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2）



**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](#_Toc51862606)

[二．项目背景 3](#_Toc51862607)

[三．项目规划和设计 4](#_Toc51862608)

[四．网络项目实施 12](#_Toc51862609)

[（一）设备基础信息配置与验证 12](#_Toc51862610)

[（二）网络搭建与网络冗余备份方案部署 12](#_Toc51862611)

[（三）移动互联网搭建与无线网络优化 18](#_Toc51862612)

[（四）实施出口安全防护与远程接入 20](#_Toc51862613)

[五．无线网络规划与实施 22](#_Toc51862614)

[（一）无线网络业务背景及需求介绍 22](#_Toc51862615)

[（二）无线网络中的业务规划 24](#_Toc51862616)

[六．提交竞赛结果文件说明 28](#_Toc51862617)

# 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

随着信息技术的深入应用，网络技术朝着智慧化方向发展，人工智能、移动互联网、云计算等信息技术深刻地影响着当前金融等各行业的格局。

海琼银行是海南省的一家商业银行，创建于1975年，其省行（一级行）位于海南省海口市，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。随着网络扁平化的改造，目前所有的二级行、支行及网点均直接连接到省行，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、外联区、服务器区、办公区、互联区五个部分。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。外联区是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。服务器区部署各类服务器及无线AC。办公区分别通过有线和无线网络为生产数据流（存/取款等与钱相关的数据）和办公数据流（OA、视频会议等与钱无关的数据）提供了服务。互联区主要通过MSTP专线连接总行、全省所有的二级行、支行及网点。

各支行/网点的业务也包括生产和办公两类。其中：生产数据主要由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。

海琼银行的智慧网络具备高速、可靠、安全的数据传输，以及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，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。而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，为区域的网络提供高效的保障服务，海琼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；此次也新建如超辰支行、积嘉支行、海富支行、鳌博网点……等多个支行和营业网点。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地实现各业务安全、高效、快速的传输，创建新时代金融网络环境，保障银行各项业务高效运营。

# 三．项目规划和设计

为了顺利实施海琼银行网络改造，优化省行的网络，为其它区域的网络提供高效的保障服务。同时，海琼银行还针对各个分支行、网点的网络进行升级、改造和优化。

**1. 项目规划与建设内容**

实施的网络信息化规划与建设内容如下所示。

（1）各支行/网点通过MSTP专线可访问省行的业务区，实现生产和办公业务各自的互通。

（2）生产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，梅钱金融公司等第三方公司能通过VPN访问银行特定资源。

**2. 项目规划与建设拓扑**

海琼银行省行及二级分支行网点改造和信息化建设拓扑如图1所示。

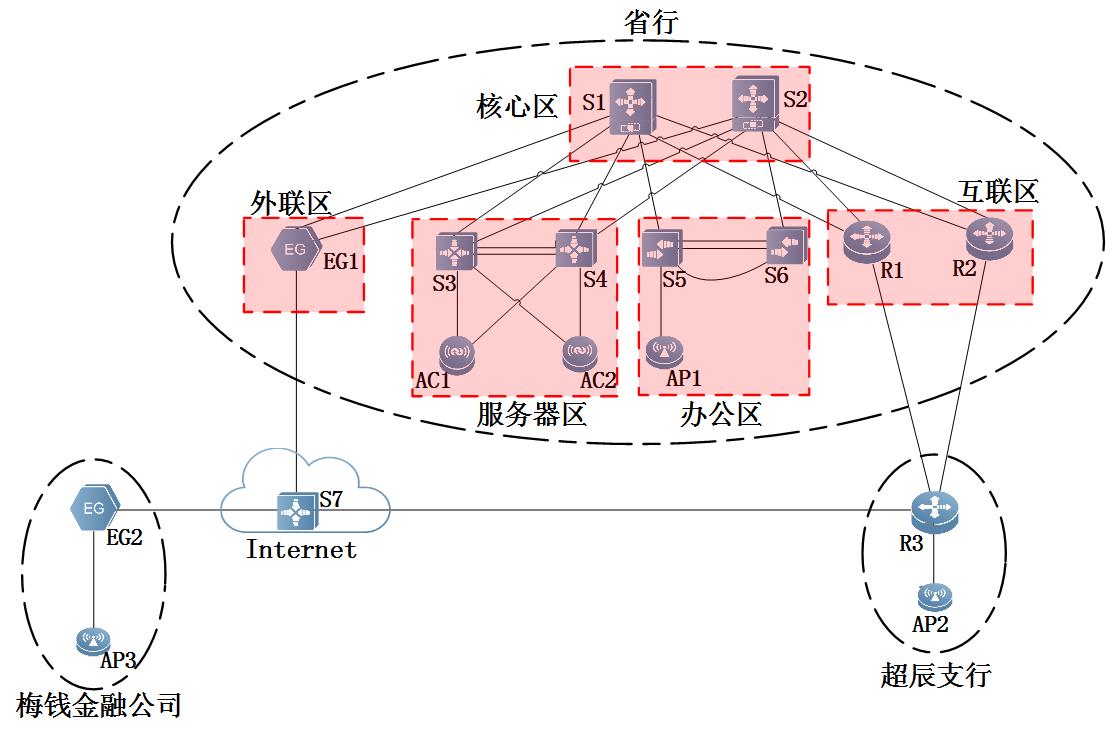


图1 海琼银行省行及二级分支行网络拓扑

**3. 项目规划与建设拓扑**

海琼银行省行以及二级分支行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）两台无线控制器作为省服务器区中的无线网络控制器，在网络拓扑中的编号为AC1和AC2。

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

（5）一台无线AP作为省行办公区无线接入点，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）省行的外联区中使用一台出口网关，把省行的外联区网络接入互联网（运营商网络），在网络拓扑中的编号为EG1。

（8） 超辰支行使用一台路由器接入省行网络，在网络拓扑中编号为R3。

（9）超辰支行无线网络使用一台无线AP接入，在网络拓扑中编号为AP2。

（10）使用一台三层可控交换机构建运营商核心网络（代表Internet网系统），在网络拓扑中编号为S7。

（11）梅钱金融公司使用一台出口网关作为网络出口，连接运营商网络，在网络拓扑中编号为EG2。

（12）梅钱金融公司内部使用一台无线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，完成设备连线。

本项目的网络物理连接表如表1所示，请根据拓扑图及网络设备物理连接表完成设备的连线。

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\_S5\_Gi0/24 | S5 | Gi0/24 |
| Gi0/5 | Connect\_To\_R1\_Gi0/0 | R1 | Gi0/0 |
| Gi0/6 | Connect\_To\_R2\_Gi0/0 | R2 | Gi0/0 |
| 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\_S6\_Gi0/24 | S6 | Gi0/24 |
| Gi0/5 | Connect\_To\_R1\_Gi0/1 | R1 | Gi0/1 |
| Gi0/6 | Connect\_To\_R2\_Gi0/1 | R2 | 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 |
| S3 | Gi0/1 | Connect\_To\_AC1\_Gi0/3 | AC1 | Gi0/3 |
| Gi0/2 | Connect\_To\_AC2\_Gi0/3 | AC2 | Gi0/3 |
| 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 | Gi0/1 | Connect\_To\_AC1\_Gi0/4 | AC1 | Gi0/4 |
| Gi0/2 | Connect\_To\_AC2\_Gi0/4 | AC2 | Gi0/4 |
| 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 |
| AC1 | Gi0/3 | Connect\_To\_S3\_Gi0/1 | S3 | Gi0/1 |
| Gi0/4 | Connect\_To\_S4\_Gi0/1 | S4 | Gi0/1 |
| AC2 | Gi0/3 | Connect\_To\_S3\_Gi0/2 | S3 | Gi0/2 |
| Gi0/4 | Connect\_To\_S4\_Gi0/2 | S4 | Gi0/2 |
| S5 | Gi0/1 | Connect\_To\_AP1\_Gi0/1 | AP1 | Gi0/1 |
| Gi0/23 | Connect\_To\_S6\_Gi0/23 | S6 | Gi0/23 |
| Gi0/24 | Connect\_To\_S1\_Gi0/4 | S1 | Gi0/4 |
| Te0/27 | Connect\_To\_S6\_Te0/27 | S6 | Te0/27 |
| Te0/28 | Connect\_To\_S6\_Te0/28 | Te0/28 |
| S6 | Gi0/23 | Connect\_To\_S5\_Gi0/22 | S5 | Gi0/23 |
| Gi0/24 | Connect\_To\_S2\_Gi0/4 | S2 | Gi0/4 |
| Te0/27 | Connect\_To\_S5\_Te0/27 | S5 | Te0/27 |
| Te0/28 | Connect\_To\_S5\_Te0/28 | Te0/28 |
| AP1 | Gi0/1 | Connect\_To\_S5\_Gi0/1 | S5 | Gi0/1 |
| R1 | Gi0/0 | Connect\_To\_S1\_Gi0/5 | S1 | Gi0/5 |
| Gi0/1 | Connect\_To\_S2\_Gi0/5 | S2 | Gi0/5 |
| Fa1/0 | Connect\_To\_R3\_Fa1/0 | R3 | Fa1/0 |
| R2 | Gi0/0 | Connect\_To\_S1\_Gi0/6 | S1 | Gi0/6 |
| Gi0/1 | Connect\_To\_S2\_Gi0/6 | S2 | Gi0/6 |
| Fa1/0 | Connect\_To\_R3\_Fa1/1 | R3 | Fa1/1 |
| R3 | Gi0/0 | Connect\_To\_AP2\_Gi0/1 | AP2 | Gi0/1 |
| Gi0/1 | Connect\_To\_S7\_Gi0/2 | S7 | Gi0/2 |
| Fa1/0 | Connect\_To\_R1\_Fa1/0 | R1 | Fa1/0 |
| Fa1/1 | Connect\_To\_R2\_Fa1/0 | R2 | Fa1/0 |
| AP2 | Gi0/1 | Connect\_To\_R3\_Gi0/0 | R3 | Gi0/0 |
| EG2 | Gi0/1 | Connect\_To\_AP3\_Gi0/1 | AP3 | Gi0/1 |
| Gi0/4 | Connect\_To\_S7\_Gi0/3 | S7 | Gi0/3 |
| AP3 | Gi0/1 | Connect\_To\_EG2\_Gi0/1 | EG2 | Gi0/1 |
| S7 | Gi0/1 | Connect\_To\_EG1\_Gi0/4 | EG1 | Gi0/4 |
| Gi0/2 | Connect\_To\_R3\_Gi0/1 | R3 | Gi0/1 |
| Gi0/3 | Connect\_To\_EG2\_Gi0/4 | EG2 | Gi0/4 |

表2 网络设备名称表

|  |  |  |
| --- | --- | --- |
| 设备名称 | 配置主机名（hostname名） | 备注 |
| S1 | SHWLQ-DataCenter-Switch-S1 | 省行核心区数据中心交换机1 |
| S2 | SHHXQ-DataCenter-Switch-S2 | 省行核心区数据中心交换机2 |
| EG1 | SHWLQ-Egress-Gateway-EG1 | 省行外联区出口网关 |
| S3 | SHFWQQ-Aggregation-Switch-S3 | 省行服务器区三层可控汇聚交换机1 |
| S4 | SHFWQQ-Aggregation-Switch-S4 | 省行服务器区三层可控汇聚交换机2 |
| AC1 | SHFWQQ-Wireless-Switch-AC1 | 省行服务器区无线控制器1 |
| AC2 | SHFWQQ-Wireless-Switch-AC2 | 省行服务器区无线控制器2 |
| S5/S6(VSU) | SHBGQ-Access-Switch-VSU | 省行二层可控接入交换机(VSU) |
| 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 |
| R3 | CCZH-Router-S7 | 超辰支行出口路由器 |
| EG2 | MQJR-Egress-Gateway-EG2 | 梅钱金融公司出口网关 |
| S7 | ISP-Aggregation-Switch-S7 | 运营商网络三层可控交换机 |

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 | \ | 10.1.1.1/30 | 互联地址 |
| Gi0/2 | \ | 10.1.2.1/30 | 互联地址 |
| Gi0/3 | \ | 10.1.2.5/30 | 互联地址 |
| Gi0/4 | \ | 10.1.3.1/30 | 互联地址 |
| Gi0/5 | \ | 10.1.4.1/30 | 互联地址 |
| Gi0/6 | \ | 10.1.4.5/30 | 互联地址 |
| Loopback 0 | \ | 11.1.0.1/32 | —— |
| S2 | Gi0/1 | \ | 10.1.1.5/30 | 互联地址 |
| Gi0/2 | \ | 10.1.2.9/30 | 互联地址 |
| Gi0/3 | \ | 10.1.2.13/30 | 互联地址 |
| Gi0/4 | \ | 10.1.3.5/30 | 互联地址 |
| Gi0/5 | \ | 10.1.4.9/30 | 互联地址 |
| Gi0/6 | \ | 10.1.4.13/30 | 互联地址 |
| Loopback 0 | \ | 11.1.0.2/32 | —— |
| EG1 | Gi0/1 | \ | 10.1.1.2/30 | 互联地址 |
| Gi0/2 | \ | 10.1.1.6/30 | 互联地址 |
| Gi0/4 | \ | 201.1.1.2/29 | ISP地址 |
| Loopback 0 | \ | 11.1.0.10/32 | —— |
| S3 | VLAN 90 | Server | 192.2.90.252/24 | 生产服务器地址Gi0/5-15 |
| VLAN 60 | Wireless | 192.3.60.252/24 | 办公区无线用户地址 |
| VLAN 100 | Manage | 192.2.100.252/24 | 设备管理地址 |
| Gi0/23 | \ | 10.1.2.2/30 | 互联地址 |
| Gi0/24 | \ | 10.1.2.10/30 | 互联地址 |
| Loopback 0 | \ | 11.1.0.3/32 | —— |
| S4 | VLAN 90 | Server | 192.2.90.253/24 | 生产服务器地址Gi0/5-15 |
| VLAN 60 | Wireless | 192.3.60.253/24 | 办公区无线用户地址 |
| VLAN 100 | Manage | 192.2.100.253/24 | 设备管理地址 |
| Gi0/23 | \ | 10.1.2.6/30 | 互联地址 |
| Gi0/24 | \ | 10.1.2.14/30 | 互联地址 |
| Loopback 0 | \ | 11.1.0.4/32 | —— |
| AC1 | VLAN 100 | Manage | 192.2.100.1/24 | 设备管理地址 |
| Loopback 0 | \ | 11.1.0.5/32 | —— |
| AC2 | VLAN 100 | Manage | 192.2.100.2/24 | 设备管理地址 |
| Loopback 0 | \ | 11.1.0.6/32 | —— |
| S5-S6  (VSU) | VLAN 110 | Office-Wire | 192.3.10.254/24 | 办公/有线用户地址Gi1/0/6至 Gi1/0/20,  Gi2/0/6至 Gi2/0/20 |
| VLAN 150 | APManage\_BGQ | 192.3.50.254/24 | 业务区AP管理地址  Gi1/0/1至 Gi1/0/5,  Gi2/0/1至 Gi2/0/5 |
| VLAN 1301 | Connect-S1 | 10.1.3.2/30 | 互联地址Gi1/0/24 |
| VLAN 1302 | Connect-S2 | 10.1.3.6/30 | 互联地址Gi2/0/24 |
| R1 | Gi0/0 | \ | 10.1.4.2/30 | 互联地址 |
| Gi0/1 | \ | 10.1.4.10/30 | 互联地址 |
| VLAN101 | \ | 10.2.1.1/30 | Fa1/0成员口 |
| Loopback 0 | \ | 11.1.0.7/32 | —— |
| R2 | Gi0/0 | \ | 10.1.4.6/30 | 互联地址 |
| Gi0/1 | \ | 10.1.4.14/30 | 互联地址 |
| VLAN201 | \ | 10.2.1.5/30 | Fa1/0成员口 |
| Loopback 0 | \ | 11.1.0.8/32 | —— |
| R3 | VLAN101 | \ | 10.2.1.2/30 | Fa1/0成员口 |
| VLAN201 | \ | 10.2.1.6/30 | Fa1/1成员口 |
| Gi0/0.10 | Production | 194.2.10.254/24 | 超辰支行生产用户 |
| Gi0/0 | APManage\_CCZH | 194.3.50.254/24 | 超辰支行AP管理 |
| Gi0/0.60 | Office | 194.3.60.254/24 | 超辰支行办公用户 |
| Gi0/1 | \ | 202.1.1.2/29 | ISP地址 |
| Loopback 0 | \ | 11.1.0.9/32 | —— |
| Tunnel 3 |  | 12.1.1.2/30 | GRE隧道接口地址 |
| EG2 | G0/1 | \ | 10.6.1.1/30 | 互联 |
| Gi0/4 | \ | 203.1.1.2/29 | 互联地址 |
| Loopback 0 | \ | 11.1.0.11/32 | —— |
| Tunnel 3 |  | 12.1.1.1/30 | GRE隧道接口地址 |
| AP3 | VLAN60 | \ | 195.1.60.254/24 | 用户地址 |
| Gi0/1 | \ | 10.6.1.2/30 | 互联 |
| S7 | Gi0/1 | \ | 201.1.1.1/29 | ISP地址 |
| Gi0/2 | \ | 202.1.1.1/29 | ISP地址 |
| Gi0/3 | \ | 203.1.1.1/29 | ISP地址 |

# 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，新的密码设置为admin1234。

（2）交换机S7进行版本更新，更新版本至指定版本，指定版本见现场的升级文件包1。

（3）无线AP3进行版本更新，更新版本至指定版本，指定版本见现场的升级文件包2。

**3. 保障全网中的网络设备安全。**

（1）需要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192.2.90.25/24。

（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192.2.90.25/24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，需要在搭建完成的虚拟交换机S5-S6的Gi1/0/10-Gi1/0/15端口上启用端口保护。

（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240秒自动恢复机制（基于接口部署策略）。

**3. 配置服务器，部署DHCP中继，保护服务器安全**

在省行网络虚拟交换机S5-S6上，配置DHCP中继，对局域网终端设备进行地址中继，使得终端用户使用DHCP Relay方式获取IP地址。具体要求如下。

（1）省行DHCP服务器安装在S2交换机上,分配以下3个网段地址：省行办公有线用户（192.3.10.0/24）、省行办公区AP（192.3.50.0/24）、省行办公区无线（192.3.60.0/24）。按照IP地址规划表（表3：IPv4地址分配表）为无线用户分配地址，为AP分配管理地址。其中，无线AP租约为永久，无线用户租约设为0.5天。

（2）为了防御局域网中出现伪造DHCP服务器与ARP欺骗安全事件发生，在安装完成虚拟交换中心交换机S5-S6上，部署DHCP安全防护功能，使用“Snooping +IP Source Guard+ARP-CHECK”技术，防护DHCP服务器安全。

其中，在超辰支行部署DHCP服务，需要配置的服务内容如下所示。

（3）超辰支行DHCP服务器搭建于R3路由器上,按照地址规划表中规划地址（表3：IPv4地址分配表），为无线生产用户（194.2.10.0/24）、办公用户（194.3.60.0/24）和AP管理（194.3.50.0/24）分配IP地址。其中：无线AP的地址租约为永久；无线用户的租约设为1天。此外，还需要配置MAC地址为AC-81-12-97-8E-C9的设备，每次获取到固定的IP地址194.2.10.5/24。

其中，在梅钱金融公司部署DHCP服务，需要配置的服务内容如下所示。

（4）梅钱金融公司DHCP服务器搭建于AP3上, 按照地址规划表中规划（表3：IPv4地址分配表）地址，配置DHCP服务器地址。

**4. 部署MSTP及VRRP技术，实现网络冗余。**

在交换机S3、S4、AC1、AC2上配置MSTP，防止二层环路。

（1）配置MSTP要求来自VLAN90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VLAN60和VLAN 100数据流经过S4交换机转发，S4失效时经过S3交换机转发。

其中，配置MSTP参数要求：region-name为test；revision版本为1；实例1包含VLAN90；实例2包含VLAN60,VLAN100。

（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连接连接AC1和AC2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），采取LACP动态聚合模式配置二层链路聚合。

表4 S3和S4的VRRP参数表

|  |  |  |
| --- | --- | --- |
| VLAN | VRRP备份组号（VRID） | VRRP虚拟IP |
| VLAN60 | 60 | 192.3.60.254 |
| VLAN90 | 90 | 192.2.90.254 |
| VLAN100 | 100 | 192.2.100.254 |

**5. 部署网络设备虚拟化，保障核心网络稳健。**

为增加网络稳健性，业务区域中两台接入交换机通过网络虚拟化技术，虚拟成一台设备集中管理，实现网络高可靠性。当网络中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，使用网络虚拟化技术，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。**

在省行以及各支行之间，部分区域使用OSPF协议组网，实现全网互联互通，具体要求如下。

（1）省行核心区与服务器区（S1、S2、S3、S4）部署OSPF 100，使用单区域（区域0）部署。

（2）省行核心区与外联区（S1、S2、EG1）部署OSPF 100，规划区域为10。

（3）优化OSPF相关配置，以尽量加快OSPF收敛。

（4）重发布路由进OSPF中使用类型1。

此外，在省行以及各支行之间，部分区域使用BGP路由协议组网，使用BGP路由协议的区域及基本要求如下。

（1）核心区（S1、S2）使用自治域号为64520，互联区及超辰支行（R1、R2、R3）自治域号为64521。

（2）省行核心区与互联区（S1、S2、R1、R2）使用互联接口地址部署EBGP。

（3）省行及各支行/网点（R1、R2、R3）使用LOOPBACK 0地址部署IBGP，其底层IGP协议使用静态路由协议。

此外，使用静态路由实现以下区域之间的网络通信。

（1）省行核心区与办公区（S1、S2、VSU）部署静态路由协议。

（2）省行服务器区中无线控制器AC1和AC2设备，与两台交换机S3和S4之间部署静态路由协议。

（3）Internet区域（EG1、EG2、R3）均使用静态路由协议。

**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，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）网络中传输的数据类型分为生产性和办公性两类。全网属于生产性数据的有2个网段：省行生产服务器网段（192.2.90.0/24）、超辰支行生产业务（194.2.10.0/24）。其余如省行办公区有线/无线网络中用户、支行办公业务、设备管理等数据均为办公类数据，具体网段见地址规划表（表3：IPv4地址分配表）。

（2）通过策略部署，使得生产性业务的传输主路径为R3-R1-S1-S3；办公性业务的传输主路径为R3-R2-S2-S4/VSU, 并且要求来回路径保持一致。

（3）主链路或主设备故障时，可无缝切换到备用链路或设备上。

（4）在使用BGP路由通告网络中，交换机S1、S2和路由器R3通过Network引入明细路由；禁止将IGP路由以重发布形式导入BGP自制系统中。

（5）在部分区域使用BGP选路策略中，要求只能在省行核心区S1、S2交换机上部署。其中，凡涉及MED值调整，要求其值必须是10、15、20；凡涉及LP值调整，要求值必须是200、300。此外，省行生产流量定义为ACL1；省行办公流量定义为ACL2；支行生产流量定义为ACL11；支行办公流量定义为ACL12。

（6）为了防止路由表洪泛，不能将BGP路由重发布到OSPF中。只能通过重发布黑洞路由的方式实现。

（7）在部署OSPF各路由图以及各接口中，凡涉及COST值的调整，要求其值必须为5或10。

**8. 在省行以及分支行部署IPv6业务。**

（1）省行（除外联区外）和超辰支行各自分别部署IPV6网络。机构内网IPV6终端可自动从网关处获取地址。

（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）省行内部通过OSPFv3路由，实现IPV6互联互通。其中：省行核心区、服务器区（S1、S2、S3、S4）属于区域0；省行互联区（S1、S2、R1、R2）属于区域10；VSU虚拟交换中心到S1/S2之间使用静态协议。

（4）IPV6业务均为办公业务，数据走向（VSU/S4）-S2-R2-R3。需要保障来回路径一致。

（5）省行与超辰支行之间建立IPV6隧道实现互联互通。其中：路由器R3和R1、R2之间均运行GRE隧道。隧道之间均运行静态路由协议。要求R2路由器的隧道为主；R1路由器的隧道作为备份链路。

（6）在省行业务区中部署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 |
| S1 | Gi0/2 | 2001:10:2::1/64 |  |  |
| Gi0/3 | 2001:10:2:4::1/64 |  |  |
| Gi0/4 | 2001:10:3::1/64 |  |  |
| Gi0/5 | 2001:10:4::1/64 |  |  |
| Gi0/6 | 2001:10:4:4::1/64 |  |  |
| S2 | Gi0/2 | 2001:10:2:8::1/64 |  |  |
| Gi0/3 | 2001:10:2:12::1/64 |  |  |
| Gi0/4 | 2001:10:3:4::1/64 |  |  |
| Gi0/5 | 2001:10:4:8::1/64 |  |  |
| Gi0/6 | 2001:10:4:12::1/64 |  |  |
| S3 | VLAN90 | 2001:192:2:90::252/64 | 90 | 2001:192:2:90::254/64 |
| VLAN60 | 2001:192:3:60::252/64 | 60 | 2001:192:3:60::254/64 |
| Gi0/23 | 2001:10:2::2/64 |  |  |
| Gi0/24 | 2001:10:2:8::2/64 |  |  |
| S4 | VLAN90 | 2001:192:2:90::253/64 | 90 | 2001:192:2:90::254/64 |
| VLAN60 | 2001:192:3:60::253/64 | 60 | 2001:192:3:60::254/64 |
| Gi0/23 | 2001:10:2:4::2/64 |  |  |
| Gi0/24 | 2001:10:2:12::2/64 |  |  |
| VSU | VLAN110 | 2001:192:3:10::254/64 |  |  |
| VLAN1301 | 2001:10:3::2/30 |  |  |
| VLAN1302 | 2001:10:3:4::2/30 |  |  |
| R1 | Gi0/0 | 2001:10:4::2/64 |  |  |
| Gi0/1 | 2001:10:4:8::2/64 |  |  |
| Tunnel1 | 2004:11:2::7/64 |  |  |
| R2 | Gi0/0 | 2001:10:4:4::2/64 |  |  |
| Gi0/1 | 2001:10:4:12::2/64 |  |  |
| Tunnel0 | 2004:11:1::8/64 |  |  |
| R3 | Gi0/0.10 | 2003:194:2:10::254/64 |  |  |
| Gi0/0.60 | 2003:194:3:60::254/64 |  |  |
| Tunnel0 | 2004:11:1::9/64 |  |  |
| Tunnel1 | 2004:11:2::9/64 |  |  |

## （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）在省行办公区的无线部署中，无线AP采用FIT AP架构，所有AP（AP1）关联到省行服务器区AC。

（2）在省行办公区无线部署中，使用S2交换机作为无线用户（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，创建省行业务区中内网的SSID为：Admin\_SHBGQ\_XX(XX现场提供)；WLANID为1；AP-GROUP为Admin\_SHBGQ。其中，内网无线用户关联SSID后，可自动获取VLAN60地址。

（5）在省行办公区无线部署中，配置省行办公区AP采用集中式转发。

**2.在超辰支行部署无线网络。**

（1）超辰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VAC进行管理。

（2）超辰支行使用R3路由器作为无线生产用户（VLAN 10）、办公用户（VLAN 60）和无线FIT AP（VLAN 50）的DHCP服务器。

（3）超辰支行无线网络部署中，创建生产用户SSID为：Admin\_CCZH\_SS\_XX(XX现场提供)；WLANID为2；AP-GROUP为Admin\_CCZH；生产用户关联SSID后，可自动获取VLAN10地址。创建超辰支行办公用户SSID为：Admin\_CCZH\_BG\_XX(XX现场提供)；WLANID为3；AP-GROUP为Admin\_CCZH；生产用户关联SSID后可自动获取VLAN60地址。

（4）超辰支行无线网络部署中，超辰支行AP采用本地转发。

**3.在无线网络中部署AC冗余，实现备份。**

在无线网络中部署AC冗余，实现备份。两台AC采用主备形式。其中，AC1为省行办公区AP主设备；AC2为超辰支行AP主设备，两AC互为备份。

所有FIT AP与AC1、AC2均建立隧道，当AP与主AC1失去连接时，能无缝切换至备用AC，并提供连续服务。

**4.在梅钱金融公司部署胖AP。**

在梅钱金融公司部署胖AP设备，具体要求如下所示。

（1）用户网关及DHCP服务器均部署在AP3上；AP3与EG2之间使用静态路由协议实现连通。

（2）配置AP3设备，在AP3上配置SSID(WLAN-ID 4)为Admin-Fat\_XX(XX现场提供)，内网无线用户关联SSID后,可自动获取 195.1.60.0/24网段地址。

**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）限制3台AP的每个射频卡最大带点人数为15人。

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

（3）调整5.8G频段的射频卡无线频率带宽至40MHz，增大数据传输带宽。

（4）为保证网络中的终端设备走到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：5.8G频段的Coverage-area-control功率调整为17db；2.4G频段的Coverage-area-control功率调整为10db。

（5）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）省行的外联区出口网关EG1上进行NAT配置，实现省行业务区办公网络（VLAN 60、VLAN 110）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201.1.1.3/29-201.1.1.5/29；生产网络及其他地址均不允许访问互联网，转换ACL定义为ACL 120。

（2）省行外联区出口网关EG1上配置，使省行的核心交换机S1的HTTP服务器（IP为11.1.0.1）的HTTP服务（TCP 80）可以通过互联网被访问，将其地址映射至运营商线路上，映射地址为201.1.1.6，映射端口58888。

（3）为了超辰支行访问Internet，实现线路备份，超辰支行部署了一条Internet出口，实现支行办公用户访问Internet。正常情况下，生产用户不允许访问Internet,ALC编号为101。其中：超辰支行出口路由器R3上NAT地址池的地址为202.1.1.3/29-201.1.1.4/29。

（4）梅钱金融公司出口网关EG2上进行NAT配置，实现其无线用户能访问Internet，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）在省行的无线办公用户（VLAN 60）上，需进行WEB认证方式访问互联网。

（3）在省行有线办公用户（VLAN 110），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。**

在梅钱金融公司出口网关EG2上，针对内网访问互联网WEB流量，限速每个IP为1000Kbps；内网中的WEB总流量不超过20Mbps。其中，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。**

由于业务需要，梅钱金融公司与超辰支行需要互相访问。为了实现互访数据的安全性，针对来往数据使用加密技术进行安全保障，具体规划如下，具体规划如下所示。

（1） 在网络安全出口设备EG2与R3出口网关之间，启用IPSec VPNOver GRE嵌套功能。

（2）配置IPSec使用静态点对点模式，esp隧道模式封装协议，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

某企业子集团最近在天地城新租用了一栋综合商住两用楼，用于公司临时办公，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，因资金紧张，经充分论证，本次无线覆盖项目拟投入18万元（网络设备采购部分），项目要求休息区、办公室、员工寝室、小型会议室均覆盖（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—104、107、110-113为独立办公室，105—106、108-109为小型会议室，1001—1016为员工寝室，预计休息区人流量为80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，部分独立办公室布为有线网络，客户希望利用原有网络。

（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的平面布局图如图2所示。

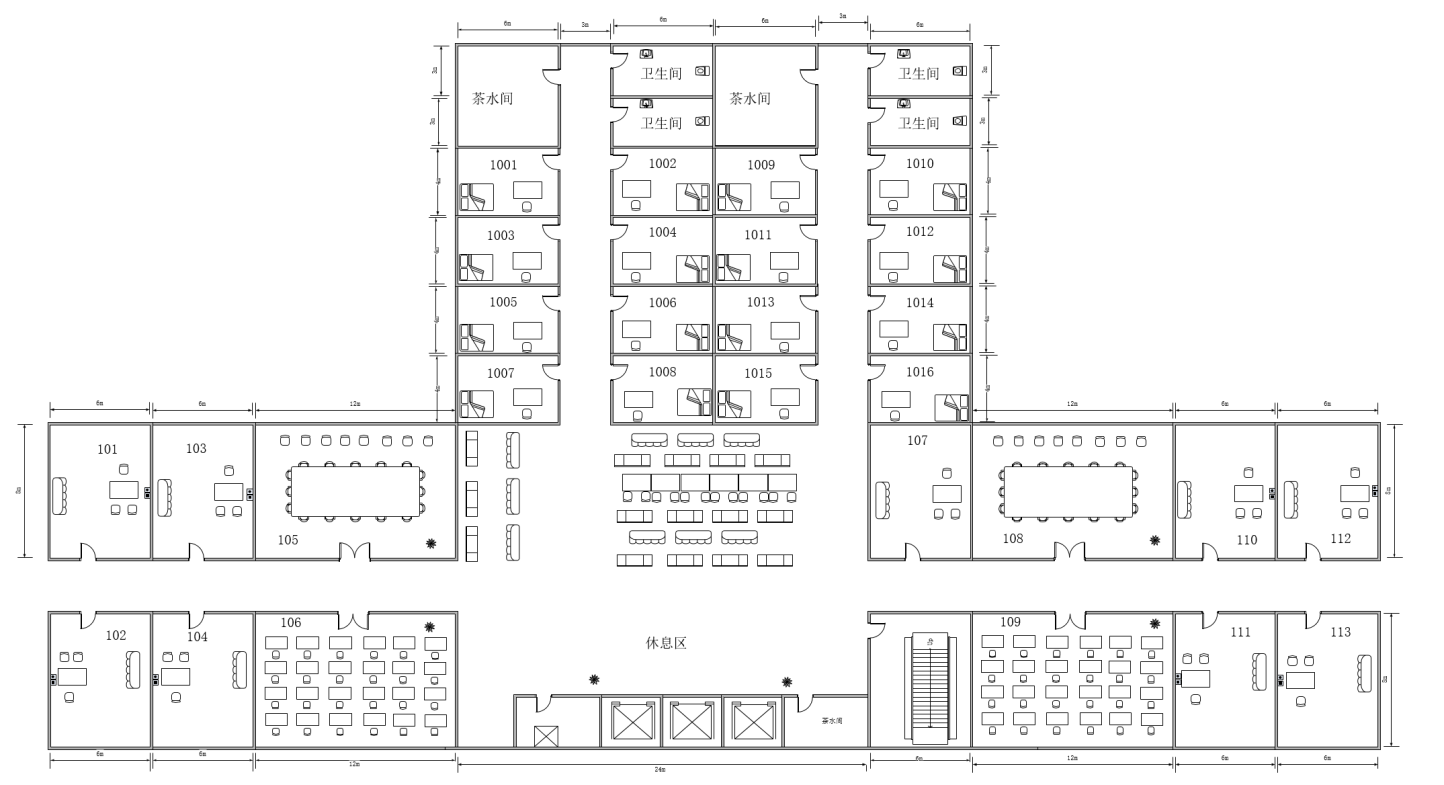


图2 平面布局图

**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（洗手间、茶水间区域无须覆盖）。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），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6，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6为准。

请将本次无线网络工程的物料清单填写到表10中。

表10 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。