**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2）



目录

[任务描述 3](#_Toc21137)

[任务清单 3](#_Toc4123)

[（一）基础配置 3](#_Toc9822)

[（二）有线网络配置 3](#_Toc25821)

[（三）无线网络配置 5](#_Toc7099)

[（四）出口网络配置 7](#_Toc32134)

[附录1：拓扑图 8](#_Toc27809)

[附录2：地址规划表 9](#_Toc10953)

# 任务描述

CII集团公司业务不断发展壮大，为适应IT行业技术飞速发展，满足公司业务发展需要，集团公司决定建设北京分校、广州分校与本部校区的信息化网络。你做为火星公司网络工程师前往CII集团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、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.为隔离网络中部分终端用户间的二层互访，在交换机S1、S2上使用端口保护。为了规避网络末端接入设备上出现环路影响全网，要求在本部与分校接入设备S1，S2，S6，S7进行防环处理。具体要求如下：接口开启BPDU防护不能接收bpduguard报文；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，重新检测是否有环路。

3.为了保证接入区DHCP服务安全及伪IP源地址攻击，具体要求如下：DHCP服务器搭建于S3上对VLAN10以内的用户进行地址分配；为了防御从非法DHCP服务器获得的地址要求在S1、S2上部署DHCP Snooping功能。

4.在本部交换机S3、S4上配置MSTP防止二层环路；要求VLAN10、VLAN20、VLAN30数据流经过S3转发，VLAN40、VLAN50、VLAN100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；实例2，包含VLAN40，VLAN50，VLAN100；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 |
| VLAN40 | 40 | 192.1.40.254 |
| VLAN50 | 50 | 192.1.50.254 |
| VLAN100(交换机间) | 100 | 192.1.100.254 |

5.本部内网使用静态路由、OSPF多协议组网。其中S3、S4、S5、EG1、EG2、R1使用OSPF协议，本部其余三层设备间使用静态路由协议。本部与分校广域网间使用静态路由协议（R1除外），各分校局域网环境使用静态路由协议。要求网络具有安全性、稳定性。具体要求如下：本部OSPF进程号为10，规划多区域；区域0（S3、S4），区域1（S3，S4，S5）,区域2（S3，S4，EG1，EG2），区域3（S4、R1）；区域1为完全NSSA区域；AP使用静态路由协议；本部与分校通过重分发引入彼此路由；要求本部业务网段中不出现协议报文；不允许重发布直连路由，Network方式发布本地明细路由；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。

4.不允许在R1设备使用IPV4静态路由。

5.本部路由器R1与北京校区路由器R2、广州校区路由器R3间属于广域网链路，其中R1-R2间所租用一条带宽为2M的线路，R1-R3间租用2条带宽均为2M的线路。本部路由器与分校路由器间属于广域网链路。需要使用PPP进行安全保护，同时提高R1与R3的链路带宽与简化网络部署的目的，现要求如下：使用CHAP协议;单向认证，用户名+验证口令方式；R1为认证服务端，R2、R3为认证客户端；用户名和密码均为test；R1与R3间使用PPP链路捆绑，捆绑组号为1。

6.考虑到广域网线路安全性较差，所以需要使用IPSec对各分校到总校的业务数据进行加密。要求使用动态隧道主模式，安全协议采用esp协议，加密算法采用3des，认证算法采用md5，以IKE方式建立IPsec SA。

7.在R1上所配置的参数要求如下：ipsec加密转换集名称为myset；动态ipsec加密图名称为dymymap；预共享密钥为明文123456；静态的ipsec加密图mymap。

8.在R2和R3上所配置的参数要求如下：ACL编号为101；静态的ipsec加密图mymap；

预共享密钥为明文123456。

9.考虑到数据分流及负载均衡的目的，针对本部与各分校数据流走向要求如下:通过修改OSPF接口COST达到分流的目的，且其值必须为5或10；OSPF通过路由引入时改变引入路由的COST值，且其值必须为5或10；本部VLAN10，VLAN20，VLAN30用户与互联网互通主路径规划为：S3-EG1；本部VLAN40用户与互联网互通主路径规划为：S4-EG2；各分校用户与互联网互通主路径规划为：S4-EG2；云平台服务器与互联网互通主路径规划为S3-EG1；主链路故障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13.5万元（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。

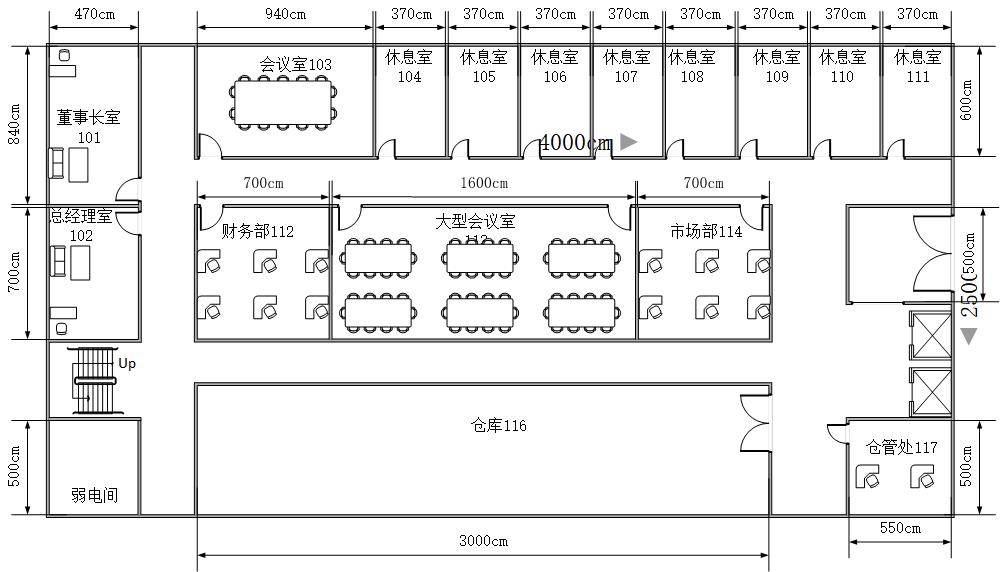


图1 平面布局图

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AC为本部无线用户DHCP服务器，使用S3、S4为本部AP的DHCP服务器,S3分配AP地址范围为其网段的1至100,S4分配AP地址范围为其网段的101至200。
2. 创建本部SSID(WLAN-ID 1)为test-ZX\_XX(XX现场提供)，AP-Group为ZX，本部无线用户关联SSID后可自动获取地址。
3. 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。
4. 为了保证合法用户连接入本部内网，本部无线用户使用MAC校验方式。在本部的AC设备上配置白名单只允许PC1（无线网卡ipconfig确定MAC地址）接入无线网络中，并设置AC白名单数量最多为10。
5. 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AP1实现同AP下用户间隔离功能。
6. 要求本部无线用户启用集中转发模式。
7. 限制AP1关联用户数最高为16。
8. 本部关闭低速率（1M,6M）应用接入。
9. 北京校区与广州校区使用无线AP胖模式进行部署。
10. AP2以透明模式进行部署，S6部署DHCP为无线终端和AP分配地址。
11. AP2创建SSID(WLAN-ID 1)为test-BJ\_XX(XX现场提供),采用WEB进行认证，认证用户名为user1,密码为XX(现场提供)。
12. AP3以路由模式进行部署，本地部署DHCP为无线终端分配地址。
13. AP3创建SSID(WLAN-ID 1)为test-GZ\_XX(XX现场提供),启用白名单校验，放通PC3无线网卡。

# （四）出口网络配置

1.本部出口网关上配置访问控制列表，允许本部、分部有线无线业务网段(ACL编号110)通过NAPT访问联通、教育网资源。

2.在本部EG1上配置，使本部核心交换S4（11.1.0.4）设备的Telnet服务可以通过互联网被访问，将其地址映射至联通线路上，映射地址为196.1.0.10。

3.需确保NAT映射数据流来回一致，启用EG源进源出功能保证任何外网用户（联通、电信、移动、教育……）均可访问映射地址196.1.0.10。

4.在本部网关上启用Web Portal认证服务，并创建user1、user2，密码均为123456；

有线用户需进行WEB认证访问互联网。

5.无线用户不需在EG上进行WEB认证即可访问互联网。

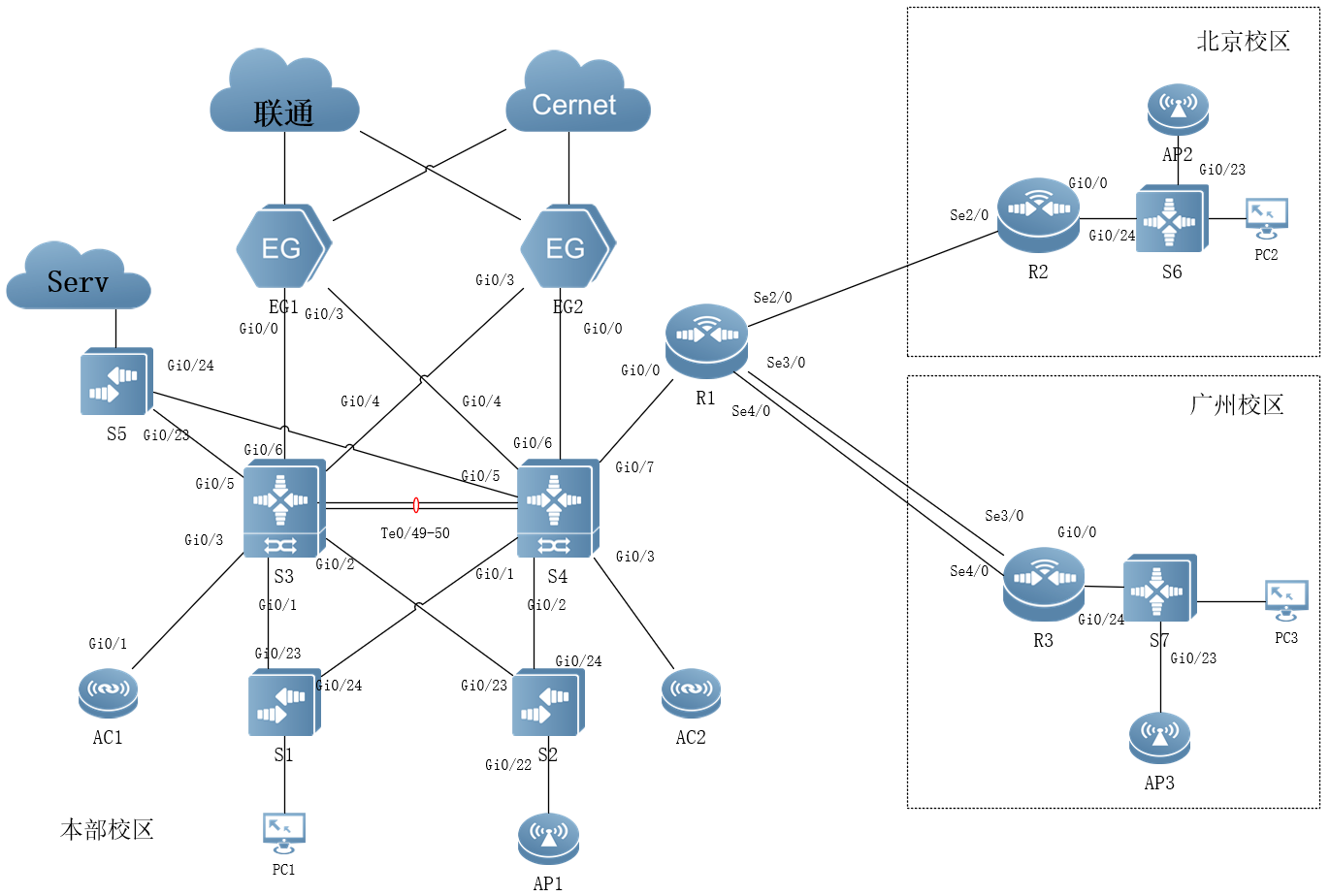
6.本部针对访问外网WEB流量限速每IP 1000Kbps，内网WEB总流量不超过100M（策略及通道名称均为：WEB）。

7.工作日（周一到周五：上午9点到下午5点）阻断并审计P2P应用软件使用（策略名称：P2P）。

8.对创建的用户user1用户上网活动不进行监控审计。

9.本部与分校用户数据流匹配EG内置联通与教育地址库，实现访问联通资源走联通线路，访问教育资源走教育线路；除联通、教育资源之外默认所有数据流在联通与教育线路间进行负载转发。

# 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 |
| VLAN50 | AP | Gi0/21至Gi0/22 | 无线AP管理 |
| VLAN100 | Manage | 192.1.100.4/24 | 设备管理VLAN |
| 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 |
| VLAN50 | AP | Gi0/21至Gi0/22 | 无线AP管理 |
| VLAN100 | Manage | 192.1.100.5/24 | 设备管理VLAN |
| 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 |
| VLAN100 | Manage | 192.1.100.252/24 | 设备管理VLAN |
| Gi0/4 |  | 10.1.0.41/30 | 互联EG2 |
| Gi0/5 |  | 10.1.0.1/30 | 互联S5 |
| Gi0/6 |  | 10.1.0.5/30 | 互联EG1 |
| 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 |
| VLAN100 | Manage | 192.1.100.253/24 | 设备管理VLAN |
| Gi0/4 |  | 10.1.0.37/30 | 互联EG1 |
| Gi0/5 |  | 10.1.0.33/30 | 互联S5 |
| Gi0/6 |  | 10.1.0.9/30 | 互联EG2 |
| Gi0/7 |  | 10.1.0.13/30 | 互联R1 |
| LoopBack 0 |  | 11.1.0.34/32 |  |
| AC1 | LoopBack 0 |  | 11.1.0.204/32 |  |
| VLAN60 | Wiressless | 192.1.60.252/24 | 无线用户 |
| Vlan100 | Manage | 192.1.100.2/24 | 管理与互联VLAN |
| AC2 | LoopBack 0 |  | 11.1.0.205/32 |  |
| VLAN60 | Wiressless | 192.1.60.253/24 | 无线用户 |
| Vlan100 | Manage | 192.1.100.3/24 | 管理与互联VLAN |
| S5 | LoopBack 0 |  | 11.1.0.5/32 |  |
| Gi0/23 |  | 10.1.0.2/30 | 互联S3 |
| Gi0/24 |  | 10.1.0.34/30 | 互联S4 |
| EG1 | Gi0/0 |  | 10.1.0.6/30 | 互联S3 |
| Gi0/1 |  | 196.1.0.1/24 | 互联EG2 |
| Gi0/2 |  | 197.1.0.1/24 | 互联EG2 |
| Gi0/3 |  | 10.1.0.38/30 | 互联S4 |
| LoopBack 0 |  | 11.1.0.11/32 |  |
| EG2 | Gi0/0 |  | 10.1.0.10/30 | 互联S4 |
| Gi0/1 |  | 196.1.0.2/24 | 互联EG1 |
| Gi0/2 |  | 197.1.0.2/24 | 互联EG1 |
| Gi0/3 |  | 10.1.0.42/30 | 互联S3 |
| LoopBack 0 |  | 11.1.0.12/32 |  |
| R1 | Gi0/0 |  | 10.1.0.14/30 | 互联S4 |
| S2/0 |  | 20.0.0.1/30 | 互联R2 |
| S3/0 |  | 10.1.0.22/30 | 捆绑组1成员 |
| S4/0 |  | 10.1.0.22/30 | 捆绑组1成员 |
| LoopBack 0 |  | 11.1.0.1/32 |  |
| R2 | Gi0/0 |  | 10.1.0.25/30 | 互联S6 |
| S2/0 |  | 20.0.0.2/30 | 互联R1 |
| LoopBack 0 |  | 11.1.0.2/32 |  |
| R3 | Gi0/0 |  | 10.1.0.29/30 | 互联S7 |
| S3/0 |  | 10.1.0.21/30 | 捆绑组1成员 |
| S4/0 |  | 10.1.0.21/30 | 捆绑组1成员 |
| LoopBack 0 |  | 11.1.0.3/32 |  |
| S6 | Gi0/24 |  | 10.1.0.26/30 |  |
| VLAN10 | Wire\_user | 194.1.10.254/24 | 分校有线用户  Gi0/1-20 |
| VLAN20 | Wireless\_user | 194.1.20.254/24 | 分校无线用户 |
| VLAN30 | AP | 194.1.30.254/24 | 分校AP  Gi0/21-23 |
| LoopBack 0 |  | 11.1.0.6/32 |  |
| S7 | Gi0/23 |  | 10.1.0.49/30 | AP |
| Gi0/24 |  | 10.1.0.30/30 |  |
| VLAN10 | Wire\_user | 195.1.10.254/24 | 分校有线用户  Gi0/1-20 |
| LoopBack 0 |  | 11.1.0.7/32 |  |
| AP3 | Gi0/1 |  | 10.1.0.50/30 |  |
| BVI20 |  | 195.1.20.254/24 | 分校无线用户 |