**2022年全国职业院校技能大赛**

**网络系统管理赛项**

模块A：网络构建

（样题5）



目录

[任务描述 3](#_Toc21021)

[任务清单 3](#_Toc24342)

[（一）基础配置 3](#_Toc28007)

[（二）有线网络配置 3](#_Toc7473)

[（三）无线网络配置 5](#_Toc20046)

[（四）出口网络配置 7](#_Toc18296)

[附录1：拓扑图 9](#_Toc3243)

[附录2：地址规划表 10](#_Toc26736)

# 任务描述

随着业务的发展，现在要对海琼银行进行全网改造，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。你做为火星公司网络工程师前往并完成网络规划与建设任务。

# 任务清单

# （一）基础配置

1.根据附录1拓扑图及附录2地址规划表，配置设备接口信息。

2.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。

3.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。配置所有交换设备的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）有线网络配置

1.在全网Trunk链路上做VLAN修剪。

2.在S5、S6的Gi0/10-Gi0/15端口上启用端口保护。

3.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。

4.在连接PC机端口上开启Portfast和BPDUguard防护功能。

5.端口被检测异常进入 Err-Disabled状态，再过240秒后会自动恢复（基于接口部署策略），重新检测是否有环路。交换机端口检测到环路，处理的方试为shutdown-Port。

6.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）。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。按照要求为无线用户和AP分配地址和管理地址，其中无线AP租约为永久，无线用户租约设为0.5天。

7.梅森金融公司DHCP服务器搭建于AP3上，按照地址规划表规划地址。

8.在交换机S3、S4、AC1、AC2上配置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。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。

9.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。

10.在交换机S3、S4连接AC1和AC2的接口上，启用“TC-IGNORE”功能。

11.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1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。

表1 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 |

12.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。

13.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。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。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。

14.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，省行核心区与外联区（S1、S2、EG1）部署OSPF 100，规划区域为10，重发布路由进OSPF中使用类型1。

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

16.省行核心区与办公区（S1、S2）部署静态路由协议，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，Internet区域（EG1、EG2、R3）均使用静态路由协议。

17.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, 并且要求来回路径保持一致，主链路或主设备故障时，可无缝切换到备用链路或设备上，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。

18.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，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。

# （三）无线网络配置

现在对海琼银行进行无线网络优化项目拟投入18万元（网络设备采购部分）平面布局如图1所示。

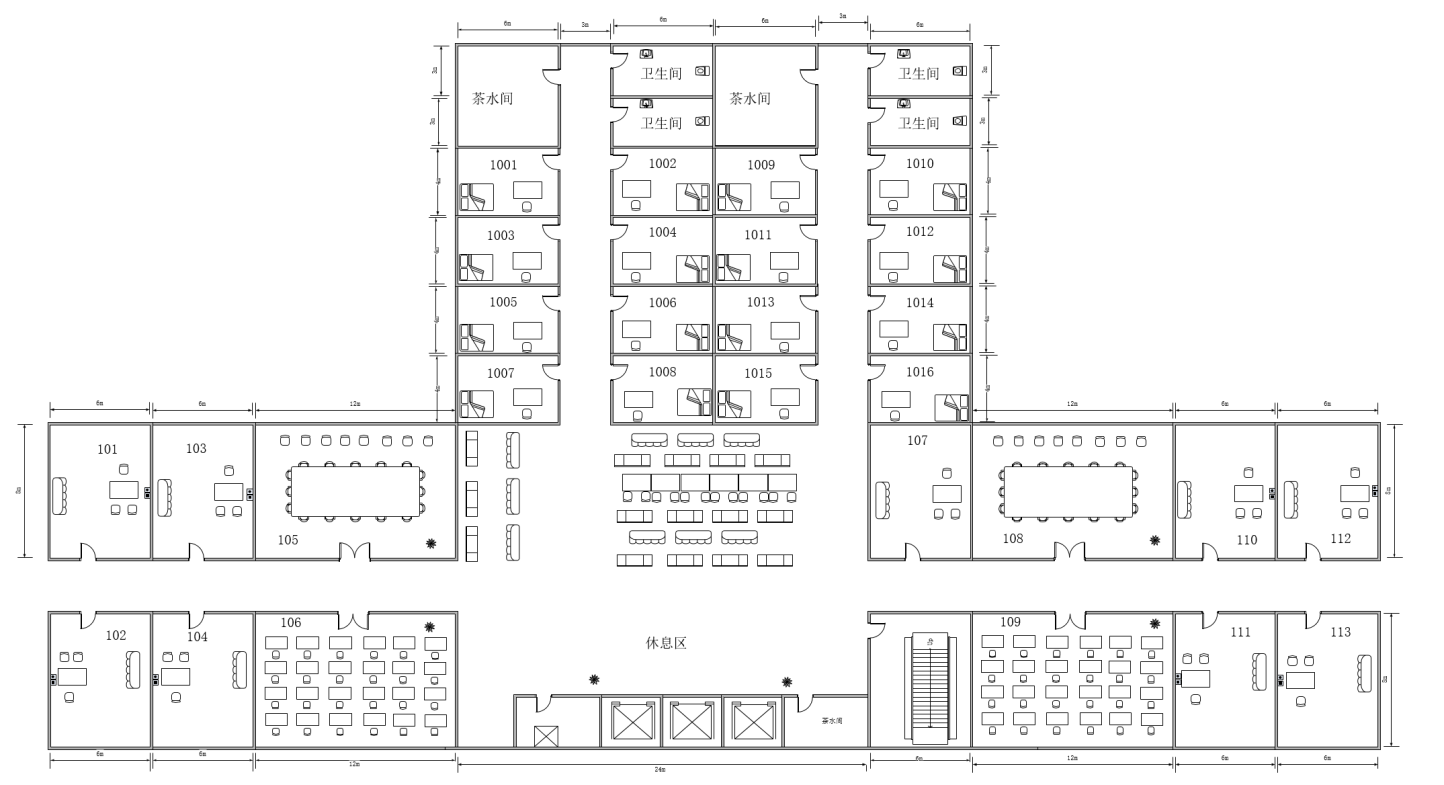


图1 平面布局图

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，洗手间、茶水间无须覆盖）。

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）。

3.根据表2无线产品价格表，制定该无线网络工程项目设备的预算表。

表2 无线产品价格表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **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）** |
| AP1 | 双频双流 | 300M/1.167G | 32/256 | 100mw | 6000 |
| AP2 | 双频双流 | 300M/600M | 32/256 | 100mw | 11000 |
| AP3 | 单频单流 | 150M | 12/32 | 60mw | 2500 |
| 线缆1 | 10米馈线 | N/A | N/A | N/A | 1600 |
| 线缆2 | 15米馈线 | N/A | N/A | N/A | 2400 |
| 天线 | 双频单流/单频单流 | N/A | N/A | N/A | 500 |
| Switch | 24口POE交换机 | N/A | N/A | 240w | 15000 |
| AC | 无线控制器 | 6\*1000M | 32/200 | 40w | 50000 |

4.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，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，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，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。

5.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，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，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，超辰支行无线网络部署中，超辰支行AP采用本地转发。

6.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。

7.在梅森金融公司部署胖AP设备，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，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。

8.5.8G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，关闭低速率（11b/g 1M、2M、5M，11a 6M、9M）应用接入，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，调整5.8G频段的射频卡无线频率带宽至40MHz。

9.限制3台AP的每个射频卡最大带点人数为15人，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)，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)。

# （四）出口网络配置

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）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。

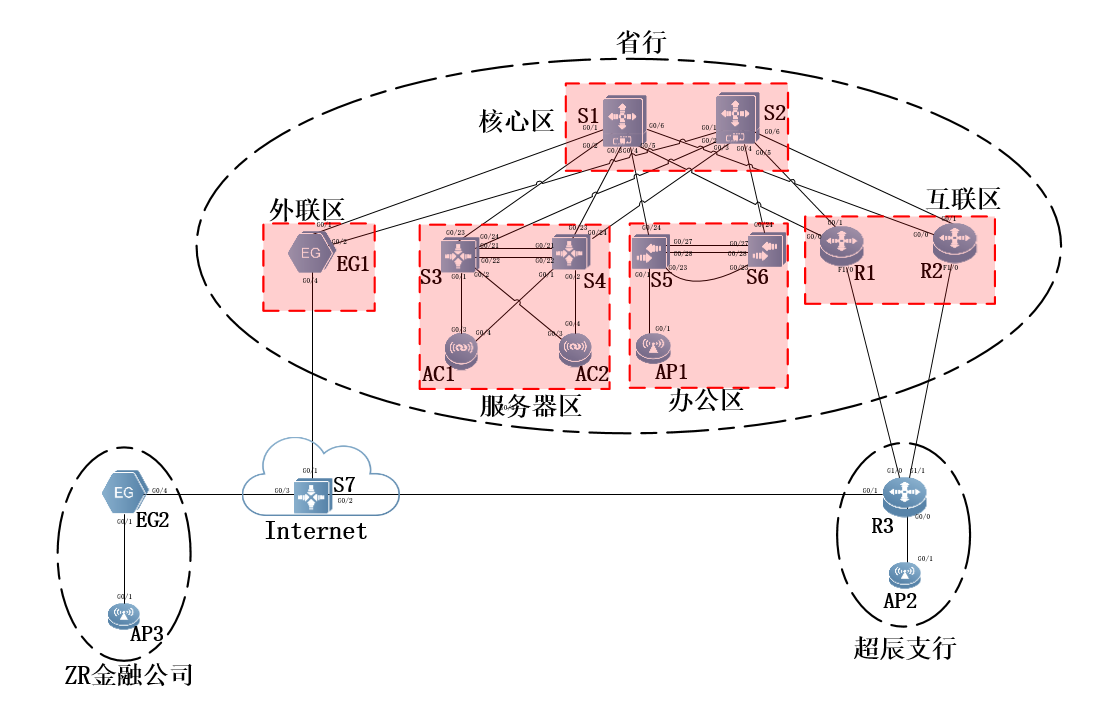
3.超辰支行部署了一条Internet出口，实现支行办公用户访问Internet。正常情况下，生产用户不允许访问Internet,ALC编号为101。其中：超辰支行出口路由器R3上NAT地址池的地址为202.1.1.3/29-201.1.1.4/29。

4.梅森金融公司出口网关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。

5.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，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，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，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，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。

6.在网络安全出口设备EG2与R3出口网关之间，启用IPSec VPNOver GRE.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admin，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。

# 附录1：拓扑图



# 附录2：地址规划表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 | Gi1/0成员口 |
| VLAN201 | \ | 10.2.1.6/30 | Gi1/1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 | —— |
| 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 | —— |
| 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 |