**“2018年江苏省职业院校技能大赛”高职组**

**计算机网络应用竞赛**

**竞赛样题**

赛题说明

# 一、竞赛内容分布

模块一：设备基础信息配置（15%）

模块二：网络搭建与网络冗余备份方案部署（20%）

模块三：移动互联网搭建与网优（20%）

模块四：出口安全防护与远程接入（20%）

模块五：云计算服务搭建与企业应用（20%）

模块六：赛场规范和文档规范（5%）

# 二、竞赛时间

竞赛时间为180分钟。

# 三、竞赛注意事项

1. 竞赛所需的硬件、软件和辅助工具由组委会统一布置，选手不得私自携带任何软件、移动存储、辅助工具、移动通信等进入赛场。

2. 请根据大赛所提供的比赛环境，检查所列的硬件设备、软件清单、材料清单是否齐全，计算机设备是否能正常使用。

3. 操作过程中，需要及时保存设备配置。比赛结束后，所有设备保持运行状态，不要拆动硬件连接。

4. 比赛完成后，比赛设备、软件和赛题请保留在座位上，禁止将比赛所用的所有物品（包括试卷和草纸）带离赛场。

5. 裁判以各参赛队提交的竞赛结果文档为主要评分依据。所有提交的文档必须按照赛题所规定的命名规则命名，不得以任何形式体现参赛院校、工位号等信息。

# 四、竞赛结果文件的提交

按照题目要求，提交符合模板的WORD文件和设备配置文件。

# 第一部分：网络规划与实施

**注意事项**

* 赛场提供一组云平台环境，已经安装好VMware WorkStation 12虚拟机系统并导入虚拟机模板镜像（Windows Server 2008 R2及CentOS 7.0）。
* 自行部署安装Windows操作系统的管理员administrator和CentOS的root的密码都是JsjWL\_2018。
* 考生在PC机上通过SecureCRT软件配置网络设备，软件已经安装在电脑中。
* 竞赛结果文件的制作请参考U盘“答题卡”文件夹中的 “交换路由无线网关设备配置答题卡.docx”、“云平台服务器配置答题卡.docx”。请注意排版，文档排版得分将计入总成绩。

**设备及文档列表**

本竞赛中所使用的网络设备及线缆如下表所示：

表1-1 设备及线缆列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **类别** | **设备** | **厂商** | **型号** | **数量** |
| 1 | 硬件 | 出口网关 | 锐捷 | RG-EG2000 | 2台 |
| 2 | 硬件 | 路由器 | 锐捷 | RG-RSR20-14E（LAB） | 3台 |
| 3 | 硬件 | 串口接口模块 | 锐捷 | RG-SIC-1HS | 6个 |
| 4 | 硬件 | 串口线缆 | 锐捷 | CAB-V.35DTE-V.35DCE | 3条 |
| 5 | 硬件 | 数据中心交换机 | 锐捷 | RG-S6000C-48GT4XS-E | 2台 |
| 6 | 硬件 | 电源模块 | 锐捷 | RG-PA70I | 2台 |
| 7 | 硬件 | VSU堆叠电缆 | 锐捷 | XG-SFP-CU1M | 2条 |
| 8 | 硬件 | 三层交换机 | 锐捷 | RG-S5750-24GT4XS-L | 3台 |
| 9 | 硬件 | 二层接入交换机 | 锐捷 | RG-S2910-24GT4XS-E | 2台 |
| 10 | 硬件 | 无线控制器 | 锐捷 | RG-WS6008 | 2台 |
| 11 | 硬件 | 无线AP | 锐捷 | RG-AP520 | 3台 |
| 12 | 硬件 | 电源适配器 | 锐捷 | RG-E-120 | 3个 |

本竞赛中使用的设备参考资料如下表所示：

表1-2文档列表

|  |  |  |
| --- | --- | --- |
| **序号** | **名称** | **位置** |
| 1 | RG-RSR20-14系列由器配置手册.pdf | PC机桌面上的“竞赛资料\网络应用\参考文档” |
| 2 | RG-S5750系列交换机配置手册.pdf | PC机桌面上的“竞赛资料\网络应用\参考文档” |
| 3 | RG-S6000E系列交换机配置手册.pdf | PC机桌面上的“竞赛资料\网络应用\参考文档” |
| 4 | RG-S2910系列交换机配置手册.pdf | PC机桌面上的“竞赛资料\网络应用\参考文档” |
| 5 | RG-AC系列无线控制器配置手册.pdf | PC机桌面上的“竞赛资料\网络应用\参考文档” |
| 6 | RG-AP系列无线接入点配置手册.pdf | PC机桌面上的“竞赛资料\网络应用\参考文档” |
| 7 | RG-EG2000系列出口网关配置手册.pdf | PC机桌面上的“竞赛资料\网络应用\参考文档” |

赛题背景

CII网络公司业务不断发展壮大，在亚太地区建立了分部。为了更好地促进分部业务的发展以及与总部的交流，需要进行分部信息化建设。同时为了更好管理数据，提供服务，公司决定建立自己的小型数据中心及云计算服务平台，以达到快速、可靠交换数据，以及增强业务部署弹性的目的。同时考虑员工移动办公的需求在总部及所有分部有线网络的基础上建设无线网络，另外为员工访问互联网申请独立的运营商线路避免访问互联网数据过多影响正常业务数据的交互，同时针对访问互联网数据进行身份认证与信息审计确保用网安全。

## 模块一：设备基础信息配置

**1、设备命名规范和设备的基础信息**

* 根据总体规划内容，将所有的设备根据命名规则修订设备名称
* 依据设备的总体规划物理连接表，配置设备的接口描述信息

**2、密码恢复和软件版本统一**

* 将分部接入交换机和总部接入交换机S1和S7做密码恢复，新的密码设置为ruijie
* 总部和分部的接入交换机S1和S7软件版本统一
* 因为项目需求，为了满足一个新增的功能产商发布了无线AP的专属的软件版本，满足软件版本的一致性，请将总部和分布的无线AP统一版本至AP\_RGOS 11.1(5)B81P3。

**3、网络设备安全技术**

* 为路由器和无线控制器开启SSH服务端功能，用户名和密码为ruijie，密码为明文类型，特权密码为ruijie。
* 为交换机开启Telnet功能，对所有Telnet用户采用本地认证的方式。创建本地用户，设定用户名和密码为ruijie，密码为明文类型，特权密码为ruijie。
* 配置所有设备SNMP消息，版本采用V2C，读写的Community为“ruijie”，只读的Community为“public”，开启Trap消息。

## 模块二：网络搭建与网络冗余备份方案部署

CII网络公司总部设有研发、市场、供应链、售后等4个部门，统一进行IP地址及业务资源的规划和分配。公司总部及亚太地区的网络拓扑结构如图1-2所示。

其中两台S6000交换机编号为S4、S5，用于服务器高速接入；两台S5750编号为S2、S3，作为总部的核心交换机；两台RSR20路由器编号为R2、R3，作为总部的核心路由器，一台EG2000编号为EG1，作为总部互联网出口网关1。一台S2910编号为S1，作为总部接入交换机；一台RSR20路由器编号为R1，作为分支机构路由器，一台EG2000编号为EG2，作为分部互联网出口网关2。一台S5750编号为S6作为分部核心交换机，一台S2910编号为S7，作为分部接入交换机。3台AP520编号为AP1，AP2，AP3分别作为总部与分部的无线接入点。



图1-2网络拓扑结构图

请根据拓扑图及网络物理连接表完成设备的连线。

设备互联规范主要对各种网络设备的互联进行规范定义，在项目实施中，如用户无特殊要求，应根据规范要求进行各级网络设备的互联，统一现场设备互联界面，结合规范的线缆标签使用，使网络结构清晰明了，方便后续的维护。如下“表1-8 网络物理连接表”。

表1-8网络物理连接表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 源设备  名称 | 设备接口 | 接口描述 | 目标设备名称 | 设备接口 |
| S1 | Gi0/1 | Con\_To\_PC1 | PC1 |  |
| S1 | Gi0/5 | Con\_To\_PC2 | PC2 |  |
| S1 | Gi0/21 | Con\_To\_AP1 | AP1 |  |
| S1 | Gi0/22 | Con\_To\_AP2 | AP2 |  |
| S1 | Gi0/23 | Con\_To\_S2\_Gi0/1 | S2 | Gi0/1 |
| S1 | Gi0/24 | Con\_To\_S3\_Gi0/1 | S3 | Gi0/1 |
| S2 | Gi0/1 | Con\_To\_S1\_Gi0/23 | S1 | Gi0/23 |
| S2 | Gi0/2 | Con\_To\_S3\_Gi0/2 | S3 | Gi0/2 |
| S2 | Gi0/3 | Con\_To\_S3\_Gi0/3 | S3 | Gi0/3 |
| S2 | Gi0/4 | Con\_To\_R2\_Gi0/0 | R2 | Gi0/0 |
| S2 | Gi0/5 | Con\_To\_AC1\_Gi0/1 | AC1 | Gi0/1 |
| S3 | Gi0/1 | Con\_To\_S1\_Gi0/24 | S1 | Gi0/24 |
| S3 | Gi0/2 | Con\_To\_S2\_Gi0/2 | S2 | Gi0/2 |
| S3 | Gi0/3 | Con\_To\_S2\_Gi0/3 | S2 | Gi0/3 |
| S3 | Gi0/4 | Con\_To\_R3\_Gi0/0 | R3 | Gi0/0 |
| S3 | Gi0/5 | Con\_To\_AC2\_Gi0/1 | AC2 | Gi0/1 |
| R2 | FA1/1 | Con\_To\_S4\_Gi0/1 | S4 | Gi0/1 |
| R2 | Gi0/0 | Con\_To\_S2\_Gi0/4 | S2 | Gi0/4 |
| R2 | Gi0/1 | Con\_To\_EG1\_Gi0/0 | EG1 | Gi0/0 |
| R2 | S2/0 | Con\_To\_R1\_S2/0 | R1 | S2/0 |
| R2 | S3/0 | Con\_To\_R3\_S3/0 | R3 | S3/0 |
| R3 | FA1/1 | Con\_To\_S5\_Gi0/1 | S5 | Gi0/1 |
| R3 | Gi0/0 | Con\_To\_S3\_Gi0/4 | S3 | Gi0/4 |
| R3 | Gi0/1 | Con\_To\_EG1\_Gi0/1 | EG1 | Gi0/1 |
| R3 | S2/0 | Con\_To\_R1\_S3/0 | R1 | S3/0 |
| R3 | S3/0 | Con\_To\_R2\_S3/0 | R2 | S3/0 |
| S4 | Gi0/1 | Con\_To\_R2\_FA1/1 | R2 | FA1/1 |
| S4 | Gi0/2 | Con\_To\_S5\_Gi0/2 | S5 | Gi0/2 |
| S4 | Gi0/5 | Con\_To\_Cloud\_M | 云平台(主用) |  |
| S4 | Te0/49 |  | S5 | Te0/49 |
| S4 | Te0/50 |  | S5 | Te0/50 |
| S5 | Gi0/1 | Con\_To\_R3\_FA1/1 | R3 | FA1/1 |
| S5 | Gi0/2 | Con\_To\_S4\_Gi0/2 | S4 | Gi0/2 |
| S5 | Gi0/5 | Con\_To\_Cloud\_B | 云平台（备用） |  |
| S5 | Te0/49 |  | S4 | Te0/49 |
| S5 | Te0/50 |  | S4 | Te0/50 |
| R1 | S2/0 | Con\_To\_R2\_S2/0 | R2 | S2/0 |
| R1 | S3/0 | Con\_To\_R3\_S2/0 | R3 | S2/0 |
| R1 | Gi0/0 | Con\_To\_S6\_Gi0/1 | S6 | Gi0/1 |
| R1 | Gi0/1 | Con\_To\_EG2\_Gi0/0 | EG2 | Gi0/0 |
| S6 | Gi0/1 | Con\_To\_R1\_Gi0/0 | R1 | Gi0/0 |
| S6 | Gi0/2 | Con\_To\_AP3\_Gi0/0 | AP3 | Gi0/0 |
| S6 | Gi0/3 | Con\_To\_S7\_Gi0/24 | S7 | Gi0/24 |
| S7 | Gi0/1 | Con\_To\_PC3 | PC3 |  |
| S7 | Gi0/24 | Con\_To\_S6\_Gi0/3 | S6 | Gi0/3 |
| EG1 | GI0/0 | Con\_To\_R2\_Gi0/1 | R2 | Gi0/1 |
| EG1 | GI0/1 | Con\_To\_R3\_Gi0/1 | R3 | Gi0/1 |
| EG1 | GI0/2 | Con\_To\_EG2\_Gi0/2 | EG2 | GI0/2 |
| EG2 | GI0/0 | Con\_To\_R1\_Gi0/1 | R1 | Gi0/1 |
| EG2 | GI0/2 | Con\_To\_EG1\_Gi0/2 | EG1 | GI0/2 |

公司有4个不同业务部门和分部，彼此间需要互联互通，同时也需要对某些业务进行互访限制。另外，各业务对网络可靠性要求较高，要求网络核心区域发生故障时的中断时间尽可能短。还有，网络部署时要考虑到网络的可管理性，并合理利用网络资源。

1. **虚拟局域网及IPv4地址部署**

为了减少广播，需要规划并配置VLAN。具体要求如下：

* 配置合理，Trunk链路上不允许不必要VLAN的数据流通过。
* 为节省IP资源，隔离广播风暴、病毒攻击，控制端口二层互访，在分部S6、S7交换机使用Private Vlan。
* 为隔离网络中部分终端用户间的二层互访，在交换机S1上使用端口保护。

根据上述信息及表1-9、表1-10，在各设备上完成VLAN配置和端口分配以及IPv4地址。

表1-9网络设备名称表

|  |  |
| --- | --- |
| 拓扑图中设备名称 | 配置主机名（hostname名） |
| S1 | ZB-S2910-01 |
| S2 | ZB-S5750-01 |
| S3 | ZB-S5750-02 |
| S4 | ZB-VSU-S6000 |
| S5 | ZB-VSU-S6000 |
| S6 | FB-S5750-01 |
| S7 | FB-2910-01 |
| R1 | FB-RSR20-01 |
| R2 | ZB-RSR20-01 |
| R3 | ZB-RSR20-02 |
| AC1 | ZB-WS6008-01 |
| AC2 | ZB-WS6008-02 |
| EG1 | ZB-EG2000-01 |
| EG2 | FB-EG2000-01 |
| AP1 | ZB-AP520-01 |
| AP2 | ZB-AP520-02 |
| AP3 | FB-AP520-01 |

表1-10 IPv4地址分配表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口或VLAN | VLAN名称 | 二层或三层规划**(XX代表工位号)** | 说明 |
| S1 | VLAN10 | Res | Gi0/1至Gi0/4 | 研发 |
| VLAN20 | Sales | Gi0/5至Gi0/8 | 市场 |
| VLAN30 | Supply | Gi0/9至Gi0/12 | 供应链 |
| VLAN40 | Service | Gi0/13至Gi0/16 | 售后 |
| VLAN50 | AP | Gi0/21至Gi0/22 | 无线AP |
| VLAN100 | Manage | 192.XX.100.4/24 | 设备管理VLAN |
| S2 | VLAN10 | Res | 192.XX.10.252/24 | 研发 |
| VLAN20 | Sales | 192.XX.20.252/24 | 市场 |
| VLAN30 | Supply | 192.XX.30.252/24 | 供应链 |
| VLAN40 | Service | 192.XX.40.252/24 | 售后 |
| VLAN50 | AP | 192.XX.50.252/24 | 无线AP |
| VLAN100 | Manage | 192.XX.100.252/24 | 设备管理VLAN |
| Gi0/4 |  | 10.XX.0.1/30 |  |
| Gi0/5 |  | TRUNK | 互联AC |
| LoopBack 0 |  | 11.XX.0.202/32 |  |
| S3 | VLAN10 | Res | 192.XX.10.253/24 | 研发 |
| VLAN20 | Sales | 192.XX.20.253/24 | 市场 |
| VLAN30 | Supply | 192.XX.30.253/24 | 供应链 |
| VLAN40 | Service | 192.XX.40.253/24 | 售后 |
| VLAN50 | AP | 192.XX.50.253/24 | 无线AP |
| VLAN100 | Manage | 192.XX.100.253/24 | 设备管理VLAN |
| Gi0/4 |  | 10.XX.0.5/30 |  |
| Gi0/5 |  | TRUNK | 互联AC |
| LoopBack 0 |  | 11.XX.0.203/32 |  |
| AC1 | LoopBack 0 |  | 11.XX.0.204/32 |  |
| VLAN60 | Wiressless | 192.XX.60.252/24 | 无线用户 |
| Vlan100 | Manage | 192.XX.100.2/24 | 管理与互联VLAN |
| AC2 | LoopBack 0 |  | 11.XX.0.205/32 |  |
| VLAN60 | Wiressless | 192.XX.60.253/24 | 无线用户 |
| Vlan100 | Manage | 192.XX.100.3/24 | 管理与互联VLAN |
| S4 | VLAN100 | Con\_To\_Cloud | 193.XX.0.1/30 | 互联云平台 |
| Gi0/1 |  | 10.XX.0.9/30 |  |
| LoopBack 0 |  | 11.XX.0.45/32 |  |
| S5 | VLAN100 | Con\_To\_Cloud | 193.XX.0.1/30 | 互联云平台(备用) |
| Gi0/1 |  | 10.XX.0.13/30 |  |
| LoopBack 0 |  | 11.XX.0.45/32 |  |
| EG1 | GI0/2 |  | 195.XX.0.1/24 | 与EG2互联 |
| GI0/0 |  | 10.XX.0.34/30 |  |
| GI0/1 |  | 10.XX.0.38/30 |  |
| LoopBack 0 |  | 11.XX.0.11/32 |  |
| EG2 | GI0/2 |  | 195.XX.0.2/24 | 与EG1互联 |
| GI0/0 |  | 10.XX.0.42/30 |  |
| LoopBack 0 |  | 11.XX.0.12/32 |  |
| R1 | S2/0 |  | 10.XX.0.17/30 |  |
| S3/0 |  | 10.XX.0.21/30 |  |
| Gi0/0 |  | 10.XX.0.25/30 |  |
| Gi0/1 |  | 10.XX.0.41/30 |  |
| LoopBack 0 |  | 11.XX.0.1/32 |  |
| R2 | Gi0/0 |  | 10.XX.0.2/30 |  |
| FA1/1(vlan100) |  | 10.XX.0.10/30 | SVI接口互联 |
| Gi0/1 |  | 10.XX.0.33/30 |  |
| S2/0 |  | 10.XX.0.18/30 |  |
| S3/0 |  | 10.XX.0.29/30 |  |
| LoopBack 0 |  | 11.XX.0.2/32 |  |
| R3 | Gi0/0 |  | 10.XX.0.6/30 |  |
| FA1/1(vlan100) |  | 10.XX.0.14/30 | SVI接口互联 |
| Gi0/1 |  | 10.XX.0.37/30 |  |
| S2/0 |  | 10.XX.0.22/30 |  |
| S3/0 |  | 10.XX.0.30/30 |  |
| LoopBack 0 |  | 11.XX.0.3/32 |  |
| S6 | Gi0/1 |  | 10.XX.0.26/30 |  |
| VLAN10 | Pvlan | 194.XX.10.254/24 | 分部有线用户 |
| VLAN20 | Wireless\_user | 194.XX.20.254/24 | 分部无线用户 |
| VLAN30 | AP | 194.XX.30.254/24 | 分部无线AP |
| VLAN100 | Manage | 194.XX.100.254/24 | 设备管理VLAN |
| LoopBack 0 |  | 11.XX.0.6/32 |  |
| S7 | VLAN10 | Pvlan |  | Primaty vlan |
| VLAN11 | Community\_vlan | Gi0/1至Gi0/4 | community vlan |
| VLAN12 | Isolated\_vlan | Gi0/5至Gi0/8 | isolated vlan |
| VLAN100 | Manage | 194.XX.100.1/24 | 设备管理VLAN |
| PC机 | PC1 |  | 自动获取 |  |
| PC2 |  | 192.XX.20.2/24 |  |
| PC3 |  | 194.XX.10.2/24 |  |

1. **MSTP及VRRP部署**

在总部交换机S2、S3上配置MSTP防止二层环路；要求所有数据流经过S2转发，S2失效时经过S3转发。所配置的参数要求如下：

* region-name为ruijie；
* revision版本为1；
* 实例值为1；
* S2作为实例中的主根， S3作为实例中的从根。
* 在S2和S3上配置VRRP，实现主机的网关冗余。所配置的参数要求如表1-11。

表1-11 S2和S3的VRRP参数表

|  |  |  |
| --- | --- | --- |
| VLAN | VRRP备份组号（VRID） | VRRP虚拟IP |
| VLAN10 | 10 | 192.xx.10.254 |
| VLAN20 | 20 | 192.xx.20.254 |
| VLAN30 | 30 | 192.xx.30.254 |
| VLAN40 | 40 | 192.xx.40.254 |
| VLAN50 | 50 | 192.xx.50.254 |
| VLAN100(交换机间) | 100 | 192.xx.100.254 |

* S2作为所有主机的实际网关，S3作为所有主机的备份网关；其中各VRRP组中高优先级设置为150，低优先级设置为120。

1. **DHCP中继与安全**

在交换机S2、S3上配置DHCP中继，对VLAN10以内的用户进行中继，使得总部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R2上；
* 为了防止DHCP服务器欺骗及用户私设静态IP地址，在S1交换机部署DHCP Snooping功能。

1. **网络设备虚拟化**

两台核心交换机通过VSU虚拟化为一台设备进行管理，从而实现高可靠性。当任意交换机或板卡故障时，都能保障能够实现设备、链路切换，保护客户业务。

* 规划S4和S5间的Te0/49-50端口作为VSL链路，使用VSU技术实现网络设备虚拟化。其中S4为主，S5为备；
* 规划S4和S5间的Gi0/2端口作为双主机检测链路，配置基于BFD的双主机检，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；
* 主设备：Domain id：1,switch id:1,priority 200；
* 备设备：Domain id：1,switch id:2,priority 150；

1. **路由协议部署**

因历史原因，总部使用静态路由、OSPF多协议组网。其中S2、S3、S4、S5、R2、R3使用OSPF协议，R2、R3与总部出口网关及分部R1间使用静态路由协议，分部使用静态路由协议。要求网络具有安全性、稳定性。具体要求如下：

* OSPF进程号为10，规划多区域0（S2、S3、R2、R3）、区域1（S4、S5、R2、R3）；
* R2、R3互联链路规划入区域0；
* 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；
* 采用浮动静态路由，主静态路由优先级为10，备份静态路由优先级为100。

注意：(S4/S5需要重发布云平台（172.16.0.0/22）静态路由至总部内网)。

1. **广域网链路配置与安全部署**

总部路由器与分部路由器间属于广域网链路，其中R1-R2间所租用线路带宽为2M，R1-R3间所租用线路带宽为1M。R2-R3间线路带宽为2M。总部路由器与分部路由器间属于广域网链路。需要使用PPP进行安全保护。PPP的具体要求如下：

* 使用CHAP协议；
* 单向认证，用户名+验证口令方式，R1为认证客户端，R2、R3为认证服务端；
* 用户名和密码均为**ruijie。**

1. **路由选路部署**

考虑到从分部到总部有两条广域网线路，且其带宽不一样。所以规划R1-R2间为主线路，R1-R3间为备线路。另外总部局域网到互联网数据，经规划R2-EG1为主线路，R3-EG1为备线路。根据以上需求，在路由器上进行合理的路由协议配置。具体要求如下：

* 修改链路或接口开销COST值，且其值必须为5或10；
* 总部用户区与互联网互通主路径规划为：S1-S2-R2-EG1;
* 总部与分部互通主路径为：S1-S2-R2-R1或（S4/S5）-R2-R1；
* 主链路故障可无缝切换到备用链路上；
* 要求来回数据流一致。

1. **PBR配置与部署**

考虑到分部到总部间有2条广域网线路，为合理利用带宽，规划从分部去往总部的SSH数据通过R1-R2的线路转发，从分部去往总部的WEB数据通过R1-R3的线路转发。为达到上述目的，采用PBR来实现。具体要求如下：

* Route-map策略名为fenliu；
* 分部去往总部的SSH数据由ACL101来定义；
* 分部去往总部的WEB数据由ACL102来定义。

1. **QoS部署**

为了防止大量用户不断突发的数据导致网络拥挤，必须对接入的用户流量加以限制。所配置的参数要求如下

* 总部设备S1的Gi0/1至Gi0/16接口处方向设置接口限速，限速10M/S；
* 分部设备R1做流量监管，G0/0接口对接收的报文进行流量控制，下行报文流量不能超过1Mbps，如果超过流量限制则将违规报文丢弃。

## 模块三：移动互联网搭建与网优

为满足“互联网+”时代下，员工移动办公的发展趋势，公司总部与分部均需要规划和部署移动互联无线网络，同时为保证无线用户安全、可靠的访问互联网，我们需要进行无线网络安全及性能优化配置，确保员工有良好的上网体验。

1. **无线网络基础部署**

* 使用AC为总部无线用户DHCP 服务器，使用（S2/S3）为总部AP的DHCP 服务器,S2分配地址范围为其网段的1至100，S3分配地址为其网段的101至200。使用S6为分部无线用户与AP DHCP服务器，为其终端自动分配地址；
* 创建总部 SSID 为 Ruijie-ZB\_XX(XX代表工位号)，AP-Group为ZB，总部无线用户关联SSID后可自动获取地址；
* 创建分部 SSID 为 Ruijie-FB\_XX(XX代表工位号)，AP-Group为FB,分部无线用户关联SSID后可自动获取地址；
* 调整信道使得总部AP间信道不冲突。

1. **AC热备部署**

* 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。

1. **无线安全部署**

具体配置参数如下：

* 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)；
* 为避免无线网络被非法用户通过SSID搜索到，并建立非法连接，需要禁用AP广播SSID，隐藏无线SSID；

1. **无线性能优化**

* 关闭低速率（1M,6M）应用接入；
* 设备总部无线用户启用集中转发模式，各分公司无线用户启用本地转发模式。

## 模块四：出口安全防护与远程接入

公司总部与分部无线用户需要通过独立的互联网线路访问外网资源，同时针对访问资源进行用户身份认证与信息审计监督，另外满足出差在外的员工可以访问总部内部服务器资源，需针对出口用户提供远程VPN功能。

1. **出口NAT部署**

具体配置参数如下：

* 总部与分部出口网关上配置访问控制列表ACL 110，仅允许无线用户与研发部门在周一到周五的上班时间通过NAPT访问互联网，NAPT映射到互联网接口上；
* 在总部EG上配置，使公司总部核心交换R2（11.XX.0.2）(XX代表工位号)设备的SSH服务可以通过互联网被访问，从互联网访问的地址是195.XX.0.20(XX代表工位号)。

1. **Web Portal用户认证部署**

* 在总部网关上启用Web Portal认证服务，并创建user1、user2;
* 设置免认证资源<http://195.XX.0.20>(XX代表工位号)。

1. **应用流量控制部署**

* 针对访问外网FTP流量限速每用户5000Kbps，内网ftp总流量不超过100M。

1. **用户行为策略部署**

* 禁止总部内网用户通过浏览器访问http://195.XX.0.2(XX代表工位号);
* 禁止总部内网用户下载后缀是.mp3类型的文件；
* 内网user1、user2访问互联网资源免审计。

1. **VPN部署**

* 分部R1至R2、R3两条专线均发生故障时确保分部可正常访问总部服务器区，要求在总部与分部EG上启用IPSEC VPN建立IPSEC隧道，实现总部与分部有线用户数据互通及加密处理。VPN需要采用隧道模式、预共享密码为 123456，加密认证方式为 ESP-DES、ESP-HASH-MD5 ，DH使用组1，与此同时总部关闭WEB认证功能。

1. **设备与网络管理部署**

* 为路由器开启SSH服务端功能，用户名和密码为admin，密码为明文类型；
* 为交换机开启Telnet功能，对所有Telnet用户采用本地认证的方式。创建本地用户，设定用户名和密码为admin，密码为明文类型。

提交竞赛结果文件（模块二、模块三、模块四）

制作竞赛结果文件：严格按照 “交换路由无线网关设备配置答题卡.docx”文档格式要求制作输出竞赛结果文件。

同时在每台设备上使用show running-config命令，将该命令下显示的结果分别保存到独立的TXT文件中，文件名以设备编号命名（S1、S2、S3、(S4/S5)、S6、S7、R1、R2、R3、AC1、AC2、EG1、EG2），并把所有的TXT文件存放在“设备配置”文件夹下。

考生将“交换路由无线网关设备配置答题卡.docx”以及“设备配置”文件夹保存到桌面上，并且拷贝到U盘上的“提交文档”目录下然后提交给现场工作人员。

*注意：考生在U盘中所提交的文件是竞赛结果的唯一依据，请考生一定确保文件确实有效，能够正常读取。如有疑问，可咨询现场工作人员。*

## 模块五：云计算服务搭建与企业应用

公司总部为了更好管理数据，提供服务，需要建立自己的小型数据中心及云计算服务平台，以达到快速、可靠交换数据，以及增强业务部署弹性的目的。

1. **云计算管理平台搭建**

根据在服务器上提供的VMware WorkStation 12虚拟化软件、Windows2008 R2和Centos7镜像安装操作系统，硬盘空间为50G，网络桥接模式。

1. **创建2台云主机，要求如下**

* 主机1：Window2008R2；CPU 2核；内存 4G；IP地址是193.XX.0.10/24网段，网关为193.XX.0.1/24；
* 主机2：Centos7.0；CPU 2核；内存 4G；IP地址是193.XX.0.20/24网段，网关为193.XX.0.1/24；
* 为主机1加载容量为20G的第二块硬盘，并分配盘符：D;
* 为主机2加载容量为10G的第二块硬盘，并设置开机自动挂载;

1. **应用部署**

* **Windows2008 R2系统配置**

1. 在Windows 2008 R2的DNS服务管理工具中添加四条主机记录，实现vpn.jnds.com，www.jnds.com，web.jnds.com，ftp.jnds.com域名的解析（解析至HTTP 服务虚机IP）。并用 nslookup 验证；
2. 建立反向简析区域完成vpn.jnds.com，www.jnds.com，web.jnds.com，ftp.jnds.com域名的反向解析，并用 nslookup 验证；
3. 配置安装 Windows server Backup 服务，新建备份计划备份路径为 c:\windows\system32\dns. 备份时间为每日13点和0点。备份到 目标卷 D；
4. 配置安全策略，使得用户在登陆错误尝试3次之后锁定，锁定时间为5分钟，锁定间隔为2分钟 并记录登陆错误信息。

* **CentOS系统配置**

1. 在CentOS系统中，利用赛场提供的CentOS镜像文件，配置本地yum源，然后完成httpd、mod\_ssl、vsftpd、软件包的安装；

Yum本地源请将光盘挂载到/mnt/cdrom目录下（目录需要自行创建）。

1. 配置http服务，建立一个web站点；
2. 使用www.jnds.com作为域名进行访问；
3. 网站根目录为/var/www/html；
4. Index.html内容使用Welcome to 2017 Computer Network Application contest!；
5. 配置https服务使原站点能使用https访问。
6. 设置SELINUX状态为Disabled；
7. 创建lvm物理卷；
8. 创建一个名为datastore的卷组，卷组的PE尺寸为16MB；
9. 逻辑卷的名称为database所属卷组为datastore，该逻辑卷由50个PE组成；
10. 将新建的逻辑卷格式化为XFS文件系统，要求在系统启动时能够自动挂在到/mnt/database目录。
11. FTP；
12. 拒绝匿名访问，只允许本地系统用户登录；
13. 所有用户主目录为/home/ftp 宿主为virtual用户；
14. 将用户使用文件的方式记录账号以及密码；
15. Ftpuser1用户只能下载不能上传以及删除文件重命名操作；
16. Ftpuser2可以下载与上传文件以及删除重命名操作；
17. Ftpadmin可以下载与上传文件以及删除重命名操作，并且权限为755；
18. 配置文件要求:

以下文件除了vsftpd.conf文件其余文件均需要自行创建

/etc/vsftpd/vsftpd.conf (ftp配置文件) /etc/pam.d/vsftpd.vu，（pam配置文件）  
/etc/vsftpd/user\_conf （该目录下ftp用户权限配置目录）

Ftpuser1，Ftpuser2，Ftpadmin 用户权限相关配置文件均在/etc/vsftpd/user\_conf 目录下。

1. 在CentOS主机中，配置基于WEB、FTP的firewall防火墙策略，实现服务的正常访问；
2. 创建一个归档备份,将/etc/sysconfig 目录打包备份至/home目录下文件名为sysconfig.tar.bz2。

提交竞赛结果文件（模块五）

制作竞赛结果文件：严格参照 “云平台服务器配置答题卡.docx”文档格式要求制作输出竞赛结果文件。

考生将“云平台服务器配置答题卡.docx”保存到桌面上，并且拷贝到U盘上的“提交文档”目录下然后提交给现场工作人员。

*注意：考生在U盘中所提交的文件是竞赛结果的唯一依据，请考生一定确保文件确实有效，能够正常读取。如有疑问，可咨询现场工作人员。*