**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7）



目录

[任务描述 2](#_Toc10192)

[任务清单 3](#_Toc22432)

[（一）基础配置 3](#_Toc13910)

[（二）有线网络配置 3](#_Toc3183)

[（三）无线网络配置 5](#_Toc15718)

[（四）出口网络配置 6](#_Toc13034)

[附录1：拓扑图 8](#_Toc4758)

[附录2：地址规划表 9](#_Toc26264)

# 任务描述

位于北京的互联网平台电子商务集团火星公司，为提升企业的运营效率，不断改造和升级网络。计划新建总部园区服务网、北京分公司网络优化、新建杭州办事处网络、上海办事处网络优化……等等。集中改造集团公司的智慧网络，你做为火星公司网络工程师需要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拓扑图及附录2地址规划表，配置设备接口信息。

2.在网络设备上，均开启SSH服务端功能。其中，用户名和密码为admin、admin123。密码为明文类型。特权密码为admin1234。

3.交换设备上部署SNMP功能。配置所有设备SNMP消息，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.在交换机S1、S2的Gi0/1-Gi0/22端口启用端口保护。

3.在S1、S2连接PC机端口上开启Portfast和BPDUguard防护功能。

4.检测到环路后处理方式Shutdown-Port。

5.如果端口检测进入 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。

6.DHCP服务器搭建于EG1上，DHCP对外服务使用loopback 0地址。

7.在S1、S2交换机部署DHCP Snooping+DAI功能。其中，DAI功能主要针对VLAN10与VLAN20启用ARP防御，要求关闭S1/S2上联口的NFPP功能。

8.在S1、S2、S3、S4上配置MSTP防止二层环路。要求VLAN10、VLAN20数据流经过S3转发，S3失效时经过S4转发。VLAN50、VLAN60、VLAN100数据流经过S4转发，S4失效时经过S3转发。region-name为test。revision版本为1。S3作为实例1的主根、实例2的从根，S4作为实例2的主根、实例1的从根。其中，主根优先级为4096，从根优先级为8192。

9.在S3和S4交换机上配置VRRP，实现主机的网关冗余，所配置的参数要求见表1。在交换机S3、S4上配置的各VRRP组中，设置高优先级设置为150，低优先级设置为120，S3、S4的2条互联链路（Gi0/22、Gi0/23）上，配置二层链路聚合，采取LACP动态聚合模式。

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 |
| VLAN50 | 30 | 192.1.50.254 |
| VLAN60 | 40 | 192.1.60.254 |
| VLAN100 | 100 | 192.1.100.254 |

10.S6和S7间的Te0/49-50端口作为VSL链路网络设备虚拟化。其中S6为主，S7为备。S6和S7间的Gi0/47端口作为双主机检测链路，配置基于双主机检测，当VSL的所有物理链路都异常断开时，备机会切换成主机，从而保障网络正常。其中，主设备：Domain id：1。switch id:1。priority 150。 description: Switch-Virtual-Switch1。备设备：Domain id：1。switch id:2。priority 120。description: Switch-Virtual-Switch2。

11.各机构内网运行OSPF，配置VAC、S5、EG2之间运行OSPF，进程号10，规划单区域：区域0。R1、R2、R3之间运行OSPF，进程号20，规划单区域：区域0VSU、R2、R3之间运行OSPF，进程号21，规划单区域：区域0。S3、S4、EG1之间运行OSPF，进程号为30。

12.要求业务网段中不出现协议报文。R1、VSU始发的终端网段以及各设备上的Loopback管理地址，均以重分发直连路由的方式注入路由;R2/EG2、R3/EG1之间互联段，均以重发布直连的方式，注入R2、R3的OSPF双进程中，R2、R3之间启用OSPF与BFD联动，以达到迅速检测运营商网络中断，快速地切换到其他备份线路，提高用户网络体验。

13.优化OSPF相关配置，以尽量加快OSPF收敛。配置重发布路由进OSPF中使用类型1。

14.分支机构之间，部署IPV6网络，实现机构之间的内网中安装的IPV6终端，可通过无状态自动从网关处获取地址。其中，IPV6地址规划如表2。

表2 PV6地址规划表

|  |  |  |
| --- | --- | --- |
| 设备 | 接口 | IPV6地址 |
| R1 | VLAN10 | 2001:194:1:10::254/64 |
| VLAN20 | 2001:194:1:20::254/64 |
| Tunnel0 | 2001:11:1:3::1/64 |
| VSU | VLAN10 | 2001:195:1:10::254/64 |
| VLAN20 | 2001:195:1:20::254/64 |
| Tunnel0 | 2001:11:1:3::2/64 |

# （三）无线网络配置

北京互联网平台电子商务集团火星公司办公区无线项目拟投入12万元（网络设备采购部分），项目公共办公区人数大概在20人左右。平面布局如图1所示。

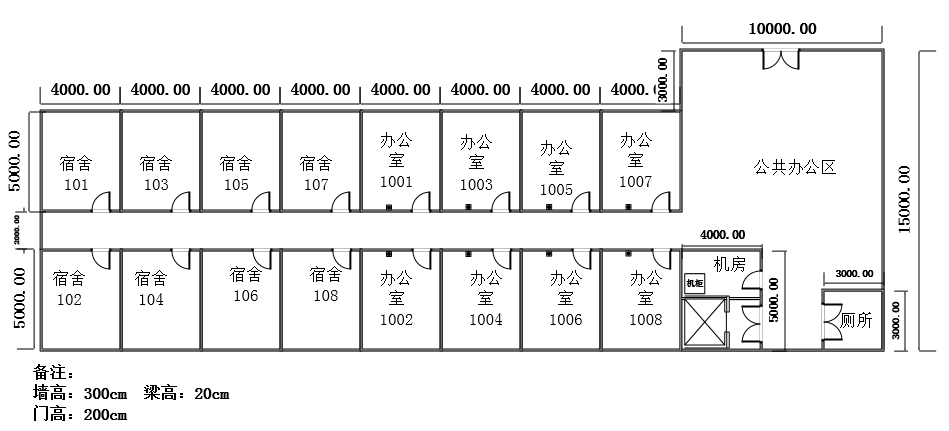


图1 平面布局图

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，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.分公司的无线网络规划中，使用EG1作为无线用户和无线FIT AP的DHCP服务器。分公司内网SSID为admin\_Fit\_XX(备注：XX现场提供)。WLANID为1。AP-Group为admin。配置内网中的无线用户在关联SSID后，即可自动获取VLAN60地址

5.配置两台AC设备，使用虚拟化方案的VAC技术，组合成1台虚拟AC。

6.AC1和AC2之间的Gi0/4-5端口作为VSL链路。其中：配置AC1为主，AC2为备。

7.AC1和AC2间的Gi0/3端口，作为双主机检测链路，配置基于双主机检测。当VSL的所有物理链路都异常断开时，备机会切换成主机，从而保障网络正常。其中，主设备为：Domain id：1。device id:1。priority 150。 description: AC-1。备设备为：Domain id：1。device id:2。priority 120。 description: AC-2。

8.在VAC与S5之间的业务线缆都规划为双线路。为提升冗余性，采用三层链路聚合。

9.AP3使用胖模式进行部署，以透明模式进行部署，管理地址为192.1.100.3/24(备注：XX现场提供)。在无线AP3上创建SSID(WLAN-ID 2)，相关参赛为：admin-Fat\_XX(备注：XX现场提供) 。其中，内网无线用户关联SSID后，可自动获取VLAN60网段地址。

10.无线用户接入无线网络时，连接Fit AP无线用户接入无线网络时采用WPA2加密方式，加密密码为XX。Fat AP部署的无线网络中，无线用户接入无线网络时采用WEB认证方式，认证用户名、密码为XX。

# （四）出口网络配置

1.出口网关上进行NAT配置，实现机构内网终端及服务器，均可访问互联网，通过NAPT方式将内网IP地址转换到互联网接口上。

2.出口网关EG1上配置，使S1交换机（192.1.100.1,其中：XX现场提供）设备的Telnet服务，可以通过互联网被访问。此外，将其地址映射至运营商线路上，映射地址为11.1.2.10，映射端口23333。

3.EG1设备，上启用Web Portal认证服务，认证用户名密码均为user1、user2。有线用户需进行WEB认证访问互联网无线用户不需在EG上进行WEB认证即可访问互联网。

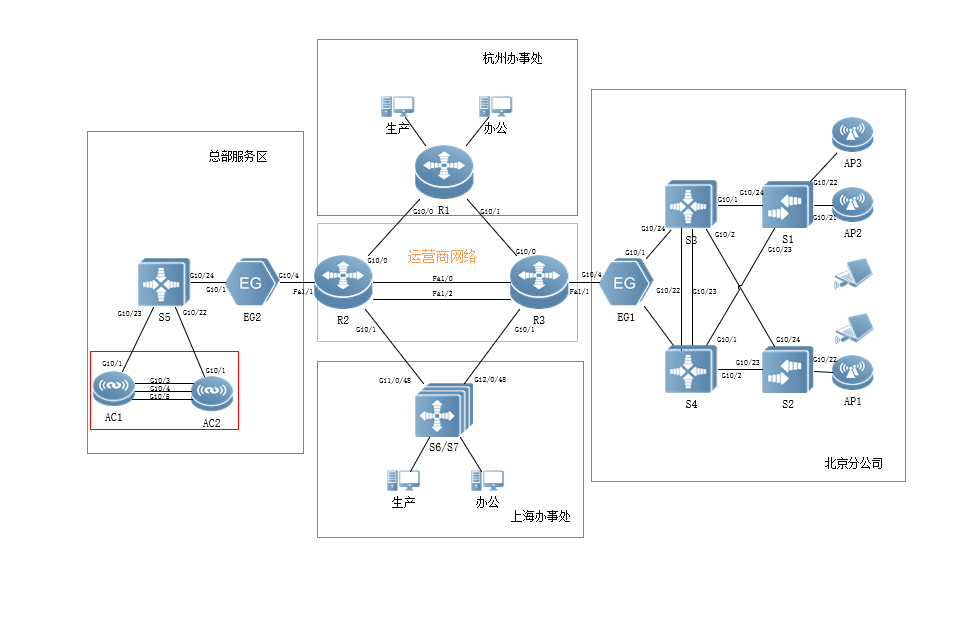
4.使用IPSec对本部到各分部的数据流进行加密。要求使用动态隧道主模式，安全协议采用esp协议，加密算法采用3des，认证算法采用md5，以IKE方式建立IPsec SA。在R1上配置ipsec加密转换集名称为myset。动态ipsec加密图名称为dymymap。预共享密钥为明文123456。静态的ipsec加密图mymap。

5.出口网关EG1上，针对内网访问互联网WEB流量限速每IP 1000Kbps，内网WEB总流量不超过20Mbps，通道名称定义为WEB。

1. 在EG1与EG2出口网关之间，启用GRE Over IPSec VPN嵌套功能。创建GRE隧道，实现内部承载OSPF协议，使其总分机构间内网连通。

7.配置IPSec安全使用静态点对点模式，要求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admin。DH使用组2。此外，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。

# 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 | Production | Gi0/1至Gi0/10 | 生产网 |
| VLAN20 | Office | Gi0/11至Gi0/20 | 办公网 |
| VLAN50 | APManage | Gi0/21至Gi0/22 | 无线AP管理 |
| VLAN60 | Wireless | \ | 无线终端 |
| VLAN100 | Manage | 192.1.100.1/24 | 设备远程管理 |
| S2 | VLAN10 | Production | Gi0/1至Gi0/10 | 生产网 |
| VLAN20 | Office | Gi0/11至Gi0/20 | 办公网 |
| VLAN50 | APManage | Gi0/21至Gi0/22 | 无线AP管理 |
| VLAN60 | Wireless | \ | 无线终端 |
| VLAN100 | Manage | 192.1.100.2/24 | 设备远程管理 |
| AP3 | BVI 100 | Manage | 192.1.100.3/24 | 设备远程管理 |
| S3 | VLAN10 | Production | 192.1.10.253/24 | 生产网 |
| VLAN20 | Office | 192.1.20.253/24 | 办公网 |
| VLAN50 | APManage | 192.1.50.253/24 | 无线AP管理 |
| VLAN60 | Wireless | 192.1.60.253/24 | 无线终端 |
| VLAN100 | Manage | 192.1.100.253/24 | 设备远程管理 |
| Gi0/24 | \ | 10.1.1.2/30 | \ |
| LoopBack 0 | \ | 10.1.0.3/32 | \ |
| S4 | VLAN10 | Production | 192.1.10.252/24 | 生产网 |
| VLAN20 | Office | 192.1.20.252/24 | 办公网 |
| VLAN50 | APManage | 192.1.50.252/24 | 无线AP管理 |
| VLAN60 | Wireless | 192.1.60.252/24 | 无线终端 |
| VLAN100 | Manage | 192.1.100.252/24 | 设备远程管理 |
| Gi0/24 | \ | 10.1.1.6/30 | \ |
| LoopBack 0 | \ | 10.1.0.4/32 | \ |
| EG1 | Gi0/1 | \ | 10.1.1.1/30 | \ |
| Gi0/2 | \ | 10.1.1.5/30 | \ |
| Gi0/4 | \ | 11.1.2.10/30 | \ |
| Tunnel 0 | \ | 11.1.5.2/30 | \ |
| LoopBack 0 | \ | 10.1.0.1/32 | \ |
| VAC | Gi1/0/1 | \ | 10.2.1.6/30 | AG1成员口 |
| Gi2/0/1 | \ | AG1成员口 |
| LoopBack 0 | \ | 10.2.0.12/32 | \ |
| S5 | Gi0/21 | \ | 193.1.0.1/30 | 云平台 |
| Gi0/22 | \ | 10.2.1.5/30 | AG1成员口 |
| Gi0/23 | \ | AG1成员口 |
| Gi0/24 | \ | 10.2.1.2/30 | \ |
| LoopBack 0 | \ | 10.2.0.5/32 | \ |
| EG2 | Gi0/1 | \ | 10.2.1.1/30 | \ |
| Gi0/4 | \ | 11.1.1.10/30 | \ |
| Tunnel 0 | \ | 11.1.5.1/30 | \ |
| LoopBack 0 | \ | 10.2.0.2/32 | \ |
| R1 | VLAN10 | Production | 194.1.10.254/24 | Gi1/1-Gi1/10 |
| VLAN20 | Office | 194.1.20.254/24 | Gi1/11-Gi1/20 |
| Gi0/0 | \ | 11.1.1.1/30 | \ |
| Gi0/1 | \ | 11.1.2.1/30 | \ |
| LoopBack 0 | \ | 11.1.0.1/32 | \ |
| R2 | VLAN10 | Con-R3-OSPF20 | 11.1.3.1/30 | 成员口Fa1/0 |
| VLAN20 | Con-EG2 | 11.1.1.9/30 | 成员口Fa1/1 |
| VLAN30 | Con-R3-OSPF21 | 11.1.4.1/30 | 成员口Fa1/2 |
| Gi0/0 | \ | 11.1.1.2/30 | \ |
| Gi0/1 | \ | 11.1.1.5/30 | \ |
| LoopBack 0 | NA | 11.1.0.2/32 | OSPF20进程 |
| LoopBack 10 | NA | 11.1.0.22/32 | OSPF21进程 |
| R3 | VLAN10 | Con-R2-OSPF20 | 11.1.3.2/30 | 成员口Fa1/0 |
| VLAN20 | Con-EG1 | 11.1.2.9/30 | 成员口Fa1/1 |
| VLAN30 | Con-R2-OSPF21 | 11.1.4.2/30 | 成员口Fa1/2 |
| Gi0/0 | \ | 11.1.2.2/30 | \ |
| Gi0/1 | \ | 11.1.2.5/30 | \ |
| LoopBack 0 | \ | 11.1.0.3/32 | OSPF20进程 |
| LoopBack 10 | \ | 11.1.0.33/32 | OSPF21进程 |
| VSU | VLAN10 | Production | 195.1.10.254/24 | Gi1/0/1-Gi1/0/40 |
| VLAN20 | Office | 195.1.20.254/24 | Gi2/0/1-Gi2/0/40 |
| Gi1/0/48 | \ | 11.1.1.6/30 | \ |
| Gi2/0/48 | \ | 11.1.2.6/30 | \ |
| LoopBack 0 | \ | 11.1.0.67/32 | \ |