**2023年全国职业院校技能大赛**

**GZ073网络系统管理赛项**

**赛题第4套**

**模块A：网络构建**



目 录

[一、任务清单 1](#_Toc132387982)

[（一）基础配置 1](#_Toc132387983)

[（二）有线网络配置 1](#_Toc132387984)

[（三）无线网络配置 3](#_Toc132387985)

[（四）出口网络配置 4](#_Toc132387986)

[（五）网络运维配置 5](#_Toc132387987)

[（六）SDN网络配置 5](#_Toc132387988)

[附录1：拓扑图 6](#_Toc132387989)

[附录2：地址规划表 7](#_Toc132387990)

# 一、任务清单

# （一）基础配置

1.根据附录1、附录2，配置设备接口信息。

2.所有交换机和无线控制器开启SSH服务，用户名密码分别为admin、Ruijie1234；密码为明文类型,特权密码为Ruijie123。

3.交换设备配置SNMP功能，向主机172.16.0.254发送Trap消息版本采用V2C，读写的Community为“Test1234”，只读的Community为“Public123”，开启Trap消息。

# （二）有线网络配置

1.在全网Trunk链路上做VLAN修剪。

2.在S7交换机使用Private Vlan。

3.在S3上只针对A公司涉密部门VLAN10网段与总部VLAN40网段流量（ACL编号100）做端口镜像，目的端口为Gi0/24，并且监控服务器也能正常访问互联网。

4.在交换机S3、S4上配置DHCP中继，对VLAN10内的用户进行中继。具体要求如下：DHCP服务器搭建于EG2上，DHCP对外服务使用loopback 0地址。

5.在交换机S3、S4上配置MSTP防止二层环路。要求VLAN10、VLAN20、VLAN30、VLAN40、VLAN100数据流经过S3转发，VLAN50、VLAN60数据流经过S4转发，S3、S4其中一台宕机时均可无缝切换至另一台进行转发。所配置的参数要求如下：region-name为test；revision版本为1；实例1，包含VLAN10、VLAN20、VLAN30、VLAN40、VLAN100；实例2，包含VLAN50,VLAN60；S3作为实例0、1中的主根，S4作为实例0、1的从根；S4作为实例2中的主根，S3作为实例2的从根；主根优先级为4096，从根优先级为8192；在S3和S4上配置VRRP，实现主机的网关冗余。所配置的参数要求如表1；S3、S4各VRRP组中高优先级设置为200，低优先级设置为110。

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 |
| VLAN20 | 20 | 192.1.20.254 |
| VLAN30 | 30 | 192.1.30.254 |
| VLAN40 | 40 | 192.1.40.254 |
| VLAN50 | 50 | 192.1.50.254 |
| VLAN60 | 60 | 192.1.60.254 |
| VLAN100 | 100 | 192.1.100.254 |

6.OSPF进程号10，规划单区域，,区域0（S3、S4、EG2）；OSPF进程号20，规划多区域，区域0（R1、R2），区域2（R1、R2、R3）；OSPF进程号30，规划单区域，区域0（AC1、EG1）。

7.总部与A公司互联链路规划至区域0，并且不允许新增OSPF进程。

8.为了方便管理，所有运行OSPF的设备router-id必须为loopback口地址。

9.S5、S6、S7使用RIP协议，RIP协议使用版本2，并且关闭自动聚合。

10.S5、S6、R1、R2使用BGP协议，BGP协议中S5、S6使用AS号100， R1、R2使用AS号200，同AS号内使用loopback口建立iBGP邻居，不同AS号使用互联接口建立eBGP邻居。

11.AC2/S4、EG1/EG2间部署静态路由协议；重发布路由进OSPF中使用类型1。

12.由于172.17.0.0/24是涉密业务网段，仅允许A公司内部访问，并且考虑到数据分流及负载均衡的目的，针对本部与分部数据流走向要求如下：

OSPF可以通过修改COST值的方式实现数据分流，并且其值为1或2;

禁止将BGP的路由条目通过重发布BGP AS方式引入RIP及OSPF中；

禁止将RIP、OSPF的路由条目通过重发布整个进程方式引入BGP中；

总部有线网段与数据中心服务器互通主路径为S3-R1-R3；

总部无线网段与数据中心服务器互通主路径为S4-R2-R3；

总部有线网络与互联网互通主路径为S3-EG2；

总部无线网络与互联网互通主路径为S4-EG2。

13.A公司涉密部门VLAN10网段与总部VLAN40网段间的互通主路径为S3-R1-S5-S7;A公司涉密部门与数据中心服务器互通的主路径为S7-S5-R1-R3;数据中心服务器与互联网互通的主路径为R3-R1-S3-EG2。

# （三）无线网络配置

CII集团公司拟投入16.5万元（网络设备采购部分），项目要求重点覆盖楼层、走廊和办公室。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）。

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. 使用S3、S4为无线用户与AP DHCP服务器，S3分配地址范围为其网段的1至100，S4分配地址为其网段的101至200（使用最短的命令实现）。 使用AC1为办事处无线用户与AP DHCP服务器。
2. 创建SSID (WLAN-ID 1)为 test-ZB\_XX(XX现场提供)，AP-Group为ZB，本部无线用户关联SSID后可自动获取地址，启用WEB认证方。
3. 创建SSID (WLAN-ID 2)为 test-BSC\_XX(XX现场提供)，AP-Group为BSC，办事处无线用户关联SSID后可自动获取地址，启用802.1X认证方式。
4. 为了减轻AC1的负担，因此AC2为主用AC，AC1为备用AC。
5. AP与AC1、AC2均建立隧道，当AP与主用AC失去连接时能无缝切换至备用AC并提供服务。
6. 避免链路不稳定，导致AP工作不正常，总部启用无线AP边缘感知功能。
7. 在同一个 AP 中的用户在某些时候出于安全性的考虑，需要将他们彼此之间进行隔离，实现用户之间彼此不能互相访问，配置同 下用AP户间隔离功能。
8. 无线用户启用本地转发模式。
9. 认证服务器（IP：192.1.100.100）建立总部认证用户user1,user2，分部认证用户user3,user4分别对应WEB、DOT1X认证；

# （四）出口网络配置

1.总部出口网关上配置访问控制列表ACL 120，仅允许用户在周一到周五的上班时间（命名为work，9:00至17:00）通过NAPT访问互联网，NAPT映射到互联网接口上，服务器上网不受限制。

2.办事处出口网关上配置访问控制列表ACL120，允许用户通过NAPT访问互联网，NAPT映射到互联网接口上。

3.办事处网关上配置端口映射，使AC1（11.1.0.204）设备的SSH服务可以通过互联网被访问，映射地址为197.1.0.5:2222。

4.在总部网关上启用Web Portal认证服务，并创建user1、user2。

5.无线用户和服务器不需要进行WEB认证即可访问互联网。

6.部署L2TP隧道进行总部对办事处路由的对接验证，验证用户名密码均为test，L2TP隧道密码为test;L2TP用户地址池为10.1.2.1—10.1.2.254;L2TP隧道中承载OSPF协议，使其总部与办事处通过OSPF进行路由交互，区域号1。

7.部署IPsec对L2TP隧道中的业务数据加密；IPsec VPN需要采用传输模式，预共享密码为test，加密认证方式为ESP-3DES、ESP-MD5-HMAC，DH使用组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)；通过运维平台监控公司总部网络内所有设备（具体设备：S1、S3-S4、EG2、AC2）。

2.通过运维平台将A公司数据中心的被监控设备纳入监控范围；通过拓扑配置功能，将公司总部和A公司数据中心的网络拓扑配置到平台中。

3.将公司总部S3、S4和互联网EG2的两条链路作为重点监测链路，纳入链路监控；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S7/S8/S9构建SDN网络，S8/S9连接SDN控制器的6653端口。

3.通过SDN控制器手工给S8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与分部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 | VLAN10 | Office10 | Gi0/1至Gi0/4 | 办公网段 |
| VLAN20 | Office20 | Gi0/5至Gi0/8 | 办公网段 |
| VLAN30 | Office30 | Gi0/9至Gi0/12 | 办公网段 |
| VLAN40 | Office40 | Gi0/13至Gi0/16 | 办公网段 |
| Gi0/23 | SDN-Manage | 192.168.1.3 | SDN管理网段 |
| S2 | VLAN10 | Office10 | Gi0/1至Gi0/4 | 办公网段 |
| VLAN20 | Office20 | Gi0/5至Gi0/8 | 办公网段 |
| VLAN30 | Office30 | Gi0/9至Gi0/12 | 办公网段 |
| VLAN40 | Office40 | Gi0/13至Gi0/16 | 办公网段 |
| Gi0/23 | SDN-Manage | 192.168.1.4 | SDN管理网段 |
| S3 | VLAN10 | Office10 | 192.1.10.252/24 | 办公网段 |
| VLAN20 | Office20 | 192.1.20.252/24 | 办公网段 |
| VLAN30 | Office30 | 192.1.30.252/24 | 办公网段 |
| VLAN40 | Office40 | 192.1.40.252/24 | 办公网段 |
| VLAN50 | AP | 192.1.50.252/24 | 无线AP管理 |
| VLAN60 | Wireless | 192.1.60.252/24 | 无线用户 |
| VLAN100 | Manage | 192.1.100.252/24 | 设备管理VLAN |
| VLAN101 | Connect | 10.1.0.53/30 | 设备互联 |
| Gi0/2 | Trunk |  | AG1成员口 |
| Gi0/3 | Trunk |  | AG1成员口 |
| Gi0/4 |  | 10.1.0.5/30 | 互联EG2 |
| Gi0/5 |  | 10.1.0.9/30 | 互联R1 |
| LoopBack 0 |  | 11.1.0.33/32 |  |
| S4 | VLAN10 | Office10 | 192.1.10.253/24 | 办公网段 |
| VLAN20 | Office20 | 192.1.20.253/24 | 办公网段 |
| VLAN30 | Office30 | 192.1.30.253/24 | 办公网段 |
| VLAN40 | Office40 | 192.1.40.253/24 | 办公网段 |
| VLAN50 | AP | 192.1.50.253/24 | 无线AP管理 |
| VLAN60 | Wireless | 192.1.60.253/24 | 无线用户 |
| VLAN100 | Manage | 192.1.100.253/24 | 设备管理VLAN |
| VLAN101 | Connect | 10.1.0.54/30 | 设备互联 |
| Gi0/2 | Trunk |  | AG1成员口 |
| Gi0/3 | Trunk |  | AG1成员口 |
| Gi0/4 |  | 10.1.0.13/30 | 互联EG2 |
| Gi0/5 |  | 10.1.0.17/30 | 互联R2 |
| LoopBack 0 |  | 11.1.0.34/32 |  |
| AC1 | LoopBack 0 |  | 11.1.0.204/32 |  |
| Gi0/1 |  | 10.1.0.1/30 | 互联EG1 |
| VLAN10 | User | 195.1.10.254/24 | Gi0/2-4 |
| VLAN20 | Wire\_user | 195.1.20.254/24 |  |
| VLAN30 | AP | 195.1.30.254/24 |  |
| AC2 | LoopBack 0 |  | 11.1.0.205/32 |  |
| VLAN100 | Manage | 192.1.100.1/24 |  |
| S5 | Gi0/1 |  | 10.1.0.45/30 | 互联S7 |
| Gi0/2 |  | 10.1.0.41/30 | 互联S6 |
| Gi0/48 |  | 10.1.0.30/30 | 互联R1 |
| LoopBack 0 |  | 11.1.0.35/32 |  |
| S6 | Gi0/1 |  | 10.1.0.50/30 | 互联S7 |
| Gi0/2 |  | 10.1.0.42/30 | 互联S5 |
| Gi0/48 |  | 10.1.0.34/30 | 互联R2 |
| LoopBack 0 |  | 11.1.0.36/32 |  |
| EG1 | GI0/0 | 　 | 10.1.0.2/30 |  |
| GI0/2 | 　 | 197.1.0.1/24 | 与EG2互联 |
| LoopBack 0 | 　 | 11.1.0.11/32 |  |
| EG2 | Gi0/0 | 　 | 10.1.0.6/30 |  |
| Gi0/1 | 　 | 10.1.0.14/30 |  |
| Gi0/2 | 　 | 197.1.0.2/24 | 与EG1互联 |
| LoopBack 0 | 　 | 11.1.0.12/32 |  |
| R1 | Gi0/0 |  | 10.1.0.10/30 | 互联S3 |
| Gi0/1 |  | 10.1.0.29/30 | 互联S5 |
| Fa1/1(Vlan300) |  | 10.1.0.25/30 | 互联R2 |
| Fa1/0(Vlan200) |  | 10.1.0.21/30 | 互联R3 |
| LoopBack 0 |  | 11.1.0.1/32 |  |
| R2 | Gi0/0 |  | 10.1.0.18/30 | 互联S4 |
| Gi0/1 |  | 10.1.0.33/30 | 互联S6 |
| Fa1/1(Vlan300) |  | 10.1.0.26/30 | 互联R1 |
| Fa1/0(Vlan200) |  | 10.1.0.37/30 | 互联R3 |
| LoopBack 0 |  | 11.1.0.2/32 |  |
| R3 | Gi0/0 |  | 10.1.0.22/30 | 互联R1 |
| Gi0/1 |  | 10.1.0.38/30 | 互联R2 |
| LoopBack 0 |  | 11.1.0.3/32 |  |
| Fa1/0（Vlan160） | Con\_To\_Cloud | 172.16.0.254/24 | 模拟云平台 |
| S7 | VLAN10 | Primary | 194.1.10.254/24 | primary vlan |
| VLAN11 | Community | Gi0/1至Gi0/8 | community vlan |
| VLAN12 | Isolated | Gi0/9至Gi0/16 | isolated vlan |
| VlAN100 | Manage | 194.1.100.254/24 |  |
| VlAN200 | Secret | 172.17.0.254/24 | 涉密业务Gi0/17-Gi0/22 |
| Gi0/23 |  | 10.1.0.46/30 | 互联S5 |
| Gi0/24 |  | 10.1.0.49/30 | 互联S6 |
| LoopBack 0 |  | 11.1.0.37/32 |  |