信安专业2022年秋大作业（6选1）

一、IPv6校园网设计

（思科CPT、GNS3或华为eNSP）

1. 按照下面的拓扑图，组网连线。

实际应用中校园网涉及多个部门，本实验选择三个部门构建网络，一个教学部分，一个学生公寓部门，一个为数据中心，存放校园网WEB服务器；接入外网网段IP为202.204.100.0/24，部分IP地址已经给出，请你正确配置网络设备，选择合适的路由协议，保证内网所有PC机均能连通外网，也就是PC能ping通路由器Router1的串口地址，外网主机能够访问内部WEB服务器。

给出每个设备的配置命令，验证截图，撰写设计报告，并提交PKT文档。

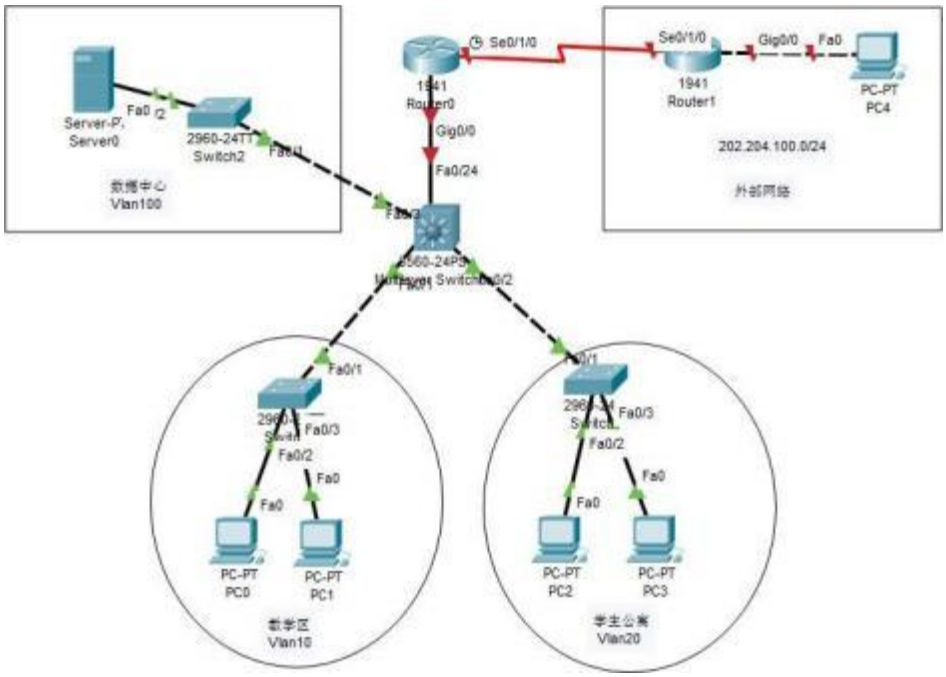


表 1　校园网设计设备餐卡地址

设备	端口	IP
三层交换机	教学区 VLAN10	192.168.10.0/24
三层交换机	学生公寓 VLAN20	192.168.20.0/24
三层交换机	数据中心 VLAN100	192.168.100.0/24
三层交换机	F 0/24	192.168.1.1/24
路由器 R0	Ge0/0	192.168.1.2/24
路由器 R0	Serial0/1/0	202.204.100.1/24
路由器 R1	Serial0/1/0	202.204.100.2/24
路由器 R1	Ge0/0	10.1.1.1/8

参照教材中给出的校园网案例，做出以下改动：

（1） 增加一个部门计通学院，校园内有4个部门：数据中心、教学区、学生公寓和计通学院；

（2） 在三层交换机上配置DHCP，实现教学区、学生公寓和计通学院3个部门的主机能够自动获取IP地址；

（3） 出口路由器同时配置静态NAT和动态NAT，静态NAT实现内部WEB服务器能够被外部主机访问，动态NAT实现内部主机能够访问互联网。

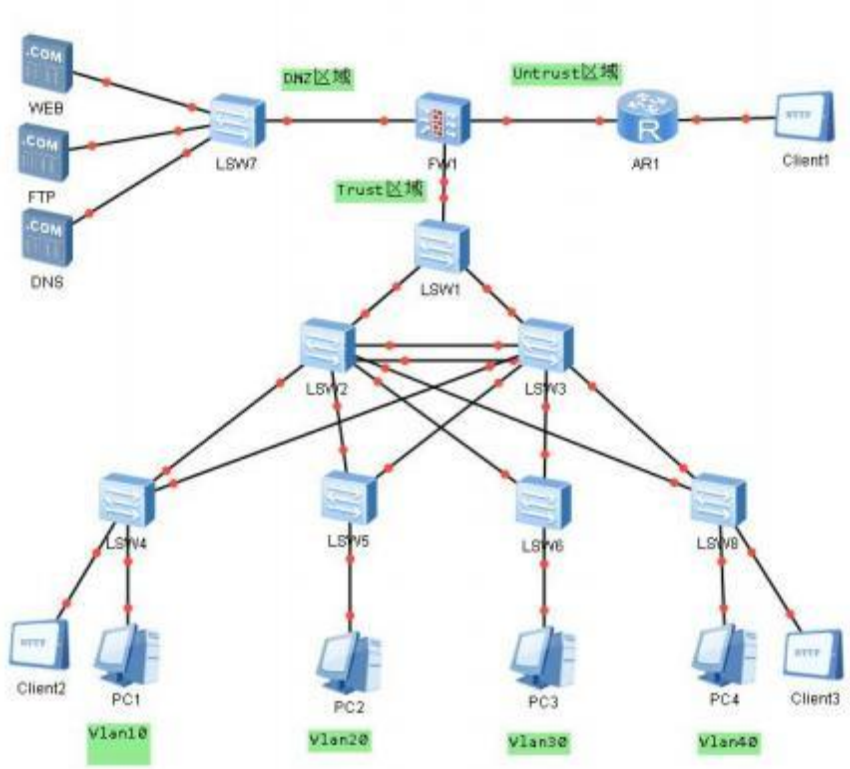
（4） 数据中心增加DNS服务器，实现校园网内部主机，能够通过域名访问WEB服务器

（5） 数据中心增加FTP服务器，实现校园网内部主机，能够访问FTP文件服务器，实现文件下载服务。

（6） 自行选择部分链路或部门分配IPv6地址，实现IPv4和IPv6在校园网中共存并且能通信，整个校园网也可以全部采用IPv6地址。

二、高可靠校园网设计

（思科GNS3或华为eNSP）



（1） 校园内有5个部门：数据中心Vlan100、教学区Vlan10、学生公寓Vlan20、计通学院Vlan30、机械学院Vlan40；

（2） 防火墙作为校园网的出口设备，防火墙上的3个端口分别连接DMZ、Trust和Untrust区域。防火墙上配置NAT和安全策略，使得内网WEB和FTP服务器能被外网主机访问，Trust区域能访问DMZ区域和外部网络。

（3） LSW2和LSW3之间配置链路聚合，提高可靠性。

（4） 交换机配置MSTP，创建两个实例（instance），LSW2是VLan10和Vlan30的主根，LSW3是Vlan20和VLan40的主根。

（5） 若采用华为eNSP，需配置虚拟路由冗余网关VRRP，主路由链路发生故障时，会自动启用备份路由。

（6） 数据中心配置WEB、FTP、DNS服务器，实现校园网内部主机能用域名访问WEB和FTP，外部网络能用IP地址访问WEB和FTP服务器。

（7） 若采用思科GNS3，可自行修改校园网设计图，出口路由器需配置路由热备份HSRP，实现负载均衡。

三、子网IP地址规划实验

（CPT、GNS3或eNSP）

某公司要建设自己网络，规划图如下图所示。公司网络分为内网和外网，内网又划分为多个区域：数据中心、销售部门、财务部门、研发部门等。公司采用三层交换机与网络服务商的路由器相连，三层交换机负责内部网络流量的转发，连接多个区域的二层交换机。公司从网络服务商处租用12个C类地址 202.204.100.1-12/24，已知网络服务商路由器外部接口地址202.204.100.2/24。

请给出设计方案，满足如下要求：

(1) 子网数目越多越好，每个子网代表一个部门，但每个子网的主机数大于30台；

(2) 所有用户都能上网，即要求所有主机都能 ping 通网络服务商路由器 Router2 的Se0/1/0 串口地址 202.204.100.2。

(3) **用同一个网络地址空间 192.168.1.0 为 VLAN10-40 分配相应地址**，子网内最小的 IP地址作网关。子网内 2 台PC，IP 地址分别设置为最小（网关除外）和最大。

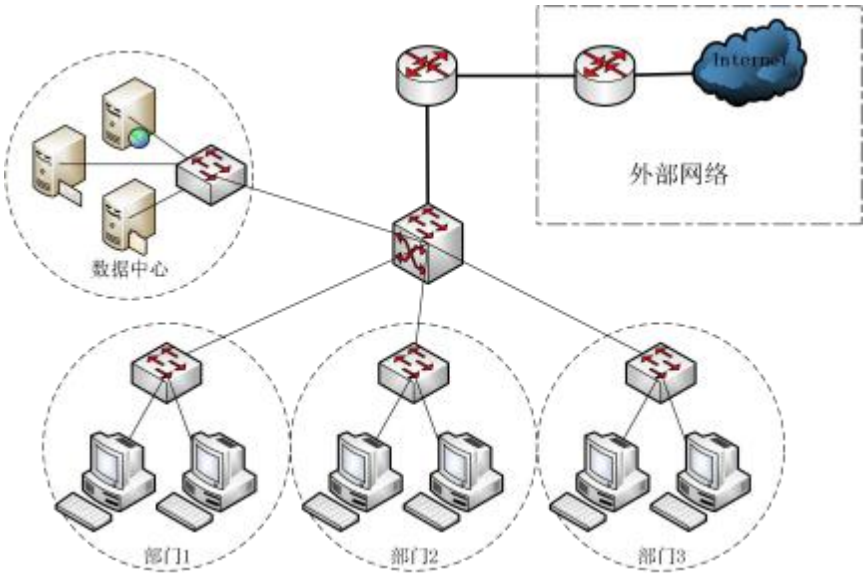
(4) 采用合适的路由（静态、RIP、OSPF），实现网络的连通性。

(5) 本实验考察IP地址的规划能力，首先确定子网的数目，确定子网可用IP地址段，完成表3，然后再配置交换机和路由器。

(6) 数据中心配置WEB、FTP、DNS服务器，使得内网主机能用域名访问WEB服务器，外部主机能用IP地址访问WEB服务器。

表 3 子网划分详细地址规划

VLAN ID	网络二进制位取值	主机二进制位取值	IP 范围	掩码	网关	主机可用 IP 段
10						
20						
30						
40						



四、RIP路由设计实验

（推荐GNS3或eNSP平台，从下面5个测试中选择4个完成）

（思科CPT功能简单，不支持认证配置，不支持抓包，所以采用华为的模拟器，需要自己学习华为的指令。eNSP也支持text文档粘贴）

（1）RIPv1 与 RIPv2 区别（自行设计拓扑图，结合 Wireshark 抓包至少给出 3 个方面的比较）。

（2）RIPv2 认证（自行设计拓扑图，给出 2 种配置方式，明文认证和密文认证）。RIPv1 不支持链路认证，RIPv2 支持链路认证，可以在路由器接口上启用 RIP 认证，有 2 种认证模式，明文认证和 MD5 认证，默认为明文认证；需要注意 RIP 不需要建立邻居关系，其认证是单向的，R1 认证了 R2，R2 为被认证方，R1 就可以接收 R2 发来的路由信息；反之，R1 没有认证 R2 时，R1 不会接收 R2 发来的路由信息。

（3）RIP 解决环路问题-水平分割：指的是 RIP 从某个接口接收到的路由信息，不会从该接口在发回给邻居设备，这样不但减少了宽带消耗，还可以防止路由环路；默认是开启的。

[R1-GigabitEthernet0/0/1]undo rip split-horizon　关闭水平分割；（默认开启）

（4）RIP 解决环路问题-毒性逆转：RIP 从某个接口接收到路由信息后（端口断开），将该路由的开销设置为 16，并从原接口发回邻居设备；利用这种方式，可以清除对方路由表中的无用路由，如果同时配置了毒性逆转和水平分割，则会选择毒性逆转，毒性逆转默认是关闭的。

[R2-GigabitEthernet0/0/1]rip poison-reverse　　开启毒性逆转；（默认关闭）

（5）RIP解决环路问题-触发更新：正常情况下，路由器30秒更新一次报文，当路由信息发生变化时，触发更新是指运行rip的设备会立即向邻居设备发送更新报文，而不必等待定时30秒更新；缩短了收敛时间。

五、OSPF路由设计实验

（推荐eNSP平台，自行设计1个案例，从下面5个选题中选择2个完成）

（思科CPT功能简单，不支持认证配置，不支持抓包，所以采用华为的模拟器，需要自己学习华为的指令。eNSP也支持text文档粘贴）

表 2 OSPF中LSA类型

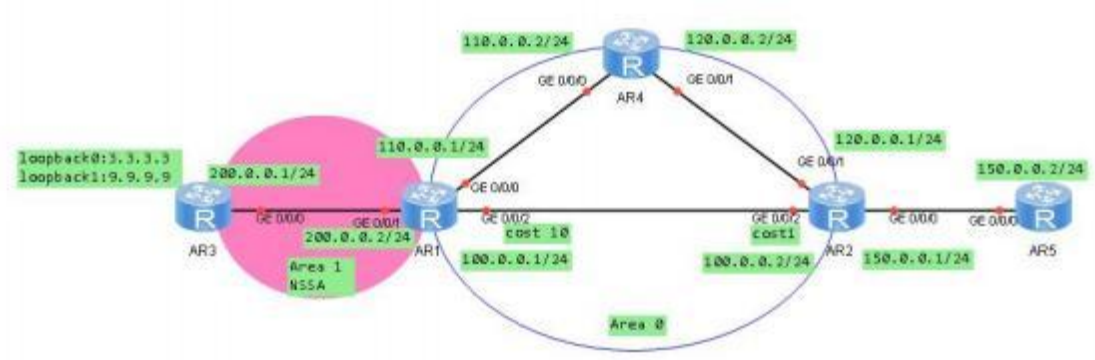
LSA 类型	描述
1	每个路由器都会发出的 1 种基本的 LSA，描述路由器的连接状态，只在区域内部传输。
2	网络 LSA：多路访问的网络中，DR 发出的 LSA，描述网络的状态信息，只在区域内传输。
3	汇总 LSA：ABR 发出的 LSA，向其他区域通告本区域的路由信息，在自治系统内部的所有区域中传输。
4	ASBR 汇总 LSA，由 ASBR 所在区域的 ABR 发出，用于向整个自治系统内部的路由器通告 ASBR 的可达性。
5	自治系统外部 LSA：ASBR 注入的自治系统外部的路由信息，此类 LSA 将传递到整个自治系统所有的区域。
7	NSSA 外部 LSA：NSSA 特殊区域内 ASBR 注入的外部路由信息。

1. OSPF认证

OSPF协议支持两种认证模式：区域认证和链路认证。区域认证，要求区域内所有设备的认证模式和密钥必须一致；链路认证，相对比较灵活，可专门针对某个邻居设置认证模式和密钥。每种认证模式下，针对加密方式的不同，又分为：明文认证、MD5加密认证、Keychain认证和Hmac-md5。明文认证，认证密钥采用明文传输，有被截获泄露的风险存在；MD5加密认证，密钥是经过MD5算法加密后传输，安全性较高；Key chain认证模式下，可以配置多个密钥，不同密钥设置不同的生效周期，安全性更高；Hmac-md5认证，可以确保通信双方交互的信息不会被篡改，增加了身份认证的技术手段，安全性也比较高。

自行设计拓扑图，实现区域认证和链路认证，采用2种以上加密方式。

2. NSSA特殊区域



(1) 修改部分端口的开销值，验证cost如何影响选路，R3选择哪条路径到达R2。

(2) 在Area0区域，了解DR和BDR选举过程。

(3) 在R3上配置2个回环接口，3.3.3.3和9.9.9.9不在OSPF宣告的范围内，R3引入直连路由，命令为：

[R3]ospf 1

[R3]import-route direct

在R1上查看路由表，验证R1是否学习到3.3.3.3和9.9.9.9网段？

(4) R1上抓取LSA报文，分析5种常见LSA报文并指名是谁发出的，type1（route-LSA），type2（network-LSA），type3（network summary-LSA），type4（Asbr summary-LSA），type5（As external LSA）。

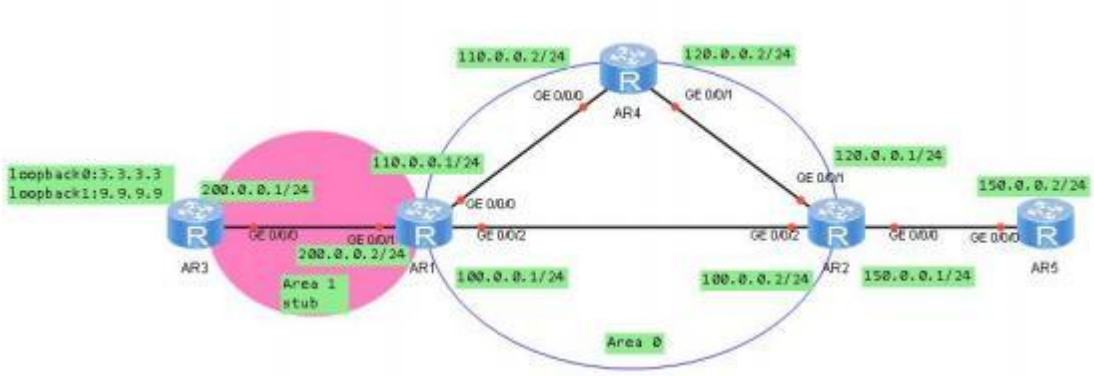
(5) 总结NSSA区域路由特点:

nssa（非完全末梢区域），默认路由是7类lsa

nssa 区域可以对外重发布路由，type7->type5

nssa 收不到type4,type5，可以收到type1,2,3

3. STUB特殊区域



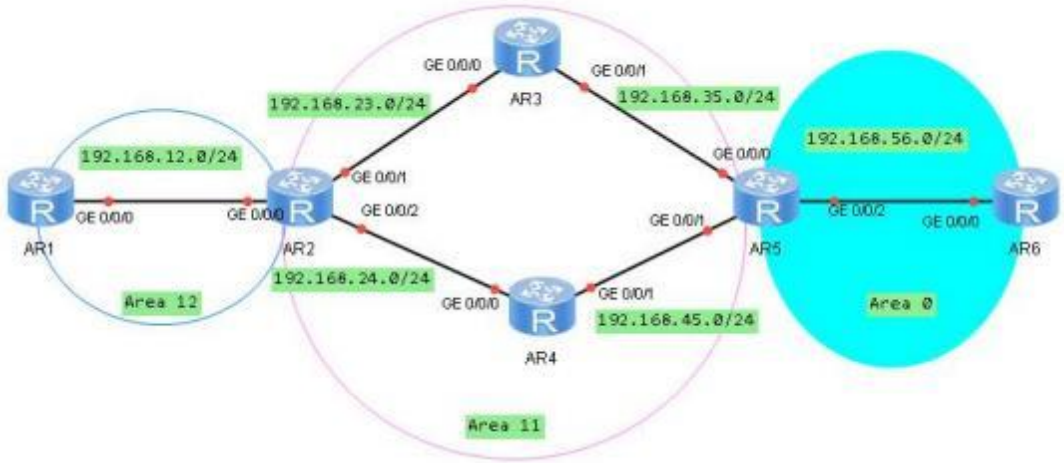
(1) Area1作为末梢区域，验证R3无法import引入外部路由。

(2) Area1作为末梢区域，R3无法学习到type4，type5路由。

(3) Area1作为末梢区域，R3可以通过abr学习到一条默认路由，以及type1，type2，type3路由。

(4) Area1如果是完全末梢区域，type3明细路由R3也学习不到。

4. OSPF虚链路

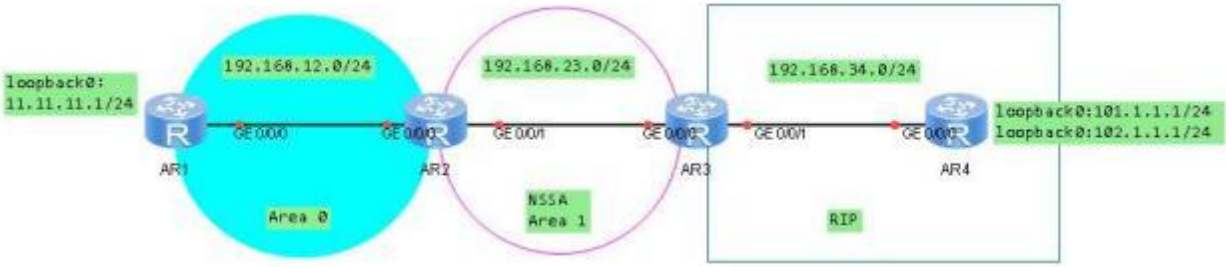


(1) 为每台路由器设置Router ID，R1的Router ID为1.1.1.1，R6的Router ID为6.6.6.6.

(2) 非骨干区Area12没有与骨干区Area0直接相连，验证R5能否学习到192.168.12.0/24网段？

(3) 正确配置虚链路，使得R5能学习到192.168.12.0/24网段。

5. OSPF特殊区域NSSA



(1) 为每台路由器设置Router ID，R1的Router ID为1.1.1.1，R4的Router ID为4.4.4.4。

(2) 在R1上配置1个回环接口，地址为11.11.11.1/32，R1在OSPF进程下，引入直连路由，命令为：

[R1]ospf 1

[R1]import-route direct

(3) 使得R2通过ospf能学习到11.11.11.0/24网段。

(4) 在R3和R4开启RIP路由，101.1.1.0和102.1.1.0网段在RIP路由范围内。

(5) 在R3上进行路由重分发，单点双向重分发，RIP重分发到OSPF，OSPF也重分发到RIP。

(6) 将Area10 区域改为NSSA区域，分别在R1、R2、R3上查看路由表，并截图，比较Area10 和NSSA区域前后的路由表变化，注意标识“O E2”和“ON2” 的改变。

(7) 在R2左右两侧分别抓包，分析LSA报文，找到5类LSA和7类LSA。

六、路由重分发

针对路由重分发，自行设计3-4个案例，有单点单向，单点双向，双点双向，重点研究一下双点双向重分发，路由协议包含RIP、OSPF、BGP、EIGRP、IS-IS等。