同济大学
TONGJI UNIVERSITY

同济大学计算机网络
课程设计实验报告

课　　题	政府办公局域网设计
姓　　名	郑博远
学　　号	**2154312**
电　　话	**18120929868**
授课老师	陆有军老师
日　　期	**2024 年 7 月**

目 录

（一） 项目概述

1.1. 项目背景

组建某政府办公局域网，设计一个拓扑结构为树形的网络，建立政府的官方网站。要求：

1. 可向外界发布信息
2. pc 通过交换机连接起来，网络之间通过路由器或交换机连接起来
3. 安全性通过防火墙的访问控制来设置
4. 在网络内部联网的分布使用的是私有 IP 地址
5. 通过路由器连接到互联网
6. 不同职能部门可以进行局域网划分

1.2. 项目需求

解决方案设计，其中必须包含：

- 设备选型
- 综合布线设计
- 拓扑图
- IP 地址规划
- 子网划分
- 路由协议的选择
- 路由器配置

（二） 可行性分析报告

2.1. 社会可行性分析

政府办公局域网能够协助政府领导处理政府日常工作，发挥服务领导、督查落实、决策研究、组织协调、公文运转等作用，重点发挥参谋助手和运转枢纽作用，其建设对社会具有积极影响。首先，提高政府办公效率是提升公共服务质量的关键，有助于加强政府与公众的互动，增强政府透明度与公信力。其次，局域网的建立可以加强政府内部的信息共享和资源优化配置，促进不同部门间的协同工作，提高决策效率。此外，政府官网的建立是对外发布信息的重要渠道，有助于公众更好地了解政府政策和服务，提升政府形象。

2.2. 技术可行性分析

本系统所采用的网络技术应具备以下特性：支持第三层交换，以确保网络能够在 IP 层面上高效地进行数据包的路由和转发；支持 OSPF 等路由协议以动态适应网络结构变化，提供最优的数据传输路径；支持多策略的 VLAN，允许基于不同策略对网络流量进行细分和管理，增强安全性和效率；实现全双工并行连接，确保物理链路之间可以实现负载均衡，并具有热备份功能，通过 HSRP 技术确保关键网络服务的高可用性和故障恢复能力；拥有足够的接口和背板速率，以确保交换机能够满足网络扩展的需求，适应未来增长；操作系统支持集群技术、双机热备份等先进技术，以便完成负载均衡、数据备份等需求。通过整合 VLAN、HSRP、NAT、OSPF、ACL、STP、DHCP 等关键技术，本系统将构建一个强大、灵活、安全的网络环境，满足政府办公的高标准需求。各个技术的可行性分析具体如下：

2.2.1. VLAN（虚拟局域网）

VLAN 技术允许在物理网络设备上创建多个逻辑网络，从而对流量进行有

效隔离和管理。在政府办公网络中，VLAN 的使用可以确保不同部门或功能组之间的数据隔离，增强安全性，同时减少不必要的广播流量，提高网络效率。

2.2.2. HSRP（热备份路由协议）

HSRP 为关键网络设备提供了高可用性解决方案。通过虚拟 IP 地址和自动故障转移机制，HSRP 确保网络中的主机在默认网关发生故障时能够无缝切换到备用路由器，从而保障网络的连续性和稳定性。

2.2.3. NAT（网络地址转换）

NAT 技术使得政府机构能够在使用私有 IP 地址的同时访问互联网资源。它不仅解决了公网 IP 地址不足的问题，还为内部网络提供了额外的安全层，因为 NAT 设备可以作为防火墙，限制外部对内部网络的直接访问。

2.2.4. OSPF（开放最短路径优先）

OSPF 这一内部网关协议能够在大型网络中动态地计算最短路径。它支持快速收敛，即网络拓扑变化时能够迅速重新计算路由，保证数据传输的高效性。在政府网络中，OSPF 可以适应复杂的网络结构和不断变化的路由需求。

2.2.5. ACL（访问控制列表）

通过 ACL 访问控制列表机制，网络管理员能够根据特定规则控制对网络资源的访问。在政府办公局域网的使用场景中，ACL 可以限制或允许特定的 IP 地址、协议类型或端口的流量，为政府网络提供精细的访问控制和安全策略。

2.2.6. STP（生成树协议）

STP 用于防止网络中的环路问题，通过建立一个逻辑树结构来确保数据包沿着最优路径单向传输。在政府网络中，STP 有助于维护网络的稳定性和可靠

性，防止广播风暴和 MAC 地址表的不一致。

2.2.7. DHCP（动态主机配置协议）

DHCP 自动化了网络设备的 IP 地址分配过程，减少了手动配置的需求，降低了地址冲突的风险。对于政府办公局域网而言，由于接入网络的设备众多，DHCP 能够简化网络管理，提高了配置效率和准确性。

2.3. 经济可行性分析

初始资金费用主要包括硬件设备的购置（如交换机、路由器、防火墙及服务器等）、软件系统采购（包括操作系统和网络管理软件等）、人力资源及人员培训支出以及人力资源配置费用，共计约 150 万元；

后期运行费用涵盖了网络设备的定期维护、软件系统的持续更新以及网络带宽的租用，预计年度维护费用、软件更新费用等合计每年 10 万元；

风险备用资金用于应对项目实施过程中可能出现的不可预见因素，如硬件损坏、工程意外、自然灾害等，预计风险备用资金约为 10 万元。

综合考虑，本项目的初始资金费用预计为 150 万元，后期运行费用预计为每年 10 万元，风险备用资金为 10 万元。本项目资金主要来源包括包括政府拨款、政府信息化建设专项资金等，通过精确的资金规划和合理的预算分配，本项目在经济上具有高度可行性。

2.4. 总结

综合以上分析，政府办公局域网项目在社会、经济和技术层面均有较高的可行性。政府办公局域网的建设能够提升政府工作效率，增强公共服务质量，资金来源较所需资金充足。技术方案成熟可靠，需专业团队实施管理。

（三） 需求分析

3.1. 需求概述

根据题目要求，我在参考了福建省人民政府门户网站提供的省政府办公厅内设机构信息[1]的情况下，对政府部门做适当简化并归纳出如下需求：

1. 网络架构需求：政府办公网络应覆盖至少六个主要部门：行政处、人事处、财金处、文教处、信息处和秘书处。不同职能部门进行局域网划分，网络设计需保证内部数据的安全流通和部门间的资源共享；

2. 访问控制需求：假设仅信息处具备访问外网的权限。要求网络设计中必须包含严格的访问控制机制，确保只有授权的用户和部门能够访问互联网；

3. 互联网服务需求：政府官方网站需部署在 web 服务器上，并且能够对外提供服务。要求 web 服务器配置正确，能够处理外部请求；

4. DNS 服务需求：网络中需包含 DNS 服务器，以提供域名解析服务，确保内部用户能够顺利访问内部和外部的网络资源；

5. DHCP 服务需求：为了方便内部设备的网络配置，需设置 DHCP 服务器，以自动分配 IP 地址和其他网络参数给网络中的客户端设备；

6. 安全性需求：考虑到政府网络的敏感性，整个网络架构必须包含多层次的安全措施，如防火墙、安全协议等，以防止未授权访问和数据泄露；

7. 私有地址使用需求：局域网内部应使用私有 IP 地址，以满足政府机构对内部网络地址的保密性和安全性要求。这些私有地址不会在互联网上路由；

8. 冗余备份需求：网络设计中必须包含冗余备份机制。关键网络设备如核心交换机和路由器应配置双机热备份，关键链路应采用双链路上联，以实现故障切换和负载均衡，确保网络在部分组件发生故障时仍能稳定运行。

3.2. 网络需求

3.2.1. 布线结构需求

- **综合布线系统需求**

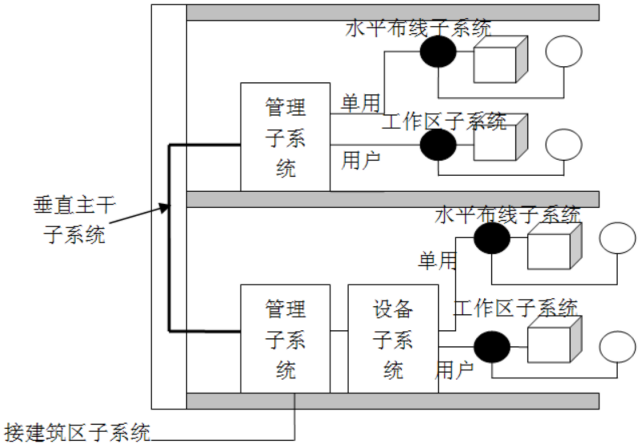

图 1　综合布线示意图

根据政府办公局域网的组成与特点，为了解决传统非结构化网络布线存在的管线交叉重叠、安装维护费用较高等问题，需采用结构化综合布线系统，利用线缆将建筑物内的各类通信设施相互连接起来，并将这些线缆集成在同一个布线系统中[2]。这样既能提升安装效率、节约线缆安装空间，同时还能节约前期的安装费用和后期的维护费用。综合布线整体上采用模块化设计，将整个系统分成若干个子系统，系统结构如图 1 所示。

- **水平布线子系统需求**

水平布线子系统将线路延伸到用户工作区，需满足政府办公局域网对于信息传输的需求。可以采用常规的 PC101004 连接，线缆采用 UTP5E 非屏蔽 8 芯双绞线（对带宽有特殊要求的个别设备也可选用光缆），最大传输速率可以达到 1000Mbps/s，能够满足政府局域网需求。同时，为了保护线缆不受磨损，在穿过底板时需要加装 PVC 管；在墙内走线或者穿过墙体时需要设置金属线槽。

对于会议室等水平面积较大的场所，为了保证水平子系统线路全覆盖，可以在中间部位设置接线间，从而降低长距离通信的损耗以保证通信质量[2]。

- **垂直主干子系统需求**

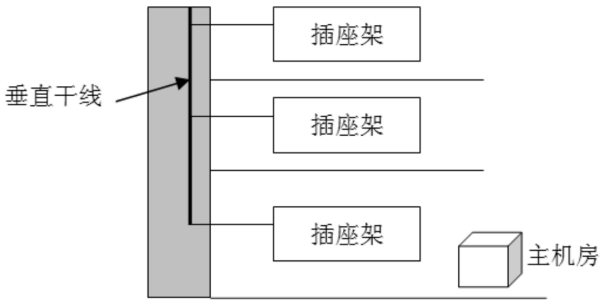

图 2　垂直主干子系统布线示意图

垂直主干子系统为建筑物内部干线电缆提供路由，确保计算机设备以及管理子系统之间正常通信，如上图所示。在线路方面，同样以双绞线电缆为主，个别设备对通信质量要求较高时可以选用光缆。基于安全性考虑，垂直干线需要埋设于金属线槽内，并且每隔 10m 至 15 m 使用扎带进行固定。在布设位置方面，垂直子系统一般位于 2 个单元的中继交叉连接点上，使网络接口尽可能的靠近通信设备，以提高通信质量。

- **工作区子系统需求**

工作区子系统的硬件设备包括电源插座、信息插座、连接器以及扩展软线等。为满足本系统需求，可选用超 5 类信息插座，内置 2 个 RJ-45 通用信息输入/输出孔[3]，用于连接水平子系统和工作区端的网络设备，其输出线和输出线均符合 EIA/TIA 568 标准。信息插座既可以安装在地面上（需要加装密封盒以防尘防水）；也可安装在墙上，与电源插座的间隔距离不得小于 20 cm。

3.2.2. 网络设备需求

需购网络设备包括：五台 100 口的三层核心交换机，用以处理大量数据传

输和复杂的路由需求；若干台 24 口的二层接入层交换机，为各个部门提供足够的接入点；网络安全设备，包括配置有入侵检测系统（IDS）和入侵防御系统（IPS）的防火墙，以及反病毒软件和漏洞管理工具，确保网络免受外部威胁；网络管理工具，以便进行网络监控、配置和维护。

此外，考虑到网络的冗余性，关键网络设备应配备冗余电源和硬件模块。为满足网络的拓展性，所选设备应支持模块化扩展。除了部署防火墙，还需在网络中实施基于角色的访问控制，确保只有授权的部门能够访问外网。

3.2.3. IP 地址规划

表 1　政府局域网 IP 地址规划表

网段名	IP 地址段	子网掩码	默认网关	设备数
服务器集群	192.168.0.0	255.255.255.0	192.168.0.254	250
行政处	192.168.1.0	255.255.255.0	192.168.1.252	250
人事处	192.168.2.0	255.255.255.0	192.168.2.252	250
财金处	192.168.3.0	255.255.255.0	192.168.3.252	250
文教处	192.168.4.0	255.255.255.0	192.168.4.252	250
信息处	192.168.5.0	255.255.255.0	192.168.5.252	250
秘书处	192.168.6.0	255.255.255.0	192.168.6.252	250

3.3. 系统需求

3.3.1. 系统要求

政府办公网络系统需承载大量终端设备，同时维持高效的数据处理和传输能力。系统应具备高度可靠性，通过冗余设计和定期数据备份预防潜在故障。系统设计应以安全性为核心，集成多层次安全措施，包括防火墙、入侵检测系

统和数据加密技术，确保政府数据的机密性和完整性。此外，系统的兼容性必须强大，能够无缝集成现有设备和软件。用户界面设计应简洁直观。

3.3.2. 网络和应用服务

网络架构设计需满足当前办公需求，并具备适应未来扩展的灵活性。采用核心层、汇聚层和接入层的分层设计确保网络稳定性和可管理性。带宽需求分析确保网络通信流畅，保证多媒体和大数据传输等场景使用通畅。

应用服务需全面支持办公应用，包括文档共享、信息发布、电子邮件和视频会议等。移动办公的普及要求系统支持移动设备接入，并提供安全的远程访问解决方案。服务器需提供 HTTP、DNS、DHCP 等服务。

3.4. 网络安全需求

3.4.1. 网络安全体系要求

网络安全体系要求构建一个多层次、全方位的防护网络，确保政府数据和信息流通的安全。具体要求包括：

1. 实施访问控制和数据加密，确保只有授权用户才能访问敏感数据，同时保护数据在传输和存储过程中的安全性；

2. 部署防火墙和入侵检测系统，以防御潜在的网络攻击和未授权访问；

3. 定期进行安全更新和漏洞管理，确保系统软件和应用程序的安全性，及时修补安全漏洞；

4. 执行日志记录和审计，以追踪网络活动，便于事后分析和责任追究；

5. 制定灾难恢复计划和数据备份策略，确保在数据丢失或系统故障时能够迅速恢复；

6. 实施网络监控和制定安全策略，以持续评估和改进网络安全状况。

3.4.2. 网络安全设计模型

首先，需在网络边界部署防火墙和入侵检测系统（IDS），以阻止外部网络未经授权对政府办公局域网内部的访问和攻击。此层还包括反病毒和反恶意软件解决方案，确保边界安全，防止恶意活动对内部网络的侵害。

其次，应当在内部网络中通过采用网络分段和 VLAN 技术来隔离不同的网络流量，增强网络的组织结构和安全性。实施访问控制列表和网络入侵检测系统以监控和保护内部流量，防止潜在的内部威胁。

此外，还需强化用户身份验证措施，通过双因素认证等技术手段确保只有授权用户能够访问敏感数据和资源；使用数据加密协议（如 SSL/TLS）来保护数据在传输和存储过程中的安全；实施实时监控和日志记录系统，以检测和响应潜在的安全事件；建立全面的安全事件响应计划，确保在面临威胁和攻击时能够迅速采取措施，修复漏洞，减轻安全事件的影响。

（四） 网络结构设计

4.1. 网络拓扑设计

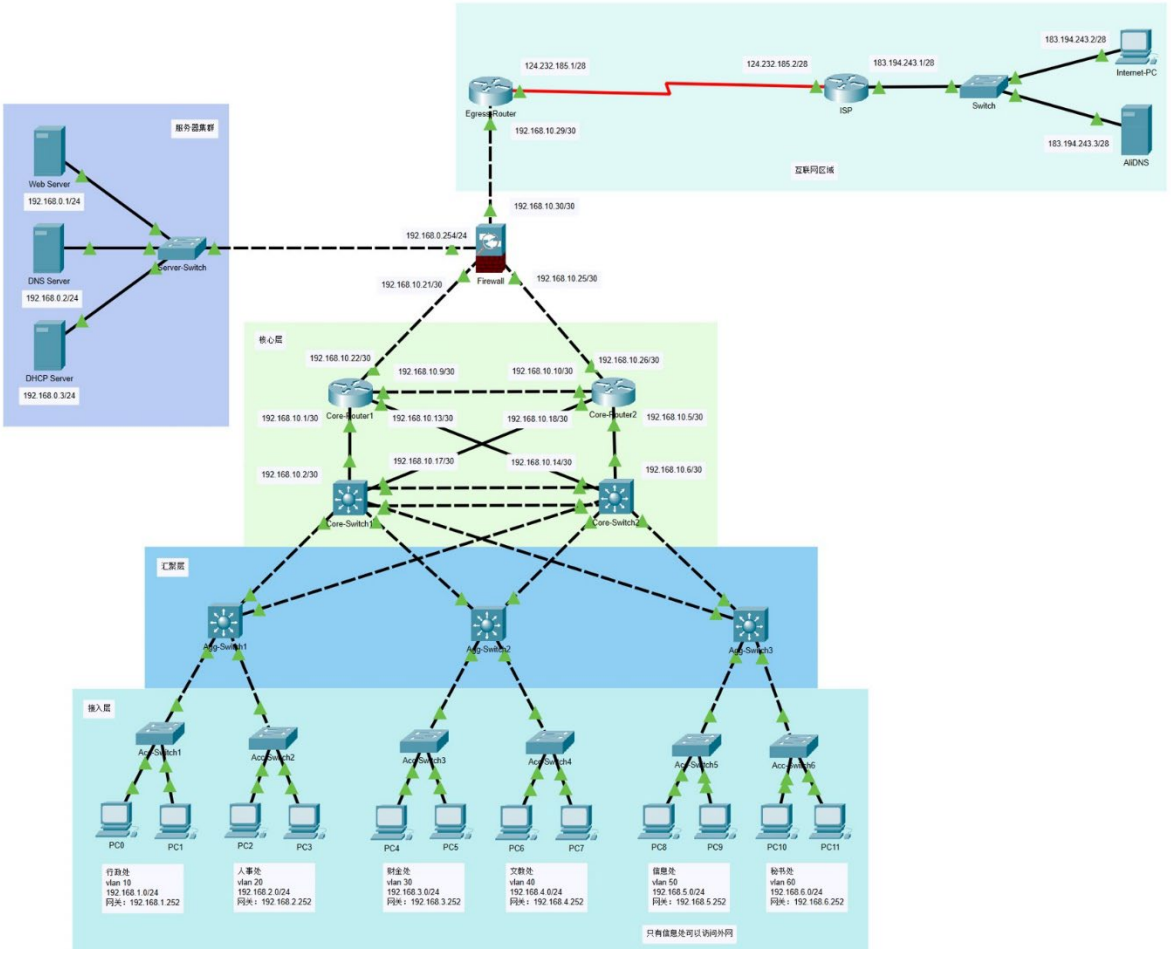

图 3　网络拓扑设计图

根据题目要求，政府办公局域网的拓扑结构设计为层次化的树形结构，采用网络分级设计模型的三层架构，由核心层、汇聚层和接入层三部分组成[4]。这种结构不仅有利于网络的管理，还便于实现负载均衡和故障隔离。网络采用了模块化的设计理念，以适应政府机构不断变化的需求。

4.1.1. 核心层

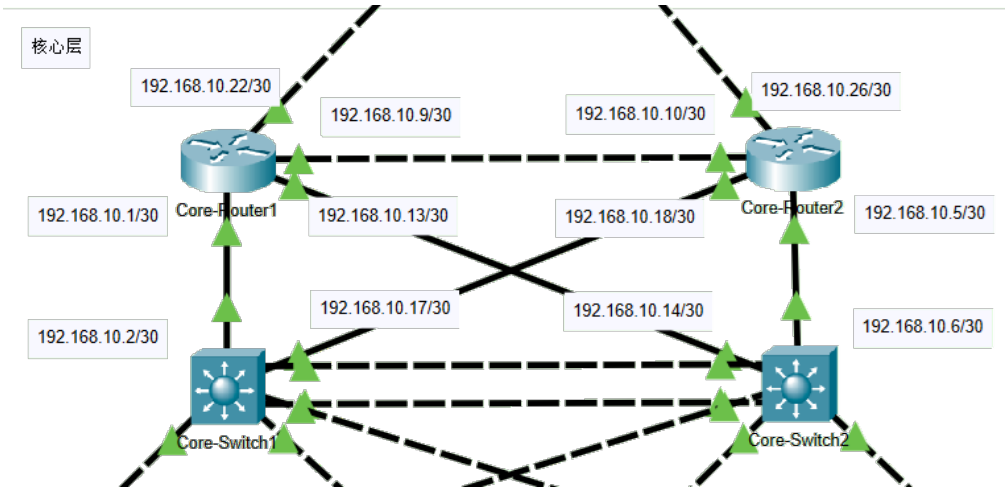

图 4　核心层拓扑图

核心层的设计采用了冗余机制，考虑到设备的故障风险，采用两两堆叠的系统，确保了路由器和交换机拥有备份单元。这种设计可以在主要设备发生故障时，迅速切换到备用设备，从而最小化服务中断的风险。冗余设计不仅适用于硬件设备，也适用于关键链路和电源供应。

为了提高网络的带宽和可靠性，核心层的交换机之间采用了链路聚合技术。链路聚合允许将多个物理链路捆绑成一个逻辑通道，这样即使某一条链路出现问题，其他链路仍然可以继续传输数据，从而增强了网络的容错能力。

核心层的交换机具备高速数据处理能力，支持第三层交换功能，可以高效地进行路由决策和数据转发。同时，核心层的路由器负责连接不同的网络区域，通过 OSPF 路由协议动态适应网络结构的变化，确保数据包能够找到最优的传输路径。此外，核心层交换机上配置了多个 VLAN 实例（VLANIF），这些实例作为不同用户群体的网关，提供了逻辑上的隔离和安全性。

4.1.2. 汇聚层

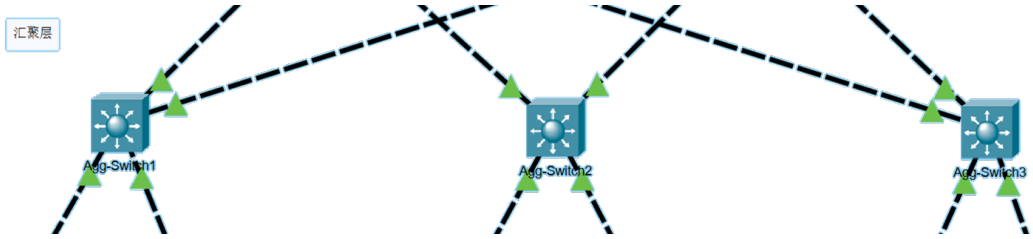

图 5　汇聚层拓扑图

汇聚层设计了三个三层交换机，用于连接接入层的行政处、人事处、财金处等不同处室的二层交换机，在汇聚设备上创建对应的 VLANIF 接口作为办公终端的网关。汇聚层的主要功能之一是将来自接入层的流量进行有效汇聚，并根据路由策略分发到核心层或其他汇聚层。这一过程中，汇聚层设备需要具备高效的数据处理能力，以应对大量数据的转发和路由。

4.1.3. 接入层

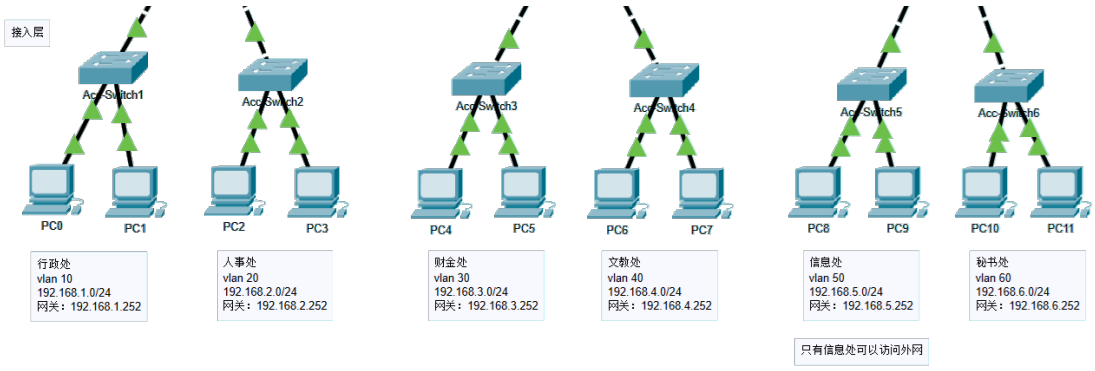

图 6　接入层拓扑图

接入层根据政府机构的不同部门进行了细致的 VLAN 划分。每个部门拥有独立的 VLAN，如行政处对应 VLAN 10，人事处对应 VLAN 20，以此类推。这样的划分有助于实现部门间的网络隔离，增强安全性。

为实现高效的网络管理并隔离广播域，接入层的交换机端口根据连接的终端设备被配置为 Access 类型，严格限制了每个端口只能属于一个 VLAN，从而

有效控制了广播流量，提升了网络性能。同时，交换机之间的连接端口被配置为 Trunk 类型，允许多个 VLAN 的数据通过，增强了网络的灵活性和扩展性。

4.1.4. 服务器集群

1. Web 服务器

为满足题目中“可对外界发布信息”的需求，通过 Web 服务器负责托管政府的官方网站，确保网站稳定运行、抵御潜在网络攻击，并支持较高的并发访问量，保证用户能够流畅地访问网站内容。此外，Web 服务器需要配置 SSL/TLS 证书，实现 HTTPS 加密传输，保护数据传输过程中的安全性。

2. DNS 服务器

DNS 服务器提供域名解析服务，将域名转换为 IP 地址，确保用户能够通过域名访问网络资源。为防止 DNS 污染并保证 DNS 安全，对于政府机构来说可以在办公局域网内自建 DNS 服务器，对内提供 DNS 服务。

3. DHCP 服务器

DHCP 服务器提供自动分配 IP 地址的服务，对于政府网络中的大量终端设备，如计算机、打印机等，DHCP 服务能够显著简化网络配置工作，并减少地址冲突的可能性。DHCP 服务器需要与网络中的其他服务（如 DNS 和 DHCP 中继）协同工作，确保终端设备能够顺利获取到正确的网络配置信息，包括 IP 地址、子网掩码、默认网关和 DNS 服务器地址等。

4.2. IP 地址与 VLAN 划分

表 2　政府局域网 IP 地址与 VLAN 划分表

网段名	IP 地址（段）	默认网关	所属 VLAN
行政处	192.168.1.0/24	192.168.1.252	vlan 10

人事处	192.168.2.0/24	192.168.2.252	vlan 20
财金处	192.168.3.0/24	192.168.3.252	vlan 30
文教处	192.168.4.0/24	192.168.4.252	vlan 40
信息处	192.168.5.0/24	192.168.5.252	vlan 50
秘书处	192.168.6.0/24	192.168.6.252	vlan 60
WEB 服务器	192.168.0.1	192.168.0.254	-
DNS 服务器	192.168.0.2	192.168.0.254	-
DHCP 服务器	192.168.0.3	192.168.0.254	-

局域网 IP 地址与 VLAN 划分详见上表。此外，192.168.10.0/24 网段被细分为多个/30 子网，以实现路由器、三层交换机等设备间的连接。每个/30 子网提供四个 IP 地址，其中两个有效地址被用作接口地址，如下图所示：

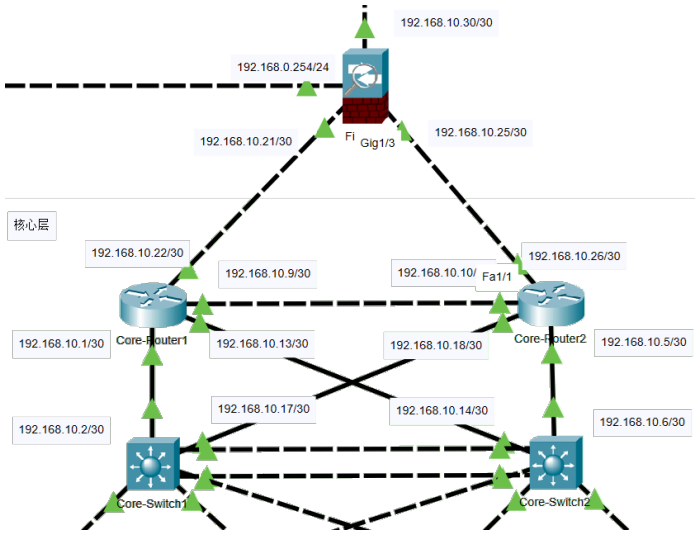

图 7　路由器、三层交换机等网络设备之间 IP 地址的配置

连接到办公局域网中的计算机的 IP 地址配置通过 DHCP 服务器自动分配。通过 DHCP（动态主机配置协议），网络中的终端设备在接入网络时能够自动获取 IP 地址、子网掩码、默认网关和其他必要的网络配置信息。

（五） 系统配置与实施

5.1. 网络设备配置

1. 首先，对交换机、路由器等网络设备的 hostname 进行重命名。重命名后，各层交换机分别名为 Core-Switch、Agg-Switch、Acc-Switch，其他网络设备也分别依照名称进行命名。

2. 在核心层、汇聚层、接入层的各个交换机上分别按需创建虚拟局域网 VLAN 10 至 VLAN 60，对应各个部门。

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#vlan 50
Switch(config-vlan)#vlan 60
Switch(config-vlan)#exit
Switch(config)#
```

3. 在两个核心交换机进行配置，配置每个 VLAN 的 IP 地址和子网掩码，并激活。例如对于 VLAN 10，核心交换机 1 的接口被分配了 IP 地址 192.168.1.253，核心交换机 2 的接口被分配了 IP 地址 192.168.1.254，子网掩码均为 255.255.255.0（VLAN10 的默认网关地址为 192.168.1.252，通过 HSRP 配置）。

```
Core-Switch1>en
Core-Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core-Switch1(config)#int vlan 10
Core-Switch1(config-if)#
```

```
%LINK-5-CHANGED: Interface Vlan10, changed state to up

Core-Switch1(config-if)#ip address 192.168.1.253 255.255.255.0
Core-Switch1(config-if)#int vlan 20
Core-Switch1(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Core-Switch1(config-if)#ip address 192.168.2.253 255.255.255.0
Core-Switch1(config-if)#int vlan 30
Core-Switch1(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Core-Switch1(config-if)#ip address 192.168.3.253 255.255.255.0
Core-Switch1(config-if)#int vlan 40
Core-Switch1(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up
Core-Switch1(config-if)#ip address 192.168.4.253 255.255.255.0
Core-Switch1(config-if)#int vlan 50
Core-Switch1(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

Core-Switch1(config-if)#ip address 192.168.5.253 255.255.255.0
Core-Switch1(config-if)#
Core-Switch1(config-if)#int vlan 60
Core-Switch1(config-if)#
%LINK-5-CHANGED: Interface Vlan60, changed state to up

Core-Switch1(config-if)#ip address 192.168.6.253 255.255.255.0
```

```
Core-Switch2>en
Core-Switch2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core-Switch2(config)#int vlan 10
Core-Switch2(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

Core-Switch2(config-if)#ip address 192.168.1.254 255.255.255.0
Core-Switch2(config-if)#int vlan 20
```

```
Core-Switch2(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Core-Switch2(config-if)#ip address 192.168.2.254 255.255.255.0
Core-Switch2(config-if)#int vlan 30
Core-Switch2(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Core-Switch2(config-if)#ip address 192.168.3.254 255.255.255.0
Core-Switch2(config-if)#int vlan 40
Core-Switch2(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up
Core-Switch2(config-if)#ip address 192.168.4.254 255.255.255.0
Core-Switch2(config-if)#int vlan 50
Core-Switch2(config-if)#
%LINK-5-CHANGED: Interface Vlan50, changed state to up

Core-Switch2(config-if)#ip address 192.168.5.254 255.255.255.0
Core-Switch2(config-if)#
Core-Switch2(config-if)#int vlan 60
Core-Switch2(config-if)#
%LINK-5-CHANGED: Interface Vlan60, changed state to up

Core-Switch2(config-if)#ip address 192.168.6.254 255.255.255.0
```

4. 在两个核心交换机上分别对 VLAN10~VLAN60 进行 HSRP 配置。通过热备份路由协议配置虚拟 IP 地址 192.168.x.252，在主路由器出现故障时提供无缝切换。由于默认优先级为 100，对于 Core-Switch1 在 VLAN10、20 和 30 设置 200 的优先级，使其成为有较高优先级的主路由器，VLAN40、50 和 60 反之。

```
Core-Switch1(config-if)#int vlan 10
Core-Switch1(config-if)#standby 10 ip 192.168.1.252
Core-Switch1(config-if)#standby 10 priority 200
Core-Switch1(config-if)#standby 10 preempt
Core-Switch1(config-if)#standby 10 track fastEthernet 0/1
```

```
Core-Switch1(config-if)#standby 10 track fastEthernet 0/2
Core-Switch1(config-if)#exit

Core-Switch1(config-if)#int vlan 20
Core-Switch1(config-if)#standby 20 ip 192.168.2.252
Core-Switch1(config-if)#standby 20 priority 200
Core-Switch1(config-if)#standby 20 preempt
Core-Switch1(config-if)#standby 20 track fastEthernet 0/1
Core-Switch1(config-if)#standby 20 track fastEthernet 0/2
Core-Switch1(config-if)#exit

Core-Switch1(config-if)#int vlan 30
Core-Switch1(config-if)#standby 30 ip 192.168.3.252
Core-Switch1(config-if)#standby 30 priority 200
Core-Switch1(config-if)#standby 30 preempt
Core-Switch1(config-if)#standby 30 track fastEthernet 0/1
Core-Switch1(config-if)#standby 30 track fastEthernet 0/2
Core-Switch1(config-if)#exit

Core-Switch1(config-if)#int vlan 40
Core-Switch1(config-if)#standby 40 ip 192.168.4.252
Core-Switch1(config-if)#standby 40 preempt
Core-Switch1(config-if)#standby 40 track fastEthernet 0/1
Core-Switch1(config-if)#standby 40 track fastEthernet 0/2
Core-Switch1(config-if)#exit

Core-Switch1(config-if)#int vlan 50
Core-Switch1(config-if)#standby 50 ip 192.168.5.252
Core-Switch1(config-if)#standby 50 preempt
Core-Switch1(config-if)#standby 50 track fastEthernet 0/1
Core-Switch1(config-if)#standby 50 track fastEthernet 0/2
Core-Switch1(config-if)#exit

Core-Switch1(config-if)#int vlan 60
Core-Switch1(config-if)#standby 60 ip 192.168.6.252
Core-Switch1(config-if)#standby 60 preempt
Core-Switch1(config-if)#standby 60 track fastEthernet 0/1
Core-Switch1(config-if)#standby 60 track fastEthernet 0/2
```

```
Core-Switch1(config-if)#exit
```

```
Core-Switch2(config-if)#int vlan 10
Core-Switch2(config-if)#standby 10 ip 192.168.1.252
Core-Switch2(config-if)#standby 10 preempt
Core-Switch2(config-if)#standby 10 track fastEthernet 0/1
Core-Switch2(config-if)#standby 10 track fastEthernet 0/2
Core-Switch2(config-if)#exit

Core-Switch2(config-if)#int vlan 20
Core-Switch2(config-if)#standby 20 ip 192.168.2.252
Core-Switch2(config-if)#standby 20 preempt
Core-Switch2(config-if)#standby 20 track fastEthernet 0/1
Core-Switch2(config-if)#standby 20 track fastEthernet 0/2
Core-Switch2(config-if)#exit

Core-Switch2(config-if)#int vlan 30
Core-Switch2(config-if)#standby 30 ip 192.168.3.252
Core-Switch2(config-if)#standby 30 preempt
Core-Switch2(config-if)#standby 30 track fastEthernet 0/1
Core-Switch2(config-if)#standby 30 track fastEthernet 0/2
Core-Switch2(config-if)#exit

Core-Switch2(config-if)#int vlan 40
Core-Switch2(config-if)#standby 40 ip 192.168.4.252
Core-Switch2(config-if)#standby 60 priority 200
Core-Switch2(config-if)#standby 40 preempt
Core-Switch2(config-if)#standby 40 track fastEthernet 0/1
Core-Switch2(config-if)#standby 40 track fastEthernet 0/2
Core-Switch2(config-if)#exit

Core-Switch2(config-if)#int vlan 50
Core-Switch2(config-if)#standby 50 ip 192.168.5.252
Core-Switch2(config-if)#standby 60 priority 200
Core-Switch2(config-if)#standby 50 preempt
Core-Switch2(config-if)#standby 50 track fastEthernet 0/1
Core-Switch2(config-if)#standby 50 track fastEthernet 0/2
Core-Switch2(config-if)#exit
```

```
Core-Switch2(config-if)#int vlan 60
Core-Switch2(config-if)#standby 60 ip 192.168.6.252
Core-Switch2(config-if)#standby 60 priority 200
Core-Switch2(config-if)#standby 60 preempt
Core-Switch2(config-if)#standby 60 track fastEthernet 0/1
Core-Switch2(config-if)#standby 60 track fastEthernet 0/2
Core-Switch2(config-if)#exit
```

5. 在交换机 Core-Switch1 和 Core-Switch2 上配置生成树协议，基于 VLAN 的生成树实例。对于 VLAN 10、20 和 30，Core-Switch1 被配置为主根桥、Core-Switch2 为次根桥，确保这些 VLAN 的流量优先通过 Core-Switch1。VLAN 40、50 和 60 反之，流量优先通过 Core-Switch2。生成树能在网络冗余和负载均衡的同时防止环路产生，增强网络的稳定性和可靠性。

```
Core-Switch1(config)#spanning-tree mode pvst
Core-Switch1(config)#spanning-tree vlan 10,20,30 root primary
Core-Switch1(config)#spanning-tree vlan 40,50,60 root secondary
```

```
Core-Switch2(config)#spanning-tree mode pvst
Core-Switch2(config)#spanning-tree vlan 10,20,30 root secondary
Core-Switch2(config)#spanning-tree vlan 40,50,60 root primary
```

6. 在核心交换机 Core-Switch1、2 上的六个 VLAN（10, 20, 30, 40, 50, 60）分别设置 IP 辅助地址 192.168.0.3（DHCP 服务器的地址），以便这些 VLAN 中的设备能够通过指定的 DHCP 服务器获取 IP 配置。

```
Core-Switch1(config)#int vlan 10
Core-Switch1(config-if)#ip helper-address 192.168.0.3
Core-Switch1(config-if)#int vlan 20
Core-Switch1(config-if)#ip helper-address 192.168.0.3
Core-Switch1(config-if)#int vlan 30
Core-Switch1(config-if)#ip helper-address 192.168.0.3
```

```
Core-Switch1(config-if)#int vlan 40
Core-Switch1(config-if)#ip helper-address 192.168.0.3
Core-Switch1(config-if)#int vlan 50
Core-Switch1(config-if)#ip helper-address 192.168.0.3
Core-Switch1(config-if)#int vlan 60
Core-Switch1(config-if)#ip helper-address 192.168.0.3
```

7. 对两个核心交换机的对应端口设置为 trunk 模式（允许多个 VLAN 的流量），并配置这些端口使用 Dot1Q 封装。

```
Core-Switch1(config)#int range fastEthernet 0/1-2, fastEthernet
0/7
Core-Switch1(config-if-range)#sw trunk encapsulation dot1q
Core-Switch1(config-if-range)#sw mode trunk
```

```
Core-Switch2(config)#int range fastEthernet 0/1-2, fastEthernet
0/7
Core-Switch2(config-if-range)#sw trunk encapsulation dot1q
Core-Switch2(config-if-range)#sw mode trunk
```

8. 在两个核心交换机上定义端口通道，并将其与对应端口绑定，实现链路聚合。将端口配置为 trunk 模式并应用 Dot1Q 封装以支持多个 VLAN 的传输。

```
Core-Switch1(config)#int port-channel 1
Core-Switch1(config-if)#sw trunk encapsulation dot1q
Core-Switch1(config-if)#int ran f0/5-6
Core-Switch1(config-if-range)#channel-group 1 mode on
Core-Switch1(config-if-range)#sw trunk encapsulation dot1q
Core-Switch1(config-if-range)#sw mode trunk
```

```
Core-Switch2(config)#int port-channel 1
Core-Switch2(config-if)#sw trunk encapsulation dot1q
Core-Switch2(config-if)#int ran f0/4-5
Core-Switch2(config-if-range)#channel-group 1 mode on
```

```
Core-Switch2(config-if-range)#sw trunk encapsulation dot1q
Core-Switch2(config-if-range)#sw mode trunk
```

9. 对两个核心交换机启用 IP 路由功能，并为两个端口 f0/3 和 f0/4 分配静态 IP 地址和子网掩码，同时禁用二层的交换功能（Core-Switch2 配置略）。

```
Core-Switch1>en
Core-Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core-Switch1(config)#ip routing
Core-Switch1(config)#int f0/3
Core-Switch1(config-if)#no sw
Core-Switch1(config-if)#ip add 192.168.10.2 255.255.255.252
Core-Switch1(config-if)#no sh
Core-Switch1(config-if)#int f0/4
Core-Switch1(config-if)#no sw
Core-Switch1(config-if)#ip add 192.168.10.17 255.255.255.252
Core-Switch1(config-if)#no sh
```

10. 在 Core-Switch1 上配置 OSPF 路由协议，并为包括 192.168.1.0 至 192.168.6.0 在内的六个网段（对应 VLAN10 至 VLAN60）以及 192.168.10.0/30、192.168.16.0/30 网络（用于网络设备连接）添加路由宣告，所有这些网络都被分配到 OSPF 区域 0。Core-Switch2 配置类似，此处省略不再赘述。

```
Core-Switch1(config)#router ospf 10
Core-Switch1(config-router)#network 192.168.1.0 0.0.0.255 area
0
Core-Switch1(config-router)#network 192.168.2.0 0.0.0.255 area
0
Core-Switch1(config-router)#network 192.168.3.0 0.0.0.255 area
0
Core-Switch1(config-router)#network 192.168.4.0 0.0.0.255 area
0
```

```
Core-Switch1(config-router)#network 192.168.5.0 0.0.0.255 area
0
Core-Switch1(config-router)#network 192.168.6.0 0.0.0.255 area
0
Core-Switch1(config-router)#network 192.168.10.0 0.0.0.3 area 0
Core-Switch1(config-router)#network 192.168.10.16 0.0.0.3 area
0
```

11. 对于汇聚层的所有交换机（Agg-Switch1 至 Agg-Swich3），将 f0/1 至 f0/4 的系列端口均设置为干道模式，允许它们传输多个 VLAN 的流量。

```
Agg-Switch1>en
Agg-Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Agg-Switch1(config)#int ran f0/1-4
Agg-Switch1(config-if-range)#sw trunk en do
Agg-Switch1(config-if-range)#sw mode trunk
```

12. 对于接入层的五个交换机，以交换机 Acc-Switch1 为例，将连接汇聚层的端口 f0/3 配置为干道模式，连接终端设备的端口范围 f0/1-2 设置为接入模式，并配置为只允许对应 VLAN 的流量通过。

```
Acc-Switch1>en
Acc-Switch1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Acc-Switch1(config)#int f0/3
Acc-Switch1(config-if)#sw mode trunk
Acc-Switch1(config-if)#int ran f0/1-2
Acc-Switch1(config-if-range)#sw mode acc
Acc-Switch1(config-if-range)#sw acc vlan 10
```

13. 继续对核心交换机进行 IP 地址与 OSPF 协议的配置。以 Core-Router1 为例，为连接核心层其他设备的四个接口分配了静态 IP 地址，并在路由配置部

分启动 OSPF 进程 30，将四个/30 子网添加到 OSPF 区域 0 中，以便进行路由协议计算和路径选择。Core-Switch2 配置类似，此处省略不再赘述。

```
Core-Router1(config)#int f0/0
Core-Router1(config-if)#ip add 192.168.10.1 255.255.255.252
Core-Router1(config-if)#no sh
Core-Router1(config-if)#int f0/1
Core-Router1(config-if)#ip add 192.168.10.13 255.255.255.252
Core-Router1(config-if)#no sh
Core-Router1(config-if)#int f1/0
Core-Router1(config-if)#ip add 192.168.10.9 255.255.255.252
Core-Router1(config-if)#no sh
Core-Router1(config-if)#int f1/1
Core-Router1(config-if)#ip add 192.168.10.22 255.255.255.252
Core-Router1(config-if)#no sh
Core-Router1(config-if)#ex
Core-Router1(config)#router ospf 30
Core-Router1(config-router)#network 192.168.10.0 0.0.0.3 area 0
Core-Router1(config-router)#network 192.168.10.20 0.0.0.3 area
0
Core-Router1(config-router)#network 192.168.10.8 0.0.0.3 area 0
Core-Router1(config-router)#network 192.168.10.12 0.0.0.3 area
0
```

14. 在防火墙上，将连接核心层、服务器集群交换机、外部路由器的端口分别命名为 inside1、inside2、inside3 和 outside。其中 inside 接口的安全等级设置为 100，outside 接口的安全等级设置为 0。为每个接口分配对应的 IP 地址，对防火墙配置 OSPF 路由协议实例 50，并声明对应的网络。

```
Firewall(config)#int g1/2
Firewall(config-if)#nameif inside1
Firewall(config-if)#security-level 100
Firewall(config-if)#ip add 192.168.10.21 255.255.255.252
Firewall(config-if)#no sh
Firewall(config-if)#int g1/3
```

```
Firewall(config-if)#nameif inside2
Firewall(config-if)#security-level 100
Firewall(config-if)#ip add 192.168.10.25 255.255.255.252
Firewall(config-if)#no sh
Firewall(config-if)#int g1/4
Firewall(config-if)#nameif inside3
Firewall(config-if)#security-level 100
Firewall(config-if)#ip add 192.168.0.254 255.255.255.0
Firewall(config-if)#no sh
Firewall(config-if)#int g1/5
Firewall(config-if)#nameif outside
Firewall(config-if)#security-level 0
Firewall(config-if)#ip add 192.168.10.30 255.255.255.252
Firewall(config-if)#no sh
Firewall(config-if)#router ospf 50
Firewall(config-router)#network 192.168.10.20 255.255.255.252
area 0
Firewall(config-router)#network 192.168.10.24 255.255.255.252
area 0
Firewall(config-router)#network 192.168.10.28 255.255.255.252
area 0
```

15. 在出口路由器 Egress-Router 上，将接口 f0/0 分配内部网络地址 192.168.10.29，并标记为 NAT 内部接口；接口 s0/1/0 分配外部网络地址 124.232.185.1，并设置为外部接口。此外，配置 s0/1/0 接口的时钟速率 64000，用于与 ISP 的连接。此外还需配置 OSPF 路由协议，并设置默认信息起源，允许路由器向 OSPF 网络中的其他路由器提供默认路由。

```
Egress-Router>en
Egress-Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Egress-Router(config)#int f0/0
Egress-Router(config-if)#ip add 192.168.10.29 255.255.255.252
Egress-Router(config-if)#no sh
Egress-Router(config-if)#ip nat inside
```

```
Egress-Router(config-if)#int s0/1/0
Egress-Router(config-if)#ip add 124.232.185.1 255.255.255.240
Egress-Router(config-if)#ip nat outside
Egress-Router(config-if)#clock rate 64000
Egress-Router(config-if)#no sh
Egress-Router(config-if)#ex
Egress-Router(config)#router ospf 50
Egress-Router(config-router)#network 192.168.10.28 0.0.0.3 area
0
Egress-Router(config-router)#default-information originate
```

16. 在 ISP 路由器上配置两个接口，分别赋予其对应的 IP 地址，用于连接政府办公局域网络的外部路由器和提供互联网服务。

```
ISP(config)#int s0/3/0
ISP(config-if)#ip add 124.232.185.2 255.255.255.240
ISP(config-if)#no sh
ISP(config-if)#int f0/0
ISP(config-if)#ip add 183.194.243.1 255.255.255.240
ISP(config-if)#no sh
```

17. 在防火墙上进行配置，创建了扩展访问控制列表（ACL），允许所有 IP 流量通过。随后将此 ACL 应用到防火墙的所有内网（inside1、inside2、inside3）和外网（outside）接口的入站和出站方向，实施统一的访问控制策略。

```
Firewall(config)#access-list acc extended permit ip any any
Firewall(config)#access-group acc in interface inside1
Firewall(config)#access-group acc in interface inside2
Firewall(config)#access-group acc in interface inside3
Firewall(config)#access-group acc in interface outside
Firewall(config)#access-group acc out interface inside1
Firewall(config)#access-group acc out interface inside2
Firewall(config)#access-group acc out interface inside3
Firewall(config)#access-group acc out interface outside
```

18. 在出口路由器 Egress-Router 上配置一个范围从 124.232.185.3 到 124.232.185.6 的 NAT 地址池 gov，用于政府内部局域网到外部互联网的 NAT 转换。创建访问控制列表 100，允许 192.168.5.0/24 网段内（VLAN50，信息处）的所有 IP 访问互联网。配置 NAT 规则，使访问控制列表 100 中定义的内部网络可以使用 NAT 地址池 gov 进行地址转换。设置默认路由将所有未知目的地的流量导向 ISP 的 IP 地址 124.232.185.2。为使得外部互联网的市民也能访问政府网站以了解最新政务信息，还需配置一条静态 NAT 规则，将内部服务器 192.168.0.1 的 80 端口流量映射到公网 IP 地址 124.232.185.7 的 80 端口，用于外部访问。

```
Egress-Router>en
Egress-Router#conf t
Egress-Router(config)#ip nat pool gov 124.232.185.3
124.232.185.6
Egress-Router(config)#access-list 100 permit ip 192.168.5.0
0.0.0.255 any
Egress-Router(config)#ip nat inside source list 100 pool gov
overload
Egress-Router(config)#ip route 0.0.0.0 0.0.0.0 124.232.185.2
Egress-Router(config)#ip nat inside source static tcp
192.168.0.1 80 124.232.185.7 80
```

5.2. 服务器配置

5.2.1. WEB 服务器

配置 WEB 服务器的 IP 地址为 192.168.0.1，子网掩码为 255.255.255.0，默认网关为 192.168.0.254。开启 WEB 服务器的 HTTP 服务功能并编写网站。

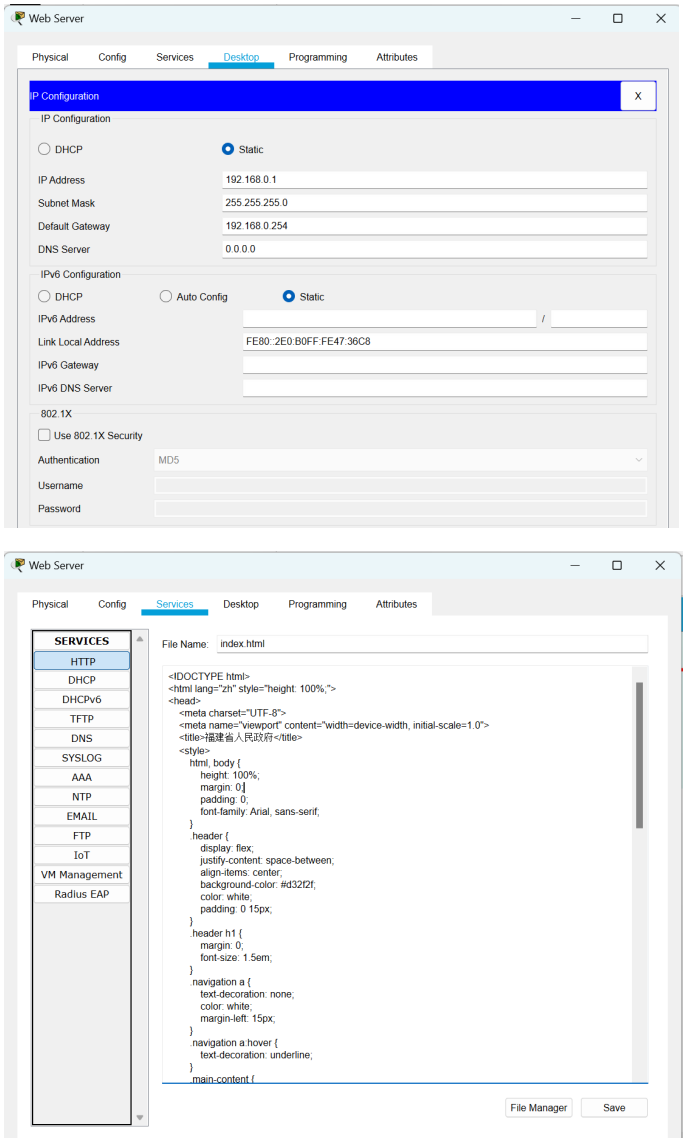

图 8　配置 WEB 服务器

5.2.2. DNS 服务器

类似地，配置 WEB 服务器的 IP 地址为 192.168.0.2，子网掩码为 255.255.255.0，默认网关为 192.168.0.254。开启服务器的 DNS 服务功能，在 DNS 服务器的配置中添加新记录，将域名 www.fujian.gov.cn 指向 IP 地址 192.168.0.1。

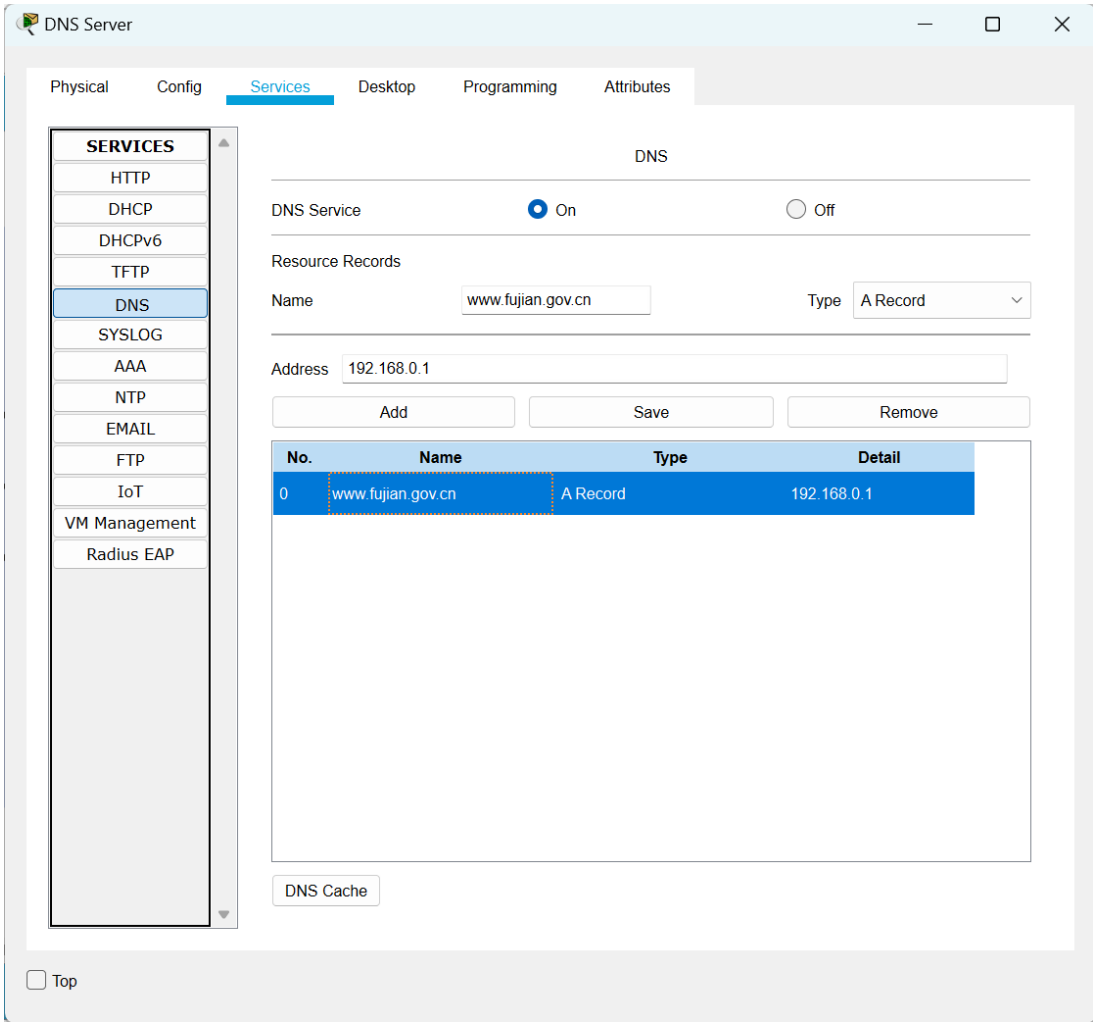

图 9　配置 DNS 服务器

5.2.3. DHCP 服务器

类似地，配置 DHCP 服务器的 IP 地址为 192.168.0.3，子网掩码为 255.255.255.0，默认网关为 192.168.0.254。开启服务器的 DHCP 服务功能，对 VLAN10 到 VLAN60 的网段分别添加地址池。以 VLAN60 为例，添加默认网关为 192.168.6.252，DNS 服务器为 192.168.0.2，起始 IP 地址为 192.168.6.0，子网掩码为 255.255.255.0，最大设备数量为 250 的地址池。配置 DHCP 服务器后，接入的终端设备无需手动配置 IP 地址，可以通过 DHCP 服务器自动获取。

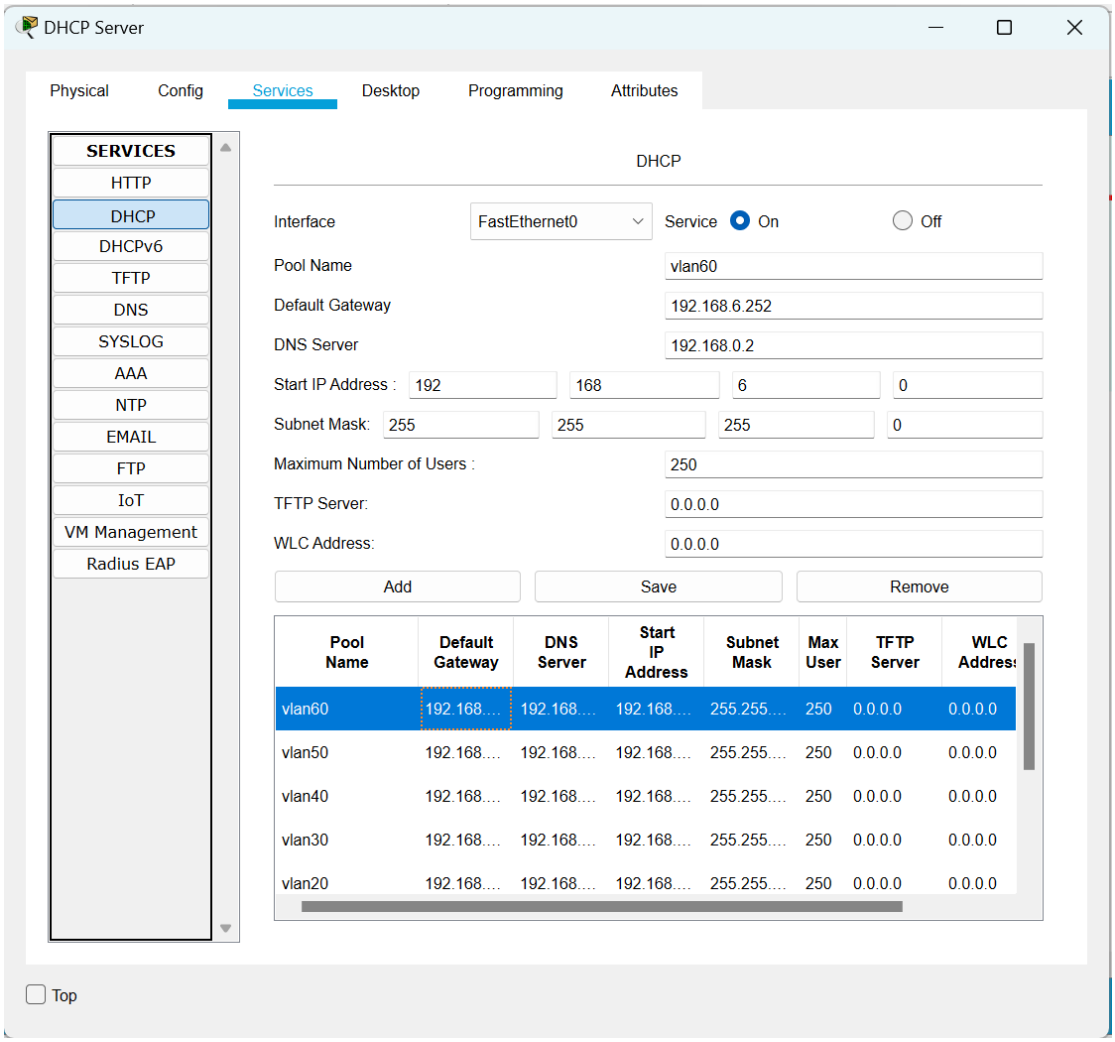

图 10　配置 DHCP 服务器

5.3. 仿真验证

1. 使用 Cisco Packet Tracer 进行仿真验证。对于网络设备，二层交换机选择 Cisco Catalyst 2960 系列交换机[5]，三层交换机选择 Cisco Catalyst 3560 系列交换机[6]，路由器选择 Cisco 2811 路由器[7]。

2. 对于各个处室的终端设备，打开 IP Config 进行配置，选择 DHCP 模式，自动获取 IP 地址、子网掩码、默认网关和 DNS 服务器的信息。

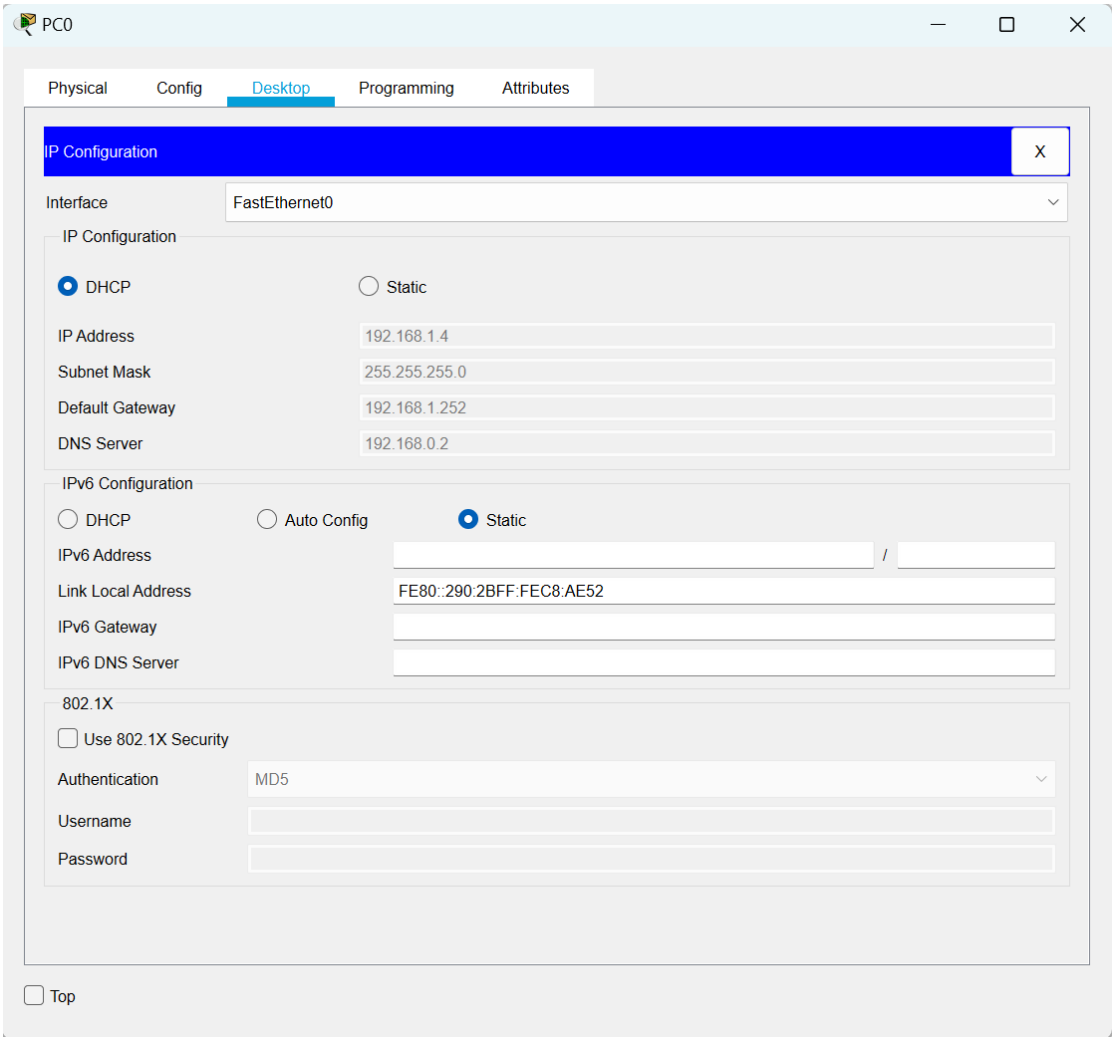

图 11　PC 通过 DHCP 进行 IP 配置

3. 相同处室的 PC 所在 VLAN 相同，可以互相 ping 通：

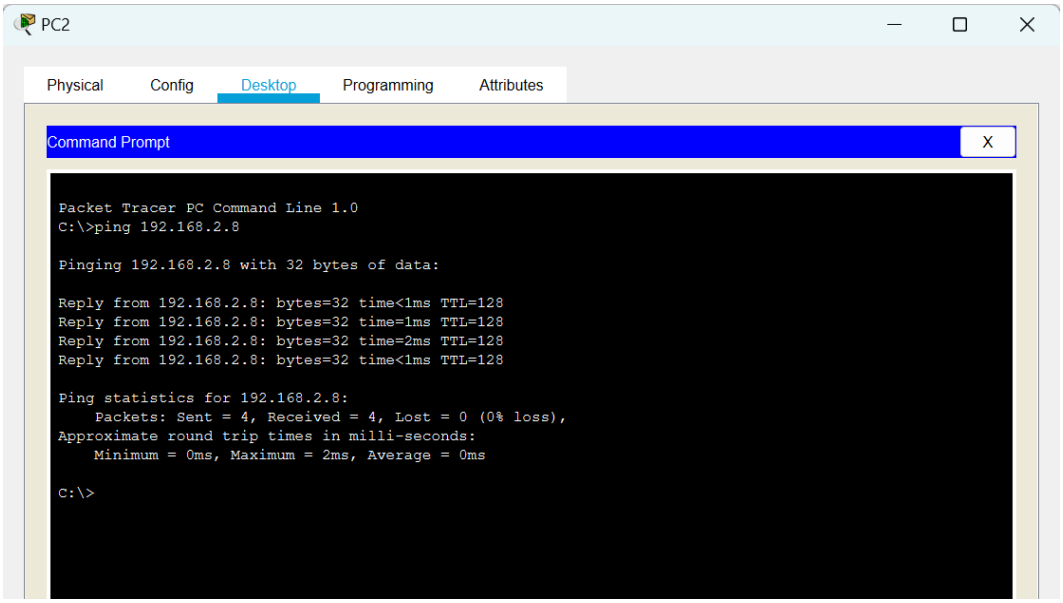

图 12　VLAN20 中的 PC 可以互相 ping 通

4. 不同处室的 PC 所在不同 VLAN 的局域网，也可以互相 ping 通：

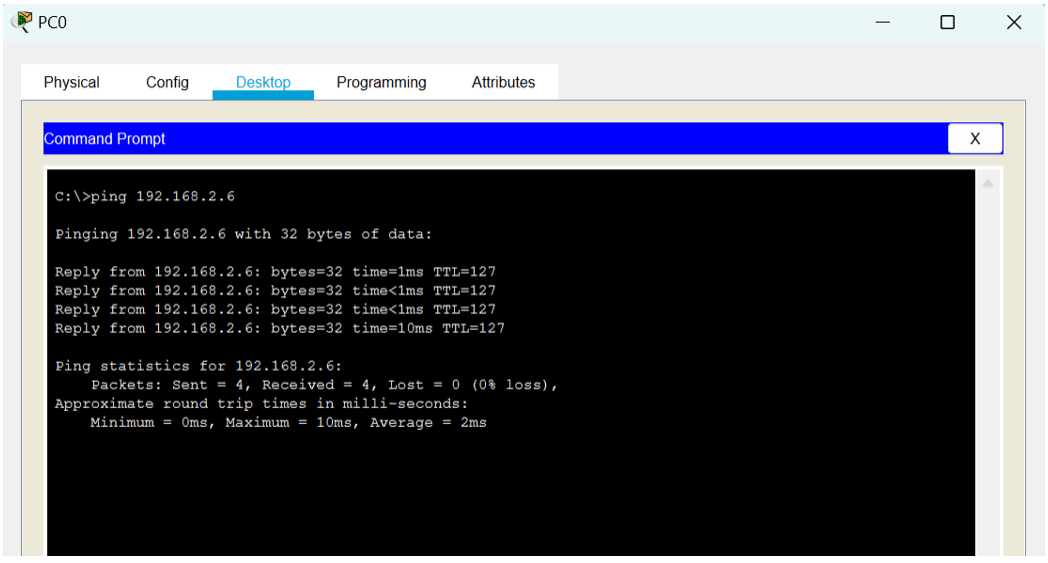

图 13　VLAN10 中的 PC 可以 ping 通 VLAN20 中的 PC

5. 处在 VLAN50（即信息处）的 PC，能够 ping 通局域网外部的 PC：

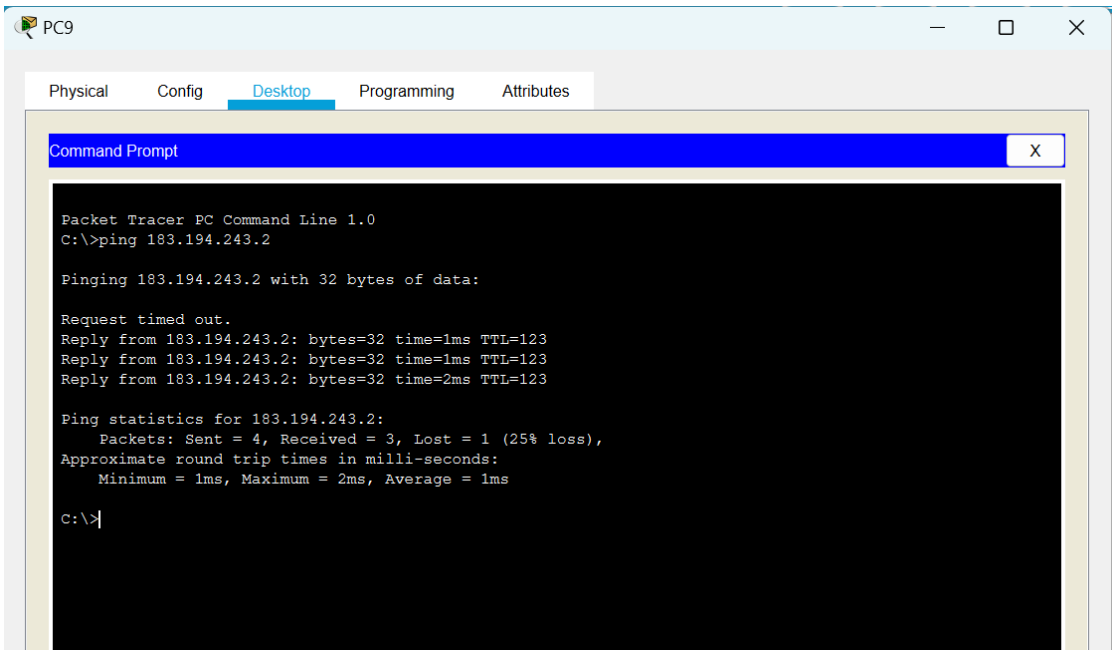

图 14　VLAN50 中的 PC 可以 ping 通局域网外部的 PC

6. 处在其他 VLAN 的 PC，无法 ping 通局域网外部的 PC：

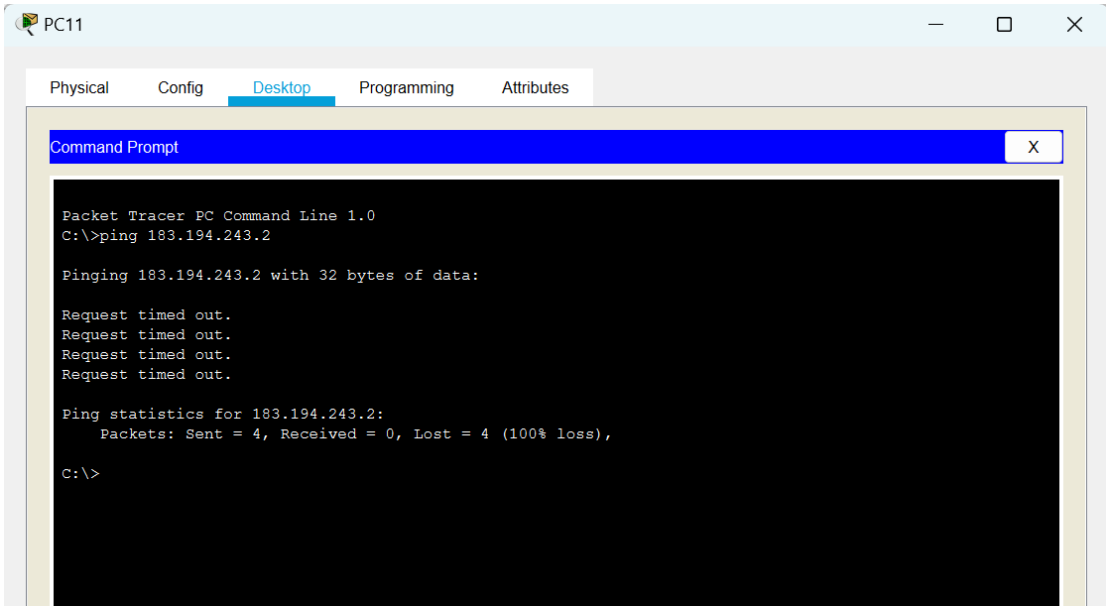

图 15　其他 VLAN 中的 PC 无法 ping 通局域网外部的 PC

7. 政府办公局域网内的 PC 可以通过浏览器访问 www.fujian.gov.cn：

图 16 局域网内的 PC 可以访问 www.fujian.gov.cn

8. 外部互联网的 PC 也可以通过浏览器访问 www.fujian.gov.cn：

图 17 外部互联网的 PC 可以访问 www.fujian.gov.cn

（六） 工程预算与进度安排

6.1. 工程预算

- 初始资金（硬件购置、软件系统采购、人员培训等）合计 150 万元；
- 后期运维（定期维护、网络带宽租用等）合计每年 10 万元；
- 风险备用资金预计约 10 万元。

6.2. 进度安排

本项目施工进度计划[8]如下表所示：

表 3　政府局域网施工进度计划表

序号	时间（日） 项目	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	办理相关证件															
2	进场															
3	通信管道建设															
4	室内镀锌线槽安装															
5	综合布线机柜安装															
6	室外光纤安装															
7	室外大对数电缆安装															
8	室内光纤安装															
9	室内大对数电缆安装															

续表 4

序号	时间（日） 项目	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
10	光纤熔接																			
11	大对数电缆端接																			
12	PVC 线管安装																			
13	网络点安装																			
14	网络点端接																			
15	网络设备安装																			
16	系统测试																			
17	试运行																			
18	整理工程资料																			
19	项目竣工验收																			

（七） 小组成员及其具体分工

7.1. 小组成员

本次课程设计作业单独成组，所有任务均由 **2154312 郑博远**独立完成。

具体任务包括计算机网络设计、实现、验证、报告撰写（项目概述、可行性分析、需求分析、网络结构设计、系统配置、工程预算及进度安排）等。

7.2. 联系方式

电话：18120929868

微信：wavesource

邮箱：zhengboyuan@tongji.edu.cn

（八） 参考资料

[1] 福建省人民政府. 福建省政府办公厅主要职责及内设机构职责[EB/OL]. (2019-11-06)[2024-08-19]. https://www.fujian.gov.cn/szf/szfjg/szfbgt/201911/t20191106_5085981.htm.

[2] 武娟.校园网网络设计及综合布线方案[J].科学技术创新,2024,(16):111-114.

[3] 胡选子，王志明，曹文梁，陈炯然，吕晓阳，王三新. 综合布线工程技术与实训教程[M]. 北京：清华大学出版社，2012.

[4] 网络技术联盟站. 网络分级设计模型的三层架构：接入层、汇聚层、核心层到底有什么说法？[EB/OL]. 华为云社区, 2024-05-26[2024-08-19]. https://bbs.huaweicloud.com/blogs/399788.

[5] 思科系统公司. Cisco Catalyst 2960 系列交换机[EB/OL]. (2019-10-31)[2024-08-20]. https://www.cisco.com/c/zh_cn/support/switches/catalyst-2960-series-switches/series.html.

[6] 思科系统公司. Cisco Catalyst 3560 系列交换机[EB/OL]. (2005-03)[2024-08-20]. https://www.cisco.com/web/CN/solutions/products_netsol/switches/products/ca3560/pdf/3560_ds_f.pdf.

[7] 思科系统公司. Cisco 2800 系列路由器[EB/OL]. [2024-08-20]. https://www.cisco.com/web/CN/partners/tools/tools_tec/tools/ds/pdf/routers_2800.pdf.

[8] 综合布线系统施工方案[EB/OL]. (2010-11-08) [2024-08-20]. https://jz.docin.com/p-420535073.html