2020年全国职业院校技能大赛改革试点赛

“网络系统管理”赛项

“网络构建”模块

（样卷1）



**全国职业院校技能大赛执委会.技术专家组**

**2020年9月**

目录

[一．说明 3](#_Toc51860187)

[二．项目背景 3](#_Toc51860188)

[三．项目规划和设计 4](#_Toc51860189)

[四．网络项目实施 13](#_Toc51860190)

[（一）设备基础信息配置与验证 13](#_Toc51860191)

[（二）网络搭建与网络冗余备份方案部署 14](#_Toc51860192)

[（三）移动互联网搭建与无线网络优化 19](#_Toc51860193)

[（四）实施出口安全防护与远程接入 21](#_Toc51860194)

[五．无线网络规划与实施 22](#_Toc51860195)

[（一）无线网络业务背景及需求介绍 22](#_Toc51860196)

[（二）无线网络中的业务规划 25](#_Toc51860197)

[六．提交竞赛结果文件说明 28](#_Toc51860198)

# 一．说明

本模块比赛时间为4小时。请合理分配竞赛时间。请仔细阅读以下要求。

1. 比赛时间结束时，请将工作站保持运行状态，评分过程需要在运行状态进行，不允许重启。由于重启造成配置丢失由考生个人负责。

2. 为了方便测试，全网允许ICMP流量通行，请将操作系统的防火墙配置为允许Ping状态。

3．默认密码：XXXXXX。

4．软件&工具:见“2020年全国职业院校技能大赛改革试点赛赛项规程”。

# 二．项目背景

陕西招财银行是一家地方性商业银行，创建于1985年，其省行（一级行）位于陕西省西安市，在全省各地市均建有二级行，各区县建立的支行及网点已超过150个。随着省行的网络扁平化改造，所有的二级行、支行及网点均需要直接连接到省行，其网络运行及维护的效率也得到了极大的提升。

为了保证网络的稳定且方便维护，省行网络分为核心区、业务区、互联区、外联区四个部分。其中：核心区作为全网的中心枢纽承担了各类业务数据流量的转发工作。业务区分别通过有线和无线网络，为生产数据流（存/取款等相关数据）和办公数据流（OA、视频会议等与钱无关的数据）提供了服务。互联区通过MSTP专线连接总行、全省所有的二级行、支行及网点。外联区通过互联网向用户提供如网上银行等线上服务，并对接第三方公司并提供相关服务；同时，省行的办公人员也能通过外联区访问Internet。

各支行/网点的业务也包括生产和办公两类。其中，生产性的数据主要由ATM机等设备通过有线方式传输；办公业务主要通过无线网络提供服务。各支行/网点的交换机通过两条MSTP专线分别将生产及办公数据传至省行。

陕西招财银行的智慧网络需要具备高速、可靠、安全的数据传输，实现高度集中计算和处理能力，为银行可持续发展铸就雄厚软实力。同时，招财银行希望在本次信息化业务建设方面，打通从供应商、采购物流、生产计划以及销售管理等多业务之间的连接环节，从而提升银行业务运营的标准化、智能化、高效化以及应对异常的能力。以上每项业务的运营对于网络稳健性、智慧性要求都带来挑战，不仅需要可靠稳定的基础网络支撑，更需要统一管理运维体系保障其庞大的业务正常运营。

为了优化省行的网络，为其它区域的网络提供高效的保障服务，陕西招财银行同时针对各个分支行、网点的网络进行升级、改造和优化。其中，对省行进行全网改造，包括调整全网拓扑实现核心网络虚拟化、部署集中式AC的智慧无线网络；保证网络在宕机时能平滑切换，保障各项业务不中断。此次也新建如龙首原支行、凤翔路支行、虎口镇网点……等多个支行和网点；同时部署网络安全整体解决方案，改变之前上网行为管理难的问题，实现员工访问网络事后可溯源，省行和各支行/网点之间传输的数据实现加密等多项安全问题；构建安全高效的网络出口，依托互联网最大限度实现各业务安全、高效、快速的传输，创建新时代金融网络环境，保障银行各项业务的高效运营。

# 三．项目规划和设计

为了顺利实施陕西招财银行全省营业网点的网络改造，优化省行的网络，为其它区域的网络提供高效的保障服务，陕西招财银行同时针对各个分支行、网点的网络进行升级、改造和优化。

1. 项目规划与建设内容

主要实施的网络信息化项目规划与建设内容如下所示。

（1）各支行/网点的网络通过MSTP专线访问省行的业务区，实现生产和办公业务互通。

（2）生产性数据通过有线网络传输、办公数据通过无线网络传输，保证其稳定性。

（3）通过路由策略部署，实现生产和办公数据按指定路径进行分流和互相备份，保证数据来回路径一致。

（4）省行及各支行网点局域网内部部署防环、防攻击、数据负载均衡等相关策略，确保局域网业务安全、可靠。

（5）保证省行特定服务器能通过外联区对外提供服务、省行的用户能正常上网，同时第三方公司能通过VPN访问银行特定资源。

**2. 项目规划与建设拓扑**

陕西招财银行全省营业网点的改造和信息化建设方案拓扑图如图1所示。

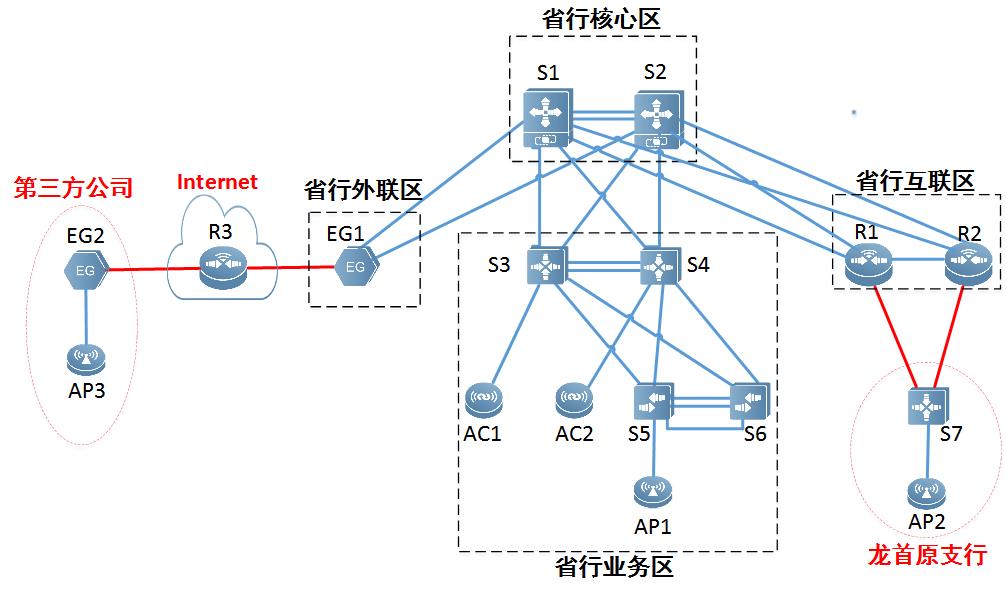


图1 陕西招财银行全省营业网点网络改造拓扑

3. 项目规划与建设拓扑

陕西招财银行省行核心网以及营业网点网络改造拓扑相关说明如下。

（1）两台数据中心交换机作为省行核心区中的核心交换机，在网络拓扑中的编号为S1和S2。

（2）两台三层可控交换机作为省行业务区中的汇聚交换机，在网络拓扑中的编号为S3和S4。

（3）两台二层可控交换机作为省行业务区中的接入交换机，在网络拓扑中的编号为S5和S6。

（4）两台无线控制器作为省行业务区中的无线网络控制器，在网络拓扑中的编号为AC1和AC2。

（5）一台无线AP作为省行业务区无线接入点，在网络拓扑中编号为AP1。

（6）省行通过互联区和支行/网点的连接，使用两台路由器接入，在网络拓扑中的编号为R1和R2。

（7）省行外联区中使用一台出口网关把省行的网络接入互联网（运营商网络），在网络拓扑中的编号为EG1。

（8）龙首原支行使用一台三层可控交换机作为支行的业务交换机，在网络拓扑中的编号为S7。

（9）龙首原支行无线网部署使用一台无线AP接入，在网络拓扑中编号为AP2。

（10）省行的外联区通过宽带链路接入运营商（Internet）路由器，运营商网络中接入路由器在网络拓扑中编号为R3。

（11）第三方公司使用一台出口网关作网络出口，在网络拓扑中编号为EG2。

（12）第三方公司使用一台无线AP部署无线网络，在网络拓扑中编号为AP3。

4. 网络拓扑连线要求与说明

在项目实施过程中，如用户无特殊要求，应根据规范要求进行各级网络设备互联，统一现场设备互联界面；使用线缆标签规范连接，使网络结构清晰明了，方便后续维护。

请根据拓扑图及网络设备物理连接表，完成设备的连线。

其中，网络物理连接表如表1所示；网络设备名称表如表2所示；网络中IPv4地址分配表如表3所示。

表1 网络设备物理连接表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 源设备名称 | 设备接口 | 接口描述 | 目标设备名称 | 设备接口 |
| S1 | Gi0/1 | Connect\_To\_EG1\_Gi0/1 | EG1 | Gi0/1 |
| Gi0/2 | Connect\_To\_S3\_Gi0/23 | S3 | Gi0/23 |
| Gi0/3 | Connect\_To\_S4\_Gi0/23 | S4 | Gi0/23 |
| Gi0/4 | Connect\_To\_R1\_Gi0/0 | R1 | Gi0/0 |
| Gi0/5 | Connect\_To\_R2\_Gi0/0 | R2 | Gi0/0 |
| Gi0/47 | Connect\_To\_S2\_Gi0/47 | S2 | Gi0/47 |
| Gi0/48 | Connect\_To\_S2\_Gi0/48 | Gi0/48 |
| S2 | Gi0/1 | Connect\_To\_EG1\_Gi0/2 | EG1 | Gi0/2 |
| Gi0/2 | Connect\_To\_S3\_Gi0/24 | S3 | Gi0/24 |
| Gi0/3 | Connect\_To\_S4\_Gi0/24 | S4 | Gi0/24 |
| Gi0/4 | Connect\_To\_R1\_Gi0/1 | R1 | Gi0/1 |
| Gi0/5 | Connect\_To\_R2\_Gi0/1 | R2 | Gi0/1 |
| Gi0/47 | Connect\_To\_S1\_Gi0/47 | S1 | Gi0/47 |
| Gi0/48 | Connect\_To\_S1\_Gi0/48 | Gi0/48 |
| S3 | Gi0/1 | Connect\_To\_AC1\_Gi0/3 | AC1 | Gi0/3 |
| Gi0/3 | Connect\_To\_S5\_Gi0/23 | S5 | Gi0/23 |
| Gi0/4 | Connect\_To\_S6\_Gi0/23 | S6 | Gi0/23 |
| Gi0/21 | Connect\_To\_S4\_Gi0/21 | S4 | Gi0/21 |
| Gi0/22 | Connect\_To\_S4\_Gi0/22 | Gi0/22 |
| Gi0/23 | Connect\_To\_S1\_Gi0/2 | S1 | Gi0/2 |
| Gi0/24 | Connect\_To\_S2\_Gi0/2 | S2 | Gi0/2 |
| S4 | Gi0/2 | Connect\_To\_AC2\_Gi0/4 | AC2 | Gi0/4 |
| Gi0/3 | Connect\_To\_S5\_Gi0/24 | S5 | Gi0/24 |
| Gi0/4 | Connect\_To\_S6\_Gi0/24 | S6 | Gi0/24 |
| Gi0/21 | Connect\_To\_S3\_Gi0/21 | S3 | Gi0/21 |
| Gi0/22 | Connect\_To\_S3\_Gi0/22 | Gi0/22 |
| Gi0/23 | Connect\_To\_S1\_Gi0/3 | S1 | Gi0/3 |
| Gi0/24 | Connect\_To\_S2\_Gi0/3 | S2 | Gi0/3 |
| S5 | Gi0/1 | Connect\_To\_AP1\_Gi0/1 | AP1 | Gi0/1 |
| Gi0/22 | Connect\_To\_S6\_Gi0/22 | S6 | Gi0/22 |
| Gi0/23 | Connect\_To\_S3\_Gi0/3 | S3 | Gi0/3 |
| Gi0/24 | Connect\_To\_S4\_Gi0/3 | S4 | Gi0/3 |
| Te0/27 | Connect\_To\_S6\_Te0/27 | S6 | Te0/27 |
| Te0/28 | Connect\_To\_S6\_Te0/28 | Te0/28 |
| S6 | Gi0/22 | Connect\_To\_S5\_Gi0/22 | S5 | Gi0/22 |
| Gi0/23 | Connect\_To\_S3\_Gi0/4 | S3 | Gi0/4 |
| Gi0/24 | Connect\_To\_S4\_Gi0/4 | S4 | Gi0/4 |
| Te0/27 | Connect\_To\_S5\_Te0/27 | S5 | Te0/27 |
| Te0/28 | Connect\_To\_S5\_Te0/28 | Te0/28 |
| AC1 | Gi0/3 | Connect\_To\_S3\_Gi0/1 | S3 | Gi0/1 |
| AC2 | Gi0/4 | Connect\_To\_S4\_Gi0/2 | S4 | Gi0/2 |
| AP1 | Gi0/1 | Connect\_To\_S5\_Gi0/1 | S5 | Gi0/1 |
| R1 | Gi0/0 | Connect\_To\_S1\_Gi0/4 | S1 | Gi0/4 |
| Gi0/1 | Connect\_To\_S2\_Gi0/4 | S2 | Gi0/4 |
| Fa1/1 | Connect\_To\_S7\_Gi0/23 | S7 | Gi0/23 |
| Fa1/0 | Connect\_To\_R2\_Fa1/0 | R2 | Fa1/0 |
| R2 | Gi0/0 | Connect\_To\_S1\_Gi0/5 | S1 | Gi0/5 |
| Gi0/1 | Connect\_To\_S2\_Gi0/5 | S2 | Gi0/5 |
| Fa1/1 | Connect\_To\_S7\_Gi0/24 | S7 | Gi0/24 |
| Fa1/0 | Connect\_To\_R1\_Fa1/0 | R1 | Fa1/0 |
| S7 | Gi0/1 | Connect\_To\_AP2\_Gi0/1 | AP2 | Gi0/1 |
| Gi0/23 | Connect\_To\_R1\_Fa1/1 | R1 | Fa1/1 |
| Gi0/24 | Connect\_To\_R2\_Fa1/1 | R2 | Fa1/1 |
| AP2 | Gi0/1 | Connect\_To\_S7\_Gi0/1 | S7 | Gi0/1 |
| EG1 | Gi0/1 | Connect\_To\_S1\_Gi0/1 | S1 | Gi0/1 |
| Gi0/2 | Connect\_To\_S2\_Gi0/1 | S2 | Gi0/1 |
| Gi0/4 | Connect\_To\_R3\_Gi0/1 | R3 | Gi0/1 |
| R3 | Gi0/0 | Connect\_To\_EG2\_Gi0/4 | EG2 | Gi0/4 |
| Gi0/1 | Connect\_To\_EG1\_Gi0/4 | EG1 | Gi0/4 |
| EG2 | Gi0/1 | Connect\_To\_AP3\_Gi0/1 | AP3 | Gi0/1 |
| Gi0/4 | Connect\_To\_R3\_Gi0/0 | R3 | Gi0/0 |
| AP3 | Gi0/1 | Connect\_To\_EG2\_Gi0/1 | EG2 | Gi0/1 |

表2 网络设备名称表

|  |  |  |
| --- | --- | --- |
| 拓扑中设备名称 | 配置主机名（hostname名） | 备注 |
| S1 | SHHXQ-DataCenter-Switch-S1 | 省行核心区核心交换机1 |
| S2 | SHHXQ-DataCenter-Switch-S2 | 省行核心区核心交换机2 |
| S3 | SHYWQ-Aggregation-Switch-S3 | 省行业务区汇聚交换机1 |
| S4 | SHYWQ-Aggregation-Switch-S4 | 省行业务区汇聚交换机2 |
| S5/S6(VSU) | SHYWQ-Access-Switch-Virtual -Switch | 省行业务区接入交换机(虚拟化) |
| AC1/AC2(VAC) | SHYWQ-Wireless-Switch | 省行业务区无线控制器(VAC) |
| R1 | SHHLQ-Router-R1 | 省行互联区互联路由器1 |
| R2 | SHHLQ-Router-R2 | 省行互联区互联路由器2 |
| S7 | LSYZH-Aggregation-Switch-S7 | 龙首原支行业务网中汇聚交换机 |
| EG1 | SHWLQ-Egress-Gateway-EG1 | 省行外联区出口网关设备 |
| R3 | ISP-Router-R3 | 运营商网络中接入路由器 |
| EG2 | DSF-Egress-Gateway-EG2 | 第三方公司出口网关 |

表3 IPv4地址分配表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口或VLAN | VLAN名称 | 二层或三层规划 | 说明 |
| S1 | Gi0/1 | \ | 10.1.3.1/30 | 互联地址 |
| Gi0/2 | \ | 10.1.1.1/30 | 互联地址 |
| Gi0/3 | \ | 10.1.1.5/30 | 互联地址 |
| Gi0/4 | \ | 10.1.2.1/30 | 互联地址 |
| Gi0/5 | \ | 10.1.2.5/30 | 互联地址 |
| Gi0/47-48  （AG1） | \ | 10.1.254.253/30 | OSPF100进程 |
| Loopback 0 | \ | 10.1.0.1/32 | —— |
| S2 | Gi0/1 | \ | 10.1.3.5/30 | 互联地址 |
| Gi0/2 | \ | 10.1.1.9/30 | 互联地址 |
| Gi0/3 | \ | 10.1.1.13/30 | 互联地址 |
| Gi0/4 | \ | 10.1.2.9/30 | 互联地址 |
| Gi0/5 | \ | 10.1.2.13/30 | 互联地址 |
| Gi0/47-48（AG1） | \ | 10.1.254.254/30 | OSPF100进程 |
| Loopback 0 | \ | 10.1.0.2/32 | —— |
| S3 | VLAN 10 | Production | 192.1.10.252/24 | 生产/有线用户地址 |
| VLAN 50 | APManage\_YWQ | 192.1.50.252/24 | 业务区AP管理地址 |
| VLAN 60 | Wireless | 192.1.60.252/24 | 办公/无线用户地址 |
| VLAN 100 | Manage | 192.1.100.252/24 | 设备管理 |
| Gi0/23 | \ | 10.1.1.2/30 | 互联地址 |
| Gi0/24 | \ | 10.1.1.10/30 | 互联地址 |
| Loopback 0 | \ | 10.1.0.3/32 | —— |
| S4 | VLAN 10 | Production | 192.1.10.253/24 | 生产/有线用户地址 |
| VLAN 50 | APManage\_YWQ | 192.1.50.253/24 | 业务区AP管理地址 |
| VLAN 60 | Wireless | 192.1.60.253/24 | 办公/无线用户地址 |
| VLAN 100 | Manage | 192.1.100.253/24 | 设备管理地址 |
| Gi0/23 | \ | 10.1.1.6/30 | 互联地址 |
| Gi0/24 | \ | 10.1.1.14/30 | 互联地址 |
| Loopback 0 | \ | 10.1.0.4/32 | —— |
| S5-S6  (虚拟化) | VLAN 10 | Production | Gi1/0/6至 Gi1/0/20,  Gi2/0/6至 Gi2/0/20 | 生产/有线用户地址 |
| VLAN 50 | APManage\_YWQ | Gi1/0/1至 Gi1/0/5,  Gi2/0/1至 Gi2/0/5 | 业务区AP管理地址 |
| VLAN 100 | Manage | 192.1.100.1/24 | 设备管理地址 |
| AC1 | VLAN 100 | Manage | 192.1.100.2/24 | 设备管理地址 |
| Loopback 0 | \ | 10.1.0.5/32 | —— |
| AC2 | VLAN 100 | Manage | 192.1.100.3/24 | 设备管理地址 |
| Loopback 0 | \ | 10.1.0.6/32 | —— |
| R1 | Gi0/0 | \ | 10.1.2.2/30 | 互联地址 |
| Gi0/1 | \ | 10.1.2.10/30 | 互联地址 |
| Fa1/0 | \ | 10.1.2.253/30 | 互联地址 |
| Fa1/1 | \ | 10.1.2.21/30 | 互联地址 |
| Loopback 0 | \ | 10.1.0.7/32 | —— |
| R2 | Gi0/0 | \ | 10.1.2.6/30 | 互联地址 |
| Gi0/1 | \ | 10.1.2.14/30 | 互联地址 |
| Fa1/0 | \ | 10.1.2.254/30 | 互联地址 |
| Fa1/1 | \ | 10.1.2.25/30 | 互联地址 |
| Loopback 0 | \ | 10.1.0.8/32 | —— |
| S7 | Gi0/23 | \ | 10.1.2.22/30 | 互联地址 |
| Gi0/24 | \ | 10.1.2.26/30 | 互联地址 |
| VLAN 410 | Production | 194.1.10.254/24  G0/11-20 | 生产/有线用户地址 |
| VLAN 450 | APManage\_YWQ | 194.1.50.254/24 | 业务区AP管理地址 |
| VLAN 460 | Wireless | 194.1.60.254/24 | 办公/无线用户地址 |
| Loopback 0 | \ | 10.1.0.9/32 | —— |
| EG1 | Gi0/1 | \ | 10.1.3.2/30 | 互联地址 |
| Gi0/2 | \ | 10.1.3.6/30 | 互联地址 |
| Gi0/4 | \ | 200.1.1.2/29 | 互联地址 |
| Tunnel0 | \ | 10.1.4.1/30 | GRE接口地址 |
| Loopback 0 | \ | 10.1.0.10/32 | —— |
| R3 | Gi0/0 | \ | 200.2.1.1/29 | 互联地址 |
| Gi0/1 | \ | 200.1.1.1/29 | 互联地址 |
| Loopback 1 | \ | 195.1.1.1/32 | —— |
| EG2 | Gi0/1.60 | \ | 195.1.60.254/24 | 用户地址 |
| Gi0/1.100 | \ | 195.1.100.254/24 | AP管理地址 |
| Gi0/4 | \ | 200.2.1.2/29 | 互联地址 |
| Tunnel0 | \ | 10.1.4.2/30 | GRE接口地址 |
| Loopback 0 | \ | 10.1.0.11/32 | —— |

# 四．网络项目实施

## （一）设备基础信息配置与验证

**1. 完成网络设备规范命名；配置网络设备基础信息。**

（1）根据网络设备名称表（表2），修订所有设备名称。

（2）依据网络设备物理连接表（表1），配置设备接口描述信息。

**2. 完成网络设备密码恢复，实现设备软件版本统一。**

（1）交换机S7做密码恢复，新密码设置为admin1234。

（2）交换机S7进行版本更新至指定版本，指定版本见现场升级文件包。

**3. 保障全网中的网络设备安全。**

（1）在所有的网络设备上都需要开启SSH服务，以保障网络设备的安全。其中，用户名密码分别为admin、admin1234；特权密码为admin1234。

（2）为方便实现对全网开展网络管理功能，网络管理员计划增设网管平台，网管平台的IP规划为172.16.0.254/24。

（3）为了实现网管平台后期上线后可用，需要在每台设备上部署SNMP功能，配置所有网络设备的SNMP消息报告机制。其中，向主机172.16.0.254发送Trap消息版本采用V2C；读写的Community为“admin”；只读的Community为“public”；开启Trap消息通告。

## （二）网络搭建与网络冗余备份方案部署

**1.在全网部署虚拟局域网，完成全网IPv4地址部署。**

为了减少全网中广播干扰，需要在全网规划和部署VLAN，需要实施的内容如下所示。

（1）全网的VLAN规划和配置合理，并在Trunk链路上不允许不必要VLAN中的数据流通过。

（2）为了隔离网络终端之间的二层互访，需要在交换机S5、S6的Gi0/6-Gi0/20端口上，启用端口保护功能。

（3）根据“网络设备名称表（表2）”、“IPv4地址分配表（表3）”中规划要求，在各设备上完成对应的VLAN、IP地址的配置。

**2. 在局域网中部署环路规避方案**

为避免网络接入设备上出现环路，影响全网运行状态。要求在网络接入交换机S5、S6上进行防环处理。具体要求如下所示。

（1） 在连接PC机端口上开启Portfast和BPDUguard防护功能。

（2）为防止接入交换机的下联端口出现用户私接集线器（Hub）设备引起办公网中的环路，需要启用RLDP协议进行防环处理。

（3）接入交换机的连接终端的接口上检测到环路后，要求处理的方式为Shutdown-Port，实现防环保护。

（4）一旦端口检测异常事件并进入Err-Disabled状态，设置300秒自动恢复机制（基于接口部署策略）。

**3. 部署DHCP中继与服务安全**

（1）在交换机S3、S4上配置DHCP中继功能，使得网络中的终端用户通过DHCP Relay方式获取IP地址。

（2）省行的DHCP服务器搭建于S1交换机上,一方面为无线网络中的用户提供地址服务；同时为网络中的无线AP设备提供管理地址（具体参数见表3：IPv4地址分配表，共3个网段：192.1.10.0/24，192.1.50.0/24，192.1.60.0/24）。其中，无线AP的地址租约为永久；无线网络中用户设备的租约为0.5天。

（3）为了防御局域网中出现伪造DHCP服务器与ARP欺骗安全事件，需要在S5、S6交换机上部署DHCP 的“Snooping+DAI”功能。其中，DAI安全功能主要针对VLAN10中用户设备启用ARP防御。

（4）为了防止网关设备连续发送大量、正常报文，被接入交换机误认是攻击事件而被丢弃，导致下联网络中的用户设备无法获取网关设备上发出ARP信息，造成无法上网，要求关闭S5、S6交换机上联口上“NFPP arp-guard”功能。

（5）调整S5、S6交换机设备上的“CPU保护机制”，其中，调整ARP带宽为1500pps。

**4. 部署MSTP及VRRP技术，实现网络冗余。**

在交换机S3、S4、S5、S6上配置MSTP防止二层环路。

（1）配置MSTP要求来自VLAN10、VLAN100中的数据流经过S3交换机转发，一旦S3交换机失效时，经过S4交换机转发。要求来自VLAN50、VLAN60中的数据流经过S4交换机转发，一旦S4交换机失效时，经过S3交换机转发。

其中，所配置的MSTP参数要求：region-name为test；revision版本为1；实例1包含VLAN10，VLAN100；实例2包含VLAN50,VLAN60。

（2）配置S3交换机作为实例1的主根、实例2的从根；配置S4交换机作为实例2的主根、实例1的从根；其中，主根交换机的优先级为4096；从根交换机的优先级为8192。

（3）在交换机S3、S4连接接入交换机S5、S6的接口上，启用“TC-IGNORE”功能，规避网络中的接入设备出现频繁的网络震荡。

（4）在交换机S3和S4上配置VRRP，实现网络中的主机的网关冗余，所配置的参数要求如表4所示。其中，在交换机S3、S4上设置各VRRP组中的高优先级设置为150，低优先级设置为120。

（5）为提升网络的冗余功能，在交换机S3与S4之间部署2条互联链路（Gi0/21、Gi0/22），并采取LACP动态聚合模式配置二层链路聚合；其它接口根据网络设备互联需要，进行静态链路聚合配置，生成聚合接口AG2。

表4 S3和S4的VRRP参数表

|  |  |  |
| --- | --- | --- |
| VLAN | VRRP备份组号（VRID） | VRRP虚拟IP |
| VLAN10 | 10 | 192.1.10.254 |
| VLAN50 | 50 | 192.1.50.254 |
| VLAN60 | 60 | 192.1.60.254 |
| VLAN100 | 100 | 192.1.100.254 |

**5. 部署网络设备虚拟化，保障核心网络稳健。**

为增加网络的稳健性，业务区域中的两台接入交换机通过核心网络虚拟化技术，虚拟成一台设备进行集中管理，从而实现网络的高可靠性。当网络中的任意一台交换机出现故障时，都能够实现设备、链路切换，保证业务不中断。

（1） 部署交换机S5和S6之间的Te0/27-28端口作为VSL链路，使用核心网络的虚拟化技术实现核心网络的虚拟化。其中：设置S5交换机为主交换机；设置S6交换机为备用交换机。

（2）规划交换机S5和S6之间的Gi0/22端口作为双主机检测链路，配置基于BFD的双主机检测。当VSL链路中的所有物理链路都异常断开时，备用交换机会切换成主机，从而保障网络正常运营。

需要配置主交换机参数信息为：Domain id：1；Switch id:1;priority 150; description:Access-Switch-Virtual-Switch1。

需要配置备交换机设备参数信息为：Domain id：1；Switch id:2；priority 120；description:Access-Switch-Virtual-Switch2。

**6. 部署全网路由协议，实现全网的互联互通。**

在省行的核心区、业务区、互联区以及各支行/网点之间，使用OSPF协议组网，实现全网的互联互通，具体要求如下。

（1）在省行的核心区与业务区（S1、S2、S3、S4）中，部署OSPF 100；使用单区域（区域0）部署。

（2）在省行的互联区和各支行/网点（S1、S2、R1、R2、S7）连接上，部署OSPF 200；使用多区域规划。其中，省行互联区（S1、S2、R1、R2）属于AREA 0；龙首原支行（R1、R2、S7）属于AREA 1。

（3） 在省行业务区，要求VLAN100设备管理地址段不参与OSPF邻居建立。

（4）在省行的业务区，要在交换机S3、S4的始发终端网段以及VLAN100设备管理地址段，均以重发布直连的方式注入路由。

（5）在交换机S1和S2之间启用OSPF与BFD联动，以达到迅速检测对端中断，快速实现备份，提高用户网络体验。

（6）优化OSPF相关配置，以尽量加快OSPF收敛。

（7）重发布路由进OSPF中使用类型1。

此外，使用静态路由实现以下区域之间的网络通信。

（8） 在AC1和AC2之间通过静态路由，使用管理地址（VLAN 100）分别与S3、S4交换机之间通信。

（9）使用静态路由实现省行的外联区之间（EG1、S1、S2）通信。

（10）使用静态路由第三方公司（EG2、AP3）之间通信。

（11）使用静态路由Internet区域（EG1、R3、EG2）之间通信。

**7. 部署部分区域路由选路，实现策略路由。**

考虑到全网中数据分流需求以及实现网络的负载均衡的目的，需要进行路由策略部署，具体要求如下所示。

（1）龙首原支行的原生产网段（VLAN 410）、办公网段（VLAN 460）需要与省行的业务区、生产办公区的业务互联互通，需要在交换机S7本地以Network发布明细路由。因业务连通的需要，所有增加的网络终端数据之间的通信，一并划入办公网段进行转发。

（2）在S3、S4交换机中引入路由时，需要进行路由标记。其中，生产网段（VLAN 10）标记为10；办公网段（VLAN 60）标记为20。因业务连通需要，所有增加的网络终端数据之间的通信，一并划入办公网段进行路由标记，路由图定义为SET\_TAG。

（3）在S1、S2交换机上，要求通过OSPF双进程实施重发布。其中，在OSPF 100进程发布至OSPF 200进程时，关联路由图定义为OSPF100\_TO\_OSPF200；在OSPF200进程发布至OSPF100进程时，关联路由图定义为OSPF200\_TO\_OSPF100。

（4）为了防止路由环路以及次优路径的风险，在S1和S2交换机上配置FILTER-LIST。其中，把OSPF200进程内路由过滤关联路由图定义为FILTER\_OSPF100\_Route；OSPF100进程内关联路由图定义为FILTER\_OSPF200\_Route。

（5）各路由图以及连接的各接口中，凡是涉及COST值的调整，要求其值必须调整为5或10。

（6）通过部署策略，使得生产网段的业务（VLAN 410-VLAN 10）的主路径为S7-R1-S1-S3-VSU；办公网段的业务（VLAN 460-VLAN 60）的主路径为S7-R2-S2-S4-VSU；并且要求来回路径一致。

（7）在交换机S1连接S2、路由器R1连接R2的主链路或主设备发生故障时，可以无缝地切换到备用链路或备用设备上。

（8）配置省区业务区中的办公数据（VLAN 60）访问Internet的路径为S4-S2-EG1；配置各支行/网点中的办公数据（VLAN 460）访问Internet的路径为：S7-R2-S2-EG1；并且要求来回路径一致。

**8. 在省行的业务区中部署IPv6业务。**

（1）在省行的业务区中部署IPv6业务，实现机构内网中的IPv6终端设备可自动从网关处获取IPv6地址。

（2）在S3、S4交换机上配置VRRP for IPv6路由，在网络中主机上实现IPv6网关冗余。其中，VRRP for IPv6与MSTP的主备状态与IPV4网络中配置保持一致。

（3）在省行的业务区中部署IPv6业务，其中，IPV6地址规划如表5所示。

**表5 IPV6地址规划表**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **设备** | **接口** | **IPV6地址** | **VRRP组号** | **虚拟IP** | **虚拟链路本地地址** |
| S3 | VLAN10 | 2001:192:10::252/64 | 10 | 2001:192:10::254/64 | FE80::4/64 |
| VLAN50 | 2001:192:50::252/64 | 50 | 2001:192:50::254/64 | FE80::4/64 |
| VLAN60 | 2001:192:60::252/64 | 60 | 2001:192:60::254/64 | FE80::4/64 |
| VLAN100 | 2001:192:100::252/64 | 100 | 2001:192:100::254/64 | FE80::4/64 |
| S4 | VLAN10 | 2001:192:10::253/64 | 10 | 2001:192:10::254/64 | FE80::4/64 |
| VLAN50 | 2001:192:50::253/64 | 50 | 2001:192:50::254/64 | FE80::4/64 |
| VLAN60 | 2001:192:60::253/64 | 60 | 2001:192:60::254/64 | FE80::4/64 |
| VLAN100 | 2001:192:100::253/64 | 100 | 2001:192:100::254/64 | FE80::4/64 |

## （三）移动互联网搭建与无线网络优化

**1.在省行的业务区中部署无线网络。**

（1）在省行的业务区中部署无线网络，无线网络架构采用FIT AP+AC的方案。区域内所有AP（AP1）都关联到双AC进行管理。

（2）在省行的业务区中，配置S1交换机作为无线网络中用户（VLAN 60）和无线FIT AP（VLAN 50）的DHCP服务器。

（3）在省行的业务区部署无线网络，设置内网中的SSID为Admin\_SHYWQ\_XX(XX现场提供)；WLANID为1；AP-GROUP为Admin\_SHYWQ。内网中的无线用户在关联SSID后，可自动获取VLAN60地址。

**2.在龙首原支行部署无线网络。**

（1）龙首原支行无线网络架构采用FIT AP+AC的方案，区域内所有AP（AP2）都关联到双AC进行管理。

（2）龙首原支行使用S7交换机作为无线网络中用户（VLAN 460）和无线网络中的FIT AP（VLAN 450）设备的DHCP服务器。

（3）在龙首原支行中配置内网的SSID为Admin\_LSYZH\_XX(XX现场提供)；WLANID为2；AP-GROUP为Admin\_LSYZH；内网中的无线用户在关联到SSID后，可自动获取VLAN460地址。

**3.在无线网络中部署AC冗余，实现备份。**

（1）在无线网络中部署AC冗余，实现备份。其中，配置AC1为主用；配置AC2为备用。此外，AP与AC1、AC2之间均需要建立隧道，规划Fit AP与双AC的VLAN100设备管理地址建立隧道建立。

（2）当AP与AC1失去连接时，能无缝切换至AC2，并提供连续服务。

**4.第三方公司胖AP部署。**

第三方公司的AP3使用胖模式进行部署，具体要求如下所示。

（1） 配置AP3设备，使用透明模式传输。其中，管理地址为195.1.100.1/24；网关地址为195.1.100.254，网关部署在EG2上。

（2）在AP3设备上，创建SSID(WLAN-ID 3)为Admin-Fat\_XX(备注：XX现场提供)，保障内网中无线网络中的用户在关联SSID后，可自动获取 195.1.60.0/24网段地址（DHCP部署在EG2上）。

**5. 保障无线网络安全。**

（1）无线网络中的用户通过Fit AP方式接入无线网络时，采用WPA2加密方式，加密密码为XX(现场提供)。

（2）无线网络中的用户通过Fat AP方式接入无线网络时，采用WEB认证方式，认证用户名、密码为XX(现场提供)。

**6.实施无线网络的性能优化**

（1）省行业务区AP（AP1）采用集中转发模式，各支行/网点AP（AP2）采用本地转发模式。

（2）限制AP的每个射频卡最大带点人数为18人。

（3）调整2.4G频段的射频卡powerlocal功率数值为20；5.8G频段的射频卡powerlocal功率数值为100。尽量降低同频干扰带来的影响。

（4）调整5.8G射频卡的无线频率带宽至40MHz，增大数据传输带宽。

（5）为保证终端走到AP覆盖的边缘区域，终端能够及时发起漫游，调整Coverage-area-control功率参数，其中：5.8G的Coverage-area-control功率调整为17db；2.4G的Coverage-area-control功率调整为10db。

（6）关闭低速率（11b/g 1M、2M、5M，11a 6M、9M）应用接入。

## （四）实施出口安全防护与远程接入

**1.出口设备上部署NAT，实现远程接入。**

出口设备上部署NAT，实现远程接入，具体配置参数如下。

（1）省行外联区出口网关EG1上进行NAT配置，实现省行业务区办公网络（VLAN 60、VLAN 460），通过NAPT方式将内网IP地址转换到互联网接口上。其中，NAT地址池的地址为200.1.1.3/29-200.1.1.5/29；生产网络（VLAN 10,VLAN 410）及其他地址均不允许访问互联网。

（2）在省行外联区的出口网关EG1上配置以下业务，使业务区中的VSU接入交换机（S5、S6，地址为192.1.100.1）的Telnet服务可以通过互联网被访问，并将其地址映射至运营商线路上，映射地址为200.1.1.6，映射端口23333。

（3）在第三方公司的出口网关EG2上，进行NAT部署，实现其无线网络中的用户能访问Internet。其中，NAT地址池与EG2的Gi0/4接口IP相同。

**2.在出口设备上部署Web Portal用户认证，实现出口安全防护。**

（1）在网关EG1上启用Web Portal认证服务。创建两个认证用户，其用户名/密码分别为：user1/user1、user2/user2。

（2）在各支行/网点用户（VLAN 460）上，使用WEB认证方式访问互联网。

（3）在省行的业务区中办公的用户（VLAN 60），不需在EG上进行WEB认证，即可访问互联网。

**3.在出口设备上应用流量控制。**

在第三方公司出口网关EG2上，针对内网访问互联网WEB流量，限速每个IP为1000Kbps；内网中WEB总流量不超过20Mbps。通道名称定义为WEB。

**4. 在出口设备上部署用户行为策略。**

（1）在第三方公司出口网关EG2上，实施基于网站访问、邮件收发、IM聊天、论坛发帖、搜索引擎等多应用，启用审计功能。

（2） 配置EG2设备安全防护，要求从周一到周六的工作时间09：00—17:00（命名为work）内，阻断并审计P2P应用软件使用,审计策略名称定义为P2P。

**5. 在出口设备上部署VPN安全。**

为了实现陕西招财银行与第三方公司之间互访数据的安全性，针对来往数据使用VPN技术进行安全保障，具体规划如下所示。

（1）在网络安全出口设备EG1与EG2之间，启用GRE Over IPSec VPN嵌套功能。

（2） 配置IPSec使用静态点对点模式；esp传输模式封装协议；isakmp策略定义加密算法采用3des；散列算法采用md5；预共享密码为ruijie；DH使用组2。转换集myset定义加密验证方式为esp-3des esp-md5-hmac，感兴趣流ACL编号为103，加密图定义为mymap。

# 五．无线网络规划与实施

某局点银行最近在天地城新租用了一栋综合商住两用楼，用于网点临时办公，对于部分已经有有线信息点的办公室利旧部署无线，要求在有线使用的同时能使用无线。本次项目因为资金紧张，经充分论证，本次无线覆盖项目拟投入17.5万元（网络设备采购部分），项目要求办公区、办公室、会议厅、寝室、展厅均覆盖（不要求覆盖茶水间、洗手间）。

## （一）无线网络业务背景及需求介绍

**1.楼宇相关信息介绍。**

（1）建筑使用说明。

该楼宇为一栋综合楼，101—106为独立办公室，107—108为小型会议室，109为大型会议室，1001—1016为员工寝室，预计展厅人流量为60人左右。

（2）建筑现场情况介绍。

该楼层室内无吊顶，开放式办公区和走廊为吊顶布置，原有强电布线室内外均采用了pvc线槽敷设，独立办公室布为有线网络，客户希望利用原有网络。墙高3米，无梁。

（3）建筑物弱电间情况介绍。

该楼宇目前有独立的弱电间整层建筑平面布局图，如图2所示。

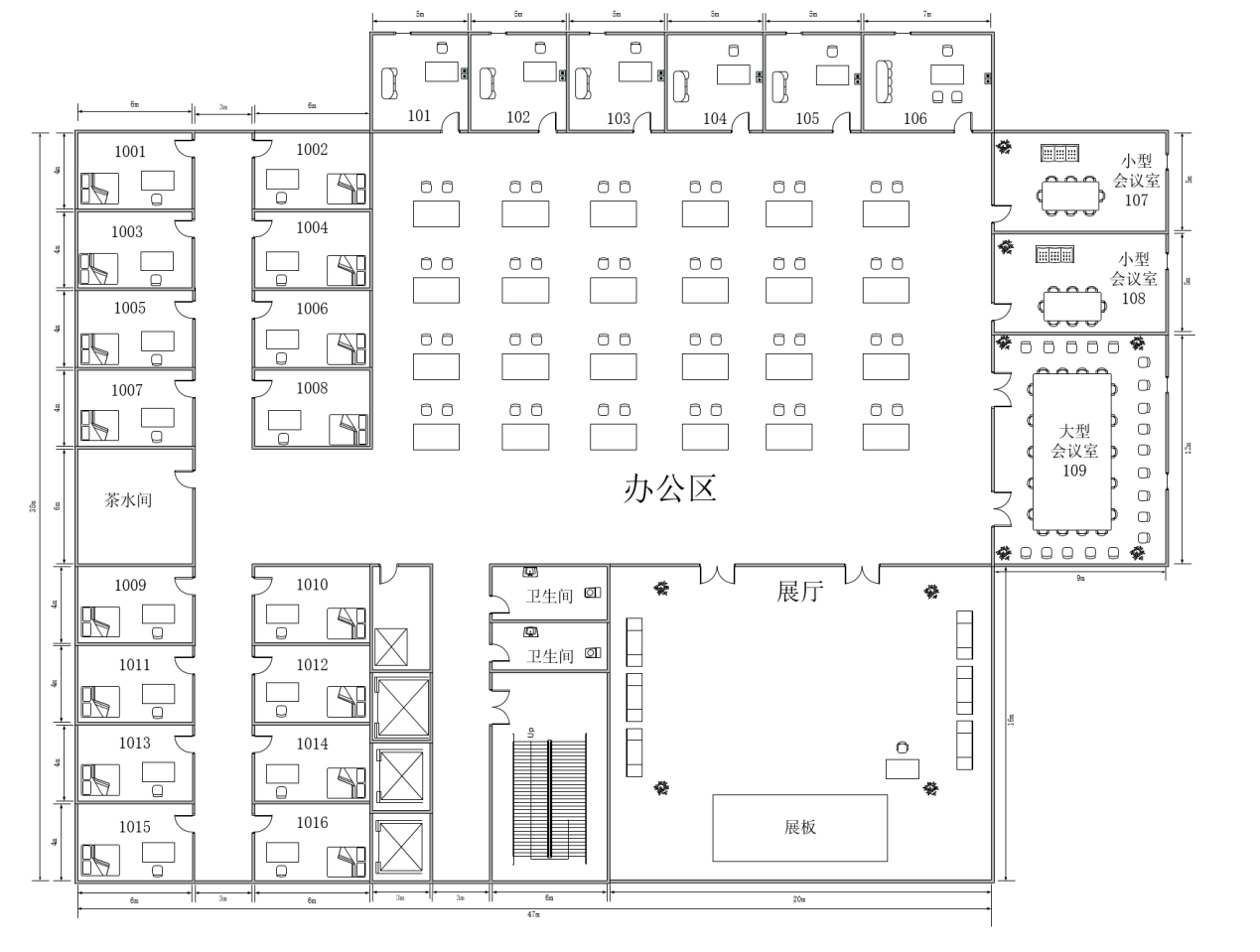


图2 平面布局图

**2.无线产品的参数与价格介绍。**

无线产品及配件价格表如表6所示。

表6 无线产品及配件价格表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **产品型号** | **产品特征** | **传输速率（2.4G/最大）** | **推荐/最大带点数** | **功率** | **价格（元）** |
| AP330-I | 双频双流 | 300M/1.167G | 32/256 | 100mW | 6000 |
| AP220-E(M)-V3.0 | 双频双流 | 300M/600M | 32/256 | 100mW | 11000 |
| RG-Cab-SMA-10m | 10米馈线 | N/A | N/A | N/A | 1600 |
| RG-Cab-SMA-15m | 15米馈线 | N/A | N/A | N/A | 2400 |
| RG-IOA-2505-S1 | 双频单流/单频单流 | N/A | N/A | N/A | 500 |
| AP110-w | 单频单流 | 150M | 12/32 | 60mW | 2500 |
| S2928G-24P | 24口POE交换机 | N/A | N/A | 240W | 15000 |
| WS6008 | 无线控制器 | 6\*1000M | 32/200 | 40W | 50000 |

**3.无线网络系统中集成物料清单。**

无线网络系统中综合布线工程材料清单如表7所示。

表7 综合布线工程材料清单

|  |  |  |  |
| --- | --- | --- | --- |
| 产品名称 | 规格 | 容纳网线数 | 单位 |
| Cat5e网络配线架 | 24口、1U | 24 | 个 |
| 理线架 | 1U | 24 | 个 |
| PVC线槽 | 20mm\*10mm\*2.8m | 1~2 | 条 |
| 25mm\*12.5mm\*2.8m | 3~4 | 条 |
| 30mm\*16mm\*2.8m | 5~7 | 条 |
| 39mm\*19mm\*2.8m | 8~12 | 条 |
| 50mm\*25mm\*2.8m | 13~22 | 条 |
| PVC线槽底盒 | 标准 | 2 | 个 |
| PVC暗盒 | 标准 | 2 | 个 |
| PVC线管 | 16mm\*2.8m | 1~3 | 条 |
| 20mm\*2.8m | 2~5 | 条 |
| 25mm\*2.8m | 4~8 | 条 |
| 金属桥架 | 50mm\*25mm | 13~22 | 米 |
| 60mm\*22mm | 13~23 | 米 |
| Cat5e网线 | 305米/箱 | N/A | 箱 |
| Cat5e水晶头 | 100个/盒 | N/A | 盒 |
| 机柜 | 6U | N/A | 个 |
| 机柜 | 12U | N/A | 个 |

## （二）无线网络中的业务规划

**1.完成楼宇中无线地勘。**

根据提供的建筑平面布局图、项目预算（设备经费）和业务需求进行AP的规划与设计，通过无线地勘软件进行AP点位设计和无线信号仿真，确保无线信号全覆盖（厕所、楼梯间区域无须覆盖）。

然后进一步做无线信道规划，并输出该层无线AP点位示意图、无线热图和网络设备清单。

（1）绘制AP点位图（包括：AP型号、编号、信道等信息，其中信道采用2.4G的1、6、11三个信道进行规划）。其中，AP点位参考示意图如图3所示。



图3 AP点位参考示意图

（2）使用无线地勘软件，输出AP点位图的2.4G频道的信号仿真热图（仿真信号强度要求大于-65db），参考示意图如图4所示。



图4 仿真热图示意图

（3）输出该无线网络工程项目设备的预算表，网络设备型号和价格依据表3，并填写表8设备清单表。

表8 设备清单

|  |  |  |  |
| --- | --- | --- | --- |
| **设备型号** | **单价** | **数量** | **总价** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 项目总预算 | | |  |

**2.完成网络系统集成工勘。**

根据AP点位部署位置和建筑物现场情况，输出无线网络工程项目施工的水平布线图、机柜安装示意图、网络配线架标签和物料清单。

（1）根据无线AP点位和建筑物现场环境，设计该无线网络的水平布线图（vsd格式）。在进行综合布线型材选型中，根据GB50311—2016要求，线槽截面利用率不能高于50%，线管截面利用率不能高于30%，且线槽/管规格选择最小规格。参考示意图如图5所示。



图5 水平布线示意图

（2）根据机柜上架设备清单，规划设备在机柜的安装位置、设备和网络配线架的标识，输出机柜安装示意图（vsd格式）。参考示意图如图6所示。



图6 机柜安装示意图

（3）根据无线AP点位编号信息，合理规划AP对应双绞线的上架位置，并在网络配线架面板做标注。

请将机柜上网络配线架的标签信息（从左到右）填写到表9中。

表9 数据配线架标签表

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 网络配线架标签表 | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

（4）工程物料清单

根据无线网络的水平布线图，计算本次无线网络工程的物料清单。其中，线缆采用平均值法进行估算，所有材料以表7为准。请将本次无线网络工程的物料清单填写到表10中。

表8 物料清单表

|  |  |  |
| --- | --- | --- |
| **物料名称** | **单位** | **数量** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# 六．提交竞赛结果文件说明

备注1：制作竞赛结果文件1：严格按照“交换路由无线网关设备配置答题卡.docx”文档格式要求制作输出竞赛结果文件，同时另存一份“PDF格式文档”（利用Office Word另存为pdf文件方式生成pdf文件）。

备注2：在每台设备上使用show running-config命令，将该命令下显示的结果分别保存到独立的TXT文件中，文件名以设备编号命名（S1、S2、S3、S4、S7、VSU、R1、R2、R3、AC1、AC2、EG1、EG2），并把所有的TXT文件存放在“设备配置”文件夹下。

备注3：考生将“交换路由无线网关设备配置答题卡.docx”“交换路由无线网关设备配置答题卡.pdf”及“设备配置”文件夹保存到桌面上，并且拷贝到U盘上的“提交文档”目录下然后提交给现场工作人员。

备注4：制作竞赛结果文件：严格按照 “无线网络勘测设计答题卡.docx”文档格式要求制作输出竞赛结果文件，同时另存一份PDF格式文档（利用Office Word另存为pdf文件方式生成pdf格式文件）。

备注5：考生将竞赛结果文件“无线网络勘测设计答题卡.docx”和“无线网络勘测设计答题卡.pdf”保存到桌面上，并且拷贝到U盘上的“提交文档”目录下然后提交给现场工作人员。

备注6：考生所提交的文件是竞赛结果的唯一依据，请考生一定确保文件确实有效，能够正常读取。如有疑问，可咨询现场工作人员。

备注7：考生在U盘中所提交的文件是竞赛结果的唯一依据，请考生一定确保文件确实有效，能够正常读取。如有疑问，可咨询现场工作人员。