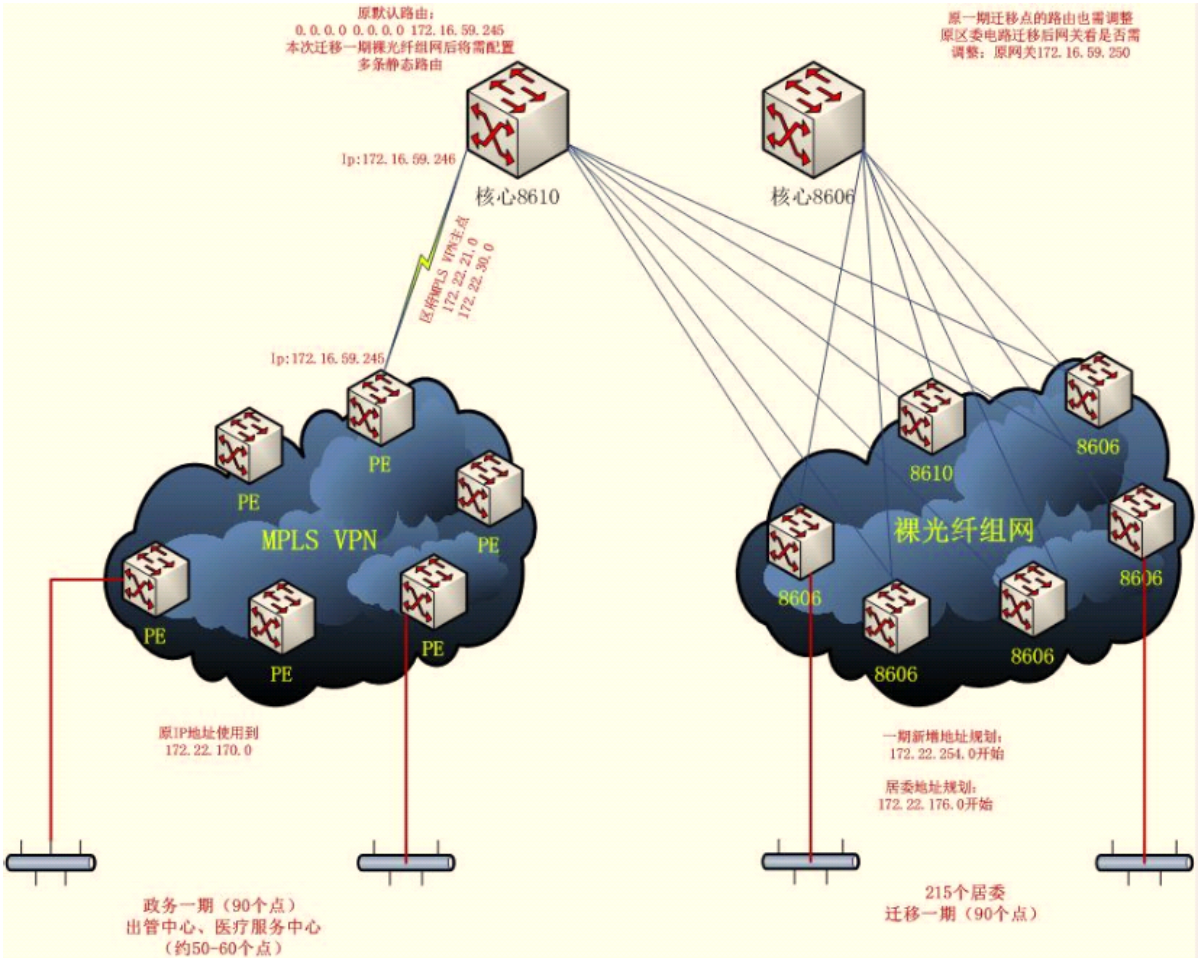


图 3-2 割接项目的目标拓扑

政务一期 IP 网段 172.22.245.0 到 172.22.251.0、172.22.1.0 到 172.22.123.0，该 IP 段迁移到裸光纤组网后，要求 IP 地址规划不变。政务一期通过静态与动态路由实现数据互访，迁移一期、新建二期通过动态路由实现数据互访。S8610 上有两条关于 172.22.0.0 的静态路由：

ip route 172.22.0.0 255.255.0.0 172.16.59.245 （下一跳属于电信的 PE）

ip route 172.22.62.0 255.255.255.0 172.16.59.245 （下一跳属于电信的 PE）

### 3.3.2 生成树设计和实施

从拓扑中可以知道，政务外网汇聚和核心之间采用双上联的二层冗余和设备冗余，实现了企业网络的高可用性，但是，二层的网络冗余有可能会引入桥接环路，如果产生桥接环路，数据包就会永远在设备间循环，占用网络带宽。而生成树协议(STP,Spanning-Tree Protocol)可以识别并防止二层环路。

它能够在实现物理路径冗余的同时避免网络中出现不良的活动环路。

**本项目中生成树设计规范为：**

■在接入、汇聚、核心启用生成树协议：STP

■核心生成树优先级：4096

■汇聚生成树优先级：16384

■接入上联汇聚口开启：bpdufilter

■接入下联接口开启：bpduguard、portfast

设计人员应该使用生成树协议，也应该通过手工指定根桥的方式来控制生成树的拓扑。在创建了生成树之后，应该使用 STP 工具箱来增强网络的总性能，并减少因拓扑变更而浪费的时间。

■BPDU 过滤（BPDU Filter）：能够限制交换机不向接入端口发送不必要的 BPDU

■BPDU 防护（BPDU Guard）：能够防止交换设备以外地连接到启用了 Portfast 特性的端口。如果将交换机连接到启用了 Portfast 特性的端口，那么就可能导致第 2 层环路或拓扑变更。

■Portfast：PortFast 能使得被配置为二层 Access 端口的接口立即进入转发状态，也就是绕过侦听状态和学习状态。它的目的是尽量缩短 Access 端口等待 STP 收敛的时间。启用 PostFast 的优势在于能够防止 DHCP 超时的问题。

配置命令如下：

**1.启用生成树协议：**

```
Ruijie>enable
Ruijie #config terminal
Ruijie(config)#spanning-tree  //打开 STP 协议
Ruijie(config)#spanning-tree mode stp  //配置生成树模式为 STP
Ruijie(config)#end  //退回到特权模式
Ruijie#show spanning-tree //核对配置条目
Ruijie#write  //保存配置
```

2.核心交换机的生成树优先级设置为 4096

```
Ruijie>enable
Ruijie#config terminal
Ruijie(config)#spanning-tree priority 4096 //配置设备优先级为 4096
Ruijie(config)#show spanning-tree
Ruijie(config)#write  //保存配置
```

3.汇聚交换机的生成树优先级设置为 16384

```
Ruijie>enable
Ruijie#config terminal
Ruijie(config)# spanning-tree priority 4096 //配置设备优先级为 16384
Ruijie(config)#show spanning-tree
Ruijie(config)#write  //保存配置
```

4. 接入交换机的上联汇聚口开启：bpdufilter

```
Ruijie>enable
Ruijie#config terminal
Ruijie(config)#interface GigabitEthernet1/1  //进入接口配置模式
Ruijie(config-if)#spanning-tree  bpdufilter  enable  // 在 接 口 打 开
bpdufilter
Ruijie(config-if)end
Ruijie#show running-config //查看配置条目
Ruijie#write  //保存配置
```

5. 接入下联接口开启：bpduguard、portfast

```
Ruijie>enable
Ruijie#config terminal
```

```
Ruijie(config)# interface range gigabitethernet 1/1 - 24
Ruijie(config-if-range)# spanning-tree bpduguard enable //在接入端口配置 bpduguard
Ruijie(config-if-range)# spanning-tree portfast //在接入端口配置 portfast
Ruijie(config-if-range)#end
Ruijie#show running-config //核实配置条目
Ruijie#copy running-config startup-config //保存配置
```

配置了 bpdufilter，bpduguard 和 portfast 这些增强特性后，使 STP 的收敛速度更快，运行效率也大幅提高。这些增强特性可以提高多层交换网络的可用性和安全性。

### 3.3.3 VLAN 规划与实施

VLAN（虚拟局域网，Virtual Local Area Network）是一组拥有共同需求且与物理位置无关的终端设备所组成的逻辑分组。VLAN 划分是基于数据流的模式来进行的。VLAN 通常氛围端到端的 VLAN 和本地 VLAN。其中端到端的 VLAN 会延伸到整个网络，而本地 VLAN 则仅仅限于建筑接入层和建筑汇聚层子模块中的交换机。此外，Trunk 是二层互联设备之间的二层点到点的链路，它可以承载多个 VLAN 的流量。不同网段的计算机通过路由器或者三层交换机进行通信。

因为 VLAN 能够将流量隔离到确定的广播域和子网中，所以不同 VLAN 中的设备不能直接通信。在汇聚层和核心层的交换机几乎都会有多个 VLAN 与其相连。有多个 VLAN 的交换机需要通过传输三层流量来让这些 VLAN 间通信。要实施 VLAN 间路由，就需要用到路由器或者三层交换机，三层交换机可以通过 SVI(交换机虚拟接口，Switch Virtual Interface）来实现 VLAN 间路由。

由于基于端口划分 VLAN 的方法最常用，所以政务外网项目中 VLAN 划分方法是基于设备端口。VLAN 的规划需要考虑一下因素：

■管理 VLAN。通过划分管理 VLAN，并对管理 VLAN 话费特殊 VLAN

ID 号和 IP 地址，可以增强网络管理工作的安全性，避免用户直接对网络管理设备的直接访问，是非常有必要的。

■服务器 VLAN。服务器是向局域网提供服务的关键，大多数情况下，局域网内部的服务器都位于局域网的核心部分，针对服务器群建立一个特定的 VLAN，可以加强服务器之间的访问，同时提高了服务器的运行的安全性。

■业务 VLAN。在网络使用中，相同的部分用户，所需要的应用服务基本是一致的。因此可以针对用户计算机的部分分布情况,划分不同的 VLAN,例如财务 VLAN,生产 VLAN。

根据具体需求和安全性考虑，政务外网一期的 VLAN 划分情况如下表所示：

| VLAN 类型 | VLAN 范围 | IP 地址范围 | 默认网关 |
|---|---|---|---|
| 管理 VLAN | VLAN 1001 | 172.22.21.145 到 172.22.21.253 | 汇聚交换机的管理 IP |
| 业务 VLAN | VLAN 300—VLAN 382 | 172.22.245. 0 到 172.22.251.0<br>172.22.1.0 到 172.22.123.0 | 汇聚交换机上的 SVI |
| 互联 VLAN | VLAN 200 | 172.22.200.247 到<br>172.22.200.254 | 上联设备对应的 SVI |

表 3-1

**配置 VLAN：**

第 1 步，在接入交换机上配置 vlan

```
Ruijie>enable
Ruijie#config terminal
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login local
Ruijie(config-line)#exec-timeout 5 30
Ruijie(config-line)#exit
Ruijie(config)#username ruijie password ruijie  //设置 telnet 用户名和密码
Ruijie(config)#spanning-tree mode stp
Ruijie(config)#interface gigabitethernet 1/1  //进入上联口
Ruijie(config-if)#medi fiber  //把端口设置为光纤口
```

```
Ruijie(config-if)#description uplink //添加端口描述
```

Ruijie(config-if)#exit

Ruijie(config)#vlan 1001 //创建管理 vlan 1001

Ruijie(config-vlan)#exit

Ruijie(config)#interface vlan 1001

Ruijie(config-if)#ip address 172.22.21.169 2455.255.255.0 //配置管理 IP

Ruijie(config-if)#ip default-gateway 172.22.21.247 //配置管理 vlan 的默认网关

Ruijie(config)#vlan 324 //创建业务 vlan

Ruijie(config-vlan)#exit

Ruijie(config)#interface rang f0/1 - 24

Ruijie(config-if-range)#switchport access vlan 324 //把端口划分到业务 vlan

Ruijie(config-if-range)#end

Ruijie#write //保存配置

第二步，在对应的网关汇聚交换机上增加对应的业务 VLAN

Ruijie#telnet 172.22.21.247 //远程登录到汇聚交换机

Username:ruijie

Password:ruijie

DX_LW>enable

DX_LW#config terminal

DX_LW(config)#vlan 324 //创建业务 vlan

DX_LW(config-vlan)#exit

DX_LW(config)#interface vlan 324

DX_LW(config-if)#ip address 172.22.90.2 //这是 vlan 324 的对应的网关地址

DX_LW(config-if)#end

DX_LW#write

### 3.3.4 IP 地址设计和设备使用规范

IP 地址是用来标识网络中一个通信实体的。例如一台主机，或者是路由器的某一个端口。而基于 IP 协议网络中传输的数据包，也都必须使用 IP 地址来进行标识。IP 地址的规划其实就是划分子网，那为什么要划分子网呢？因为划分子网有如下好处：

■缩减网络流量，优化网络性能。不同子网中的广播地址不同，而在相同子网中的广播地址是相同的。试想一下，如果申请了一个 B 类地址 173.1.0.0/16，该子网中可以容纳 65534 台主机，6 万多台计算机在同一个子网中，广播量非常巨大。路由器和三层交换机的 VLAN 创建了广播域，创建的广播域越多，其广播域的规模就越小，并且在每个网段上的无关流量也就会越低。

■简化管理。与一个巨大的网络相比，在一组比较小的互联网络中，判断并孤立网络所出现的故障会比较容易。

■增加了网络的安全性。划分子网后，子网之间的通信就需要通过路由器，不但可以隔离广播域，还可以在路由器上实现访问控制，限制不同网络之间的权限，提高网络的安全性。

政务外网第二期的 **IP 地址规划**，见表 3-2：

| 设备类型 | 设备型号 | 地址 | VLAN 1000 ip | VLAN 1001 ip | 互联VLAN | 核心汇聚互联IP | ROUTER-ID |
|---|---|---|---|---|---|---|---|
| 核心 | 8610 | 中山七区府8楼机房 | 172.22.30.254 | 172.22.21.254 | 200 | 172.22.200.254 | 172.22.200.254 |
| 核心 | 8606 | 中山七区府8楼机房 | 172.22.30.253 | 172.22.21.253 | 200 | 172.22.200.253 | 172.22.200.253 |
| | | | | | | | |
| 汇聚 | 8610 | 荔枝湾 | 172.22.30.247 | 172.22.21.247 | 200 | 172.22.200.247 | 172.22.200.247 |
| 汇聚 | 8606 | 观绿 | 172.22.30.248 | 172.22.21.248 | 200 | 172.22.200.248 | 172.22.200.248 |
| 汇聚 | 8606 | 西华 | 172.22.30.249 | 172.22.21.249 | 200 | 172.22.200.249 | 172.22.200.249 |
| 汇聚 | 8606 | 花地 | 172.22.30.250 | 172.22.21.250 | 200 | 172.22.200.250 | 172.22.200.250 |
| 汇聚 | 8606 | 芳村 | 172.22.30.251 | 172.22.21.251 | 200 | 172.22.200.251 | 172.22.200.251 |
| 汇聚 | 8606 | 流花 | 172.22.30.252 | 172.22.21.252 | 200 | 172.22.200.252 | 172.22.200.252 |

核心和汇聚的 IP 地址规划

| IP地址规划<br>（172.22.176.0开始） | 网关VLAN | 网关 | 子网掩码 | 管理<br>VLAN | 管理IP |
|---|---|---|---|---|---|
| 172.22.176.2到172.22.176.63 | 1761 | 172.22.176.1 | 255.255.255.192 | 1000 | 172.22.30.1 |
| 172.22.176.66到172.22.176.127 | 1762 | 172.22.176.65 | 255.255.255.192 | 1000 | 172.22.30.2 |
| 172.22.176.130到172.22.176.191 | 1763 | 172.22.176.129 | 255.255.255.192 | 1000 | 172.22.30.3 |
| 172.22.176.194到172.22.176.254 | 1764 | 172.22.176.193 | 255.255.255.192 | 1000 | 172.22.30.4 |
| 172.22.177.2到172.22.177.63 | | 172.22.177.1 | 255.255.255.192 | 1000 | 172.22.30.5 |
| 172.22.177.66到172.22.177.127 | | 172.22.177.65 | 255.255.255.192 | 1000 | 172.22.30.6 |
| 172.22.177.130到172.22.177.191 | | 172.22.177.129 | 255.255.255.192 | 1000 | 172.22.30.7 |
| 172.22.177.194到172.22.177.254 | | 172.22.177.193 | 255.255.255.192 | 1000 | 172.22.30.8 |

.

.

.

. （中间省略多行）

.

.

| IP地址规划<br>（172.22.176.0开始） | 网关VLAN | 网关 | 子网掩码 | 管理<br>VLAN | 管理IP |
|---|---|---|---|---|---|
| 172.22.241.2到172.22.241.63 | 2411 | 172.22.241.1 | 255.255.255.192 | 1001 | 172.22.21.139 |
| 172.22.241.66到172.22.241.127 | 2412 | 172.22.241.65 | 255.255.255.192 | 1001 | 172.22.21.140 |
| 172.22.241.130到172.22.241.191 | 2413 | 172.22.241.129 | 255.255.255.192 | 1001 | 172.22.21.141 |
| 172.22.241.194到172.22.242.254 | 2414 | 172.22.241.193 | 255.255.255.192 | 1001 | 172.22.21.142 |
| 172.22.242.2到172.22.242.63 | 2421 | 172.22.242.1 | 255.255.255.192 | 1001 | 172.22.21.143 |
| 172.22.242.66到172.22.242.127 | 2422 | 172.22.242.65 | 255.255.255.192 | 1001 | 172.22.21.144 |

表 3-2

从表中可以得知，IP 地址选用 B 类私有 IP 地址范围（172.16.0.0 到 172.31.255.255 ） 中 的 172.22.176.0 到 172.22.242.255 ， 子 网 掩 码 是 255.255.255.192。每个子网的网关地址为子网中第一个可用的 IP 地址。

命名在满足客户易用性目标方面起到了非常关键的作用，简短而有意义的名字可以帮助用户非常简洁地定位服务的位置：设计人员应该从资源的角度设计出易用性，可管理性强的命名模型，以便于提高网络用户的体验度。

政务外网二期的项目中，**VLAN 的命名规范**如下图所示：