

习题答案

项目 1 安装和卸载 Windows Server 2003

一、填空题

1. Windows Server 2003 Web 版、Windows Server 2003 标准版、Windows Server 2003 企业版、Windows Server 2003 数据中心（Data Center）版
2. FAT、FAT32、NTFS NTFS
3. 每服务器
4. 128MB 1.5GB
5. winnt32 /s:F:\i386 /unattend:a:\unattend.txt setupmgr.exe

二、选择题

1. C
2. D
3. B

三、简答题

1. 简述 Windows Server 2003 各版本的特点。

（1）Windows Server 2003 Web 版

Web 版是专为用作 Web 服务器而构建的操作系统。

（2）Windows Server 2003 标准版

标准版是为小型企业和部门使用而设计的，其可靠性、可伸缩性和安全性能满足小型局域网构建的要求，基本功能包括文件共享、打印共享和 Internet 共享等。标准服务器支持最大 4GB 的内存，支持 4 路的对称多处理器，但是不支持服务器的集群。

（3）Windows Server 2003 企业版

企业版是为满足大中型的企业需要而设计的，有 32 位和 64 位两个版本。企业服务器除了包括标准服务器的全部功能外，还有更强大的功能，支持 8 路的对称多处理器。32 位和 64 位两个版本都支持 64GB 的内存，还支持服务器的集群。

（4）Windows Server 2003 数据中心（Data Center）版

数据中心版是功能最强大的版本，是应企业需要运行大负载、关键性应用而设计的，具有强大的可伸缩性、可用性和高度的可靠性，有 32 位和 64 位两个版本。

2. 简述如何构建一个安全的 Windows Server 2003 系统。

- （1）安装杀毒软件。
- （2）设置自动更新。
- （3）定期手动更新安装补丁。

项目 2 组建 WINDOWS SERVER 2003 对等网

一、填空题

1. 对等式网络 (peer-to-peer)、客户服务器网络 (Client/Server)
2. 包括协议、客户和服务
3. 硬件资源、软件资源
4. \$
5. 完全控制、更改、读取。
6. ×
7. 1.5

二、简答题

1. 简述工作组和域的区别。

(1) 工作组 Work Group

在一个网络内，可能有成百上千台电脑，如果这些电脑不进行分组，都列在“网上邻居”内，可想而知会有多么乱。为了解决这一问题，Windows 9x/NT/2000/2003 就引用了“工作组”这个概念，将不同的电脑一般按功能分别列入不同的组中，如财务部的电脑都列入“财务部”工作组中，人事部的电脑都列入“人事部”工作组中。你要访问某个部门的资源，就在“网上邻居”里找到那个部门的工作组名，双击就可以看到那个部门的电脑了。

那么怎么加入工作组呢？其实很简单，你只需要右击你的 Windows 桌面上的“网上邻居”，在弹出的菜单中选择“属性”，点击“标识”，在“计算机名”一栏中添加你想好的名字，在“工作组”一栏中添加你想加入的工作组名称。

如果你输入的工作组名称以前没有，那么相当于新建一个工作组，当然只有你的电脑在里面。计算机名和工作组的长度不能超过 15 个英文字符，可以输入汉字，但是不能超过 7 个。“计算机说明”是附加信息，不填也可以，但是最好填上一些这台电脑主人的信息，如“技术部主管”等。单击[确定]按钮后，Windows 98 提示需要重新启动，按要求重新启动之后，再进入“网上邻居”，就可以看到你所在工作组的成员了。

一般来说，同一个工作组内部成员相互交换信息的频率最高，所以你一进入“网上邻居”，首先看到的是你所在工作组的成员。如果要访问其他工作组的成员，需要双击“整个网络”，就会看到网络上所有的工作组，双击工作组名称，就会看到里面的成员。

你也可以退出某个工作组，只要将工作组名称改动即可。不过这样在网上别人照样可以访问你的共享资源，只不过换了一个工作组而已。你可以随便加入同一网络上的任何工作组，也可以离开一个工作组。“工作组”就像一个自由加入和退出的俱乐部一样，它本身的作用仅仅是提供一个“房间”，以方便网上计算机共享资源的浏览。

(2) 域 Domain

与工作组的“松散会员制”有所不同，“域”是一个相对严格的组织。“域”指的是服务器控制网络上的计算机能否加入的计算机组合。

实行严格的管理对网络安全是非常必要的。在对等网模式下，任何一台电脑只要接入网络，就可以访问共享资源，如共享 ISDN 上网等。尽管对等网络上的共享文件可以加访问密码，但是非常容易被破解。在由 Windows 9x 构成的对等网中，数据是非常不安全的。

在“域”模式下，至少有一台服务器负责每一台联入网络的电脑和用户的验证工作，相当于一个单位的门卫一样，称为“域控制器 (Domain Controller, 简称为 DC)”。“域控制器”中包含了由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当电脑联入网

络时，域控制器首先要鉴别这台电脑是否是属于这个域的，用户使用的登录账号是否存在、密码是否正确。如果以上信息不正确，域控制器就拒绝这个用户从这台电脑登录。不能登录，用户就不能访问服务器上有权限保护的资源，只能以对等网用户的方式访问 Windows 共享出来的资源，这样就一定程度上保护了网络上的资源。

想把一台电脑加入域，仅仅使它和服务在“网上邻居”能够相互看到是远远不够的，必须要由网络管理员进行把这台电脑加入域的相关操作。操作过程由服务器端设置和客户端设置构成。

① 服务器端设置

以系统管理员身份在已经设置好 Active Directory（活动目录）的 Windows Server 2003 上登录，点击“开始/程序/管理工具/Active Directory 用户和计算机”，在程序界面中右击“computers”（计算机），在弹出的菜单中单击“新建/计算机”，填入想要加入域的计算机名即可。要加入域的计算机名最好为英文，否则系统会提示中文计算机名可能会引起一些问题。

② 客户端设置

首先要确认计算机名称是否正确，然后在桌面“网上邻居”上右击鼠标，点击“属性”出现网络属性设置窗口，确认“主网络登录”为“Microsoft 网络用户”。

选中窗口上方的“Microsoft 网络用户”（如果没有此项，说明没有安装，点击[添加]安装“Microsoft 网络用户”项）。点击[属性]按钮，出现“Microsoft 网络用户 属性”对话框，选中“登录到 Windows NT 域”复选框，在“Windows NT 域”中输入要登录的域名。

Windows 98 会提示需要重新启动计算机，重新启动后，会出现一个登录对话框。在输入正确的域用户账号、密码以及登录域之后，就可以使用 Windows Server 2003 域中的资源了。请注意，这里的域用户账号和密码，必须是网络管理员为用户建的那个账号和密码，而不是由本机用户自己创建的账号和密码。如果没有将计算机加入域，或者登录的域名、用户名、密码有一项不正确，就会出现错误信息。

2. 安装一个新的设备通常需几个步骤？

安装一个新的设备通常需 3 个步骤：

- （1）把设备连接在计算机上；
- （2）安装适当的设备驱动程序；
- （3）配置设备的属性。

3. Windows Server 2003 中集成的防火墙有什么用处？

防火墙可以阻止网络中的其他计算机对本地计算机的主动访问，保护本地计算机上的资源，不妨碍本地计算机对其他计算机的主动访问。

4. 为什么要有驱动程序的数字签名？

驱动程序是设备在 Windows 下能够正常工作的保证，不同的设备厂家都会提供 Windows 下的驱动程序，微软为了保证这些驱动程序一定和 Windows 兼容，会对被微软认可的驱动程序进行数字签名。对于那些没有获得微软签名的驱动程序，微软不推荐使用。这样将会最大限度保护计算机及网络的安全。

5. 用户配置文件和硬件配置文件各有何作用？用在什么场合？

（1）用户配置文件

用户配置文件是存储当前桌面环境、应用程序设置以及个人数据的文件夹和数据的集合，还包括所有登录到某台计算机上所建立的网络连接。由于用户配置文件提供的桌面环境与用户最近一次登录到该计算机上所用的桌面相同，因此就保持了用户桌面环境及其他设置的一致性。

主要用在需要为用户配置一致的桌面环境及其他设置的情况。

（2）硬件配置文件

计算机有多种多样的硬件,某一时候需要启用一些硬件而禁用另一些硬件;在另一时候,又需要禁用不同的硬件。这种情况下可以使用硬件配置文件,硬件配置文件记录了各种硬件设备的资源、驱动程序、启用或者禁用的状态等。可以针对每一种工作需要建立一个硬件配置文件,当系统启动时选择预先设置好的硬件配置文件即可。

主要用在快速切换不同的工作环境情况下。

项目 3 管理活动目录与用户

一、填空题

1. 域、域控制器
2. DCPROMO
3. 活动目录
4. 平等、双向可传递的、活动目录
5. 域控制器、独立服务器、成员服务器
6. 本地账户、域账户、内置账户
7. 本地组 域组
8. 非域控制器的“本地安全账户数据库 (SAM)”、域控制器的活动目录数据库 (SAM)

二、选择题

1. C
2. C

三、判断题

1. √ 2. √ 3. √ 4. × 5. √ 6. √ 7. × 8. √

四、简答题

1. 什么时候需要安装多个域树?

当网络中有多个域名,而这些域名的名字不连续的时候,如一个是 ab.com,另一个是 cd.com,要为每个域建立一个域树。

2. 简述什么是活动目录、域、活动目录树和活动目录林。

什么是活动目录呢?活动目录就是 Windows 网络中的目录服务。所谓目录服务,有两方面内容:目录和与目录相关的服务。活动目录是一个分布式的目录服务,信息可以分散在多台不同的计算机上,保证用户能够快速访问,因为多台计算机上有相同的信息,所以在信息容错方面具有很强的控制能力。既提高了管理效率,又使网络应用更加方便。

域是在 Windows NT/2000/2003 网络环境中组建客户机/服务器网络的实现方式。所谓域,是由网络管理员定义的一组计算机集合,实际上就是一个网络。在这个网络中,至少有一台称为域控制器的计算机,充当服务器角色。在域控制器中保存着整个网络的用户账号及目录数据库,即活动目录。构建域后,管理员可以对整个网络实施集中控制和管理。

当需要配置一个包含多个域的网络时,应该将网络配置成域目录树结构。域目录树是一种树型结构。在整个域目录树中,所有域共享同一个活动目录,即整个域目录树中只有一个活动目录。在配置一个较大规模的企业网络时,可以配置为域目录树结构,比如将企业总部的网络配置为根域,各分支机构的网络配置为子域,整体上形成一个域目录树,以实现集中管理。

如果网络的规模比域目录树还要大，甚至包含了多个域目录树，这时可以将网络配置为域目录林（也称森林）结构。域目录林由一个或多个域目录树组成。域目录林中的每个域目录树都有惟一的命名空间，它们之间并不是连续的。在整个域目录林中存在着一个根域，这个根域是域目录林中最先安装的域。

3. 简述什么是信任关系。

信任关系是网络中不同域之间的一种内在联系。只有在两个域之间创建了信任关系，这两个域才可以相互访问。在通过 Windows Server 2003 系统创建域目录树和域目录林时，域目录树的根域和子域之间，域目录林的不同树根之间都会自动创建双向的、传递的信任关系，有了信任关系，使根域与子域之间、域目录林中的不同树之间可以互相访问，并可以从其他域登录到本域。

4. 为什么在域中常常需要 DNS 服务器？

Windows Server 2003 使用 DNS 服务器来登记域控制器的 IP 地址、各种资源的定位等。

5. 活动目录中存放了什么信息？

活动目录存放了域林中的各种信息，包括用户、组的信息，域的架构等都分别存放在域林中的各个域控制器上的活动目录中。

6. 简述工作组和域的区别。

（1）工作组 Work Group

在一个网络内，可能有成百上千台电脑，如果这些电脑不进行分组，都列在“网上邻居”内，可想而知会有多么乱。为了解决这一问题，Windows 9x/NT/2000/2003 就引用了“工作组”这个概念，将不同的电脑一般按功能分别列入不同的组中，如财务部的电脑都列入“财务部”工作组中，人事部的电脑都列入“人事部”工作组中。你要访问某个部门的资源，就在“网上邻居”里找到那个部门的工作组名，双击就可以看到那个部门的电脑了。

那么怎么加入工作组呢？其实很简单，你只需要右击你的 Windows 桌面上的“网上邻居”，在弹出的菜单中选择“属性”，点击“标识”，在“计算机名”一栏中添入你想好的名字，在“工作组”一栏中添入你想加入的工作组名称。

如果你输入的工作组名称以前没有，那么相当于新建一个工作组，当然只有你的电脑在里面。计算机名和工作组的长度不能超过 15 个英文字符，可以输入汉字，但是不能超过 7 个。“计算机说明”是附加信息，不填也可以，但是最好填上一些这台电脑主人的信息，如“技术部主管”等。单击[确定]按钮后，Windows 98 提示需要重新启动，按要求重新启动之后，再进入“网上邻居”，就可以看到你所在工作组的成员了。

一般来说，同一个工作组内部成员相互交换信息的频率最高，所以你一进入“网上邻居”，首先看到的是你所在工作组的成员。如果要访问其他工作组的成员，需要双击“整个网络”，就会看到网络上所有的工作组，双击工作组名称，就会看到里面的成员。

你也可以退出某个工作组，只要将工作组名称改动即可。不过这样在网上别人照样可以访问你的共享资源，只不过换了一个工作组而已。你可以随便加入同一网络上的任何工作组，也可以离开一个工作组。“工作组”就像一个自由加入和退出的俱乐部一样，它本身的作用仅仅是提供一个“房间”，以方便网上计算机共享资源的浏览。

（2）域 Domain

与工作组的“松散会员制”有所不同，“域”是一个相对严格的组织。“域”指的是服务器控制网络上的计算机能否加入的计算机组合。

实行严格的管理对网络安全是非常必要的。在对等网模式下，任何一台电脑只要接入网络，就可以访问共享资源，如共享 ISDN 上网等。尽管对等网络上的共享文件可以加访问密码，但是非常容易被破解。在由 Windows 9x 构成的对等网中，数据是非常不安全的。

在“域”模式下，至少有一台服务器负责每一台联入网络的电脑和用户的验证工作，相

当一个单位的门卫一样，称为“域控制器（Domain Controller，简称为 DC）”。“域控制器”中包含了由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当电脑联入网络时，域控制器首先要鉴别这台电脑是否是属于这个域的，用户使用的登录账号是否存在、密码是否正确。如果以上信息不正确，域控制器就拒绝这个用户从这台电脑登录。不能登录，用户就不能访问服务器上有权限保护的资源，只能以对等网用户的方式访问 Windows 共享出来的资源，这样就一定程度上保护了网络上的资源。

想把一台电脑加入域，仅仅使它和服务器在“网上邻居”能够相互看到是远远不够的，必须要由网络管理员进行把这台电脑加入域的相关操作。操作过程由服务器端设置和客户端设置构成。

① 服务器端设置

以系统管理员身份在已经设置好 Active Directory（活动目录）的 Windows Server 2003 上登录，点击“开始/程序/管理工具/Active Directory 用户和计算机”，在程序界面中右击“computers”（计算机），在弹出的菜单中单击“新建/计算机”，填入想要加入域的计算机名即可。要加入域的计算机名最好为英文，否则系统会提示中文计算机名可能会引起一些问题。

② 客户端设置

首先要确认计算机名称是否正确，然后在桌面“网上邻居”上右击鼠标，点击“属性”出现网络属性设置窗口，确认“主网络登录”为“Microsoft 网络用户”。

选中窗口上方的“Microsoft 网络用户”（如果没有此项，说明没有安装，点击[添加]安装“Microsoft 网络用户”项）。点击[属性]按钮，出现“Microsoft 网络用户 属性”对话框，选中“登录到 Windows NT 域”复选框，在“Windows NT 域”中输入要登录的域名。

Windows 98 会提示需要重新启动计算机，重新启动后，会出现一个登录对话框。在输入正确的域用户账号、密码以及登录域之后，就可以使用 Windows Server 2003 域中的资源了。请注意，这里的域用户账号和密码，必须是网络管理员为用户建的那个账号和密码，而不是由本机用户自己创建的账号和密码。如果没有将计算机加入域，或者登录的域名、用户名、密码有一项不正确，就会出现错误信息。

7. 简述通用组、全局组和本地域组的区别。

① 本地域组

本地域组的概念是在 Windows 2000 中引入的。本地域组主要用于指定其所属域内的访问权限，以便访问该域内的资源。对于只拥有一个域的企业而言，建议选择“本地域组”选项。它的特征如下：

- 本地域组内的成员可以是任何一个域内的用户、通用组与全局组，也可以是同一个域内的本地域组，但不能是其他域内的域本地组。
- 域本地组只能访问同一个域内的资源，无法访问其他不同域内的资源。也就是说，当在某台计算机上设置权限时，可以设置同一域内的本地域组的权限，但无法设置其他域内的本地域组的权限。

② 全局组

全局组主要用于组织用户，即可以将多个被赋予相同权限的用户账户加入到同一个全局组内。其特征如下：

- 全局组内的成员，只能包含所属域内的用户与全局组，即只能将同一个域内的用户或其他全局组加入到全局组内。
- 全局组可以访问任何一个域内的资源，即可以在任何一个域内设置全局组的使用权限，无论该全局组是否在同一个域内。

③ 通用组

通用组可以设置在所有域内的访问权限，以便访问所有域资源。其特征如下：

- I 通用组成员可以包括整个域林（多个域）中任何一个域内的用户，但无法包含任何一个域内的本地域组。
- I 通用组可以访问任何一个域内的资源，也就是说，可以在任何一个域内设置通用组的权限，无论该通用组是否在同一个域内。

这意味着，一旦将适当的成员添加到通用组，并赋予通用组执行任务的权利和赋予成员适当的访问资源权限，成员就可以管理整个企业。管理企业最有效的方式就是使用通用组，而不必使用其他类型的组。

8. 如果源域控制器有多个复制伙伴，在默认情况下将以 3 秒为间隔向每个伙伴相继发出通知。为什么？

3 秒的通知间隔可避免来自复制伙伴的更新请求同时到达，而使源域控制器应接不暇。

9. 什么是紧急复制？紧急复制主要用在什么场合？

对于站点内的某些目录更新，复制会立即发生。这种立即复制称为紧急复制。主要应用于重要的目录更新，包括账户锁定的指派以及账户锁定策略、域密码策略或域控制器账户上密码的更改。

项目 4 配置与管理 DNS 服务器

一、填空

- 1. 域名解析 2. 分级 3. com 4. CNAME
- 5. ping , nslookup 6. 递归查询、转寄查询

二、选择题

- 1.A; 2.A; 3.C

三、简答题

1. DNS 的查询模式有哪几种？

按照 DNS 搜索区域的类型，DNS 的区域可分为正向搜索区域和反向搜索区域。正向搜索是 DNS 服务器要实现的主要功能，它根据计算机的 DNS 名称解析出相应的 IP 地址，而反向搜索则是根据计算机的 IP 地址解析出它的 DNS 名称。

（1）正向查询

其查询方式有两种：递归查询和转寄查询。

递归查询：当收到 DNS 工作站的查询请求后，DNS 服务器在自己的缓存或区域数据库中查找，如找到则返回结果，如找不到，返回错误结果。即 DNS 服务器只会向 DNS 工作站返回两种信息：要么是在该 DNS 服务器上查到的结果，要么是查询失败。该 DNS 服务器不会主动地告诉 DNS 工作站另外的 DNS 服务器的地址，而需要 DNS 工作站自行向该 DNS 服务器询问。“递归”的意思就是有来有往，并且来、往的次数是一致的。一般由 DNS 工作站提出的查询请求便属于递归查询。

转寄查询（又称迭代查询）：当收到 DNS 工作站的查询请求后，如果在 DNS 服务器中没有查到所需数据，该 DNS 服务器便会告诉 DNS 工作站另外一台 DNS 服务器的 IP 地址，然后，再由 DNS 工作站自行向此 DNS 服务器查询，依次类推一直到查到所需数据为止。如果到最后一台 DNS 服务器都没有查到所需数据，则通知 DNS 工作站查询失败。“转寄”的意思就是，若在某地查不到，该地就会告诉你其它地方的地址，让你转到其它地方去查。一般

在 DNS 服务器之间的查询请求便属于转寄查询（DNS 服务器也可以充当 DNS 工作站的角色）。

（2）反向查询

反向型查询的方式与递归查询和转寄查询两种方式都不同，递归查询和转寄查询都是正向查询，而反向查询则恰好相反，它是从客户机收到一个 IP 地址，而返回对应的域名。

2. DNS 的常见的资源记录有哪些？

SOA：初始授权记录。

NS：名称服务器记录，指定授权的名称服务器。

A：主机记录，实现正向查询，建立域名到 IP 地址的映射。

CNAME：别名记录，为其它资源记录指定名称的替补。

PTR：指针记录，实现反向查询，建立 IP 地址到域名的映像。

MX：邮件交换记录，指定用来交换或者转发邮件信息的服务器。

3. DNS 的管理与配置流程是什么？

（1）安装和管理 DNS 服务器。

（2）创建和管理 DNS 区域。

（3）设置 DNS 服务器。

（4）设置 DNS 客户端。

4. DNS 服务器的属性中的“转发器”的作用是什么？

转发器主要用来帮助解析该 DNS 服务器不能回答的 DNS 查询时可转到另一个 DNS 服务器的 IP 地址。如果服务器是根服务器，则没有转发器属性对话框。

5. 什么是 DNS 服务器的动态更新？

Windows 2000/2003 系统在 DNS 客户端和服务端支持 DNS 动态更新，允许在每个区域上启用或禁用动态更新。默认情况下，DNS 客户端服务在配置用于 TCP/IP 时，将动态更新 DNS 中的主机资源记录。Windows 2000/XP/2003 计算机支持动态 DNS，通过动态更新协议，允许 DNS 客户机变动时自动更新 DNS 服务器上的资源记录，而不需管理员的干涉。除了在 DNS 客户端和服务端之间实现 DNS 动态更新外，还可通过 DHCP 服务器来代理 DHCP 客户机向支持动态更新的 DNS 服务器进行 DNS 记录更新。

四、案例分析

分析：企业内部员工在访问 Intranet 资源时，使用企业内部的 DNS 服务器提供解析；访问 Internet 时，需要使用 ISP 提供的 DNS 服务器来完成域名解析。

解决办法：使用 DNS 服务器的“转发器”功能，可以很方便地实现用户的需求。在 DNS 服务器的属性选项卡中，选择“转发器”选项卡。在“所选域的转发器的 IP 地址列表”中添加 ISP 提供的 DNS 服务器的 IP 地址即可。

项目 5 配置与管理 DHCP 服务器

一、填空题：

1. DHCPDISCOVER、DHCPOFFER、DHCPREQUEST、DHCPACK
2. 169.254.0.1 到 169.254.255.254
3. 服务器选项、作用域选项、类别选项和保留选项

4. ipconfig ipconfig/release ipconfig/renew

二、选择题:

1. C; 2. B; 3. D; 4.C; 5.D

三、简答题:

1. 动态 IP 地址方案有什么优点和缺点?

优点: 减少网络管理员管理 IP 地址的工作量; 提高 IP 地址的使用率, 节约 IP 地址。

缺点: 主机获得的 IP 地址不固定, 对于提供网络服务的主机不适用; 需要 DHCP 服务器。

2. 简述 DHCP 服务器的工作过程。

- (1) DHCP 客户机发送 IP 租用请求。
- (2) DHCP 服务器提供 IP 地址。
- (3) DHCP 客户机进行 IP 租用选择。
- (4) DHCP 服务器 IP 租用认可。

3. 如何备份与还原 DHCP 数据库?

(1) 备份 DHCP

先停止 DHCP 服务, 然后将%systemroot%\System32\dhcp\backup\new 文件夹内的所有内容进行备份, 可以备份到其他磁盘、磁带机上, 以备系统出现故障时还原。或者直接将%systemroot%\System32\dhcp 文件中的 dhcp.mdb 数据库文件备份出来。

(2) 还原过程:

- ① 停止 DHCP 服务。
- ② 在%Systemroot%\system32\dhcp (数据库文件的路径) 目录下, 删除 J50.log, j50xxxxx.log 和 dhcp.tmp 文件。
- ③ 拷贝备份的 dhcp.mdb 到%Systemroot%\system32\dhcp 目录下。
- ④ 重新启动 DHCP 服务。

四、案例分析

1. 分析: 原因可能是没有获得正确的 IP 地址, 因为人事部和财务部一般不设置在一个网段内。用户的计算机搬到财务部后需要重新获得一个 IP 地址。

解决办法: 可以根据财务部的 IP 地址范围为用户手动设置一个 IP 地址。最好的方法是选择自动获得 IP 地址, 一般情况下企业内部都安装有 DHCP 服务器, 可以使用 IPCONFIG/RELEASE 命令, 先释放掉计算机现有的 IP 地址, 然后使用 IPCONFIG/RENEW 命令重新获得一个新的 IP 地址就可以了。也可以直接使用 IPCONFIG/RENEW 命令获得新的 IP 地址。

2. 分析: 因为新添加的作用域与 DHCP 服务器不在同一个子网中, 所以新建的作用域中的 IP 地址不能自动分配给客户端计算机。

解决办法: 创建超级作用域, 将所有的作用域都添加到这个超级作用域中。

项目 6 配置与管理 IIS 服务器

一、判断题

1. √ 2. √ 3. × 4. √ 5. √

二、简答题

1. 简述架设多个 Web 网站的方法。

架设多个 Web 网站可以通过以下三种方式。

- I 使用不同 IP 地址架设多个 Web 网站。
- I 使用不同端口号架设多个 Web 网站。
- I 使用不同主机头架设多个 Web 网站。

在创建一个 Web 网站时,要根据企业本身现有的条件,如投资的多少、IP 地址的多少、网站性能的要求等,选择不同的虚拟主机技术。

2. IIS 6.0 提供的服务有哪些?

IIS 提供了基本服务,包括发布信息、传输文件、支持用户通信和更新这些服务所依赖的数据存储。

- (1) 万维网发布服务。
- (2) 文件传输协议服务。
- (3) 简单邮件传输协议服务。
- (4) 网络新闻传输协议服务。
- (5) IIS 管理服务。

3. 什么是虚拟主机?

虚拟主机是在一台 Web 服务器上,可以为多个单独域名提供 Web 服务,并且每个域名都完全独立,包括具有完全独立的文档目录结构及设置,这样域名之间完全独立,不但使用每个域名访问到的内容完全独立,并且使用一个域名无法访问其他域名提供的网页内容。

4. 在 IIS 5.0 中创建 FTP 服务器与在 IIS 6.0 中创建 FTP 服务器最大的区别是什么?

FTP 用户隔离是 IIS 6.0 的新增特性,它使 ISP 和应用服务提供商可以为客户提供上传文件和 Web 内容的个人 FTP 目录。FTP 用户隔离相当于专业 FTP 服务器的用户目录锁定功能,实际上是将用户限制在自己的目录中,防止用户查看或覆盖其他用户的内容。

5. 简述创建 FTP 虚拟站点的用户隔离方式。

当使用用户隔离方式时,所有用户的主目录都在单一 FTP 主目录下,每个用户均被限制在自己的主目录中,用户名必须与相应的主目录相匹配,不允许用户浏览除自己主目录之外的其他内容。如果用户需要访问特定的共享文件夹,需要为该用户再创建一个虚拟根目录。如果 FTP 是独立的服务器,并且用户数据需要相互隔离,那么,应当选择该方式。需要注意的是,当使用该模式创建了上百个主目录时,服务器性能会大幅下降。

项目 8 配置与管理打印服务器

一、填空题

- 1. 打印服务器+打印机、打印服务器+网络打印机
- 2. 本地打印机、网络接口打印机

3. 多
4. 打印机池
5. Administrators 组、域控制器上的 Print Operator Server Operator

二、简答题

1. 简述打印机、打印设备和打印服务器的区别。

(1) 打印设备：实际执行打印的物理设备，可以分为本地打印设备和带有网络接口的打印设备。根据使用的打印技术，可以分为针式打印设备、喷墨打印设备和激光打印设备。

(2) 打印机：即逻辑打印机，打印服务器上的软件接口。当发出打印作业时，作业在发送到实际的打印设备之前先在逻辑打印机上进行后台打印。

(3) 打印服务器：连接本地打印机，并将打印机共享出来的计算机系统。网络中的打印客户机将作业发送到打印服务器处理，因此打印服务器需要有较高的内存以处理作业，对于较频繁的或大尺寸文件的打印环境，还需要打印服务器上有足够的磁盘空间以保存打印假脱机文件。

2. 简述共享打印机的好处，并举例。

最主要的是节省资源、充分利用资源。

3. 为什么用多个打印机连接同一打印设备？

由于只有一台打印设备，无法区分不同打印文档的优先级。为一台打印设备建立多台打印机，可以给不同打印机设置不同的优先级，以便用户将重要的文档发送到具有最高优先级的打印机，这些文档总是在低优先级的打印机的文档前打印。

项目 9 配置与管理电子邮件服务器

一、填空题：

1. SMTP;
2. 本地 Windows 账户身份验证，Active Directory 集成的身份验证，加密密码文件身份验证

二、选择题

1. D

项目 10 配置路由和远程访问

一、填空题：

1. route print
2. PPTP (Point-to-Point Tunneling Protocol，点对点隧道协议)、L2TP (Layer Two Tunneling Protocol，第二层隧道协议)。
3. 15、16

二、选择题

1.A; 2.B

三、简答题:

1. 什么是专用地址和公用地址?

(1) 专用地址

要使小型办公室或家庭办公室中的多个计算机能通过 Internet 进行通信, 每个计算机都必须有自己的公用地址。IP 地址是有限的资源, 为网络中数以亿计的主机都分配公用的 IP 地址是不可能的。因此, NIC 为公司专用网络提供了保留网络 IP 专用的方案。这些专用网络 ID 包括:

- I 子网掩码为 255.0.0.0 的 10.0.0.0 (一个 A 类的地址)
- I 子网掩码为 255.240.0.0 的 172.160.0.0 (一个 B 类的地址)
- I 子网掩码为 255.255.0.0 的 192.168.0.0 (一个 C 类的地址)

这些范围内的所有地址都称为专用地址。局域网 (LAN) 可根据自己的计算机的多少和网络的拓扑结构进行选择。

(2) 公用地址

Internet 使用 TCP/IP 协议, 所有连入 Internet 的计算机必须有一个惟一合法的 IP 地址, 它由 Internet 网络信息中心 (简称 NIC) 分配。NIC 分配的 IP 地址, 称为公用地址或合法的 IP 地址。一般的单位或家庭由 Internet 服务提供商 (ISP) 处申请获得公用合法的 IP 地址, ISP 向 Inter NIC 申请得到某一序列号 IP 地址, 然后再租借给用户。

2. 把局域网连接到 Internet 有几种方法?

将局域网接入 Internet 有很多方法。

- (1) 通过路由器连接到 Internet。
- (2) Internet 连接共享 (ICS)。
- (3) 通过 NAT。
- (4) 通过代理服务器连接到 Internet。

3. 网络地址转换 NAT 的功能是什么?

网络地址转换器 NAT (Network Address Translator) 位于使用专用地址的 Intranet 和使用公用地址的 Internet 之间。从 Intranet 传出的数据包由 NAT 将它们的专用地址转换为公用地址。从 Internet 传入的数据包由 NAT 将它们的公用地址转换为专用地址。这样在内网中计算机使用未注册的专用 IP 地址, 而在与外部网络通信时使用注册的公用 IP 地址, 大大降低了连接成本。同时 NAT 也起到将内部网络隐藏起来, 保护内部网络的作用, 因为对外部用户来说只有使用公用 IP 地址的 NAT 是可见的。

4. 简述地址转换的原理, 即 NAT 的工作过程。

NAT 地址转换协议的工作过程主要有以下四步:

- (1) 客户机将数据包发给运行 NAT 的计算机。
- (2) NAT 将数据包中的端口号和专用的 IP 地址换成它自己的端口号和公用的 IP 地址, 然后将数据包发给外部网络的目的主机, 同时记录一个跟踪信息在映像表中, 以便向客户机发送回答信息。
- (3) 外部网络发送回答信息给 NAT。
- (4) NAT 将所收到的数据包的端口号和公用 IP 地址转换为客户机的端口号和内部网络使用的专用 IP 地址并转发给客户机。

5. 下列不同技术有何异同?

- (1) NAT 与路由的比较

- 1 NAT 可将大量未注册的网络内部的专用地址转换为个别的公用地址，降低了网络成本。
- 1 NAT 提供了路由所不支持的网络安全性。
- 1 因为要进行地址转换，所以 NAT 要比路由占用更多的网络资源，并且不是支持所有的协议。
- (2) NAT 与代理服务器
- 1 二者都提供地址转换功能且提供网络的安全性。
- 1 代理服务器需配置端口，且提供对客户访问数据的缓存功能。
- (3) NAT 与 Internet 共享
- 1 NAT 与 Internet 共享功能相同，只是 Internet 共享的配置简单。
- 1 Internet 共享只适用于小型的网络。需要固定的内部 IP 地址、只能使用一个公用 IP 地址，只允许单个内部网络接口。

项目 11 安全管理 Windows Server 2003

一、填空题

1. 读取 (Read)、写入 (Write)、列出文件夹内容 (List Folder Contents)、读取和运行 (Read & Execute)、修改 (Modify)、完全控制 (Full Control)
2. 访问权限
3. 权限、加密、压缩、磁盘配额

二、判断题

1. √ 2. √ 3. √ 4. √ 5. × 6. √ 7. √

三、简答题

1. 简述 FAT、FAT32 和 NTFS 文件系统的区别。

在推出 FAT32 文件系统之前，通常 PC 机使用的文件系统是 FAT16。像基于 MS-DOS，Win 95 等系统都采用了 FAT16 文件系统。在 Win 9X 下，FAT16 支持的分区最大为 2GB。我们知道计算机将信息保存在硬盘上称为“簇”的区域内。使用的簇越小，保存信息的效率就越高。在 FAT16 的情况下，分区越大簇就相应的要增大，存储效率就越低，势必造成存储空间的浪费。并且随着计算机硬件和应用的不断提高，FAT16 文件系统已不能很好地适应系统的要求。在这种情况下，推出了增强的文件系统 FAT32。同 FAT16 相比，FAT32 主要具有以下特点：

(1) 同 FAT16 相比 FAT32 最大的优点是可以支持的磁盘大小达到 2TB (2047GB)，但是不能支持小于 512MB 的分区。基于 FAT32 的 Win 2000 可以支持分区最大为 32GB；而基于 FAT16 的 Win 2000 支持的分区最大为 4GB。

(2) 由于采用了更小的簇，FAT32 文件系统可以更有效率地保存信息。如两个分区大小都为 2GB，一个分区采用了 FAT16 文件系统，另一个分区采用了 FAT32 文件系统。采用 FAT16 的分区簇大小为 32KB，而 FAT32 分区的簇只有 4KB 的大小。这样 FAT32 就比 FAT16 的存储效率要高很多，通常情况下可以提高 15%。

(3) FAT32 文件系统可以重新定位根目录和使用 FAT 的备份副本。另外 FAT32 分区的启动记录被包含在一个含有关键数据的结构中，减少了计算机系统崩溃的可能性。

NTFS 和 FAT32 分区的区别到底是啥呢？

当然了 NTFS 和 FAT32 都是目前比较流行的磁盘分区格式，由 FAT 到 FAT16→FAT32 →NTFS，NTFS 功能强一些。

(1) NTFS 支持文件加密和分别管理功能（也就是著名的 EFS 加密格式），可为用户提供更高层次的安全保证。

(2) NTFS 具有更好的磁盘压缩性能，可进一步满足小硬盘用户的需要（读取会慢一些）。

(3) NTFS 最大支持高达 2TB（1TB=1024GB）的大硬盘，而且它的性能不会随着磁盘容量的增大而降低。

由此可见，NTFS 格式具有许多独特的优点。不过，它也有一个缺点，那就是该磁盘文件格式不能被除它自己之外的其他操作系统所识别（NT 4.0 也不例外），这就对数据交流造成了一定的影响，也就不支持 DOS 操作系统了，不过还是值得支持。

所以，只使用 Windows 2000/2003 的用户应首选使用 NTFS 格式，要是同时使用 Windows 2000/2003 和其他操作系统，则应谨慎从事。最好将磁盘划分为多个不同的磁盘分区，将 Windows 2000/2003 安装到其中的一个磁盘分区并选择使用 NTFS 格式；将其他操作系统安装到另外的磁盘分区中并使用 FAT 或 FAT32 格式。

NTFS 文件系统（下有详解）

NTFS 文件系统是一个基于安全性的文件系统，是 Windows NT 所采用的独特的文件系统结构，它是建立在保护文件和目录数据基础上，同时照顾节省存储资源、减少磁盘占用量的一种先进的文件系统。使用非常广泛的 Windows NT 4.0 采用的就是 NTFS 4.0 文件系统（下面讲的是 5.0，不好意思，哈哈），相信它所带来的强大的系统安全性一定给广大用户留下了深刻的印象。Win 2000 采用了更新版本的 NTFS 文件系统 NTFS 5.0，它的推出使得用户不但可以像 Win 9X 那样方便快捷地操作和管理计算机，同时也可享受到 NTFS 所带来的系统安全性。

NTFS 5.0 的特点主要体现在以下几个方面：

(1) NTFS 可以支持的分区（如果采用动态磁盘则称为卷）大小可以达到 2TB。而 Win 2000 中的 FAT32 支持分区的大小最大为 32GB。

(2) NTFS 是一个可恢复的文件系统。在 NTFS 分区上用户很少需要运行磁盘修复程序。NTFS 通过使用标准的事物处理日志和恢复技术来保证分区的一致性。发生系统失败事件时，NTFS 使用日志文件和检查点信息自动恢复文件系统的一致性。

(3) NTFS 支持对分区、文件夹和文件的压缩。任何基于 Windows 的应用程序对 NTFS 分区上的压缩文件进行读写时不需要事先由其他程序进行解压缩，当对文件进行读取时，文件将自动进行解压缩；文件关闭或保存时会自动对文件进行压缩。

(4) NTFS 采用了更小的簇，可以更有效率地管理磁盘空间。在 Win 2000 的 FAT32 文件系统的情况下，分区大小在 2GB~8GB 时簇的大小为 4KB；分区大小在 8GB~16GB 时簇的大小为 8KB；分区大小在 16GB~32GB 时，簇的大小则达到了 16KB。而 Win 2000 的 NTFS 文件系统，当分区的大小在 2GB 以下时，簇的大小都比相应的 FAT32 簇小；当分区的大小在 2GB 以上时（2GB~2TB），簇的大小都为 4KB。相比之下，NTFS 可以比 FAT32 更有效地管理磁盘空间，最大限度地避免了磁盘空间的浪费。

(5) 在 NTFS 分区上，可以为共享资源、文件夹以及文件设置访问许可权限。许可的设置包括两方面的内容：一是允许哪些组或用户对文件夹、文件和共享资源进行访问；二是获得访问许可的组或用户可以进行什么级别的访问。访问许可权限的设置不但适用于本地计算机的用户，同样也应用于通过网络的共享文件夹对文件进行访问的网络用户。与 FAT32 文件系统下对文件夹或文件进行访问相比，安全性要高得多。另外，在采用 NTFS 格式的 Win 2000

中,应用审核策略可以对文件夹、文件以及活动目录对象进行审核,审核结果记录在安全日志中,通过安全日志就可以查看哪些组或用户对文件夹、文件或活动目录对象进行了什么级别的操作,从而发现系统可能面临的非法访问,通过采取相应的措施,将这种安全隐患减到最低。这些在 FAT32 文件系统下,是不能实现的。

(6) 在 Win 2000 的 NTFS 文件系统下可以进行磁盘配额管理。磁盘配额就是管理员可以为用户所能使用的磁盘空间进行配额限制,每一用户只能使用最大配额范围内的磁盘空间。设置磁盘配额后,可以对每一个用户的磁盘使用情况进行跟踪和控制,通过监测可以标识出超过配额报警阈值和配额限制的用户,从而采取相应的措施。磁盘配额管理功能的提供,使得管理员可以方便合理地为用户分配存储资源,避免由于磁盘空间使用的失控可能造成的系统崩溃,提高了系统的安全性。

(7) NTFS 使用一个“变更”日志来跟踪记录文件所发生的变更。

选取 FAT32 和 NTFS 的建议:在系统的安全性方面,NTFS 文件系统具有很多 FAT32 文件系统所不具备的特点,而且基于 NTFS 的 Win 2000/2003 运行要快于基于 FAT32 的 Win 2000/2003;而在与 Win 9X 的兼容性方面,FAT32 优于 NTFS。所以在决定 Win 2000/2003 中采用什么样的文件系统时应从以下几点出发:

- (1) 计算机是单一的 Win 2000 系统,还是采用多启动的 Win 2000 系统;
- (2) 本地安装的磁盘的个数和容量;
- (3) 是否有安全性方面的考虑等。

基于以上的考虑,如果要在 Win 2000/2003 中使用大于 32GB 的分区的话,那么只能选择 NTFS 格式。如果计算机作为单机使用,不需要考虑安全性方面的问题,更多地注重与 Win 9X 的兼容性,那么 FAT32 是最好的选择。如果计算机作为网络工作站或更多的追求系统的安全性,而且可以在单一的 Win 2000/2003 模式下运行,强烈建议所有的分区都采用 NTFS 格式;如果要兼容以前的应用,需要安装 Win 9X 或其它的操作系统,建议做成多启动系统,这就需要两个以上的分区,一个分区采用 NTFS 格式,另外的分区采用 FAT32 格式,同时为了获得最快的运行速度建议将 Win 2000/2003 的系统文件放置在 NTFS 分区上,其它的个人文件则放置在 FAT32 分区中。

2. 重装 Windows Server 2003 后,原来加密的文件为什么无法打开?

EFS 内置于 Windows 2003 中的 NTFS 文件系统中。利用 EFS 可以启用基于公共密钥的文件级或者文件夹级的保护功能。

新安装系统的管理员账号与原系统尽管名称相同,但他们的公钥与私钥是不一样的,因此无法打开原来加密的文件。

3. 特殊权限与标准权限的区别是什么?

标准 NTFS 权限通常提供了必要的保证资源被安全访问的权限,如果要分配给用户特定的访问权限,就需要设置 NTFS 特殊权限。标准权限可以说是特殊 NTFS 权限的特定组合。特殊 NTFS 权限包含了各种情况下对资源的访问权限,它规定了用户访问资源的所有行为。为了简化管理,将一些常用的特殊 NTFS 权限组合起来并内置到操作系统中形成标准 NTFS 权限。

4. 如果一位用户拥有某文件夹的 Write 权限,而且还是该文件夹 Read 权限的成员,该用户对该文件夹的最终权限是什么?

由于 NTFS 权限的累加性,该用户有写(Write)和读(Read)的权限。

5. 如果某员工离开公司,应当做什么来将他或她的文件所有权转给其他员工?

必须以 Administrator 身份登录以接管员工的文件和文件夹的所有权;再将“取得所有权”特殊权限分配给另一员工,使该员工可以接管那些文件和文件夹的所有权。

6. 如果一位用户拥有某文件夹的 Write 权限和 Read 权限,但被拒绝对该文件夹内某

文件的 Write 权限，该用户对该文件的最终权限是什么？

用户有读权限，但没有写权限。因为，拒绝权限高于其他权限。

7. 什么是本地安全策略？

在 Windows Server 2003 中，为了确保计算机的安全，允许管理员对本地安全进行设置，从而达到提高系统安全性的目的。Windows Server 2003 对登录到本地计算机的用户都定义了一些安全设置。所谓本地计算机是指用户登录执行 Windows Server 2003 的计算机，在没有活动目录集中管理的情况下，本地管理员必须为计算机进行设置以确保其安全。例如，限制用户如何设置密码、通过账户策略设置账户安全性、通过锁定账户策略避免他人登录计算机、指派用户权限等。将这些安全设置分组管理，就组成了 Windows Server 2003 的本地安全策略。

8. 如何设置本地安全策略？

Windows Server 2003 在“管理工具”菜单提供了“本地安全设置”控制台，可以集中管理本地计算机的安全设置原则，使用管理员账户登录到本地计算机，即可打开“本地安全设置”控制台。

要控制台中，可以对“本地安全策略”中的“密码安全设置”、“账户锁定策略密码安全”、“用户权限分配”进行设置。

9. 简述组策略的概念？

(1) 组策略通常是系统管理员为加强整个域或网络共同的策略而设置并进行管理的。组策略会影响到用户账户、组、计算机和组织单位，它是存储在 Active Directory 中的配置，一个对象可能有多个组策略来创建动态环境。通过使用组策略，就可以利用其广泛特性，包括从安全锁定桌面到应用程序分发，从脚本处理到文件和文件夹复制。这个特性集能够用于帮助对其桌面需要最小控制的用户，还可以帮助登录到网络进行系统管理的系统管理员。

(2) 组策略是配置的集合，可以把它应用到 Active Directory 中的一个或多个对象上，这些设置包含在组策略对象 GPO (Group Policy Object) 内。

(3) Windows Server 2003 组策略 (GP) 应用程序层次通常首先是站点，其次是域，再次是 OU。

10. 试着创建一组策略对象，并将此组策略对象应用到 Active Directory 域中。

(自己做一下)

11. Windows Server 2003 的审核策略包含哪几种？

Windows Server 2003 允许设置的审核策略，包括如下几项。

(1) 审核策略更改：跟踪用户权限或审核策略的改变。

(2) 审核登录事件：跟踪用户登录、注销任务或本地系统账户的远程登录服务。

(3) 审核对象访问：跟踪对象何时被访问以及访问的类型。例如，跟踪对文件夹、文件、打印机等的使用。用对象的属性（如文件夹或文件的“安全”选项卡）可配置对指定事件的审核。

(4) 审核过程跟踪：跟踪诸如程序启动、复制、进程退出等事件。

(5) 审核目录服务访问：跟踪对 Active Directory 对象的访问。

(6) 审核特权使用：跟踪用户何时使用了不应有的权限（超越了与登录或退出有关的权限）。

(7) 审核系统事件：跟踪重新启动、启动或关机等的系统事件，或影响系统安全或安全日志的事件。

(8) 审核账户登录事件：跟踪用户账户登录和退出。

(9) 审核账户管理：跟踪某个用户账户或组是何时建立、修改和删除的，它是何时改

名、启用或禁止的，其密码是何时设置或修改的。

12. 试着更改几项审核策略，并在安全日志中查看相应的记录。

（自己做一下）

13. 通过对默认安全模板（setup security.inf）的安全设置进行适当修改，创建为一个新的安全模板（newsecurity.inf），并将其策略导入到域的组策略对象中。

（自己做一下）

14. 提高 Windows Server 2003 的安全可以从哪些方面着手？

（1）启用密码复杂性要求。提高密码的破解难度主要是通过采用提高密码复杂性、增加密码长度、提高更换频率等措施来实现，密码长度不宜太短。最好是字母、数字及特殊字符的组合，并且注意及时更换新密码。

（2）启用账户锁定策略。为了方便用户，Windows Server 2003 系统在默认情况下并未启用密码锁定策略。此时，很容易遭受黑客通过自动登录工具和密码猜解字典进行的攻击，甚至可以进行暴力模式的攻击。账户锁定策略就是指定该账户无效登录的最大次数。例如，设置锁定登录最大次数为 5 次，这样只允许 5 次登录尝试。如果 5 次登录全部失败，就会锁定该账户。

（3）删除共享。通过共享来入侵一个系统是最为方便的一种方法。如果防范不严，最简单的方法就是利用系统隐含的管理共享。因此，只要黑客能够扫描到 IP 和用户密码，就可连接到共享上。因此，为了安全最好关掉所有的共享，包括默认的管理共享。下面给出如何关闭系统的默认共享的操作。