**2023年全国职业院校技能大赛**

**GZ073网络系统管理赛项**

**赛题第7套**

**模块A：网络构建**



目 录

[任务清单 1](#_Toc132395254)

[（一）基础配置 1](#_Toc132395255)

[（二）有线网络配置 1](#_Toc132395256)

[（三）无线网络配置 3](#_Toc132395257)

[（四）出口网络配置 4](#_Toc132395258)

[（五）网络运维配置 5](#_Toc132395259)

[（六）SDN网络配置 5](#_Toc132395260)

[附录1：拓扑图 6](#_Toc132395261)

[附录2：地址规划表 7](#_Toc132395262)

# 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、admin1234；密码为明文类型,特权密码为admin。

3.交换机配置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“Test”，只读的Community为“public”，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.为隔离部分终端用户间的二层互访，在交换机S1的Gi0/5-Gi0/16端口启用端口保护。

3.要求在吉林分部接入设备S1进行防环处理。具体要求如下：终端接口开启BPDU防护不能接收 BPDU报文；终端接口下开启 RLDP防止环路，检测到环路后处理方式为 Shutdown-Port；连接终端的所有端口配置为边缘端口；如果端口被 BPDU Guard检测进入 Err-Disabled状态，再过 300 秒后会自动恢复（基于接口部署策略），重新检测是否有环路。

4.在交换机S3、S4上配置DHCP中继，对VLAN10内的用户进行中继，使得本部PC1用户使用DHCP Relay方式获取IP地址。具体要求如下：DHCP服务器搭建于VSU上，地址池命名为Pool\_VLAN10，DHCP对外服务使用loopback 0地址；为了防御动态环境局域网伪DHCP服务欺骗，在S1交换机部署DHCP Snooping功能。

5.为了防止伪 IP 源地址攻击， 导致出口路由器会话占满，要求S1交换机部署端口安全，接口Gi0/1只允许PC1通过。

6.在吉林分部交换机S1、S3、S4上配置MSTP防止二层环路；要求所有数据流经过S4转发，S4失效时经过S3转发。所配置的参数要求如下：region-name为test；revision版本为1；S3作为实例中的从根， S4作为实例中的主根；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** |
| VLAN10 | 10 | 192.1.10.254 |
| VLAN20 | 20 | 192.1.20.254 |
| VLAN30 | 30 | 192.1.30.254 |
| VLAN100(交换机间) | 100 | 192.1.100.254 |

7.S6和S7间部署虚拟化，其中S7为主，S6为备；规划S6和S7间的Gi0/48端口作为双主机检测链路，配置基于BFD的双主机检；主设备：Domain id：1,switch id:2,priority 150, description: S6000-2;备设备：Domain id：1,switch id:1,priority 120, description: S6000-1。

8.广州总部与吉林分部内网均使用OSPF协议组网，访问互联网均使用默认路由。具体要求如下：总部S5、AC1、AC2、EG1间运行OSPF，进程号为10；吉林分部EG2、S3、S4、S6/S7间运行OSPF，进程号为10； 要求业务网段中不出现协议报文；要求所有路由协议都发布具体网段；为了管理方便，需要发布Loopback地址;优化OSPF相关配置，以尽量加快OSPF收敛；重发布路由进OSPF中使用类型1。

9.吉林分部部署IPV6网络实现内网IPV6终端通过无状态自动从网关处获取地址；

10.在S3和S4上配置VRRP for IPv6，实现主机的IPv6网关冗余;VRRP与MSTP的主备状态与IPV4网络一致；IPV6地址规划如下表2：

表2 IPV6地址规划表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | IPV6地址 | VRRP组号 | 虚拟IP |
| S3 | VLAN10 | 2001:193:10::252/64 | 10 | 2001:193:10::254/64 |
| VLAN20 | 2001:193:20::252/64 | 20 | 2001:193:20::254/64 |
| VLAN30 | 2001:193:30::252/64 | 30 | 2001:193:30::254/64 |
| S4 | VLAN10 | 2001:193:10::253/64 | 10 | 2001:193:10::254/64 |
| VLAN20 | 2001:193:20::253/64 | 20 | 2001:193:20::254/64 |
| VLAN30 | 2001:193:30::253/64 | 30 | 2001:193:30::254/64 |

11.由于公司在吉林设有分部。为总部及分部之间互联互通，申请运营商专线业务。针对运营商组网部署要求如下：R1、R2、R3部署IGP OSPF动态路由进程号为20，实现直连网段互联互通。

12.R1、R2、R3间部署BGP联盟,联盟AS号为100, 使用Loopback接口建立Peer;R1与R2的成员AS号为64512，R3的成员AS号为64523。

13.运营商R1、R2、R3各自通告EG1、EG2的直连网段到BGP中，以汇总B段静态路由的方式进行发布，当运营商路由器与EG直连链路断开时，可通过其他路由器与EG互通。

14.考虑到数据分流及负载均衡的目的，具体要求如下：可通过修改OSPF 路由COST达到分流的目的，且其值必须为5或10；吉林分部有线IPV4用户与互联网互通主路径规划为：S4-S7-EG2;主链路故障时可无缝切换到备用链路上。

# （三）无线网络配置

CII集团公司拟投入9.5万元（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3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3 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.使用S5作为广州总部无线用户和无线AP的DHCP 服务器。

5.创建财务部内网 SSID 为 test-CW\_XX(XX现场提供)，WLAN ID 为1；创建研发部内网 SSID 为 test-YF\_XX(XX现场提供)，WLAN ID 为2。

6.AP-Group为ZB，内网无线用户关联SSID后可自动获取地址。

7.本部AC1为主用，AC2为备用。AP与AC1、AC2均建立隧道，当AP与AC1失去连接时能无缝切换至AC2并提供服务。

8.研发部用户接入无线网络时需要采用WPA2加密方式，加密密码为XX(现场提供)；

9.启用白名单校验，仅放通PC2无线终端。

10.要求内网无线网络均启用集中转发模式。

11.为了保障本部每个用户的无线体验，针对WLAN ID 1下的每个用户的下行平均速率为 800KB/s ，突发速率为1600KB/s。

12.配置AP3最大带点人数为30人。

13.通过时间调度，要求每周一至周五的21:00至23:30期间关闭研发部无线服务。设置AP2最小接入信号强度为-65dBm。

14.关闭低速率（11b/g 1M、2M、5M，11a 6M、9M）应用接入。

# （四）出口网络配置

1.出口网关及出口路由器上进行NAT配置实现总部与分部的所有用户(ACL 110)均可访问互联网，通过NAPT方式将内网用户IP地址转换到互联网接口上。

2.广州总部EG1针对访问外网WEB流量限速每IP 1000Kbps，内网WEB总流量不超过50Mbps（策略名称WEB）。

3.广州总部EG1基于网站访问、邮件收发、IM聊天、论坛发帖、搜索引擎多应用启用审计功能。

4.广州总部EG1周一到周五工作时间09：00-17:00（命名为work）阻断并审计P2P应用软件使用（策略名称P2P）。

5.为了实现总部与分部互访数据的安全性，要求使用IPSec对总部到分部的数据流进行加密ACL（编号为101）。为此规划如下：要求使用动态隧道主模式，预共享密码为 test，加密认证方式为 ESP-3DES、ESP-MD5-HMAC，DH使用组2;总分机构间数据通信及加密通过运营商R1联通节点作为中转设备；总部无线IPV4用户与分部IPV4用户互通主路径规划为：AC1-S5-EG1-EG2-S7-S4(EG1/EG2间运行VPN隧道)。

6.本部与分部用户数据流匹配EG内置联通、电信与教育地址库，实现访问联通资源走联通线路，访问电信资源走电信线路，访问教育网资源走教育网线路。

7.除联通、电信、教育资源之外默认所有数据流在三条线路间进行负载转发。

# （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)，通过运维平台监控本部所有设备。

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S6、S7和EG2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/S4构建SDN网络，S2连接SDN控制器的6653端口。

3.通过SDN控制器手工给S2下发流表项使其S2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

| **设备** | **接口或VLAN** | **VLAN名称** | **二层或三层规划** | **说明** |
| --- | --- | --- | --- | --- |
| S1 | VLAN10 | Yanfa | Gi0/1至Gi0/4 | 研发部 |
| VLAN20 | Xiaoshou | Gi0/5至Gi0/8 | 销售部 |
| VLAN30 | Caiwu | Gi0/9至Gi0/12 | 财务部 |
| Vlan100 | Manage | 192.1.100.1/24 | 管理与互联VLAN |
| S2 | VLAN10 | Yanfa | Gi0/1至Gi0/4 | 研发部 |
| VLAN20 | Xiaoshou | Gi0/5至Gi0/8 | 销售部 |
| VLAN30 | Caiwu | Gi0/9至Gi0/12 | 财务部 |
| Gi0/24 | SDN-Manage | 192.168.1.3 | SDN管理网段 |
| S3 | VLAN10 | Yanfa | 192.1.10.252/24 | 研发部 |
| VLAN20 | Xiaoshou | 192.1.20.252/24 | 销售部 |
| VLAN30 | Caiwu | 192.1.30.252/24 | 财务部 |
| Vlan100 | Manage | 192.1.100.252/24 | 管理与互联VLAN |
| Gi0/24 |  | 10.1.0.1/30 | 　 |
| LoopBack 0 | 　 | 11.1.0.33/32 |  |
| S4 | VLAN10 | Yanfa | 192.1.10.253/24 | 研发部 |
| VLAN20 | Xiaoshou | 192.1.20.253/24 | 销售部 |
| VLAN30 | Caiwu | 192.1.30.253/24 | 财务部 |
| Vlan100 | Manage | 192.1.100.253/24 | 管理与互联VLAN |
| Gi0/24 |  | 10.1.0.5/30 | 　 |
| LoopBack 0 | 　 | 11.1.0.34/32 |  |
| S6/S7 | Gi1/0/1 |  | 10.1.0.2/30 |  |
| Gi2/0/1 |  | 10.1.0.6/30 |  |
| Gi1/0/2 |  | 10.1.0.9/30 |  |
| Gi2/0/2 |  | 10.1.0.13/30 |  |
| LoopBack 0 | 　 | 11.1.0.67/32 |  |
| EG1 | Gi0/0 |  | 10.1.0.18/30 |  |
| Gi0/2 |  | 20.1.0.1/29 |  |
| Gi0/3 |  | 30.1.0.1/29 |  |
| Gi0/4 |  | 40.1.0.1/29 |  |
| LoopBack 0 | 　 | 11.1.0.11/32 |  |
| EG2 | Gi0/0 |  | 10.1.0.10/30 |  |
| Gi0/1 |  | 10.1.0.14/30 |  |
| Gi0/2 |  | 20.1.0.9/29 |  |
| Gi0/3 |  | 30.1.0.9/29 |  |
| Gi0/4 |  | 40.1.0.9/29 |  |
| LoopBack 0 | 　 | 11.1.0.12/32 |  |
| S5 | VLAN10 | AP | 194.1.10.254/24 |  |
| Gi0/1至Gi10 |
| VLAN20 | Caiwu\_Wifi | 194.1.20.254/24 |  |
| VLAN30 | Yanfa\_Wifi | 194.1.30.254/24 |  |
| Vlan100 | Manage | 194.1.100.254/24 |  |
| Gi0/24 |  | 10.1.0.17/30 |  |
| LoopBack 0 | 　 | 11.1.0.5/32 |  |
| AC1 | Vlan100 | Manage | 194.1.100.251/24 |  |
| LoopBack 0 | 　 | 11.1.0.204/32 |  |
| AC2 | Vlan100 | Manage | 194.1.100.252/24 |  |
| LoopBack 0 | 　 | 11.1.0.205/32 |  |
| R1 | Gi0/0 |  | 20.1.0.6/29 |  |
| Gi0/1 |  | 20.1.0.14/29 |  |
| Gi1/0(vlan100) |  | 12.1.0.1/30 |  |
| Loopback0 |  | 11.1.0.1/32 |  |
| R2 | Gi0/0 |  | 30.1.0.6/29 |  |
| Gi0/1 |  | 30.1.0.14/29 |  |
| Gi1/0(vlan100) |  | 12.1.0.2/30 |  |
| Gi1/1(vlan101) |  | 23.1.0.1/30 |  |
| Loopback0 |  | 11.1.0.2/32 |  |
| R3 | Gi0/0 |  | 40.1.0.6/29 |  |
| Gi0/1 |  | 40.1.0.14/29 |  |
| Gi1/1(vlan101) |  | 23.1.0.2/30 |  |
| Loopback0 |  | 11.1.0.3/32 |  |