2020年全国职业院校技能大赛改革试点赛

“网络系统管理”赛项

“网络构建”模块

（样卷3）



**全国职业院校技能大赛执委会.技术专家组**

**2020年9月**

目录

[一．说明 3](#_Toc51612391)

[二．项目背景 3](#_Toc51612392)

[三．项目规划和设计 4](#_Toc51612393)

[四．网络项目实施 13](#_Toc51612394)

[（一）网络设备基础信息配置与验证 13](#_Toc51612395)

[（二）网络搭建与网络冗余备份方案部署 14](#_Toc51612396)

[（三）移动互联网搭建与无线网络优化 20](#_Toc51612397)

[（四）实施出口安全防护与远程接入 22](#_Toc51612398)

[五．无线网络规划与实施 24](#_Toc51612399)

[（一）无线网络业务背景及需求介绍 24](#_Toc51612400)

[（二）无线网络中的业务规划 27](#_Toc51612401)

[六．竞赛结果文件提交说明 30](#_Toc51612402)

# 一．说明

本模块比赛时间为4小时。请合理分配竞赛时间。请仔细阅读以下要求。

1. 比赛时间结束时，请将工作站继续保持运行状态，评分过程需要在运行状态下进行。关机后不允许再重新启动。

2. 为了方便测试，全网允许ICMP流量通行，请允许操作系统中防火墙处于允许Ping的开放状态。

3．默认密码：XXXXXX。

4．软件&工具:见“2020年全国职业院校技能大赛改革试点赛赛项规程”。

# 二．项目背景

随着信息技术深入应用，网络技术朝着信息化、智慧化、虚拟化方向发展，人工智能、移动互联网、云计算等信息技术深刻影响着当前智慧校园网络布局。

西安泰和职业技术学院是陕西省的一所全日制专科学校，创建于1975年，目前，有以计算机网络为代表的13个专业。学校本部原有1栋行政楼、1栋教学楼、1个图书馆、5栋宿舍楼、1栋教工楼、2个食堂和1个体育馆。

近期新建成完成的1栋学院本部网络也将投入使用。同时，为了响应教育部新出台的产教融合政策，学校与当地知名的网络公司合作，在新校区建立了产融实训基地，为校企合作的发展迈出了重要的一步。

随着网络虚拟化、大数据、云计算和数据中心等热点技术的发展，学校今年又投资建了云数据中心，一期项目需要搭建机房骨干网络以及展示区网络。其中，云数据中心需要具备高速、可靠、安全的数据传输，以及高度集中计算和处理能力，为学院的可持续发展铸就雄厚软实力。

学校希望在本次的信息化业务建设方面，打通从招生、就业、学生管理、教学管理以及资源管理等多部门业务之间的连接环节，从而提升学校在各项信息化管理和运维能力，实现校园网管理和运维的标准化、智能化、高效化以及应对异常的能力。而以上每项业务的运维都对现有校园网络的稳健性、智慧性要求都带来挑战，不仅需要可靠稳定的基础网络支撑，更需要统一管理运维体系，保障其庞大的业务正常运营。

为了优化学院本部现有的网络，建设学院的产融实训基地与云数据中心网络，学院同时还针对学校的核心机房、学院本部网络、产融基地、云数据中心的现有网络进行升级、改造和优化。

需要在学院的网络中部署网络安全整体解决方案，改变之前上网行为管理难的问题，实现师生访问网络事后可溯源；校本部与产融基地、云数据中心之间传输的数据实现加密等多项安全问题。构建安全高效的网络出口，依托互联网最大限度实现各业务安全、高效、快速的传输，创建新时代园区网络环境，保障学校各项业务的高效运营。

# 三．项目规划和设计

为了顺利实施西安泰和职业技术学院网络改造，优化学院网络环境，为学院网络提供保障服务，需要对学院网络升级、改造和优化。

**1. 项目规划与建设内容**

主要实施的网络信息化项目规划与建设内容如下所示。

（1）校本部的校园网建立双核心网络架构，学院本部网络采用双汇聚、双接入的方式，以保证网络的冗余性，增强网络稳健性。

（2）校本部的采用双出口网络架构，其中一条出口保证师生访问互联网需求；另一条出口保证访问产融实训基地和云数据中心。

（3）实现网络虚拟化，实现校本部、产融实训基地和云数据中心的AP，全部关联到云数据中心的VAC上。

（4）校本部、产融实训基地和云数据中心之间运行VPN，使学院的各个部门网络通过公网通信时，更加安全可靠。

**2. 项目规划与建设拓扑**

西安泰和职业技术学院网络改造和建设拓扑如图1所示。

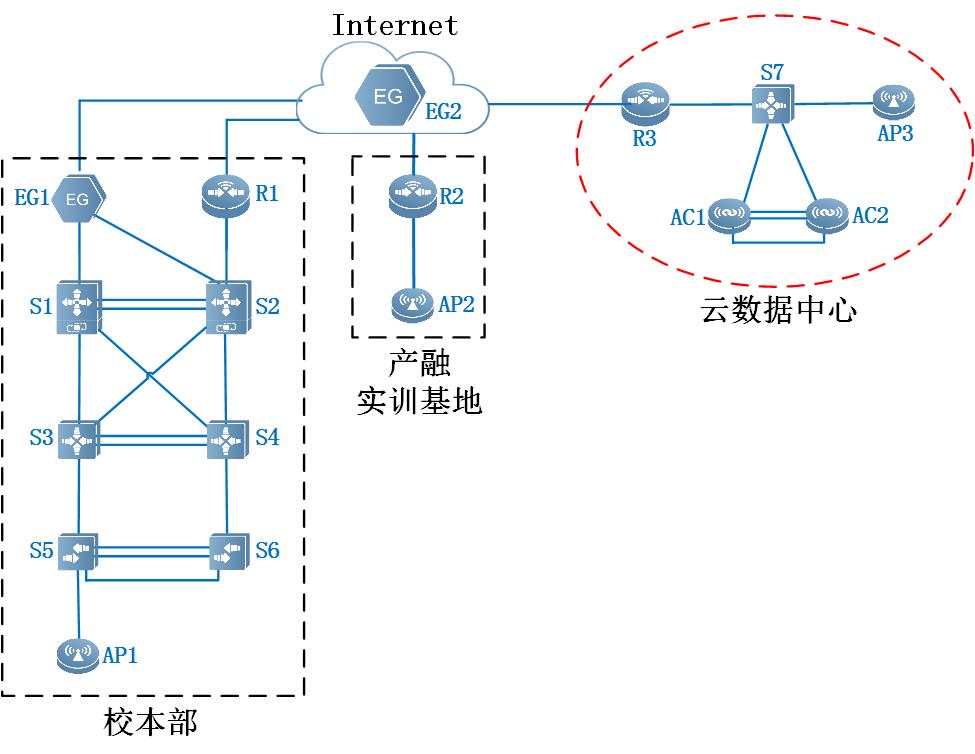


图1 西安泰和职业技术学院网络改造拓扑

**3. 项目规划与建设拓扑**

西安泰和职业技术学院的校园网络改造拓扑相关说明如下。

（1）使用两台数据中心交换机作为校本部网络中的核心交换机，在网络拓扑中的编号为S1和S2。

（2）使用两台三层可控交换机作为校本部网络中的汇聚交换机，在网络拓扑中的编号为S3和S4。

（3）使用两台二层可控交换机作为校本部网络中的接入交换机，在网络拓扑中的编号为S5和S6。

（4）使用一台无线AP作为校本部网络中的无线接入点，在网络拓扑中的编号为AP1。

（5）学院本部的网络使用一台出口网关设备，把校园网本部网络接入互联网，在网络拓扑中的编号为EG1。

（6）学院校园网本部的网络中部分业务，使用一台路由器做出口，在网络拓扑中的编号为R1。

（7）在运营商网络（代表Internet）中，使用一台出口网关组网，在网络拓扑中的编号为EG2。

（8）学院的产融实训基地中安装了一台出口路由器接入互联网，在网络拓扑中的编号为R2。

（9）在学院的产融实训基地的无线网络部署中，使用一台无线AP接入，在网络拓扑中编号为AP2。

（10）学院的云数据中心安装了一台出口路由器接入互联网，在网络拓扑中编号为R3。

（11）在学院的云数据中心安装了一台三层可控交换机，作为云数据中心的核心交换机，在网络拓扑中编号为S7。

（12）在学院的云数据中心安装了两台无线控制器，作为无线网络的控制中心，在网络拓扑中的编号为AC1和AC2。

（13）在学院的云数据中心使用一台无线AP作无线网络接入，在网络拓扑中编号为AP3。

**4. 网络拓扑连线要求与说明**

在项目实施过程中，如用户无特殊要求，应根据规范要求进行各级网络设备之间的互联，统一现场设备的互联界面；使用线缆标签规范连接，使网络结构清晰明了，方便后续维护。

请根据拓扑及网络设备物理连接表，完成设备连线。其中，网络物理连接表如表1所示；网络设备名称表如表2所示；网络中IPv4地址分配表如表3所示。

表1 ：网络设备物理连接表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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 | Connect\_To\_S3\_Gi0/23 | S3 | Gi0/23 |
| Gi0/2 | Connect\_To\_S4\_Gi0/23 | S4 | Gi0/23 |
| Gi0/45 | Connect\_To\_S2\_Gi0/45 | S2 | Gi0/45 |
| Gi0/46 | Connect\_To\_S2\_Gi0/46 | Gi0/46 |
| Gi0/48 | Connect\_To\_EG1\_Gi0/0 | EG1 | Gi0/0 |
| S2 | Gi0/1 | Connect\_To\_S3\_Gi0/24 | S3 | Gi0/24 |
| Gi0/2 | Connect\_To\_S4\_Gi0/24 | S4 | Gi0/24 |
| Gi0/45 | Connect\_To\_S1\_Gi0/45 | S1 | Gi0/45 |
| Gi0/46 | Connect\_To\_S1\_Gi0/46 | Gi0/46 |
| Gi0/47 | Connect\_To\_EG1\_Gi0/1 | EG1 | Gi0/1 |
| Gi0/48 | Connect\_To\_R1\_Gi0/0 | R1 | Gi0/0 |
| S3 | Gi0/1 | Connect\_To\_S5\_Gi0/24 | S5 | Gi0/24 |
| Gi0/21 | Connect\_To\_S4\_Gi0/21 | S4 | Gi0/21 |
| Gi0/22 | Connect\_To\_S4\_Gi0/22 | Gi0/22 |
| Gi0/23 | Connect\_To\_S1\_Gi0/1 | S1 | Gi0/1 |
| Gi0/24 | Connect\_To\_S2\_Gi0/1 | S2 | Gi0/1 |
| S4 | Gi0/1 | Connect\_To\_S6\_Gi0/24 | S6 | Gi0/24 |
| Gi0/21 | Connect\_To\_S3\_Gi0/21 | S3 | Gi0/21 |
| Gi0/22 | Connect\_To\_S3\_Gi0/22 | Gi0/22 |
| Gi0/23 | Connect\_To\_S1\_Gi0/2 | S1 | Gi0/2 |
| Gi0/24 | Connect\_To\_S2\_Gi0/2 | S2 | Gi0/2 |
| S5 | Gi0/1 | Connect\_To\_AP1\_Gi0/1 | AP1 | Gi0/1 |
| Gi0/23 | Connect\_To\_S6\_Gi0/23 | S6 | Gi0/23 |
| Gi0/24 | Connect\_To\_S3\_Gi0/1 | S3 | Gi0/1 |
| Te0/27 | Connect\_To\_S6\_Te0/27 | S6 | Te0/27 |
| Te0/28 | Connect\_To\_S6\_Te0/28 | te0/28 |
| S6 | Gi0/23 | Connect\_To\_S5\_Gi0/23 | S5 | Gi0/23 |
| Gi0/24 | Connect\_To\_S4\_Gi0/1 | S4 | Gi0/1 |
| Te0/27 | Connect\_To\_S5\_Te0/27 | S5 | Te0/27 |
| Te0/28 | Connect\_To\_S5\_Te0/28 | te0/28 |
| AP1 | Gi0/1 | Connect\_To\_S5\_Gi0/1 | S5 | Gi0/1 |
| EG1 | Gi0/0 | Connect\_To\_S1\_Gi0/48 | S1 | Gi0/48 |
| Gi0/1 | Connect\_To\_S2\_Gi0/47 | S2 | Gi0/47 |
| Gi0/4 | Connect\_To\_EG2\_Gi0/0 | EG2 | Gi0/0 |
| R1 | Gi0/0 | Connect\_To\_S2\_Gi0/48 | S2 | Gi0/48 |
| Gi0/1 | Connect\_To\_EG2\_Gi0/1 | EG2 | Gi0/1 |
| EG2 | Gi0/0 | Connect\_To\_EG1\_Gi0/4 | EG1 | Gi0/4 |
| Gi0/1 | Connect\_To\_R1\_Gi0/1 | R1 | Gi0/1 |
| Gi0/2 | Connect\_To\_R2\_Gi0/1 | R2 | Gi0/1 |
| Gi0/3 | Connect\_To\_R3\_Gi0/1 | R3 | Gi0/1 |
| R2 | Gi0/0 | Connect\_To\_AP2\_Gi0/1 | AP2 | Gi0/1 |
| Gi0/1 | Connect\_To\_EG2\_Gi0/2 | EG2 | Gi0/2 |
| AP2 | Gi0/1 | Connect\_To\_R2\_Gi0/0 | R2 | Gi0/0 |
| R3 | Gi0/0 | Connect\_To\_S7\_Gi0/24 | S7 | Gi0/24 |
| Gi0/1 | Connect\_To\_EG2\_Gi0/3 | EG2 | Gi0/3 |
| S7 | Gi0/1 | Connect\_To\_AC1\_Gi0/4 | AC1 | Gi0/4 |
| Gi0/2 | Connect\_To\_AC2\_Gi0/4 | AC2 | Gi0/4 |
| Gi0/3 | Connect\_To\_AP3\_Gi0/1 | AP3 | Gi0/1 |
| Gi0/24 | Connect\_To\_R3\_Gi0/0 | R3 | Gi0/0 |
| AC1 | Gi0/1 | Connect\_To\_AC2\_Gi0/1 | AC2 | Gi0/1 |
| Gi0/2 | Connect\_To\_AC2\_Gi0/2 | Gi0/2 |
| Gi0/3 | Connect\_To\_AC2\_Gi0/3 | Gi0/3 |
| Gi0/4 | Connect\_To\_S7\_Gi0/1 | S7 | Gi0/1 |
| AC2 | Gi0/1 | Connect\_To\_AC1\_Gi0/1 | AC1 | Gi0/1 |
| Gi0/2 | Connect\_To\_AC1\_Gi0/2 | Gi0/2 |
| Gi0/3 | Connect\_To\_AC1\_Gi0/3 | Gi0/3 |
| Gi0/4 | Connect\_To\_S7\_Gi0/2 | S7 | Gi0/2 |
| AP3 | Gi0/1 | Connect\_To\_S7\_Gi0/3 | S7 | Gi0/3 |

表2 ：网络设备名称表

|  |  |  |
| --- | --- | --- |
| 拓扑图中名称 | 配置主机名（hostname名） | 备注 |
| S1 | XBBHX-DataCenter-Switch-S1 | 校本部网络中的核心交换机1 |
| S2 | XBBHX-DataCenter-Switch-S2 | 校本部网络中的核心交换机2 |
| S3 | XBBHJ-Aggregation-Switch-S3 | 校本部网络中的汇聚交换机1 |
| S4 | XBBHJ-Aggregation-Switch-S4 | 校本部网络中的汇聚交换机2 |
| S5/S6(VSU) | XBBJR-Access-Switch-Virtual | 校本部接入交换机(网络虚拟设备) |
| EG1 | XBBCK-Egress-Gateway-EG1 | 校本部网络中的用户出口网关 |
| R1 | XBBCK-Router-R1 | 校本部网络中的业务出口路由器 |
| EG2 | ISP-Egress-Gateway-EG2 | 运营商网络中的出口网关 |
| R2 | CJSX-Router-R2 | 产教实训基地网络中的出口路由器 |
| R3 | YZX-Router-R3 | 云数据中心网络中的出口路由器 |
| S7 | YZX-Aggregation-Switch-S7 | 云数据中心网络中的核心交换机 |
| AC1/AC2(VAC) | YZX-Wireless-Switch-VAC | 云数据中心无线控制器(VAC) |

表3：IPv4地址分配表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口或VLAN | VLAN名称 | 二层或三层规划 | 说明 |
| S1 | Gi0/1 | \ | 10.1.1.1/30 | 互联地址 |
| Gi0/2 | \ | 10.1.1.5/30 | 互联地址 |
| AG1（Gi0/45-Gi0/46） | \ | 10.1.1.253/30 | 互联地址 |
| Gi0/48 | \ | 10.1.1.250/30 | 互联地址 |
| Loopback 0 | \ | 10.1.0.1/32 | —— |
| S2 | Gi0/1 | \ | 10.1.1.9/30 | 互联地址 |
| Gi0/2 | \ | 10.1.1.13/30 | 互联地址 |
| AG1（Gi0/45-Gi0/46） | \ | 10.1.1.254/30 | 互联地址 |
| Gi0/47 | \ | 10.1.1.245/30 | 互联地址 |
| Gi0/48 | \ | 10.1.1.242/30 | 互联地址 |
| Loopback 0 | \ | 10.1.0.2/32 | —— |
| S3 | VLAN 10 | Wire | 192.1.10.252/24 | 有线用户地址 |
| VLAN 50 | APManage\_YWQ | 192.1.50.252/24 | 校本部AP管理地址 |
| VLAN 60 | Wireless | 192.1.60.252/24 | 无线用户地址 |
| VLAN 100 | Manage | 192.1.100.252/24 | 设备管理地址 |
| Gi0/23 | \ | 10.1.1.2/30 | 互联地址 |
| Gi0/24 | \ | 10.1.1.10/30 | 互联地址 |
| Loopback 0 | \ | 10.1.0.3/32 | —— |
| S4 | VLAN 10 | Wire | 192.1.10.253/24 | 有线用户地址 |
| VLAN 50 | APManage\_YWQ | 192.1.50.253/24 | 校本部AP管理地址 |
| VLAN 60 | Wireless | 192.1.60.253/24 | 无线用户地址 |
| VLAN 100 | Manage | 192.1.100.253/24 | 设备管理地址 |
| Gi0/23 | \ | 10.1.1.6/30 | 互联地址 |
| Gi0/24 | \ | 10.1.1.14/30 | 互联地址 |
| Loopback 0 | \ | 10.1.0.4/32 | —— |
| VSU（S5-S6) | VLAN 10 | Wire | Gi1/0/6至 Gi1/0/20, Gi2/0/6至 Gi2/0/20 | 有线用户地址 |
| VLAN 50 | APManage\_YWQ | Gi1/0/1至 Gi1/0/5, Gi2/0/1至 Gi2/0/5 | 校本部AP管理地址 |
| VLAN 100 | Manage | 192.1.100.1/24 | 设备管理地址 |
| EG1 | Gi0/0 | \ | 10.1.1.249/30 | 互联地址 |
| Gi0/1 | \ | 10.1.1.246/30 | 互联地址 |
| Gi0/4 | \ | 100.1.1.2/29 | 联通出口地址 |
| Loopback 0 | \ | 10.1.0.5/32 | —— |
| R1 | Gi0/0 | \ | 10.1.1.241/30 | 互联地址 |
| Gi0/1 | \ | 101.1.1.2/29 | 电信出口地址 |
| Loopback 0 | \ | 10.1.0.6/32 | —— |
| EG2 | Gi0/0 | \ | 100.1.1.1/29 | ISP联通地址 |
| Gi0/1 | \ | 101.1.1.1/29 | ISP电信地址 |
| Gi0/2 | \ | 101.2.1.1/29 | ISP电信地址 |
| Gi0/3 | \ | 101.3.1.1/29 | ISP电信地址 |
| R2 | Gi0/0 | \ | 194.1.50.254/24 | 产融基地AP管理地址 |
| Gi0/0.60 | \ | 194.1.60.254/24 | 产融基地无线学员地址 |
| Gi0/0.70 | \ | 194.1.70.254/24 | 产融基地无线教练地址 |
| Gi0/1 | \ | 101.2.1.2/29 | 电信出口地址 |
| Loopback 0 | \ | 10.2.0.1/32 | —— |
| R3 | Gi0/0 | \ | 10.3.1.253/30 | 互联地址 |
| Gi0/1 | \ | 101.3.1.2/29 | 电信出口地址 |
| Loopback 0 | \ | 10.3.0.1/32 | —— |
| S7 | VLAN 550 | APManage\_YWQ | 195.1.50.254/24 | 云中心AP管理地址 |
| VLAN 560 | Wireless | 195.1.60.254/24 | 云中心无线用户地址 |
| VLAN 100 | Manage | 195.1.100.254/24 | 云中心设备管理地址 |
| Gi0/24 | \ | 10.3.1.254/30 | 互联地址 |
| Loopback 0 | \ | 10.3.0.2/32 | —— |
| VAC | VLAN 100 | Manage | 195.1.100.1/24 | 设备管理地址 |
| Loopback 0 | \ | 10.3.0.3/32 | —— |

# 四．网络项目实施

## （一）网络设备基础信息配置与验证

**1. 完成网络设备规范命名；配置网络设备基础信息。**

（1）根据网络设备名称表（表2：网络设备名称表），修订所有设备名称。

（2）依据网络设备物理连接表（表1：网络设备物理连接表），配置设备接口描述信息。

**2. 完成网络设备密码恢复，实现设备软件版本统一。**

（1）在交换机S7上做密码恢复，新的密码设置为admin1234。

（2）在交换机S7上进行版本更新，更新版本至指定版本，指定版本见现场提供的设备软件版本升级文件包（见文件XXXXX）。

**3. 保障全网中的网络设备安全。**

（1）需要在所有网络设备上，都需要开启SSH服务，以保障网络设备的安全。其中，用户名和密码分别为admin、admin1234；特权密码为admin1234。

（2）为方便对全网开展网络管理，网络管理员增设网管平台，网管平台IP规划为172.16.0.254/24。

（3）为实现网管平台后期上线后可用，需要在每台设备上部署SNMP功能，配置所有网络设备的SNMP消息报告机制。其中，向主机172.16.0.254发送Trap消息版本采用V2C；读写的Community为“admin”；只读的Community为“public”；开启Trap消息通告。

## （二）网络搭建与网络冗余备份方案部署

**1.在全网部署虚拟局域网，完成全网IPv4地址部署。**

为了减少全网广播干扰，在全网规划和部署VLAN，需要实施内容如下所示。

（1）全网VLAN规划和配置合理，在Trunk链路上禁止不必要VLAN中的数据流通过。

（2）为了隔离网络终端之间的二层互访，需要在交换机S5、S6的Gi0/6-Gi0/20端口上，启用端口保护功能。

（3）根据“表2：网络设备名称表”、“表3：IPv4地址分配表”中规划要求，在各台设备上完成相应的VLAN信息、IP地址的配置。

**2. 在局域网中部署环路规避方案**

为避免网络接入设备上出现环路，影响全网运行状态。要求在网络接入交换机S5、S6上进行防环处理。具体要求如下所示。

（1）在连接PC机端口上开启Portfast和BPDUguard防护功能。

（2）为防止接入交换机下联端口出现用户私接集线器（Hub），引起办公网中的环路，需要启用RLDP协议进行防环处理。

（3）接入交换机的连接终端的接口上检测到环路后，要求处理的方式为Shutdown-Port，实现防环保护。

（4）一旦端口检测异常事件并进入Err-Disabled状态，设置300秒自动恢复机制（基于接口部署策略）。

**3. 部署DHCP中继与服务安全**

在学校本部网络中，部署DHCP中继与服务安全如下所示。

（1）在交换机S3、S4上配置DHCP中继功能，使得网络中的终端用户通过DHCP Relay方式获取IP地址。

其中，DHCP服务器搭建在学院的EG1上,按照地址规划表（表3：IPv4地址分配表）中地址规划，为有线用户、无线用户和AP的管理地址（共3个网段，192.1.10.0/24、192.1.50.0/24、192.1.60.0/24，其中，具体地址规划见“表3：IPv4地址分配表”。配置无线AP的租约为永久；配置无线用户设备的租约设为0.5天。

（2）为了防御局域网中出现伪造DHCP服务器与ARP欺骗安全事件发生，需要在校本部网络中的接入交换机S5、S6上，部署DHCP 的“Snooping+DAI”功能。其中，DAI安全功能主要针对VLAN10中用户设备启用ARP防御。

（3）为了防止校本部中的网关设备连续发送大量、正常报文，被接入交换机误认为是攻击事件而被丢弃，导致下联网络中的用户设备，无法获取网关设备上发出的ARP信息，造成无法上网，要求关闭S5、S6交换机的上联口上的“NFPP的arp-guard”功能。

（4）调整校本部中的接入交换机S5、S6设备上的“CPU保护机制”。其中，调整ARP的带宽为1500pps。

其中，在产融实训基地中需要部署DHCP中继与服务安全如下所示。

（5）产融实训基地中DHCP服务器搭建于R2上,按照地址规划表（表3：IPv4地址分配表），为无线网络中用户地址和AP管理地址（共3个网段，194.1.50.0/24、194.1.60.0/24、194.1.70.0/24）提供地址分配任务。其中，配置无线AP的租约为永久，无线用户的租约设为1天。

其中，云数据中心部署DHCP中继与服务安全如下所示。

（6）云数据中心DHCP服务器搭建于S7交换机上,按照地址规划表（表3：IPv4地址分配表）规划内容，为无线管理员和AP管理地址（共2个网段，195.1.50.0/24、195.1.60.0/24）提供地址分配任务。其中，配置无线AP的租约为永久，无线用户的租约设为1天。

（7） 在云数据中心DHCP服务器保留“195.1.60.101/24~195.1.60.150/24”这50个IP地址，用作机房运维的静态IP地址，其余地址均正常通过DHCP分配使用。

**4. 部署MSTP及VRRP技术，实现网络冗余。**

在校本部的S3、S4、S5、S6交换机上配置MSTP防止二层环路。

（1）在校本部的网络中配置MSTP,要求来自VLAN10、VLAN100中的数据流经过S3交换机转发，一旦S3交换机失效时，经过S4交换机转发。要求来自VLAN50、VLAN60中的数据流经过S4交换机转发，一旦S4交换机失效时，经过S3交换机转发。其中，配置MSTP参数如下所示：region-name为test；revision版本为1；实例1包含VLAN10，VLAN100；实例2包含VLAN50,VLAN60。

（2）配置校本部网络中的S3交换机作为实例1的主根、实例2的从根；配置S4交换机作为实例2的主根、实例1的从根。其中，主根交换机的优先级为4096；从根交换机的优先级为8192。

（3）校本部网络中汇聚交换机S3、S4连接接入交换机S5、S6接口上，启用“TC-IGNORE”功能，规避网络中接入设备出现频繁网络震荡影响全网震荡。

（4）在校本部网络中汇聚交换机S3和S4上配置VRRP，实现网络中的主机的网关冗余，所配置的参数要求如表4所示。其中，在交换机S3、S4上设置各VRRP组中的高优先级设置为150，低优先级设置为120。

（5）为提升校本部网络的冗余功能，在汇聚交换机S3与S4之间部署2条互联链路（Gi0/21、Gi0/22），并采取LACP动态聚合模式配置二层链路聚合。其它接口根据网络互联需要，进行静态链路聚合配置，生成聚合接口AG2。

表4：交换机S3和S4上的VRRP参数表

|  |  |  |
| --- | --- | --- |
| VLAN | VRRP备份组号（VRID） | VRRP虚拟IP |
| VLAN10 | 10 | 192.1.10.254 |
| VLAN50 | 50 | 192.1.50.254 |
| VLAN60 | 60 | 192.1.60.254 |
| VLAN100 | 100 | 192.1.100.254 |

**5. 部署网络设备虚拟化，保障核心网络稳健运行。**

为增加网络的稳健性，校本部网络中两台接入交换机，通过网络设备虚拟化技术，配置成一台虚拟网络设备进行集中管理，实现网络的高可靠性。当网络中的任意一台交换机出现故障，都能够实现设备、链路切换，保证业务不中断。

（1）部署校本部网络中两台接入交换机S5和S6之间的Te0/27-28端口作为VSL链路，使用网络设备虚拟化实现接入层网络的虚拟化。其中：配置S5交换机为主交换机；配置S6交换机为备用交换机。

（2）两台接入交换机S5和S6之间Gi0/22端口作为双主机检测链路，配置基于BFD双主机检测。当VSL链路中所有物理链路都异常断开时，备用交换机切换成主机，保障网络正常运营。其中，需要配置主交换机参数信息为：Domain id：1；Switch id:1;priority 150; description:Access-Switch-Virtual-Switch1。需要配置备交换机设备参数信息为：Domain id：1；Switch id:2；priority 120；description:Access-Switch-Virtual-Switch2。

**6. 部署全网路由协议，实现全网的互联互通。**

在校本部的网络中使用多区域OSPF协议组网（OSPF 100），实现全网的互联互通，具体要求如下。

（1）配置两台核心交换机（S1、S2）的Loopback 0口以及之间互相连接的心跳线（Gi0/45和Gi0/46的三层聚合口），都在区域0中发布路由。

（2）配置校本部网络中的出口区域（S1、S2、EG1、R1）接口，都在区域10中发布路由。

（3）配置校本部网络中的核心网络（S1、S2、S3、S4）中接口 ，都在区域20中发布路由。

（4）要求业务网段（VLAN 10、VLAN 50、VLAN 60、VLAN100）中不，出现协议报文。

（5）要求校本部网络中S3、S4交换机上的始发网段，以及各台网络设备（S1、S2、S3、S4、EG1、R1）上配置的Loopback管理地址，均使用network发布明细路由。

（6）校本部网络中的S1和S2交换机之间，启用OSPF与BFD联动，一旦监控到对端设备中断，能快速地切换到其他备份线路，提高用户网络体验。

（7）优化全网的OSPF配置，尽量加快OSPF路由收敛。

（8）外部重发布路由进入OSPF路由中，使用类型1。

（9）使用静态路由实现产融实训基地、云数据中心区域之间的网络通信，实现和校本部网络的连通。

**7. 部署部分区域路由选路，实现策略路由。**

考虑到全网中数据分流需求以及实现网络的负载均衡的目的，需要进行路由策略部署，具体要求如下所示。

（1）通过策略部署，使得数据的来回路径一致，需要配置的信息如下所示。

实现校本部网络中的有线用户，在访问互联网流量路径为：VSU-S3-S1-EG1。

实现校本部网络中的无线用户，访问互联网的流量路径为：VSU-S4-S2-EG1。

实现校本部有线网络中的用户，访问学校的云数据中心和产融实训基地的流量路径为：VSU-(S3/S4)-S2-R1。

（2）通过策略部署，熟悉主链路或S1/S2、S3/S4等主设备故障时，可无缝切换到备用链路或备用设备上。

（3）配置策略路由时，各路由图以及各接口中凡涉及COST值的调整，需要配置COST值必须为5或10。

**8. 在省行的业务区中部署IPv6业务。**

（1）在校本部的网络部署IPv6业务，实现学校内网中的IPv6终端设备可自动从网关设备上获取IPv6地址。

（2）在校本部汇聚交换机S3、S4上配置VRRP for IPv6路由技术，在校本部网络中的主机上实现IPv6网关冗余。其中，VRRP for IPv6冗余路由、MSTP的主备状态均需与IPV4网络中配置的相关信息保持一致。

（3）在校本部的网络中部署IPv6业务。其中，IPV6地址规划如表5所示。

（4）在校本部网络中的网络设备S1、S2、S3、S4、R1之间，部署多区域的OSPFv3路由,需要配置进程为10，保障OSPFv3路由区域划分与IPV4网络中配置的OSPFv2路由保持一致。

（5）在云数据中心网络中（R3、S7、VAC）部署IPV6静态路由协议，实现云数据中心网络中所有IPV6终端之间互联互通。

（6）在校本部网络的出口路由器R1和云数据中心网络的出口R3之间，部署IPV6 GRE隧道技术，隧道内部配置静态路由协议，实现学院全网的IPV6终端之间的互联互通。

表5：IPV6地址规划表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | IPV6地址 | VRRP组号 | 虚拟IP |
| S1 | Gi0/1 | 2001:10::1/64 |  |  |
| Gi0/2 | 2001:10:4::1/64 |  |  |
| AG1 | 2001:10:252::1/64 |  |  |
| S2 | Gi0/1 | 2001:10:8::1/64 |  |  |
| Gi0/2 | 2001:10:12::1/64 |  |  |
| AG1 | 2001:10:252::2/64 |  |  |
| Gi0/48 | 2001:10:240::2/64 |  |  |
| S3 | VLAN10 | 2001:192:10::252/64 | 10 | 2001:192:10::254/64 |
| VLAN50 | 2001:192:50::252/64 | 50 | 2001:192:50::254/64 |
| VLAN60 | 2001:192:60::252/64 | 60 | 2001:192:60::254/64 |
| VLAN100 | 2001:192:100::252/64 | 100 | 2001:192:100::254/64 |
| Gi0/23 | 2001:10::2/64 |  |  |
| Gi0/24 | 2001:10:8::2/64 |  |  |
| S4 | VLAN10 | 2001:192:10::253/64 | 10 | 2001:192:10::254/64 |
| VLAN50 | 2001:192:50::253/64 | 50 | 2001:192:50::254/64 |
| VLAN60 | 2001:192:60::253/64 | 60 | 2001:192:60::254/64 |
| VLAN100 | 2001:192:100::253/64 | 100 | 2001:192:100::254/64 |
| Gi0/23 | 2001:10:4::2/64 |  |  |
| Gi0/24 | 2001:10:12::2/64 |  |  |
| VSU | VLAN100 | 2001:192:100::1/64 |  |  |
| R1 | Gi0/0 | 2001:10:240::1/64 |  |  |
| Tunnel0 | 2004:11:1:1::1/64 |  |  |
| R3 | Gi0/0 | 2003:10:252::1/64 |  |  |
| Tunnel0 | 2004:11:1:1::2/64 |  |  |
| S7 | VLAN100 | 2003:195:100::254/64 |  |  |
| VLAN550 | 2003:195:50::254/64 |  |  |
| VLAN560 | 2003:195:60::254/64 |  |  |
| Gi0/24 | 2003:10:252::2/64 |  |  |
| VAC | VLAN100 | 2003:195:100::1/64 |  |  |

## （三）移动互联网搭建与无线网络优化

**1.在校本部的网络中部署无线网络。**

（1）在校本部的网络中部署无线网络，无线网络架构采用FIT AP架构。校本部的网络中所有AP（AP1）都需要关联到云数据中心网络中的VAC设备上。

（2）在校本部的网络中，配置出口网关EG1作为无线网络中用户（VLAN 60）和无线FIT AP（VLAN 50）的DHCP服务器。

（3）在校本部网络中创建内网SSID为：Admin\_XBB\_XX(备注：XX现场提供)；WLANID为1；AP-GROUP为Admin\_XBB。其中，校本部内网中的无线用户关联SSID后，即可自动获取VLAN60地址提供的地址。

**2.在产融实训基地部署无线网络。**

（1）在产融实训基地中部署的无线网络架构，采用FIT AP+AC的方案。该区域内所有AP（AP2）都需要关联到云数据中心的VAC设备上。

（2）在产融实训基地网络中，使用R2路由器作为DHCP服务器，为无线网络中的用户（VLAN 60、VLAN 70）和无线FIT AP（VLAN 50）分配地址。

（3）在产融实训基地中配置双SSID广播。其中，创建学员的SSID为Admin\_CR\_XY\_XX(备注：XX现场提供)；WLANID为2；AP-GROUP为Admin\_CR；配置内网中无线用户在关联SSID后，可自动获取VLAN60地址。创建教练的SSID为Admin\_CR\_JL\_XX(备注：XX现场提供)；WLANID为3；AP-GROUP为Admin\_CR，配置内网中无线用户关联SSID后，可自动获取VLAN70地址。

**3.在云数据中心的展示区中部署无线网络。**

（1）在云数据中心的展示区中部署无线网络，采用FIT AP架构，区域内所有AP（AP3）都关联到云数据中心的VAC设备上。

（2）在云数据中心的展示区中，配置S7交换机作为DHCP服务器，为本网中的无线网络内部用户（VLAN 560）和无线FIT AP（VLAN 550）分配地址。

（3）在云数据中心的展示区的内网中配置SSID。其中，Admin\_YSJZX\_XX(备注：XX现场提供)；WLANID为4；AP-GROUP为Admin\_YSJZX。配置内网无线用户关联SSID后，可自动获取VLAN560地址。

**4.在无线网络中部署AC冗余，实现备份。**

（1）在云数据中心的展示区的无线网络中部署AC冗余，实现无线备份。两台AC使用网络设备虚拟化技术实现VAC技术，完成虚拟AC配置。

（2）配置AC1和AC2设备的Gi0/1和Gi0/2端口作为VSL链路。其中：配置AC1为主控设备；AC2为备用设备。配置主设备参数为：Domain id：1；device id:1；priority 150； description: AC-1。配置备设备基本参数为：Domain id：1；device id:2；priority 120； description: AC-2。

（3）配置AC1和AC2设备的Gi0/3端口的互连链路作为BFD链路。

（4）校本部网络中的AP1设备与虚拟网络设备VAC之间，通过出口路由器R1和R3之间的VPN隧道，配置Capwap隧道建立通信连接。

（5）产教融合实训基地中的无线AP2设备与虚拟网络设备VAC之间，通过VAC的互联网映射地址，配置Capwap隧道建立通信连接。

**5. 保障无线网络安全。**

（1）产融实训基地与云数据中心的无线用户在接入无线网络时，采用WPA2加密方式。其中，配置加密算法为AES，身份认证方式为预共享密钥，秘钥为XX（备注：XX现场提供）。

（2）校本部网络中的无线用户在接入无线网络时，采用内置PORTAL认证方式。其中，用户名/密码为：user1/user1；user2/user2。

**6.实施无线网络的性能优化**

（1）配置校本部和产融实训基地的无线AP设备（AP1、AP2），采用本地转发模式；配置云数据中心网络中无线AP设备（AP3），采用集中转发模式。

（2）限制全网中每台无线AP设备上的每个射频卡最大带点人数为15人。

（3）调整2.4G频段的射频卡Powerlocal功率数值为20；调整5.8G频段的射频卡Powerlocal功率数值为100；尽量降低同频干扰带来的影响。

（4）在全网中关闭低速率（11b/g 1M、2M、5M，11a 6M、9M）应用接入。

（5）在校本部网络中，为接入同一台AP中的无线用户，在某些时候出于安全性的考虑，需要将它们彼此之间进行隔离，实现无线用户之间彼此不能互相访问，配置校本部网络中AP1设备下同AP下用户间隔离功能。

## （四）实施出口安全防护与远程接入

**1.出口设备上部署NAT，实现远程接入。**

出口设备上部署NAT，实现远程接入，具体配置参数如下。

（1）在校本部网络中出口网关EG1上，配置NAT地址映射，实现校本部网络中的用户通过NAPT方式，将内网IP地址映射到本地互联网接口上。其中，NAT地址池中映射的地址为：100.1.1.3/29-100.1.1.4/29。

（2）在校本部网络中的出口路由器R1上，配置NAT地址映射，实现校本部的网络中的用户，在访问产融实训基地和云数据中心网络中的数据时，通过NAPT端口地址映射方式，将内网IP地址转换到互联网接口上。其中，配置的NAT地址池的映射地址为：101.1.1.3/29-101.1.1.4/29。

（3）在产融实训基地的出口路由器R2上，配置NAT地址映射，实现基地内部的用户访问互联网时，通过NAPT方式将内网IP地址转换到互联网接口上。其中，NAT地址池的地址与出口路由器的R2设备的出接口地址相同。

（4）在云数据中心出口路由器R3上，配置NAT地址映射，实现内部用户在访问互联网时，通过NAPT方式将内网IP地址转换到互联网接口上。其中，NAT地址池的映射地址为：101.3.1.3/29 ~ 101.3.1.4/29。

（5）在云数据中心的出口路由器R3上，配置NAPT端口映射，使网络中的一台HTTP服务器（195.1.100.254/24）上的HTTP服务（TCP 80）,可以通过互联网被访问到，将其地址映射至运营商线路上，映射地址为101.3.1.5，映射端口58888。

（6）在云数据中心网络的出口路由器R3上，配置IP映射，将VAC设备的loopback接口地址映射至101.3.1.6。

**2.在出口设备上部署Web Portal用户认证，实现出口安全防护。**

在校本部的网关EG1设备上，启用Web Portal认证服务。创建两个认证用户，其用户名/密码分别为：user1/user1、user2/user2。

**3.在出口设备上应用流量控制。**

（1）在校本部出口网关EG1设备上，将校本部网络中的用户访问互联网的WEB流量，限速每个IP为1000Kbps，内网WEB总流量不超过20Mbps，通道名称定义为WEB。

（2）在ISP网络的组网设备EG2出口网关上，按照各出口线路（原带宽均为1Gbps）申请的带宽进行限速。需要配置参数为：校本部出口路由器R1设备的带宽限速为200Mbps（备注：通道名称为R1）。产教融合实训基地网络中的出口路由器R2设备的带宽限速为500Mbps（备注：道名称为R2）。云数据中心网络中出口路由器R3设备的带宽限速为800Mbps（备注：通道名称为R3）。

**4. 在出口设备上部署用户行为策略。**

（1）在校本部出口网关EG1设备上，配置用户安全策略，实施基于网站访问、邮件收发、IM聊天、论坛发帖、搜索引擎多应用，启用安全审计功能。

（2）在校本部出口网关EG1设备上，配置安全防护，要求在周一到周六的工作时间09：00—17:00内（备注：命名为work），阻断并审计P2P应用软件使用。其中，审计策略名称定义为P2P。

（3）在ISP网络中的组网设备EG2上，要求对个别敏感词“大赛真题”和“如何作弊”进行过滤。

**5. 在出口设备上部署VPN安全。**

为了实现校本部、产融实训基地和云数据中心网络之间数据访问的安全，针对网络中传输数据，需要使用VPN技术进行安全保障，具体规划如下所示。

（1）在R1、R2和R3的出口路由器之间，启用IPSec VPN功能。其中：配置IPSec安全防范使用动态隧道模式，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。配置转换集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。

（2）在校本部出口网关EG1设备上，配置SSLVPN安全，实现访问地址为https://100.1.1.2；拨入客户端获取地址为192.1.20.0/24；DNS为8.8.8.8；隧道资源名称为Server中包含192.1.50.24与192.1.100.1;登录用户名/密码为user1/user1、user2/user2。

# 五．无线网络规划与实施

本项目为校医院的网络改造项目。为满足移动医疗信息化建设要求，医院希望通过本次项目改造实现员工休息室、护士站、住院区、门诊区、输液区和候诊区六个区域的无线覆盖，走廊可不需覆盖。

为减低投资成本，本项目需要充分考虑利用原有的有线网络投资资源，拟用于购置无线设备的预算为16.5万元。

## （一）无线网络业务背景及需求介绍

**1.楼宇相关信息介绍。**

1.建筑使用说明。

该楼宇为医院综合楼，二楼为社区医院，拥有员工休息室、护士站、住院区、门诊区、输液区和候诊区六个区域。预计护士站人流量20人左右，输液区和候诊区确保信号覆盖即可。

2.建筑现场情况介绍。

该楼宇室内无吊顶，原有强电布线室内外均采用了pvc线槽敷设。

3.建筑物弱电间情况介绍。

该楼宇目前有独立的弱电间，整层建筑的平面布局图如图2所示。



图2 平面布局图

**2.无线产品的参数与价格介绍。**

无线产品及配件价格表如表6所示。

表6：无线产品及配件价格表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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） |
| AP330-I | 双频双流 | 300M/1.167G | 32/256 | 100mW | 6000 |
| AP220-E(M)-V3.0 | 双频双流 | 300M/600M | 32/256 | 100mW | 11000 |
| RG-Cab-SMA-10m | 10米馈线 | N/A | N/A | N/A | 1600 |
| RG-Cab-SMA-15m | 15米馈线 | N/A | N/A | N/A | 2400 |
| RG-IOA-2505-S1 | 双频单流/单频单流 | N/A | N/A | N/A | 500 |
| AP110-w | 单频单流 | 150M | 12/32 | 60mW | 2500 |
| S2928G-24P | 24口POE交换机 | N/A | N/A | 240W | 15000 |
| WS6008 | 无线控制器 | 6\*1000M | 32/200 | 40W | 50000 |

**3.无线网络系统中集成物料清单。**

无线网络系统中需要使用的综合布线工程材料清单如表7所示。

表7：综合布线工程材料清单

|  |  |  |  |
| --- | --- | --- | --- |
| 产品名称 | 规格 | 容纳网线数 | 单位 |
| Cat5e网络配线架 | 24口、1U | 24 | 个 |
| 理线架 | 1U | 24 | 个 |
| PVC线槽 | 20mm\*10mm\*2.8m | 1~2 | 条 |
| 25mm\*12.5mm\*2.8m | 3~4 | 条 |
| 30mm\*16mm\*2.8m | 5~7 | 条 |
| 39mm\*19mm\*2.8m | 8~12 | 条 |
| 50mm\*25mm\*2.8m | 13~22 | 条 |
| PVC线槽底盒 | 标准 | 2 | 个 |
| PVC暗盒 | 标准 | 2 | 个 |
| PVC线管 | 16mm\*2.8m | 1~3 | 条 |
| 20mm\*2.8m | 2~5 | 条 |
| 25mm\*2.8m | 4~8 | 条 |
| 金属桥架 | 50mm\*25mm | 13~22 | 米 |
| 60mm\*22mm | 13~23 | 米 |
| Cat5e网线 | 305米/箱 | N/A | 箱 |
| Cat5e水晶头 | 100个/盒 | N/A | 盒 |
| 机柜 | 6U | N/A | 个 |
| 机柜 | 12U | N/A | 个 |

## （二）无线网络中的业务规划

**1.完成楼宇中无线地勘。**

根据提供的建筑平面布局图、项目预算（设备经费）和业务需求，进行全网中无线AP的点位的规划与设计。然后，再通过无线地勘软件进行AP点位设计和无线信号仿真；确保全网中无线信号全覆盖（备注：厕所、楼梯间区域无须覆盖）。

然后，进一步做无线信道规划，并输出该层需要安装的无线AP设备的点位示意图、无线热图；并输出无线网络设备清单。

（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。其中，AP点位参考示意图如图3所示。



图3 AP点位参考示意图

（2）使用无线地勘软件，输出AP点位图在2.4G频段上的信号仿真热图（备注：仿真信号强度要求大于-65db），参考示意图如图4所示。



图4 仿真热图示意图

（3）完成点位设计之后，输出该无线网络工程项目中需要的设备预算表。其中，需要的网络设备型号和价格依据表6所示。最后，填写表8设备清单表。

表8：设备清单

|  |  |  |  |
| --- | --- | --- | --- |
| 设备型号 | 单价 | 数量 | 总价 |
| …… | …… | …… | …… |
|  |  |  |  |
|  |  |  |  |
| 项目总预算 | | |  |

**2.完成网络系统集成工勘。**

根据AP点位部署位置和建筑物现场情况，输出无线网络工程项目中的施工水平布线图、机柜安装示意图、网络配线架标签和物料清单。

（1）根据无线AP点位和建筑物现场环境，设计该无线网络的水平布线图（备注：vsd格式）。在进行综合布线型材选型中，根据国标文件GB50311—2016的要求，线槽截面利用率不能高于50%，线管截面利用率不能高于30%，且线槽/管规格选择最小规格。设计的参考示意图如图5所示。



图5 水平布线示意图

（2）根据机柜上架设备清单，规划设备在机柜的安装位置、设备和网络配线架的标识，输出机柜安装示意图（备注：vsd格式）。参考示意图如图6所示。



图6 机柜安装示意图

（3）根据无线AP点位编号信息，合理规划AP设备以及对应双绞线的上架位置，并在网络配线架面板做标注。

请将机柜上网络配线架的标签信息（从左到右）填写到表9中。

表9： 数据配线架标签表

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 网络配线架标签表 | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

（4）工程物料清单

根据无线网络水平布线图，计算本次无线网络工程的物料清单。其中：线缆采用平均值法进行估算，所有材料以表7为准。

请将本次无线网络工程的物料清单填写到表10中。

表10： 物料清单表

|  |  |  |
| --- | --- | --- |
| **物料名称** | **单位** | **数量** |
| …… | …… | …… |
|  |  |  |
|  |  |  |

# 六．竞赛结果文件提交说明

说明1：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，另存一份“PDF格式文档”（备注：利用Office Word中另存为pdf文件方式，生成pdf文件）。

说明2：在每台设备上使用show running-config命令，将该命令下显示的结果，分别保存为独立的“\*.txt”文件中。其中，文件名要以设备的编号命名（备注：S1、S2、S3、S4、S7、VSU、R1、R2、R3、AC1、AC2、EG1、EG2）；并把所有的“\*.txt”文件，集中存放在新建的“设备配置”文件夹下。

说明3：考生将“交换路由无线网关设备配置答题卡.docx”、“交换路由无线网关设备配置答题卡.pdf”、“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。

说明4：严格按照 “无线网络勘测设计答题卡.docx”文档格式要求，制作输出竞赛结果文件。同时，另存一份PDF格式文档（备注：利用Office Word另存为pdf文件方式生成pdf格式文件）。

说明5：考生将竞赛结果文件“无线网络勘测设计答题卡.docx”和“无线网络勘测设计答题卡.pdf”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。

说明6：考生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。