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4）



**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](#_Toc51771119)

[二．项目背景 3](#_Toc51771120)

[三．项目规划和设计 4](#_Toc51771121)

[四．网络项目实施 12](#_Toc51771122)

[（一）网络设备基础信息配置与验证 12](#_Toc51771123)

[（二）网络搭建与网络冗余备份方案部署 13](#_Toc51771124)

[（三）移动互联网搭建与无线网络优化 19](#_Toc51771125)

[（四）实施出口安全防护与远程接入 21](#_Toc51771126)

[五．无线网络规划与实施 23](#_Toc51771127)

[（一）无线网络业务背景及需求介绍 23](#_Toc51771128)

[（二）无线网络中的业务规划 26](#_Toc51771129)

[六．竞赛结果文件提交说明 29](#_Toc51771130)

# 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，请允许操作系统中的防火墙处于允许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

为适应IT行业技术飞速发展，提升员工素养和技术能力水平，满足公司业务发展需要，某CII教育集团公司决定建设本部企业大学、附属医院以及企业大学北京分校。

为了促进本部企业大学与分校的交流沟通，需要进行企业大学信息化建设。为更好管理业务数据，为教育信息化提供服务，集团公司决定建立企业大学云计算数据中心，从而实现高速、可靠的传输数据和存储数据，针对各地驻外办事处为保证通知质量与效率，为此CII集团引入二级运营商VIP专线业务实现驻外办事处间的高速互访。同时，扩展出口运营商及带宽分别接入当地二级运营商的联通，电信及教育网服务节点，二级运营商对外提供联通、电信及教育网宽带接入与专线VIP接入服务。

考虑企业大学移动办公的需求，本部及分校将提供有线和无线网络服务，并在网络出口部署出口网关设备，对访问互联网数据进行身份认证与信息审计，实现安全可靠的网络互联。

# 三．项目规划和设计

为了顺利实施某CII教育集团建设的本部企业大学、附属医院以及企业大学北京分校网络改造，优化网络环境，为集团网络提供保障服务，需要对集团的网络升级、改造和优化。

**1. 项目规划与建设内容**

主要实施网络项目规划与建设内容如下所示。

（1）在本部与分校均需要部署无线网络，满足移动办公和移动教学需求。

（2）部署防止环路、数据负载均衡等策略，确保接入层业务安全可靠。

（3）在出口实施单设备多运营商的链路备份方案，实现企业大学高速、高效的访问外网。

（4）总分机构之间部署链路冗余备份和链路加密等功能，实现安全可靠的数据传输。

（5）网络设计应针对OA办公、云教学平台系统、门户网站等关键业务高可用做具体策略部署；针对特殊业务部门应用，应做安全访问策略部署。

（6）各驻外办事处间通过专线接入二级运营商网络确保服务质量，并部署IPV4/IPV6双栈协议实现办事处间互联互通。

**2. 项目规划与建设拓扑**

某CII教育集团建设的本部企业大学、附属医院以及企业大学北京分校网络拓扑如图1所示。

**3. 项目规划与建设拓扑**

企业大学信息化建设方案拓扑相关说明如下所示。

（1）网络中安装两台出口网关作为企业大学总部与北京分部出口，在网络拓扑中的编号为EG1和EG2。

（2）网络中安装两台数据中心交换机，用作上海与杭州驻外办事处接入交换机，在网络拓扑中的编号为为S6和S7。

（3）网络中安装两台三层可控交换机作为本部的核心交换机，在网络拓扑中的编号为为S3和S4。

（4）网络中安装两台二层可控交换机用作本部接入交换机，在网络拓扑中的编号为为S1和S2。

（5）网络中安装两台无线控制器，用作企业大学本部和分校无线网络控制，在网络拓扑中的编号为AC1和AC2。

（6）网络中使用一台三层可控交换机用作分校接入交换机，在网络拓扑中的编号为S5。

（6）网络中安装三台无线接入AP，分别为本部与分校无线接入点，在网络拓扑中的编号为为AP1，AP2，AP3。

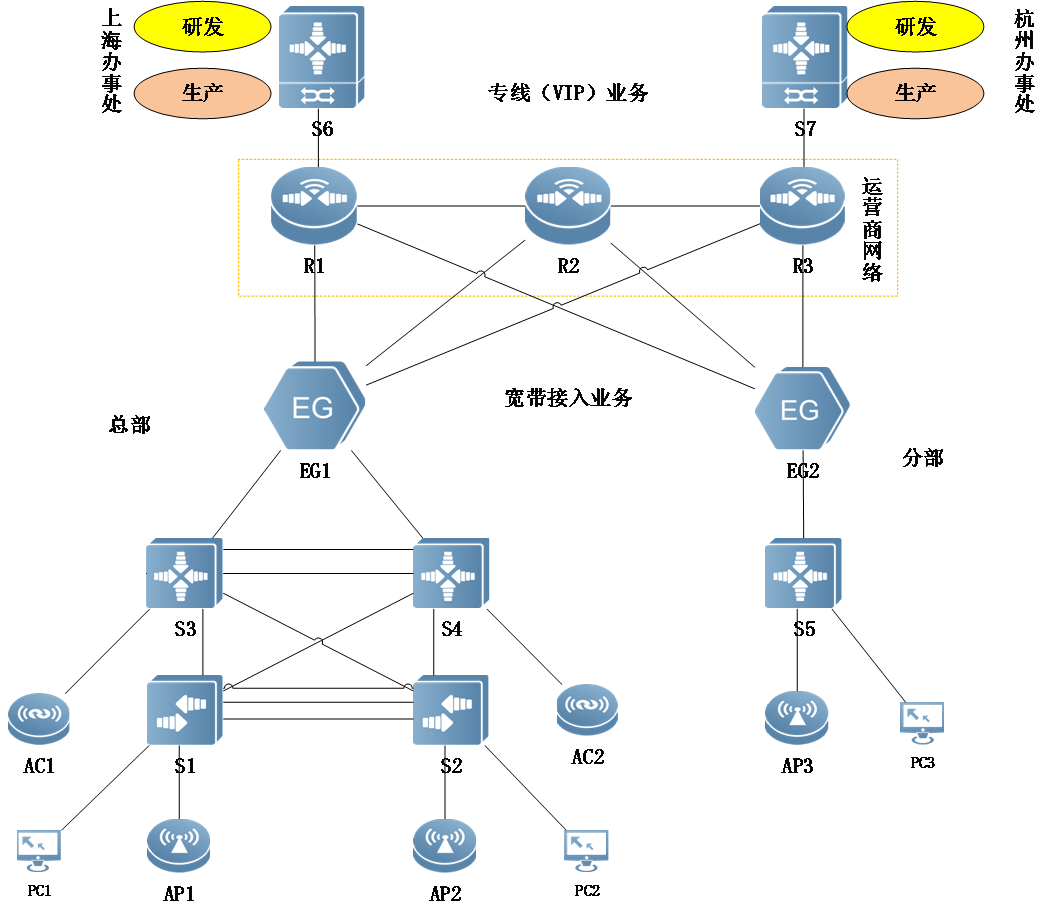


图1 某CII教育集团建设本部企业大学网络拓扑

（7）在二级运营商服务网络节点中，安装三台模块化路由器作接入，在网络拓扑中的编号为R1、R2和R3。其中，R1作为联通服务接入点，R2作为电信服务接入点，R3作为教育网服务接入点。

**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\_PC1 | PC1 |  |
| S1 | Gi0/21 | Connect\_To\_AP1\_Gi0/1 | AP1 | Gi0/1 |
| S1 | Gi0/22 | BFD | S2 | Gi0/22 |
| S1 | Gi0/23 | Connect\_To\_S3\_Gi0/1 | S3 | Gi0/1 |
| S1 | Gi0/24 | Connect\_To\_S4\_Gi0/1 | S4 | Gi0/1 |
| S1 | Te0/27 | Connect\_To\_S2\_Te0/27 | S2 | Te0/27 |
| S1 | Te0/28 | Connect\_To\_S2\_Te0/28 | S2 | Te0/28 |
| S2 | Gi0/1 | Connect\_To\_PC2 | PC2 |  |
| S2 | Gi0/21 | Connect\_To\_AP2\_Gi0/1 | AP2 | Gi0/1 |
| S2 | Gi0/22 | BFD | S1 | Gi0/22 |
| S2 | Gi0/23 | Connect\_To\_S3\_Gi0/2 | S3 | Gi0/2 |
| S2 | Gi0/24 | Connect\_To\_S4\_Gi0/2 | S4 | Gi0/2 |
| S2 | Te0/27 | Connect\_To\_S1\_Te0/27 | S1 | Te0/27 |
| S2 | Te0/28 | Connect\_To\_S1\_Te0/28 | S1 | Te0/28 |
| S3 | Gi0/1 | Connect\_To\_S1\_Gi0/23 | S1 | Gi0/23 |
| S3 | Gi0/2 | Connect\_To\_S2\_Gi0/23 | S2 | Gi0/23 |
| S3 | Gi0/3 | Connect\_To\_AC1\_Gi0/1 | AC1 | Gi0/1 |
| S3 | Gi0/4 | Connect\_To\_S4\_Gi0/4 | S4 | Gi0/4 |
| S3 | Gi0/5 | Connect\_To\_S4\_Gi0/5 | S4 | Gi0/5 |
| S3 | Gi0/24 | Connect\_To\_EG1\_Gi0/0 | EG1 | Gi0/0 |
| S4 | Gi0/1 | Connect\_To\_S1\_Gi0/24 | S1 | Gi0/24 |
| S4 | Gi0/2 | Connect\_To\_S2\_Gi0/24 | S2 | Gi0/24 |
| S4 | Gi0/3 | Connect\_To\_AC2\_Gi0/1 | AC2 | Gi0/1 |
| S4 | Gi0/4 | Connect\_To\_S3\_Gi0/4 | S3 | Gi0/4 |
| S4 | Gi0/5 | Connect\_To\_S3\_Gi0/5 | S3 | Gi0/5 |
| S4 | Gi0/24 | Connect\_To\_EG1\_Gi0/1 | EG1 | Gi0/1 |
| S5 | Gi0/1 | Connect\_To\_PC3 | PC3 |  |
| S5 | Gi0/21 | Connect\_To\_AP3\_ Gi0/1 | AP3 | Gi0/1 |
| S5 | Gi0/24 | Connect\_To\_EG2\_Gi0/0 | EG2 | Gi0/0 |
| S6 | Gi0/24 | Connect\_To\_R1\_ Gi0/0 | R1 | Gi0/0 |
| S7 | Gi0/24 | Connect\_To\_R3\_ Gi0/0 | R3 | Gi0/0 |
| AC1 | Gi0/1 | Connect\_To\_S3\_Gi0/3 | S3 | Gi0/3 |
| AC2 | Gi0/1 | Connect\_To\_S4\_Gi0/3 | S4 | Gi0/3 |
| EG1 | Gi0/0 | Connect\_To\_S3\_Gi0/24 | S3 | Gi0/24 |
| EG1 | Gi0/1 | Connect\_To\_S4\_Gi0/24 | S4 | Gi0/24 |
| EG1 | Gi0/2 | Connect\_To\_R1\_Fa1/1 | R1 | Fa1/1 |
| EG1 | Gi0/3 | Connect\_To\_R2\_Fa1/1 | R2 | Fa1/1 |
| EG1 | Gi0/4 | Connect\_To\_R3\_Fa1/1 | R3 | Fa1/1 |
| EG2 | Gi0/0 | Connect\_To\_S5\_Gi0/24 | S5 | Gi0/24 |
| EG2 | Gi0/2 | Connect\_To\_R1\_Fa1/2 | R1 | Fa1/2 |
| EG2 | Gi0/3 | Connect\_To\_R2\_Fa1/2 | R2 | Fa1/2 |
| EG2 | Gi0/4 | Connect\_To\_R3\_Fa1/2 | R3 | Fa1/2 |
| R1 | Gi0/0 | Connect\_To\_S6\_Gi0/24 | S6 | Gi0/24 |
| R1 | Se2/0 | Connect\_To\_R2\_ Se2/0 | R2 | Se2/0 |
| R1 | Fa1/1 | Connect\_To\_EG1\_Gi0/2 | EG1 | Gi0/2 |
| R1 | Fa1/2 | Connect\_To\_EG2\_Gi0/2 | EG2 | Gi0/2 |
| R2 | Se2/0 | Connect\_To\_R1\_ Se2/0 | R1 | Se2/0 |
| R2 | Se3/0 | Connect\_To\_R3\_ Se3/0 | R3 | Se3/0 |
| R2 | Fa1/1 | Connect\_To\_EG1\_Gi0/3 | EG1 | Gi0/3 |
| R2 | Fa1/2 | Connect\_To\_EG2\_Gi0/3 | EG2 | Gi0/3 |
| R3 | Gi0/0 | Connect\_To\_S7\_Gi0/24 | S7 | Gi0/24 |
| R3 | Se3/0 | Connect\_To\_R2\_ Se3/0 | R2 | Se3/0 |
| R3 | Fa1/1 | Connect\_To\_EG1\_Gi0/4 | EG1 | Gi0/4 |
| R3 | Fa1/2 | Connect\_To\_EG2\_Gi0/4 | EG2 | Gi0/4 |

表2 ：网络设备名称表

|  |  |  |
| --- | --- | --- |
| 拓扑图中设备名称 | 配置主机名（hostname名） | 备注 |
| S1 | BX-VSU-Access-Switch | 本部接入交换机 |
| S2 | 本部接入交换机 |
| S3 | BX-Aggregation-Switch-01 | 本部的核心交换机 |
| S4 | BX-Aggregation-Switch-02 | 本部的核心交换机 |
| S5 | FX-Aggregation-Switch-01 | 分校接入交换机 |
| S6 | ZW-DataCenter-Switch-01 | 上海驻外办事处接入交换机 |
| S7 | ZW-DataCenter-Switch-02 | 杭州驻外办事处接入交换机 |
| R1 | ISP-Router-01 | 运营商服务网络接入路由 |
| R2 | ISP-Router-02 | 运营商服务网络接入路由 |
| R3 | ISP-Router-03 | 运营商服务网络接入路由 |
| AC1 | BX-Wireless-Switch-01 | 企业大学本部无线网络控制 |
| AC2 | BX-Wireless-Switch-02 | 企业大学分校无线网络控制 |
| EG1 | BX-Egress-Gateway-01 | 企业大学总部网关 |
| EG2 | FX-Egress-Gateway-01 | 北京分部出口网关 |
| AP1 | BX-Access-Point-01 | 本部与分校的无线接入点 |
| AP2 | BX-Access-Point-02 | 本部与分校的无线接入点 |
| AP3 | FX-Access-Point-01 | 本部与分校的无线接入点 |
| 备注：字母含义说明如下。其中，BX:本校；FX：分校；ZW：驻外；ISP：运营商。 | | |

表3：IPv4地址分配表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口或VLAN | VLAN名称 | 二层或三层规划(XX现场提供) | 说明 |
| S1 | VLAN10 | JXL | Gi0/1至Gi0/4 | 教学楼 |
| VLAN20 | SYL | Gi0/5至Gi0/8 | 实验楼 |
| VLAN30 | BGL | Gi0/9至Gi0/12 | 办公楼 |
| VLAN40 | TSG | Gi0/13至Gi0/16 | 图书馆 |
| VLAN50 | AP | Gi0/20至Gi0/21 | 无线AP管理 |
| VLAN100 | Manage | 192.XX.100.12/24 | 设备管理VLAN |
| S2 | VLAN10 | JXL | Gi0/1至Gi0/4 | 教学楼 |
| VLAN20 | SYL | Gi0/5至Gi0/8 | 实验楼 |
| VLAN30 | BGL | Gi0/9至Gi0/12 | 办公楼 |
| VLAN40 | TSG | Gi0/13至Gi0/16 | 图书馆 |
| VLAN50 | AP | Gi0/20至Gi0/21 | 无线AP管理 |
| VLAN100 | Manage | 192.XX.100.12/24 | 设备管理VLAN |
| S3 | VLAN10 | JXL | 192.XX.10.252/24 | 教学楼 |
| VLAN20 | SYL | 192.XX.20.252/24 | 实验楼 |
| VLAN30 | BGL | 192.XX.30.252/24 | 办公楼 |
| VLAN40 | TSG | 192.XX.40.252/24 | 图书馆 |
| VLAN100 | Manage | 192.XX.100.252/24 | 设备管理VLAN |
| Gi0/1 | Trunk | \ | AG1成员口 |
| Gi0/2 | Trunk | \ | AG1成员口 |
| Gi0/3 | Trunk | \ | \ |
| Gi0/4 | Trunk | \ | AG3成员口 |
| Gi0/5 | Trunk | \ | AG3成员口 |
| Gi0/24 | \ | 10.1.0.2/30 | \ |
| LoopBack 0 | \ | 11.1.0.33/32 | \ |
| S4 | VLAN10 | JXL | 192.XX.10.253/24 | 教学楼 |
| VLAN20 | SYL | 192.XX.20.253/24 | 实验楼 |
| VLAN30 | BGL | 192.XX.30.253/24 | 办公楼 |
| VLAN40 | TSG | 192.XX.40.253/24 | 图书馆 |
| VLAN100 | Manage | 192.XX.100.253/24 | 设备管理VLAN |
| Gi0/1 | Trunk | \ | AG2成员口 |
| Gi0/2 | Trunk | \ | AG2成员口 |
| Gi0/3 | Trunk | \ | \ |
| Gi0/4 | Trunk | \ | AG3成员口 |
| Gi0/5 | Trunk | \ | AG3成员口 |
| Gi0/23 | \ | \ | 云平台（备用） |
| Gi0/24 | \ | 10.1.0.6/30 | \ |
| LoopBack 0 | \ | 11.1.0.34/32 | \ |
| AC1 | LoopBack 0 | \ | 11.1.0.204/32 | \ |
| VLAN50 | AP | 192.XX.50.252/24 | 无线AP管理 |
| 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 | \ | 11.1.0.205/32 | \ |
| VLAN50 | AP | 192.XX.50.253/24 | 无线AP管理 |
| VLAN60 | Wiressless | 192.XX.60.253/24 | 无线用户 |
| Vlan100 | Manage | 192.XX.100.3/24 | 管理与互联VLAN |
| EG1 | GI0/0 | \ | 10.1.0.1/30 | \ |
| GI0/1 | \ | 10.1.0.5/30 | \ |
| GI0/2 | \ | 20.1.0.6/29 | \ |
| GI0/3 | \ | 30.1.0.6/29 | \ |
| GI0/4 | \ | 40.1.0.6/29 | \ |
| LoopBack 0 | \ | 11.1.0.11/32 | \ |
| LoopBack 1 | \ | 12.1.0.1/24 | \ |
| EG2 | GI0/0 | \ | 10.1.0.9/30 | \ |
| GI0/2 | \ | 20.1.0.14/29 | \ |
| GI0/3 | \ | 30.1.0.14/29 | \ |
| GI0/4 | \ | 40.1.0.14/29 | \ |
| LoopBack 0 | \ | 11.1.0.12/32 | \ |
| LoopBack 1 | \ | 12.1.0.2/24 | \ |
| S5 | Gi0/24 | \ | 10.1.0.10/30 | \ |
| VLAN10 | Primary\_vlan | 194.XX.10.254/24 | primary vlan |
| VLAN11 | Community\_vlan | Gi0/1至Gi0/4 | community vlan |
| VLAN12 | Isolated\_vlan | Gi0/5至Gi0/8 | isolated vlan |
| VLAN20 | AP | 194.XX.20.254/24 | 分校无线AP管理 |
| VLAN30 | Wiressless\_users1 | 194.XX.30.254/24 | 分校无线用户 |
| VLAN40 | Wiressless\_users2 | 194.XX.40.254/24 | 分校无线用户 |
| LoopBack 0 | \ | 11.1.0.5/32 | \ |
| AP3 | Gi0/1 | \ | DHCP动态获取 | \ |
| R1 | Gi0/0 | \ | 50.1.0.9/30 | \ |
| Se2/0 | \ | 50.1.0.1/30 | \ |
| VLAN10 | Con-EG1 | 20.1.0.1/29 | 成员口Fa1/1 |
| VLAN20 | Con-EG2 | 20.1.0.9/29 | 成员口Fa1/2 |
| LoopBack 0 | \ | 11.1.0.1/32 | \ |
| R2 | Se2/0 | \ | 50.1.0.2/30 | \ |
| Se3/0 | \ | 50.1.0.5/30 | \ |
| VLAN10 | Con-EG1 | 30.1.0.1/29 | 成员口Fa1/1 |
| VLAN20 | Con-EG2 | 30.1.0.9/29 | 成员口Fa1/2 |
| LoopBack 0 | \ | 11.1.0.2/32 | \ |
| R3 | Gi0/0 | \ | 50.1.0.13/30 | \ |
| Se3/0 | \ | 50.1.0.6/30 | \ |
| VLAN10 | Con-EG1 | 40.1.0.1/29 | 成员口Fa1/1 |
| VLAN20 | Con-EG2 | 40.1.0.9/29 | 成员口Fa1/2 |
| LoopBack 0 | \ | 11.1.0.3/32 | \ |
| S6 | VLAN10 | Develop | 60.1.10.254/24 | Gi0/1至Gi0/4 |
| VLAN20 | Product | 60.1.20.254/24 | Gi0/5至Gi0/8 |
| Gi0/24 | \ | 50.1.0.10/30 | \ |
| LoopBack 0 | \ | 11.1.0.6 | \ |
| S7 | VLAN10 | Develop | 70.1.10.254/24 | Gi0/1至Gi0/4 |
| VLAN20 | Product | 70.1.20.254/24 | Gi0/5至Gi0/8 |
| Gi0/24 | \ | 50.1.0.14/30 | \ |
| LoopBack 0 | \ | 11.1.0.7 | \ |
| PC机 | PC1 | \ | 自动获取 | 根据测试需求灵活调整终端位置及网段 |
| PC2 | \ | 自动获取 |
| PC3 | \ | 194.XX.10.1/24 |

# 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）根据总体规划内容，将所有的设备根据命名规则修订设备名称（表2 ：网络设备名称表），修订所有设备名称。

（2）依据设备的总体规划端口连接表，配置设备的接口描述信息表（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）在接入交换机S5做密码恢复，新的密码设置为admin1234。

（2）在接入交换机S5上进行版本更新至指定版本，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）在分校的无线接入AP3进行版本更新至指定版本，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）需要在交换机和无线控制器上开启SSH服务端功能。其中，用户名和密码均为admin；密码为明文类型；特权密码为admin。

（2）为路由器和出口网关开启Telnet功能，对所有Telnet用户采用本地认证的方式。创建本地用户的登录的用户名和密码均为admin；密码为明文类型；特权密码为admin。

（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，在分校S5交换机配置Private Vlan技术，优化IP地址资源。

（3）为隔离部分终端用户间的二层互访，在交换机S5的Gi0/1-Gi0/16端口启用端口保护。

（3）根据上述总体要求，并根据“表2：网络设备名称表”、“表3：IPv4地址分配表”中规划，在各台设备上完成相应VLAN信息、IP地址配置。

**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S1、S2上进行防环处理。具体要求如下所示。

（1）在连接PC机终端接口上，开启BPDU防护不能接收BPDU报文。

（2）在终端接口下开启RLDP防止环路，检测到环路后处理方式为Shutdown-Port。

（3）配置连接终端的所有端口配置为边缘端口；

（4）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。

（5）为了规避高流量报文风暴对网络的冲击，在交换机S5上针对用户终端接口的广播，组播，未知名单播启用风暴限制，限制级别2。

**3. 部署DHCP中继与服务安全**

在交换机S3、S4上配置DHCP中继，对VLAN10内的用户通过中继方式获取地址，使得本部PC1用户使用DHCP Relay方式获取IP地址。具体要求如下所示。

（1）DHCP服务器搭建于EG1上，地址池命名为Pool\_VLAN10。其中，DHCP对外服务使用loopback 0地址。

（2）为了防御动态地址获取的环境中，在局域网内部出现伪DHCP服务欺骗，在S1、S2交换机部署DHCP Snooping功能。

（3）为了防止大量网关发送的正常的相关报文，被接入交换机误认为是攻击被丢弃，从而导致下联用户无法获取网关的ARP信息而无法上网，要求关闭S1/S2上联口的NFPP功能。

（4）全局设置NFPP日志缓存容量为1024，打印相同log的阈值为300s。

（5）调整校本部中的交换机上“CPU保护机制”。其中，调整CPU保护机制中ARP阈值500pps。

（6）为了防止伪 IP 源地址攻击， 导致出口路由器会话占满，要求S5交换机部署端口安全，接口Gi0/1只允许PC3通过。

**4. 部署MSTP及VRRP技术，实现网络冗余。**

在本部交换机S1、S2、S3、S4上配置MSTP防止二层环路；要求所有有线数据流经过S3转发，S3失效时经过S4转发。

所配置的参数要求如下：

（1）region-name为ruijie。

（2）revision版本为1。

（3）S3作为实例中的主根， S4作为实例中的从根。

（4）主根优先级为4096，从根优先级为8192。

（5）在S3和S4上配置VRRP，实现主机的网关冗余，配置参数要求如表4。

（6）S3、S4各VRRP组中高优先级设置为150，低优先级设置为120。

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.XX.10.254 |
| VLAN20 | 20 | 192.XX.20.254 |
| VLAN30 | 30 | 192.XX.30.254 |
| VLAN40 | 40 | 192.XX.40.254 |
| VLAN100(交换机之间) | 100 | 192.XX.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，网络中S1和S2交换机之间通过网络设备虚拟化技术，配置成一台虚拟网络设备集中管理，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）规划S1和S2间的Te0/27-28端口作为VSL链路，使用VSU技术实现网络设备虚拟化。其中S1为主，S2为备。

（2）规划S1和S2间的Gi0/22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。

其中，需要配置主设备参数为：Domain id：1；switch id:1；priority 150； description: Access-Switch-Virtual-Switch1。

需要配置备设备参数为：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。**

本部与分校内网中均使用OSPF协议组网，实现全网的互联互通；此外，本部、分校与互联网之间使用静态路由协议实现连通。具体要求如下。

（1）本部网络中S3、S4、EG1、AC1、AC2设备之间运行OSPF，进程号为10，规划多区域。其中：区域0（S3、S4、EG1），区域1（S3、S4、AC1、AC2）。

（2）配置AC1、AC2的OSPF接口不参与DR/BDR选举。

（3）实现区域1部署为完全NSSA类型，进而简化AC1,AC2路由条目。

（4）分部的EG2、S5之间运行OSPF。其中，进程号为10，规划为单区域区域0（EG2、S5）。

（5）要求业务网段中不出现协议报文。

（6）要求所有路由协议都发布具体网段。

（7）为了管理方便，需要发布Loopback地址。

（8）优化OSPF相关配置，以尽量加快OSPF收敛。

（9）外部重发布路由进入OSPF路由中，使用类型1。

**7.总部和分部的机构之间，部署IPV6路由协议。**

（1）在总部与分校之间部署IPV6网络，实现总分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。

（2）在驻外办事处间，部署IPV6网络，实现办事处之的间IPV6业务终端互联互通。其中，IPV6地址规划如表5所示。

（3）在S3和S4上配置VRRP for IPv6，实现主机的IPv6网关冗余。

（4）在S3和S4上部署VRRP与MSTP主备状态，与IPV4网络保持一致。

（5）在AC1和AC2上部署的VRRP的主备状态，与AC热备状态保持一致。

（6）总部无线终端获取IPV6地址后通过静态路由部署实现总部无线与有线用户IPV6互联互通。

（7）驻外办事处S6/S7交换机之间，通过动态6to4隧道技术，实现办事处之间的局域网中安装的IPV6终端之间互联互通；并且，隧道内运行静态路由协议，业务网段以明细路由进行部署。

表5：IPV6地址规划表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | IPV6地址 | VRRP组号 | 虚拟IP |
| S3 | VLAN10 | 2001:192:10::252/64 | 10 | 2001:192:10::254/64 |
| VLAN20 | 2001:192:20::252/64 | 20 | 2001:192:20::254/64 |
| VLAN30 | 2001:192:30::252/64 | 30 | 2001:192:30::254/64 |
| VLAN40 | 2001:192:40::252/64 | 40 | 2001:192:40::254/64 |
| VLAN100 | 2001:192:100::252/64 | 100 | 2001:192:100::254/64 |
| S4 | VLAN10 | 2001:192:10::253/64 | 10 | 2001:192:10::254/64 |
| VLAN20 | 2001:192:20::253/64 | 20 | 2001:192:20::254/64 |
| VLAN30 | 2001:192:30::253/64 | 30 | 2001:192:30::254/64 |
| VLAN40 | 2001:192:40::253/64 | 40 | 2001:192:40::254/64 |
| VLAN100 | 2001:192:100::253/64 | 100 | 2001:192:100::254/64 |
| AC1 | VLAN60 | 2001:192:60::252/64 | 60 | 2001:192:60::254/64 |
| VLAN100 | 2001:192:100::2/64 | 110 | 2001:192:100::1/64 |
| AC2 | VLAN60 | 2001:192:60::253/64 | 60 | 2001:192:60::254/64 |
| VLAN100 | 2001:192:100::3/64 | 110 | 2001:192:100::1/64 |
| S5 | VLAN10 | 2001:194:10::254/64 | \ | \ |
| VLAN20 | 2001:194:20::254/64 | \ | \ |
| VLAN30 | 2001:194:30::254/64 | \ | \ |
| VLAN40 | 2001:194:40::254/64 | \ | \ |
| S6 | VLAN10 | 2001:195:10::254/64 | \ | \ |
| VLAN20 | 2001:195:20::254/64 | \ | \ |
| Tunnel0 | 自行计算，前缀64位 | \ | \ |
| S7 | VLAN10 | 2001:196:10::254/64 | \ | \ |
| VLAN20 | 2001:196:20::254/64 | \ | \ |
| Tunnel0 | 自行计算，前缀64位 | \ | \ |

**8. 运营商EGP路由协议部署。**

上海办事处与杭州办事处均有生产与研发部门，为了确保办事处之间，各业务部门的网络的互联互通，提升效率和质量。为此申请二级运营商专线业务，针对运营商组网及驻外办事处网络部署要求如下所示。

（1）在R1、R2、R3直连接口上封装PPP协议，部署IGP中OSPF动态路由实现直连网段之间互联互通。

（2）在S6、S7交换机上只配置直连路由，不使用任何路由协议。

（3）在R1、R2及R2、R3之间部署IBGP路由协议。其中：AS号为100, 使用Loopback接口建立Peer。

（4）部署R2路由器作为R1与R3路由器的路由反射器RR。

（5）在R1、S6互联设备上部署EBGP。其中，AS号为110，使用直连接口建立Peer。

（6）在R3、S7互联设备上部署EBGP。其中，AS号为120, 使用直连接口建立Peer。

（7）办事处业务网段通告至二级运营商的路由条目，只有一条汇总后的B段路由，且保证汇总后路径信息不丢失。

（8）二级运营商通告宽带业务接入网段至办事处，R1路由器通过汇总B段静态路由的方式进行发布。

**9.策略路由部署。**

北京的分校中不同业务部门，实现和上海与杭州驻外办事处有业务互访需求，具体要求如下所示。

（1）北京分校内网VLAN10终端，通过R1服务节点中转访问上海办事处。

（2）北京分校内网VLAN40终端，通过R3服务节点中转访问杭州办事处。

（3）当EG2与R1、R3服务节点间链路失效时，可自动切换到R2服务节点进行转发。

（4）配置Route-map策略名为Fenliu。其中：分校VLAN10流量由ACL101（编号101）来定义。分校VLAN40流量由ACL102（编号102）来定义。

（5）为加快广域网线路异常时，策略路由可快速收敛转发，为此部署Track检测。创建编号为Track1, Track2, Track3的策略，分别检测本端广域网联通，电信，教育网接口状态，一旦接口协议状态为DOWN，即刻进行切换。

**10. 在网络中部署路由选路。**

考虑到数据分流及负载均衡的目的，具体要求如下所示。

（1）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。

（2）本部有线IPV4用户与互联网互通主路径规划为：VSU-S3-EG1。

（3）本部无线IPV4用户与互联网互通主路径规划为：AC2-S4-EG1。

（4）主链路故障可无缝切换到多条备用链路上。

**11.在网络中部署QoS。**

为了防止突发数据过大并导致网络拥挤，必须对接入的用户流量加以限制。具体要求如下

（1）在本部接入设备S5的Gi0/1至Gi0/16接口的入方向上，设置接口限速，限速10Mbps,猝发流量1024 kbytes。

（2） 在二级运营商R3的服务节点的带宽为2Mbps的S3/0接口上，做流量整形。

（3）在二级运营商R3服务节点在G0/0接口做流量监管，上行报文流量不能超过10Mbps；Burst-normal为1M bytes；burst-max为2M bytes。如果超过流量限制，则将违规报文丢弃。

## （三）移动互联网搭建与无线网络优化

为满足互联网+时代下移动教学的发展趋势，促进校园信息化建设，本部校区与分校均需要规划和部署无线网络。同时，为保证不同学生利用无线安全、可靠的访问互联网，需要进行无线网络安全及性能优化配置，确保师生有良好的上网体验。

**1.无线网络基础部署。**

（1）在总部的网络中部署无线网络，使用AC1和AC2作为总部网络中的无线用户和无线AP的DHCP 服务器，使用S5交换机作为分校网络中的无线用户和无线AP的DHCP服务器。

（2）在总部的内网中创建SSID为admin-BX\_XX(XX现场提供)；WLANID 为1；AP-Group为BX。其中，本部内网中配置无线用户关联SSID后，即可自动获取地址。

**2.在无线网络部署AC热备。**

在总部的网络部署AC热备。其中，AC2为主用，AC1为备用。终端中的无线AP与AC1、AC2之间的连接均需建立隧道；当AP与AC2失去连接时，能无缝切换至AC1并提供服务。

**3.在无线网络部署胖AP热备。**

在北京校区使用胖AP无线模式进行部署，具体要求如下所示。

（1）AP3以透明模式进行部署，在S5交换机上配置DHCP服务器，为无线终端及AP分配地址；且AP每次均获取地址均为194.XX.20.2(XX现场提供)。

（2）在无线AP3上创建SSID(WLAN-ID 1)，配置相关的参赛信息 ：admin-BJ\_XX\_1(备注：XX现场提供)。其中，分校内网无线用户关联SSID后,可自动获取分校VLAN30网段地址。

（3）在无线AP3创建SSID(WLAN-ID 2) 为 ：admin-BJ\_XX\_2(备注：XX现场提供),分校内网无线用户关联SSID后,可自动获取分校VLAN40网段地址。

**4.在无线网络部署无线安全部署。**

（1）在总部网络中的无线用户接入无线网络时，需要采用WPA2加密方式，加密密码为XX(备注：XX现场提供)。

（2）在分部网络中的无线用户接入无线网络时，需要采用WEB认证方式，认证用户名为user1密码为XX(备注：XX现场提供)。

（3）在分部网络中，启用白名单校验，仅放通PC3无线终端。

**5.在无线网络中优化无线性能。**

（1）要求总部内网无线网络启用本地转发模式。

（2）为了保障总部每个用户的无线体验，针对WLAN ID 1下的每个用户，配置下行平均速率为 800KB/s，突发速率为1600KB/s。

（3）配置总部每AP最大带点人数为45人。

（4）配置总部通过时间调度，要求每周一至周五的21:00至23:30期间关闭无线服务。

（5）配置总部设置用户最小接入信号强度为-65dBm。

（6）配置总部关闭低速率（11b/g 1M、2M、5M，11a 6M、9M）应用接入。

## （四）实施出口安全防护与远程接入

本部校区与分校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。

**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）出口网关上进行NAT，配置实现本部与分校的所有用户，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）在本部EG1上配置，使本部核心交换S4（11.1.0.34）设备的SSH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20.1.0.2。

（3）本部内网主机有访问上海办事处S6设备的Telnet服务需求，但本部内网因网络规划要求不能引入外部路由。同时，上海办事处网络运维人员考虑安全需要，也不希望将S6设备（11.1.0.6）地址对外公布。为此，在出口网关上进行NAT地址转化，将S6真实地址映射至20.1.0.20。

**2.在出口设备上部署全局流表策略。**

在用户没有防火墙做限制的情况下，如果遇到大量的伪源IP攻击，或者是端口扫描时，会把设备的流表给占满，而导致正常的数据无法建流而被丢弃，为此要求总部部署全局流表防火墙，ACL（编号为102）策略要求如下。

（1）放通所有IP到本设备外网接口的ICMP、Telnet协议。

（2）放通内网终端IP到外网所有资源的访问。

（3）放通任意IP来访问映射的内网交换机的资源。

（4）根据上下文要求放通设备已启用的功能协议端口。

**3.在出口设备上部署Web Portal用户认证。**

（1）在本部网关上启用Web Portal认证服务，并创建user1、user2，密码均为XX（备注：XX现场提供）。

（2）本部有线用户需进行WEB认证访问互联网。

（3）本部无线用户不需在EG上进行WEB认证即可访问互联网。

**4.在出口设备上应用流量控制。**

在分校的出口网关EG2连接联通线路，针对访问外网WEB流量，限速每IP 1000Kbps，内网WEB总流量不超过50Mbps。

**5.在出口设备上部署用户行为策略。**

（1）分校EG2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。

（2）分校EG2周一到周五工作时间09：00-17:00（备注：命名为work）阻断并审计P2P应用软件使用。

（3）禁止分校内网用户通过浏览器访问http://40.1.0.9。

**6.在出口设备上部署数据分流与负载均衡。**

（1）实现本部与分校用户数据流，匹配EG中的内置联通、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。

（2）除联通、电信、教育资源之外，默认所有数据流在三条线路之间，进行负载转发。

（3）配置分校内的出口网关EG2设备，每天晚上6点到10点（备注：命名为Night）通过联通线路上网流量压力较大，可以将P2P应用软件流量在此时间段内引流到电信线路。

**7. 在出口设备上部署VPN安全。**

为了为了实现总部与分部互访数据的安全性，同时要求总部对分部路由器采用本地的用户名、密码方式进行验证，为此规划如下。

（1）部署L2TP隧道进行本部对分部路由的对接验证，验证用户名密码均为admin；L2TP隧道密码为admin。

（2）配置L2TP用户地址池为：12.1.0.1—12.1.0.254；Virtual-Template及Virtual-ppp接口均引用本地loopback 1接口地址。

（3）配置L2TP隧道中承载OSPF协议，使其总部与分部通过OSPF进行路由交互，区域号0。

（4）部署IPSec对L2TP隧道中的业务数据加密。其中：IPSec VPN需要采用传输模式、预共享密码为 admin；加密认证方式为 ESP-3DES；ESP-MD5-HMAC ，DH使用组2。

（5）总部网络和分部的机构之间，数据通信及加密通过二级运营商R1联通节点作为中转设备。

（6）本部有线IPV4用户与分部IPV4用户互通的主路径规划为：VSU-S3-EG1-EG2-S5(备注：EG1/EG2间运行VPN隧道)。

# 五．无线网络规划与实施

某CII教育集团公司最近在广州新租用了一栋楼层用于公司临时办公场所，由于原楼层未进行信息化改造，考虑到短期租用，公司建议通过部署无线来实现网络接入，用于采购无线设备的预算为11万。

## （一）无线网络业务背景及需求介绍

**1.业务背景及需求介绍。**

1.无线终端情况如下说明。

（1）办公室区域：有台式电脑、笔记本电脑、手机。

（2）部门办公区域：有台式电脑、笔记本电脑、手机。

（3）培训与会议区域：有台式电脑、手机。。

2.建筑现场情况介绍。

该楼宇是个回型建筑，中间是个回型空地，无吊顶，原有强电布线室内均采用了pvc线槽敷设。经了解培训室与会议室使用时都超过10人，走廊与厕所不需要实现覆盖。

3.建筑物弱电间情况介绍。

该楼宇有独立的弱电间，弱电间位于107房间，平面布局如图2所示。

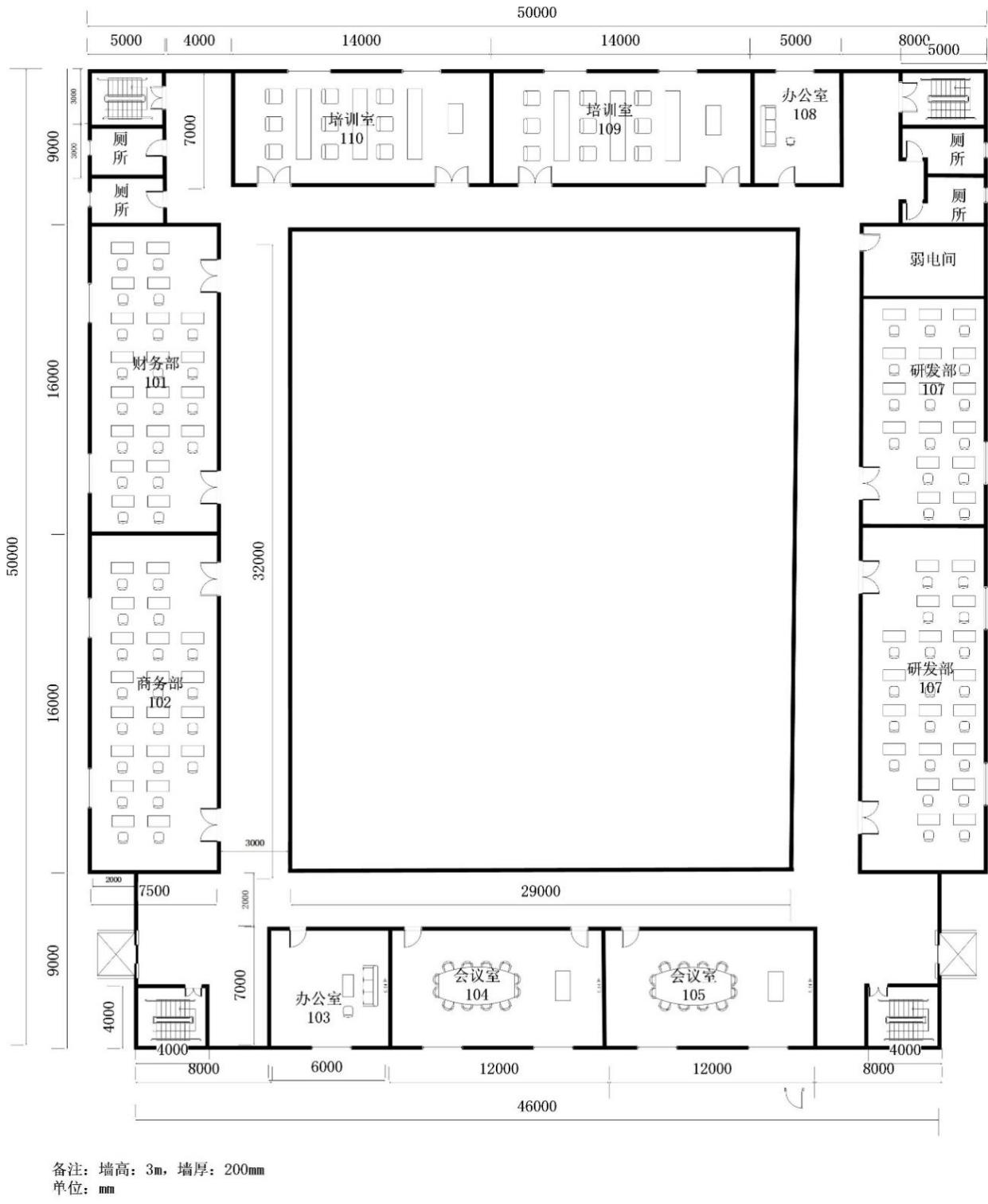


图2 平面布局图

**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。