

# 2016 年全国职业院校技能大赛

## 网络搭建与应用 中职组

### 一、评分标准制定原则、评分方法、评分细则

#### （一）评分标准的制定原则

竞赛评分严格按照公平、公正、公开的原则，评分标准注重考察参赛选手以下三个方面的能力和水平：

1. 网络系统组建、配置与应用、安全配置与防护的正确性、规范性和合理性；
2. 相关文档的准确性与规范性；
3. 团队风貌、团队协作与沟通、组织与管理能力；

#### （二）评分方法：过程性评分

1. 参赛队成绩由裁判委员会统一评定；
2. 评分流程：根据参赛队伍（选手）在分步操作过程中的规范性、合理性以及完成质量等，评分裁判依据评分标准按步给分并加权汇总的评分方法。流程如下：

①参赛队伍（选手）按比赛要求进行操作，评分裁判对照评分表即时判分。每模块评分裁判 2 人，结果取平均分；

②两名记分员在监督人员的现场监督下，对参赛队伍（选手）的评分结果进行分步汇总并计算平均分，所有步骤成绩的加权汇总值作为该参赛队伍（选手）的最后得分；

③裁判长当天公布评分结果，并由裁判长、监督人员和仲裁

人员签字后确认；

④在竞赛过程中，参赛选手如有不服从裁判判决、扰乱赛场秩序、舞弊等不文明行为的，由裁判长按照规定扣减相应分数，情节严重的取消比赛资格，比赛成绩记0分。

### （三）评分细则

序号	具体内容		分值及评分细则
1	网络配置 50%	网络综合布线安装和施工	完成设备连接,保证和测试物理连通性
2		IP地址划分实施	完成子网划分、IP规划实施
3		网络调试	完成指定的交换路由、广域网和无线的配置
4		硬件防火墙配置	完成企业网的相关策略配置
5		WEB应用安全	完成对web应用防火墙的安装和策略配置
6		网络配置优化	完成网络优化配置
7		无线网络安全技术	完成无线网络安全配置
8	系统配置管理 50%	操作系统安装(Windows/Linux)	完成操作系统的安装和配置
9		配置常用服务(Windows/Linux)	能够熟练安装配置各类应用服务、系统管理和数据库安装调试
10		服务器虚拟化 服务器集群	掌握虚拟化技术,使用服务器集群技术
11		操作系统安全技术	掌握操作系统方面安全技术配置

基于竞赛保密性的考虑，竞赛详细评分细则结合竞赛试题由竞赛执委会和命题专家共同制定。

#### 附：主要竞赛知识点和技能点

序号	内容模块	具体内容	说明
1	网络基本配置	网络综合布线安装和施工	综合布线基础：设备安装、网络布线、设备连接、端口标识、电源接入；物理连通性检测、链路质量（基于GB50312-2007）检测、端口检测等
2		IP地址划分实施	VLSM、CIDR等

3		交换基本配置	VLAN、STP、RSTP、MSTP、802.1X、交换安全、端口聚合、端口镜像、VRRP 等
4		路由基本配置	静态、RIP、OSPF 等路由协议、NTP、DHCP、TELNET、策略路由等
5		无线配置	设置、分配、接入、开通等
6		广域网配置	PPP、NAT、NAPT 等
7	服务器配置与管理	操作系统安装 (Windows/Linux)	能够熟练安装操作系统，并能对操作系统进行安全配置和应用管理
8		配置常用服务 (Windows/Linux)	能够根据企业的应用需求，熟练安装和配置 AD、DNS、WEB、FTP、E-MAIL、DHCP、代理等常用服务并进行数据库配置与管理
9		服务器虚拟化 服务器集群	能够熟练掌握虚拟化技术完成特定环境配置；使用服务器集群技术来实现网络的负载均衡
10		操作系统安全技术	WINDOWS SERVER 域安全配置、文件系统安全配置、权限管理、配置 CA 服务、系统防火墙防护等
11	网络安全与网络优化	防火墙配置	能够在企业网络中部署防火墙，使用防火墙规则保护内网服务安全，在防火墙上实现路由、NAT 转换、防 DDOS 攻击；实现包过滤、URL 过滤、P2P 流量控制等
12		网络优化	利用 ACL、QOS 等配置，实现网络优化
13		VPN 技术	利用 VPN 实现远程安全接入和站点到站点的 IPSEC VPN 等
14		无线网络安全与优化	配置无线网络 WEP 加密、MAC 认证接入控制等；配置二层漫游、三层漫游、无线桥接（点对点）、负载均衡等、无线桥接（点对多点），信道自动调整
15		WEB 应用安全	WEB 攻击防护、一体化防篡改、网站监测技术、拒绝攻击防护、智能 APP 防护

## 二、建议使用的比赛器材、技术平台和场地要求

### （一）网络设备竞赛器材（硬件平台）

序号	设备名称	设备型号 (神州数码)	数量	备注
1	路由器	DCR-2655	3	沿用往届设备
2	路由器线缆	CR-V35MT-V35FC	3	沿用往届设备

3	三层交换机	DCRS-5650-28	2	沿用往届设备
4	光纤模块	SFP-SX-L	4	
5	二层交换机	DCS-3950-28C	2	沿用往届设备
6	多核防火墙	DCFW-1800E-N3002	1	设备升级，配置与老设备相同
7	安全网关	DCFW-1800S-H-V2	1	沿用往届设备
8	web 应用防火墙	DCFW-1800-WAF-LAB	1	新设备
9	无线交换机	DCWS-6028	1	沿用往届设备
10	无线接入点	WL8200-I2	3	新设备，配置与老设备相同
11	POE 模块	DCWL-PoEINJ-G+	1	沿用往届设备
12	PC 机	CPU 主 频>=3.5GHZ, >=四核 心 八线程 内存>=8G 硬盘>=1T 支持硬件虚拟化	4	

## （二）软件技术平台：

主要为比赛的应用系统环境提供的操作系统软件和办公软件，操作系统主要由 Windows 系统和 Linux 系统两部分组成，软件主要为 Microsoft Office 和解压缩工具等。

Windows 系统平台主要由服务器版和桌面版组成，桌面版主要采用 Windows 7(中文版)，服务器版主要采用 Windows 2008 Server(中文版)、Windows 2012 Server(中文版)；Linux 系统平台主要采用 Centos 6.5 服务器版本；办公软件的版本为 Microsoft Office 2010(中文版)。

具体软件参数如下所示：

1. 微软 Windows 7（中文版） 试用版；
2. Centos 6.5（32 位+64 位）；
3. WINRAR 5.21(中文版) 试用版 ；
4. 微软 Microsoft Office 2010(中文版) 试用版；

5. 微软 Windows Server 2008 (中文版) 试用版;
6. 微软 Windows Server 2012 (中文版) 试用版;
7. 数据库软件 MySQL Enterprise Edition 试用版本;
8. Oracle VM Virtual Box 4.3.12 免费版;
9. SecureCRT;
10. VMware vSphere 5.5 60 天试用版;
11. 存储模拟软件 openfileresa-2.99.1 开源软件;

# 2016 年全国职业院校技能大赛

## 网络搭建与应用竞赛样题

(总分 1000 分)

---

---

### 竞赛时间

竞赛时间为 180 分钟。

### 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所有设备需要通过文档的方式保存，把所有网络设备的配置保存为 TXT 文件，名称与设备名称一致，防火墙中图形界面操作步骤需要截图保存。并将所有文档保存至桌面 BACKUP 文件夹中，若缺少文件，涉及到该文件对应设备下的所有分值记为 0 分。

⑦竞赛结果文件电子版需要按照监考老师的要求，在竞赛结束前复制到监考老师提供的 U 盘进行保存。

⑧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，文档中有对应题目的小标题，截图有截图的简要说明，否则按无效内容处理。

## 项目简介

某集团公司经过业务发展，总公司在北京市，在上海设置了分公司，为了实现快捷的信息交流和资源共享，需要构建统一网络，整合公司所有相关业务流程。采用单核心的网络架构的网络接入模式，采用路由器接入城域网专用链路来传输业务数据流。总公司为了安全管理每个部门的用户，使用 VLAN 技术将每个部门的用户划分到不同的 VLAN 中。分公司采用路由器接入互联网络和城域网专用网络，总公司的内网用户采用无线接入方式访问网络资源。

为了保障总公司与分公司业务数据流传输的高可用性，使用防火墙进行保证网络安全，采用 QOS 技术对公司重要的业务数据流进行保障。网络采用 OSPF 动态路由协议和 RIP 动态路由协议。

拓扑结构图

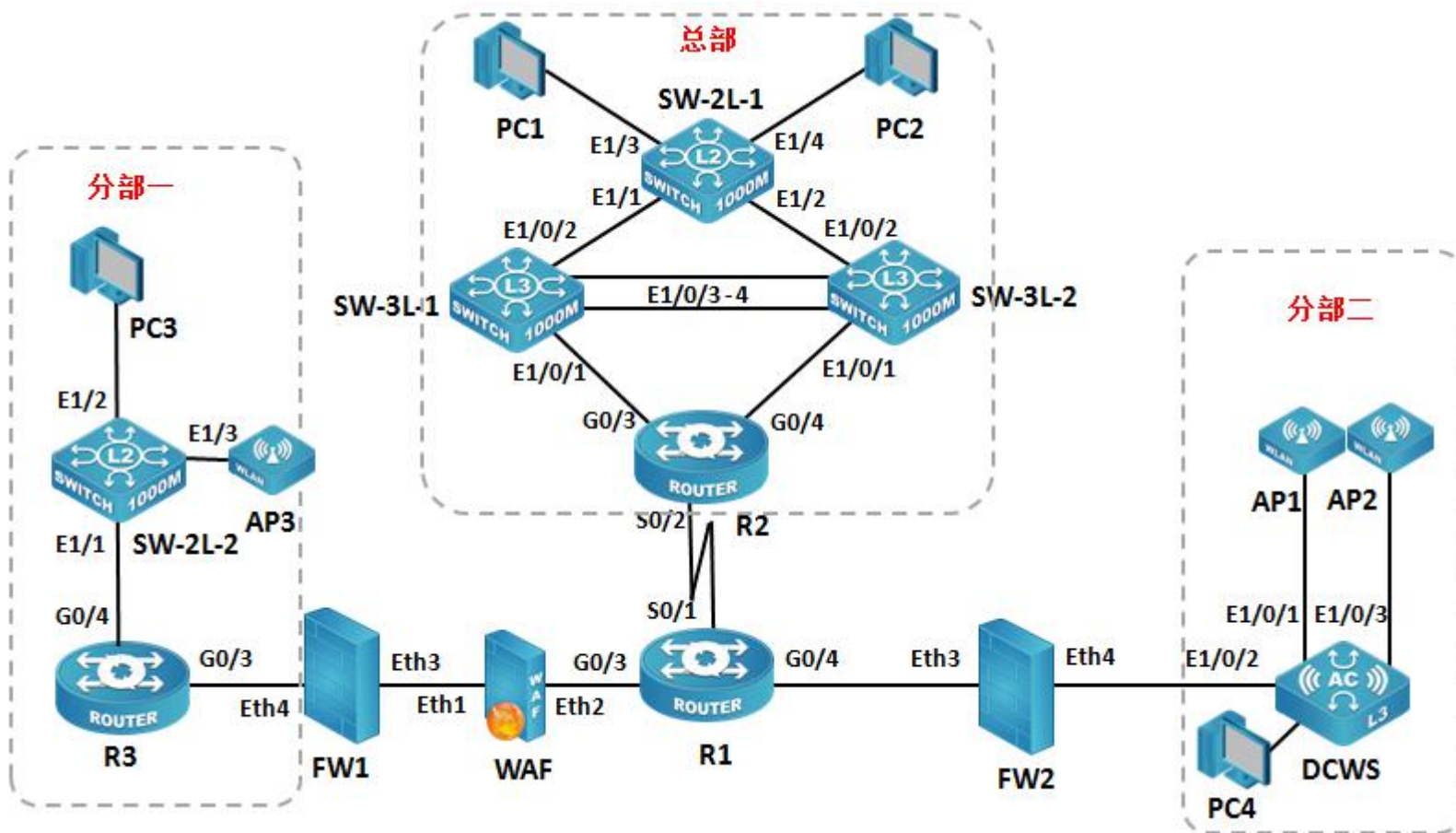




表 1 网络设备连接表

A 设备连接至 B 设备			
设备名称	接口	设备名称	接口
R1	G 0/3	WAF	Eth 2
R1	G 0/4	FW2	Eth 3
R1	S 0/1	R2	S 0/2
R2	G 0/3	SW-3L-1	E 1/0/1
R2	G 0/4	SW-3L-2	E 1/0/1
R3	G 0/3	FW1	Eth 4
R3	G 0/4	SW-2L-2	E 1/1
DCWS	E 1/0/2	FW2	Eth 4
DCWS	E 1/0/1	AP1	
DCWS	E 1/0/3	AP2	
WAF	Eth 1	FW1	Eth 3
WAF	Eth 2	R1	G 0/3
SW-3L-1	E 1/0/3	SW-3L-2	E 1/0/3
SW-3L-1	E 1/0/2	SW-2L-1	E 1/1
SW-3L-2	E 1/0/4	SW-3L-2	E 1/0/4
SW-3L-2	E 1/0/2	SW-2L-1	E 1/2
PC1	NIC	SW-2L-1	E 1/3
PC2	NIC	SW-2L-1	E 1/4
PC3	NIC	SW-2L-2	E 1/2
PC4	NIC	DCWS	E 1/0/4

表 2. 网络设备 IP 地址分配表

表 2 网络设备 IP 地址分配表

设备	设备名称	设备接口	IP 地址
路由器	R-1	G 0/3	200.201.1.1/30
		G 0/4	200.200.2.1/30
		S 0/1	200.200.3.1/30
		Loopback0	200.200.200.200/32
	R-2	G 0/3	10.10.10.1/30
		G 0/4	10.10.10.5/30
		S 0/2	200.200.3.2/30
	R-3	G 0/3	10.10.10.10/30
G 0/4		_____	
三层交换机	SW3-1	VLAN10 SVI	192.168.10.1/24
		VLAN20 SVI	192.168.20.1/24
		VLAN30 SVI	192.168.30.1/24
		VLAN40 SVI	192.168.40.1/24
		VLAN 1 SVI	10.10.10.2/30
	SW3-2	VLAN10 SVI	192.168.10.2/24
		VLAN20 SVI	192.168.20.2/24
		VLAN30 SVI	192.168.30.2/24
		VLAN40 SVI	192.168.40.2/24
		VLAN 1 SVI	10.10.10.6/30
防火墙 1	FW-1	Eth3	200.200.1.2/30
		Eth4	10.10.10.9/30
防火墙 2	FW-2	Eth3	200.200.2.2/30
		Eth4	10.10.100.0/24
WAF	WAF	Eth1	200.200.1.1/30
	WAF	Eth2	200.201.1.2/30
无线控制器	DCWS	E1/0/24	10.10.100.200/24

表 3. 服务器 IP 地址分配表

宿主机	虚拟主机名称	域名信息	服务角色	系统及版本信息	IPv4 地址信息
Server 1	Win2008-A1	dc. 2015Network.com	域控制器 DNS 服务器 CA 证书服务器	Windows Server 2003 R2	IP: 192.168.1.1
	Win2012-A1	dhcp. 2015Network.com	DHCP 服务器	Windows Server 2008 R2	IP: 192.168.1.2
	Centos-A1	smb. jnds.net	SAMBA 共享服务器	Centos 6.5	IP: 192.168.1.3
Server 2	Win2012-B2	nps. 2015Network.com	FTP 服务器 RADIUS 服务器	Windows Server 2008 R2	IP: 192.168.1.4
	Centos-B1	raid. jnds.net	逻辑卷及磁盘阵列服务	Centos 6.5	IP: 192.168.1.5
	Centos-B2	ftp. jnds.net ftp1. jnds.net ftp2. jnds.net	FTP 文件服务器	Centos 6.5	IP: 192.168.1.105 IP: 192.168.1.106 IP: 192.168.1.107
Server 3	Win2008-C2	tj. 2015Network.com	子域控制器	Windows Server 2003 R2	IP: 192.168.1.6
	Centos-C1	dns. jnds.net	BIND 域名服务器	Centos 6.5	IP: 192.168.1.109
Server 4	Centos-D1	dns. jnds.net	MySQL	Centos 6.5	IP: 192.168.1.161

# 竞赛题目

## 网络搭建部分（300分）

### 1、物理连接与 IP 地址划分（50分）

- (1) 按照网络拓扑图制作以太网网线，并连接设备。要求符合 T568A 和 T568B 的标准，其线缆长度适中。（30分）
- (2) 根据“拓扑结构图”和“表 2:网络设备 IP 地址分配表”所示，对网络中的所有设备接口配置 IP 地址。（20分）

### 2、交换机配置（90分）

- (1) 为交换机设备命名，命名规则参考为表 1 中的“设备名称”。（5分）
- (2) 在两台三层交换设备上开启 telnet 管理功能，同时要求每台网络设备只允许 5 条线路管理网络设备,管理设备使用 2015DCN 做为用户名,口令为 telnet123, enable 密码为 pwd@dcn。（10分）
- (3) 根据需求完成 vlan;（10分）
- (4) 总部的交换网络中，有 4 个 VLAN; 财务部使用 VLAN10，名字为 CW，生产部使用 VLAN20，名字为 SC，销售部使用 VLAN30，名字为 XS，技术部使用 VLAN40，名字 JS;
- (5) 分部一的交换网络中，共 2 个 VLAN，分别为 VLAN100、VLAN200;
- (6) 按下表要求将端口加入 VLAN:

设备名称	VLAN	端口
SW-2L-1	10	E 1/3
	20	E 1/4
	30	E 1/5 - 6
	40	E 1/7 - 8
SW-2L-2	100	E 1/2
	200	E 1/3

- (7) 使用端口汇聚技术,在 SW-3L-1 与 SW-3L-2 之间的链路启用端口汇聚,汇聚接口为动态方式,要求 SW-3L-1 为主动端,负载分担方式基于源、目的地 MAC 及 IP 地址。(15 分)
- (8) 配置生成树协议,要求启用 MSTP 协议, name 为 2015DCN, revision-level 1,
- 实例 1 中包括 VLAN10、20;实例 2 中包括 VLAN30、40;要求 SW-3L-1 为实例 1 的主根, SW-3L-2 为实例 2 的主根,并互为备份根(10 分)
- (9) 在三层交换机上启用路由功能,实现 VLAN 间互通。(10 分)
- (10) 在三层交换之间启用 VRRP 协议,为 VLAN、10、20、30、40 实现网关备份,组地址为该 VLAN 中的最后一个可用 IP,SW-3L-1 为 VLAN10、20 的 master; SW-3L-2 为 30、40 的 master,且互为备份,开启抢占功能(20 分)
- (11) 为 PC1 双向流量进行分析,网络分析仪将安装在 SW-2L-1 的 Ethernet1/20 接口下,请把相应流量映射给 Ethernet1/20 接口。(10 分)

### 3、 路由器配置与调试 (80 分)

- (12) 为路由设备命名,命名规则参考为表 1 中的“设备名称”。(5 分)

(13) 把下面的设备 RID 设置上，要求不能增加接口的相关信息。(5 分)

设备名称	RID
R-2	2.2.2.2
SW-3L-1	5.5.5.5
SW-3L-2	6.6.6.6

- (1) R2、SW-3L-1、SW-3L-2 三台设备运行 OSPF，实现内外互通，并在 R2 下发默认路由 (20 分)
- (2) 在 R3 配置单臂路由，实现 VLAN100、200 互通 (10 分)
- (3) FW1、R3 之间运行 RIPv2 路由协议，并在 FW1 下发默认路由 (20 分)
- (4) 在 R3 连接 FW2 的端口上进行端口限速，限制速率上行 2000Kbps，下行 1000Kbps (20 分)

#### 4、广域网配置 (50 分)

- (1) 总部网络允许 VLAN10、VLAN20、VLAN30、VLAN40 的用户通过源 NAT 访问外网，类型为端口 NAT。(20 分)
- (2) 分别在 FW1、FW2 上配置 NAT，实现内外访问外网。(20 分)
- (3) R-1 与 R-2 间并采用 PPP 封装，PAP 认证方式，R1 主认证方，用户名称为 DCN001 名称，密码：123456。(10 分)

#### 5、无线配置 (30 分)

- (1) 无线控制器建立 1 个 SSID,SSID 为 DCN01SSID 设置为隐藏，工作信道为自动；使用无线控制器提供 DHCP 服务，动态分配 IP 地址和网关，DNS

地址为：202.106.0.20，其分配的地址段为自行计算，需要排除网关，地址租约为2天。（10分）

- (2) AP1 与 AP2 配置无线漫游，实现 AP1 与 AP2 信道合理分配（10分）；
- (3) 为了控制带宽，保证正常使用，配置连接 AP1 的用户上行速度为2Mbps，下行速度为 5Mbps； AP2 上的用户配置二层隔离；（5分）
- (4) AP3 建立 1 个 SSID,SSID 为 DCNguest，开放给来访用户使用，不认证加密；（5分）

## 服务器架设（450 分）

拓扑图中共有四台物理计算机，每台物理计算机使用 VirtualBox 安装 2 个虚拟计算机，按照地址规划中安装相应服务，具体要求如下所述：

### Windows 操作系统部分（200 分）

#### 【说明】

（1）题目中所涉及 Windows 操作系统的 administrator 管理员以及其他普通用户密码均为 2015Netw1rk（注意区分大小写），若未按照要求设置密码，涉及到该操作的所有分值记为 0 分。

（2）虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

（3）除非作特殊说明，在同一主机下需要安装相同操作系统版本的虚拟机时，可采用 Oracle VM VirtualBox 软件自带的克隆系统功能实现。

（4）所有系统镜像文件及试题所需的其它软件均存放在每台主机的 D:\soft 文件夹中，并将题目要求的截图内容以.jpg 格式存储于桌面 BACKUP 文件夹中。

（5）题目要求的虚拟机均安装于每台主机的 D:\virtualPC 目录，即路径



为 D: \virtualPC\虚拟主机名称。

(一) 在 **Server 1** 上完成如下操作:(本题 **95** 分)

**1、完成虚拟主机的创建(30 分)**

1) 安装虚拟机 “Win2008-A1”，具体要求为内存为 **1G**，硬盘 **20G**,网卡为桥接模式；虚拟机分区分别为 C、D、E；主分区一个，容量 **10G**；扩展分区为 **10G**，两个逻辑分区分别为 **5G**。(10 分)

2) 在虚拟机 “Win2008-A1” 中添加 **ISCSI** 控制器，再添加三块 **ISCSI** 虚拟硬盘，其每块硬盘的大小为 **5G**；制作成一个 **RAID-5** 卷，磁盘盘符为 **F:\**。(10 分)

3) 安装虚拟机 “Win2012-A1”，具体要求为内存为 **1G**，硬盘 **20G**，并将该虚拟机加入到域中。(10 分)

**2、在主机 Win2008-A1 中完成域控制器的部署 (55 分)**

1) 将在虚拟机 “ Win2008-A1 ” 配置为主域控制器。域名为 **2015Network.com**，NetBIOS 域名为 **2015Network**，服务器的 FQDN 为 **2015Network. 2015Network.com**，域的功能级别为 **2003** 模式。同时，该服务器为 **DNS** 服务器，负责解析 **2015Network.com** 域名。实现 **DNS** 转发功能。(10 分)

2) 创建 4 个全局组，分别为 **group1**，**group2**，**group3**，**group4**，每个

组都创建 2 个用户，依次分别为 **manager1/uer1**、**manager2/uer2**、**manager3/uer3**、**manager4/uer4**，用户的初始密码为“用户名+1”，用户首次登录时须更改密码。采用复杂密码，密码长度最小为 8 位，密码最长存留其为 15 天，帐户锁定阈值为 2 次，如果到过阈值需要锁定 15 分钟。(10 分)

3) 设置文件服务器，根据组的不同，在 **RAID5** 卷中建立 4 个共享文件夹，文件夹的名字分别为 **group1- group4**，共享权限设置为：其他组的成员仅可以浏览，本组的 **user** 可以上传文件，本组的 **manager** 具有完全控制权。所有的 **manager** 在该 **RAID5** 卷中的使用空间为 **1G**，超过 **800M** 报警；**user** 使用空间为 **500M**，超过 **400M** 报警。(10 分)

4) 制定备份计划，每周一的午夜 0 点对活动目录进行正常备份，每周二至周五的午夜 0 点对活动目录进行增量备份，并将备份放置在 **RAID5** 卷中。(5 分)

5) 配置组策略，要求所有域内计算机“关闭自动播放”，所有用户不能使用 **media player** 软件，而部门经理和总经理除外。(10 分)

6) 在此域控制器上安装证书 **CA** 服务，并要求能够通过 **WEB** 申请证书。(10 分)

### **3、在主机 Win2012-A1 中完成 DHCP 服务器的部署（10 分）**

安装 **DHCP** 服务，为内网的用户主机动态分配 **IPv4** 地址，建立作用域，作用域的名称采用对应 **VLAN** 的名称，超级作用域的名称为 **DHCPSEVER**，为用户分配网关、**DNS** 服务器及域名；此后将 **DHCP** 服务管理器有关超级作用域内

容展开并截图存储为 dhcp.jpg; (10 分)

(二) 在 **Server 2** 上完成如下操作: (本题 55 分)

**1、完成虚拟主机的创建(5 分)**

1) 安装虚拟机 “Win2012-B1”, 其内存为 1G, 硬盘 20G, 将服务器加入至 Windows 域中; (5 分)

**2、在主机 Win2012-B1 中完成 RADIUS 服务器的部署 (30 分)**

1) 安装 RADIUS 服务, 配置此服务器为 RADIUS 服务器, 为网络提供 RADIUS 认证; (20 分)

2) 为了保障安全策略数据传送的安全性, 需要对 RADIUS 服务器与域控制器服务器之间的数据传输采用 IPsec 方式加密; 并在命令提示符中键入 netsh ipsec static show policy all( 后将输出截图并存储为 ipsec.jpg; (10 分)

**3、在主机 Win2012-B1 中完成 FTP 服务器的部署 (20 分)**

1) 域名为 [ftp.2015Network.com](http://ftp.2015Network.com), 端口号为 2121, 只有内网用户才能访问 FTP 站点。要求站点主目录为 e:\ 2015Network.com, 允许匿名登录, 只能下载文件; 使用 FTP 命令登录时, FTP 站点欢迎消息为: “欢迎访问 FTP 服务器!” ,日志文件记录到 c:\ftproot\LogFiles 目录下。(20 分)

(三) 在 **Server 3** 上完成如下操作: (本题 50 分)

**1、完成虚拟主机的创建(10 分)**

1) 在虚拟机“Win2008-C1”，其内存为 1G，硬盘 20G，并将服务器加入到 Windows 域环境；(5 分)

## 2、在主机 Win2008-C1 中完成子域控制器的部署 (40 分)

1) 配置此服务器为 2015Network.com 域的子域控制器，子域名 tj.2015Network.com，为并要求与父域建立双向的信任关系；(20 分)

2) 为了保障域数据传送的安全性，需要对父域控制器服务器与子域控制器服务器之间传输数据时，采用 IPSec 加密的方式进行传输；(20 分)

## Linux 操作系统部分（250 分）

### 【说明】

1、所有 Linux 操作系统的 root 用户的密码为 123456，若未按要求设置密码，涉及到该操作系统下的所有分值记为 0 分。

2、虚拟主机的 IP 属性设置请按照网络拓扑结构图以及“表 3：服务器 IP 地址分配表”的要求设定。

3、除有特别规定外，其他未明确规定用户密码均与用户名相同。

4、所有操作系统镜像文件及试题所需的其他软件均存放于每台计算机的 D:\soft 文件夹中。

5、题目要求的虚拟机均安装于每台主机的 D: \virtualPC 目录，即路径为 D: \virtualPC\虚拟主机名称。

一、在 **Server 1** 上完成如下操作: (本题 60 分)

(一) 完成虚拟主机的创建(10 分)

1、安装虚拟机“Centos-A1”,具体要求为内存 768MB,硬盘 20GB; 分区大小为: SWAP 分区大小为 1024M; /boot 分区大小为 500M, 文件类型为 ext4; /根分区大小为 8G, 文件类型为 ext4; /home 分区大小为 3G, 文件类型为 ext4。

(10 分)

(二) 在主机 **Centos-A1** 中完成 **Samba** 共享服务器的部署 (50 分)

1、在此服务器中安装配置 Samba 服务,创建四个用户 user1, user2, user3, manager, user1 和 user2 属于 finance 组, user3 属于 sales 组, manager 属于 manager 组。(10 分)

2、建立共享目录 /opt/finance\_share, /opt/sales\_share, /opt/public\_share。(5 分)

3、finance 组的用户对目录 finance 共享有读写权限。sales 组的用户对目录 sales\_share 共享有读写权限, 目录 public\_share 允许所有人只读权限。manger 对所有目录均有读写权限。要求新建立的文件的权限是用户本身有完全权限, 其它所有用户只有读取权。在 linux 系统和 WINDOWS 中能用 SAMBA 的共享打印机。(10 分)

4、将目录/opt/public\_share 共享, 共享名为 share, 创建用户 Tonny, 此用户不具有登陆系统功能, 允许所有用户访问 public\_share, 具有读取和写入权限, 无论是什么用户登录这个共享目录, 在共享目录中建立的文件都是 Tonny 的。(10 分)

5、能够共享 samba 的计算机必须在 192.168.20.0/24 网段中。开机自启动 samba, 并且在每周 2、5 的零点重启 samba 服务。(15 分)

**二、在 Server 2 上完成如下操作: (本题 90 分)**

**(一) 完成虚拟主机的创建 (10 分)**

1、安装虚拟机“Centos-B1”,具体要求为内存 512MB, 硬盘 10GB; (5

分)

2、安装虚拟机“Centos-B2”,具体要求为内存 512MB,硬盘 10GB; (5 分)

(二) 在主机 **Centos-B1** 中完成磁盘管理的部署(55 分)

1、在“Centos-B1”中额外添加 5 块硬盘，容量分别为 2G; (10 分)

2、此操作需要 3 块硬盘，以前两块硬盘为基础建立冗余阵列 RAID1; 要求每周 5 晚 24 点系统自动将第三块硬盘作为热备盘加入到 RAID1 中实现阶段性数据备份; (20 分)

3、此操作需要 1 块硬盘，通过格式化建立两个主分区以及一个逻辑分区，利用这三个分区建立条带卷，要求条带容量为 16K，条带卷容量为 300M，并挂载到本地系统根目录下自建的 disk1 文件夹，且要求实现开机自动挂载; (15 分)

4、此操作需要 1 块硬盘，通过格式化建立两个主分区以及一个逻辑分区，创建一个逻辑卷。逻辑卷命名为 engineering，属于卷组 vol，且大小为 10 个扩展; 在卷组 vol 的逻辑卷每个扩展的大小为 32MiB; 使用 vfat 格式化这个新的逻辑卷，此逻辑卷在系统启动的时候应该能自动挂在到/mnt/engineering. (10 分)

(三) 在主机 **Centos-B2** 中完成 FTP 服务器的部署 (25 分)

1、Linux 服务器提供网站服务，现采用提供虚拟主机基于域名 ftp.jnds.net 的 FTP 服务，实现对网站 www.jnds.net 维护的功能。(5 分)

2、为网站管理员创建一个 FTP 帐户 **webmaster**，将其加入到 **ftp** 组中，其登录的主目录为 **WEB** 站点的主目录 **/var/www/jnds.net**，设置其为系统帐户，但却没有登录系统的权限，备注该用户为“**FTP User**”。(10 分)

3、利用该帐户登录后，可对 **WEB** 站点根目录及其子目录下的文件进行上传、下载、创建子目录、更名和删除操作，用户只能对自己的 **WEB** 站点根目录及其下面的目录文件操作，不允许切换到上级目录，不允许匿名用户登录和访问。(10 分)

### 三、在 **Server 3** 上完成如下操作：(本题 50 分)

#### (一) 完成虚拟主机的创建 (10 分)

1、安装名为“**Centos-C1**”的虚拟机，具体要求为硬盘大小为 **12GB**，内存为 **768MB**，系统为 **Centos6.5**。分区大小为：**SWAP** 分区大小为 **1024M**；**/boot** 分区大小为 **500M**，文件类型为 **ext4**；其余为 **/**分区，文件类型为 **ext4**；(10 分)

#### (二) 在主机 **Centos-C1** 中完成 **BIND** 域名服务器及系统基本配置。(40 分)

1、在此服务器中安装配置 **bind** 服务，负责区域“**jnds.net**”内主机解析，五台主机分别为 **dns.jnds.net**、**www.jnds.net**、**bbs.jnds.net**、**smb.jnds.net**、**ftp.jnds.net** 以及 **mail.jnds.net**，做好正反向 **DNS** 服务解析，对访问 **jnds.net**



域的解析转发给 Win2008\_A1; (20 分)

2、为用户提供域名解析禁止 ip 为 192.168.20.251 的机器解析。(5 分)

3、新建目录 /tmp/jnds，配置该目录的权限。复制文件 /etc/fstab 到 /tmp/jnds。配置 /tmp/jnds/fstab 权限。文件 /var/tmp/fstab 所有者是 root，属于 root 组，文件 /var/tmp/fstab 不能被任何用户执行，用户 sunny 可读和可写 /tmp/jnds/fstab，用户 mike 既不能读也不能写 /tmp/jnds/fstab，所有其他用户对 /tmp/jnds/fstab 目录有只读权限。(15 分)

四、在 Server 4 上完成如下操作：(本题 50 分)

(一) 完成虚拟主机的创建(10 分)

1、安装名为“Centos-D1”的虚拟机，具体要求为硬盘大小为 30GB，内存为 4096MB，分区大小为：SWAP 分区大小为 4096M；/boot 分区大小为 500M，文件类型为 ext4；/home 分区大小为 20G，文件类型为 ext4，其余为 / 分区，文件类型为 ext4；(15 分)；系统为 Centos6.5。  
(10 分)

(二) 在主机 Centos-D1 中完成 MySQL 数据库服务器的部署 (40 分)

1、采用 MySQL 数据库作为认证来源，创建用户认证数据库为 www，建立保存用户名及密码的表名为 users，建立 web1 以及 web2 两个用户，将其密码均设置为 6666，并对密码采用 password 函数加密，表结构如下；(50 分)

字段名	数据类型	主键	自增
-----	------	----	----

ID	int	是	是
Name	varchar(10)	否	否
birthday	datetime	否	否
Sex	char(1)	否	否
Password	Char (8)	否	否

## 安全策略部分 (250 分)

### 1、 防火墙配置 (40 分)

- (1) FW1 禁止访问 [www.taobao.com](http://www.taobao.com) (10 分)
- (2) FW2 为了保证带宽的正常使用,限制 P2P 应用的下行带宽最高为 10M。  
(10 分)
- (3) FW1 限制 VALN100、200 的用户仅在工作日(周一到周五, 9: 00-18: 00) 允许访问网络。(20 分)

### 2、 Web 安全防护配置 (40 分)

- (1) 阻止常见的 WEB 攻击数据包访问到公司内网服务器。(10 分)
- (2) 防止某源 IP 地址在短时间内发送大量的恶意请求,影响公司网站正常服务。大量请求的确认值是: 10 秒钟超过 3000 次请求。(10 分)
- (3) 对公司网站进行安全评估,检查网站是否存在安全漏洞,便于在攻击没有发生的情况下提前做出防护措施。(10 分)

- (4) 禁止 HTTP 请求和应答中包含敏感字段“暴力”的报文经过 WAF 设备。  
(10 分)

### 3、 网络配置优化 ( 60 分 )

- (1) 为了增加设备管理安全性, R2、R3 上开启 SSH 方式登录, SSH 登录用户分别为 R2SSH 和 R3SSH, 密码为 Network2015 (注意区分大小写) (30 分)。
- (2) 限制 R2 的 SSH 登陆, 仅允许 IP 地址为 192.168.10.10 的用户登录。(30 分)

### 4、 VPN 技术应用 ( 100 分 )

- (1) FW1 与 FW2 配置 IPSec VPN 的方式 进行互联。要求使用隧道模式, 数据加密算法采用 3DES、认证算法采用 md5 (100 分)。

### 5、 无线网络安全 ( 10 分 )

- (1) AP1 用户接入无线网络时需要输入密码, 加密模式为 wpa-personal, 其口令为: chinaskill; AP2 用户接入无线网络时需要输入密码, 加密模式为 TKIP-personal, 其口令为: dcn12345 (5)
- (2) 阻止 MAC 地址为 F0-DE-F1-F2-8C-CC 的主机连接的无线网络。(5 分)