**2023年全国职业院校技能大赛**

**GZ073网络系统管理赛项**

**赛题第2套**

**模块A：网络构建**



目 录

[**任务描述 1**](#_Toc132381781)

[**任务清单 1**](#_Toc132381782)

[**（一）基础配置 1**](#_Toc132381783)

[**（二）有线网络配置 1**](#_Toc132381784)

[**（三）无线网络配置 2**](#_Toc132381785)

[**（四）出口网络配置 4**](#_Toc132381786)

[**（五）网络运维配置 5**](#_Toc132381787)

[**（六）SDN网络配置 5**](#_Toc132381788)

[**附录1：拓扑图 6**](#_Toc132381789)

[**附录2：地址规划表 7**](#_Toc132381790)

# 任务描述

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。

# 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. 交换机S7做密码恢复，新密码设置为admin1234。
3. 在所有的网络设备上开启SSH服务，用户名密码分别为admin、admin1234。特权密码为admin1234。
4. 交换设备上部署SNMP功能，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）有线网络配置

1. 在全网Trunk链路上做VLAN修剪。
2. 在支行连接PC机端口上开启Portfast和BPDUguard防护功能。
3. 支行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）。
5. 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。
6. 在S1上搭建DHCP服务器,为网络中的无线AP设备提供管理地址（具体参数见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）。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。
7. 在S3和S4上配置VRRP，所配置的参数要求如表1所示。，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。
8. 在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1 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 |

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. 优化OSPF相关配置，以尽量加快OSPF收敛。
6. 重发布路由进OSPF中使用类型1。
7. 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。
8. 使用静态路由实现省行的外联区之间（EG1、S1、S2）通信。
9. 使用静态路由第三方公司（EG2、AP3）之间通信。
10. 使用静态路由Internet区域（EG1、R3、EG2）之间通信。
11. 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。
12. 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。
13. 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。
14. 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。

# （三）无线网络配置

陕西招财银行的某局点银行实施无线覆盖工程，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），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、楼梯区域无须覆盖）。

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 |

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，启用WEB认证方。
4. 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。
5. 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。
6. 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，启用802.1X认证方式。
7. 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。
8. 当AP与AC1失去连接时，能无缝切换至AC2。
9. 第三方公司的AP3使用胖模式进行部署，具体要求如下所示。
10. 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。
11. 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）。
12. 认证服务器（IP：192.1.100.100）建立省行认证用户user1,user2，支行认证用户user3,user4分别对应WEB、DOT1X认证；
13. 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)。
14. 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。

# （四）出口网络配置

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。
3. 在网络安全出口设备EG1与EG2之间，启用GRE Over IPSec VPN嵌套功能。
4. 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test。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）网络运维配置

1. 完成整网连通后，进入网络监控运维阶段，运维软件已安装在PC1的虚拟机OPMSrv中(访问运维平台的URL为http://192.1.100.100)，通过运维平台监控省行网络内所有设备（具体设备：S1-S6、EG1、R1、R2、AC1、AC2）。
2. 通过运维平台将省行核心网的被监控设备纳入监控范围；通过拓扑配置功能，将省行核心网的网络拓扑配置到平台中。
3. 将省行核心网S1、S2和省行外联区EG1的两条链路作为重点监测链路，纳入链路监控。
4. 自定义监控大屏（名称：Chinaskills\_network），将网络拓扑、设备运行状态（CPU使用率）、链路运行状态实时显示在大屏中。

# （六）SDN网络配置

1. SDN控制器登录地址：192.168.1.2/24，默认用户密码为admin/test@123。
2. 使用S4/S5/S6构建SDN网络，S5/S6连接SDN控制器的6653端口。S5/S6所有业务流转发需经SDN控制器统一控制管理。
3. 通过SDN控制器手工给S5下发一条流表项名称为drop的流表，执行动作为丢弃，并在交换机上查看流表，测试普通PC禁止ping通高性能PC。
4. 通过SDN控制器流表管理实现PC1/PC2与省行各核心网段互联互通。

# 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 | \ | 10.1.3.1/30 | 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 | 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 |
| Gi0/23 | SDN-Manage | 192.168.1.3 | SDN管理网段 |
| S6 | 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 |
| Gi0/23 | SDN-Manage | 192.168.1.4 | SDN管理网段 |
| 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 | 194.1.10.254/24G0/11-20 | 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 | —— |