**2023年全国职业院校技能大赛**

**GZ073网络系统管理赛项**

**赛题第8套**

**模块A：网络构建**



目 录

[任务清单 1](#_Toc132395927)

[（一）基础配置 1](#_Toc132395928)

[（二）有线网络配置 1](#_Toc132395929)

[（三）无线网络配置 3](#_Toc132395930)

[（四）出口网络配置 5](#_Toc132395931)

[（五）网络运维配置 6](#_Toc132395932)

[（六）SDN网络配置 6](#_Toc132395933)

[附录1：拓扑图 7](#_Toc132395934)

[附录2：地址规划表 8](#_Toc132395935)

# 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.所有设备开启SSH认证，用户名：admin，密码：987123Aa,特权密码为admin123!,密码呈现需加密。所有交换机开启Telnet功能，对所有Telnet用户采用本地认证的方式。

3.S7设备启用SNMPv3功能，用户名Admin!@#，隶属于group组，认证方式为md5，认证密码为password!@#，加密算法为des56，加密密码为password#@!，安全级别为priv；用户admin对MIB默认视图具有读写权限；交换机能主动向主机172.16.0.254发送验

证加密消息。

# （二）有线网络配置

1.在全网Trunk链路上做VLAN修剪；控制用户安全接入，局域网安全设备启用端口保护功能；

2.局域网接入设备启用环路检测功能，规避不同设备间、同一设备不同端口、同一设备单点下的多种环路现象，检测环路后处理方式为shutdown-port；

3.DHCP服务器搭建于R1/R2、R3和EG2上；总部局域网启用DHCP安全防护机制，通过硬件IP/MAC表项过滤匹配保证主机安全，针对有线用户启用ARP防御；

4.总部配置MSTP防止二层环路；要求所有有线数据流经过S1转发。配置参数要求：region-name为ruijie；revision版本为1；主根优先级4096，从根优先级8192；

5.在S1与S2上配置VRRP；其中S1为主设备，优先级255；S2为备设备，优先级120；在R1与R2上为VLAN100配置VRRP，其中R1为主设备，优先级255；R2为备设备，优先级120；

6.交换机S1与S2之间（Gi0/47、Gi0/48）配置二层链路聚合，采取LACP动态聚合模式；

7.总部使用OSPF协议组网，OSPF进程号10；规划多区域组网，区域0（R1、R2、S1、S2），区域1（S1、S2、AC1、AC2）；优化OSPF配置尽量加快OSPF收敛，AC1与AC2不参与DR/BDR的选举，尽可能精简AC1和AC2的路由表条目，重发布路由进OSPF域中使用类型1；

8.联通运营商S5和S6设备启用OSPF协议，进程号20，区域0；

9.联通运营商只维护宽带业务，对于专线业务和客户私网地址不做转发；

10.S1、S2、R1、R2、R3使用BGP路由协议，总部为AS100，分部为AS200；R1、R2与R3建立EBGP邻居；S1、S2、R1、R2建立全互联IBGP邻居（通过LOOPBACK0）；总部与分部所有路由必须通过network命令来发布，总部路由通过重分布引入分部；

11.分部（R3、S7）采用单区域OSPF协议，进程号30；

12.总部R1与EG1、R2与EG2建立GRE隧道，隧道内运行OSPF协议，实现总部与办事处互联互通；广州办事处内部的OSPF进程号11，区域号0；上海办事处内部的OSPF进程号12，区域号0；

13.启用IPsec VPN加密GRE隧道内流量，对总部/分部和办事处的数据流进行保护，尽可能减小IPSEC报文封装长度；

14.联通运营商、公司总部和分部以OSPF LSA5 OE1的方式引入路由，并基于业务网段各自汇总发布B类路由（包括宽带业务、VLAN10、VLAN20和VLAN30）；

15.过滤非必须路由，使用路由策略名称filter；如需修改路由开销，IGP必须设定5或10，BGP必须设定50或100；

16.业务路径要求：总部访问分部主路径为：S1-R1-R3-S7；总部访问互联网：S1-R1-S5；分部访问互联网：S7-R3-R1-S5；所有数据路径要求来回一致；

17.IPv6网络建设要求：总部R1/R2通过管理VLAN与分部R3的环回口建立6to4动态隧道，实现总部与分部间IPv6互联互通；总分部IPv6地址自行规划计算，隧道内启用静态路由协议，总部R1/R2/S1/S2间启用OSPFv3协议；OSPFv3进程号10，区域0，优化配置，加快收敛速度，业务网段不允许出现协议报文。S1、S2、S7启用IPv6网络，实现有线与无线客户端的IPv6终端可自动从网关处获取地址，IPv6地址规划如下：

**表1 IPV6地址规划表**

|  |  |  |
| --- | --- | --- |
| 设备 | 接口 | IPV6地址 |
| S1 | VLAN20 | X:Y:Z::254/64 |
| VLAN30 | 2001:192:1::254/64 |
| Gi0/4 | 2001:11:1::2/64 |
| Gi0/5 | 2001:21:1::2/64 |
| S2 | VLAN20 | X:Y:Z::253/64 |
| VLAN30 | 2001:192:1::253/64 |
| Gi0/4 | 2001:21:1::2/64 |
| Gi0/5 | 2001:12:1::2/64 |
| R1 | Gi0/0 | 2001:11:1::1/64 |
| Gi0/1 | 2001:12:1::1/64 |
| R2 | Gi0/0 | 2001:21:1::1/64 |
| Gi0/1 | 2001:22:1::1/64 |
| R3 | Gi0/0 | 2001:37:1::1/64 |
| S7 | VLAN20 | X:Y:Z::254/64 |
| Gi0/24 | 2001:37:1::2/64 |

# （三）无线网络配置

集团拟投入10.5万元（网络设备采购部分），项目要求重点覆盖楼层、走廊、会议室大厅和办公室。平面布局如图1所示。

本次无线网络要求设备均通过2.4G频段接入（信道1、6、11），访客采用5G频段（信道149,153,157,161）。



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，卫生间、楼梯和电梯区域无需覆盖）；

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.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2；

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） |
| 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 |

4.创建总部 SSID 1为 Ruijie-ZB\_XX(XX现场提供)，AP-Group为ZB；创建分部 SSID 2为 Ruijie-FB\_XX(XX现场提供)，AP-Group为FB；创建上海办事处 SSID 3为 Ruijie-SH\_XX(XX现场提供)，AP-Group为SH；

5.AP与AC1、AC2均建立隧道，当AP与主用AC1失去连接时能无缝切换至AC2并提供服务；

6.省公司总部与分公司无线用户接入无线网络时需要采用基于 WPA2 加密方式，其口令为 XXX(现场提供)；

7.要求所有无线用户均启用本地转发模式；限制AP1、AP2、AP3关联用户数最多为16人；关闭低速率（11b/g 1M、2M、5M，11a 6M、9M）应用接入；

8.调整2.4G频段射频卡powerlocal功率数值为20，5.8G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。

# （四）出口网络配置

1.出口网关上配置访问控制列表，允许所有用户(ACL编号110)在每天08：30-17:00（命名为work）通过NAPT访问互联网，NAPT映射到互联网接口上；

2. 在办事处EG网关上启用Web Portal认证服务，并创建user1、user2；无线用户访问互联网免WEB认证；

3. 在办事处EG针对内网访问外网WEB流量限速每IP 500Kbps，WEB总流量不超过50Mbps，通道名称定义为WEB；

4.EG对敏感词“供应链企业资料”和“员工薪酬明细”进行过滤；

5.禁止局域网用户通过浏览器访问http://15.1.0.2

# （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)，通过运维平台监控总部所有设备。

2.通过运维平台将被监控设备纳入监控范围；通过拓扑配置功能，将网络拓扑配置到平台中；

3.将R1、R2和R3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S2/S3构建SDN网络，S3连接SDN控制器的6653端口。

3.通过SDN控制器手工给S3下发流表项使其S3下终端可与业务网段互联互通。

# 附录1：拓扑图



# 附录2：地址规划表

表4 IPv4地址分配表

| **设备** | **接口或VLAN** | **二层或三层规划** | **说明** |
| --- | --- | --- | --- |
| S1 | VLAN10 | 172.17.10.254/24 | AP管理 |
| VLAN20 | 172.17.20.254/24 | 无线用户 |
| VLAN30 | 172.17.30.254/24 | 有线用户 |
| VLAN100 | 172.17.100.254/24 | 设备管理 |
| Gi0/5 | 10.1.0.14/30 | 互联R2 |
| Gi0/4 | 10.1.0.1/30 | 互联R1 |
| Gi0/47 |  | AG成员 |
| Gi0/48 |  | AG成员 |
| LoopBack 0 | 11.1.0.33/32 | Router ID |
| S2 | VLAN10 | 172.17.10.253/24 | AP管理 |
| VLAN20 | 172.17.20.253/24 | 无线用户 |
| VLAN30 | 172.17.30.253/24 | 有线用户 |
| VLAN100 | 172.17.100.253/24 | 设备管理 |
| Gi0/5 | 10.1.0.10/30 | 互联R1 |
| Gi0/4 | 10.1.0.5/30 | 互联R2 |
| Gi0/47 |  | AG成员 |
| Gi0/48 |  | AG成员 |
| LoopBack 0 | 11.1.0.34/32 | Router ID |
| S3 | Gi0/24 | 192.168.1.3 | SDN管理网段 |
| S4 | VLAN100 | 172.20.100.254/24 | 设备管理 |
| AC1 | VLAN100 | 172.17.100.1/24 | 设备管理 |
| LoopBack 0 | 11.1.0.204/32 |  |
| AC2 | VLAN100 | 172.17.100.2/24 | 设备管理 |
| LoopBack 0 | 11.1.0.205/32 |  |
| S5 | Gi0/1 | 15.1.0.1/30 | 互联EG1 |
| Te0/28 | 56.1.0.1/30 | 互联S6 |
| Gi0/24 | 51.1.0.1/30 | 互联R1 |
| LoopBack 0 | 11.1.0.5/32 | Router ID |
| S6 | Gi0/1 | 26.1.0.1/30 | 互联EG2 |
| Gi0/2 | 63.1.0.1/30 | 互联R3 |
| Te0/28 | 56.1.0.2/30 | 互联S5 |
| Gi0/24 | 62.1.0.1/30 | 互联R2 |
| LoopBack 0 | 11.1.0.6/32 | Router ID |
| S7 | VLAN10 | 172.18.10.254/24 | AP管理 |
| VLAN20 | 172.18.20.254/24 | 无线用户 |
| VLAN30 | 172.18.30.254/24 | Pvlan |
| VLAN31 | Gi0/1至Gi0/4 | Community\_vlan |
| VLAN32 | Gi0/5至Gi0/8 | Isolated\_vlan |
| VLAN100 | 172.18.100.254/24 | 设备管理 |
| Gi0/24 | 10.1.0.42/30 | 互联R3 |
| LoopBack 0 | 11.1.0.7/32 | Router ID |
| EG1 | Gi0/1 | 15.1.0.2/30 | 互联S5 |
| Gi0/2 | 172.19.10.254/24 | 互联PC |
| Tunnel 0 | 11.1.1.1/24 |  |
| LoopBack 0 | 11.1.0.11/32 | Router ID |
| EG2 | Gi0/1 | 26.1.0.2/30 | 互联S6 |
| Gi0/2.10 | 172.20.10.254/24 | AP管理 |
| Gi0/2.20 | 172.20.20.254/24 | 无线用户 |
| Tunnel 0 | 22.1.1.1/24 |  |
| LoopBack 0 | 11.1.0.12/32 | Router ID |
| R1 | Gi0/0 | 10.1.0.2/30 | 互联S1 |
| Gi0/1 | 10.1.0.9/30 | 互联S2 |
| Gi1/0 | 172.16.0.254/24 | VLAN100 |
| Gi1/1 | 10.1.0.21/30 | Svi101成员口 |
| Gi1/2 | 51.1.0.2/30 | Svi102成员口 |
| Tunnel 0 | 11.1.1.2/24 |  |
| LoopBack 0 | 11.1.0.1/32 | Router ID |
| R2 | Gi0/0 | 10.1.0.6/30 | 互联S2 |
| Gi0/1 | 10.1.0.13/30 | 互联S1 |
| Gi1/0 | 172.16.0.253/24 | VLAN100 |
| Gi1/1 | 10.1.0.25/30 | Svi101成员口 |
| Gi1/2 | 62.1.0.2/30 | Svi102成员口 |
| Tunnel 0 | 22.1.1.2/24 |  |
| LoopBack 0 | 11.1.0.2/32 | Router ID |
| R3 | Gi0/1 | 63.1.0.2/30 | 互联S6 |
| Gi0/0 | 10.1.0.41/30 | 互联S7 |
| Gi1/0 | 10.1.0.22/30 | Svi100成员口 |
| Gi1/1 | 10.1.0.26/30 | Svi101成员口 |
| LoopBack 0 | 11.1.0.3/32 | Router ID |