

# 第4章 网络及其服务配置

---

# 本章内容

---

- **网络配置**
- **Web服务器**
- **FTP服务器**
- **Samba服务器**
- **Mail服务器**

# 网络拓扑结构示例

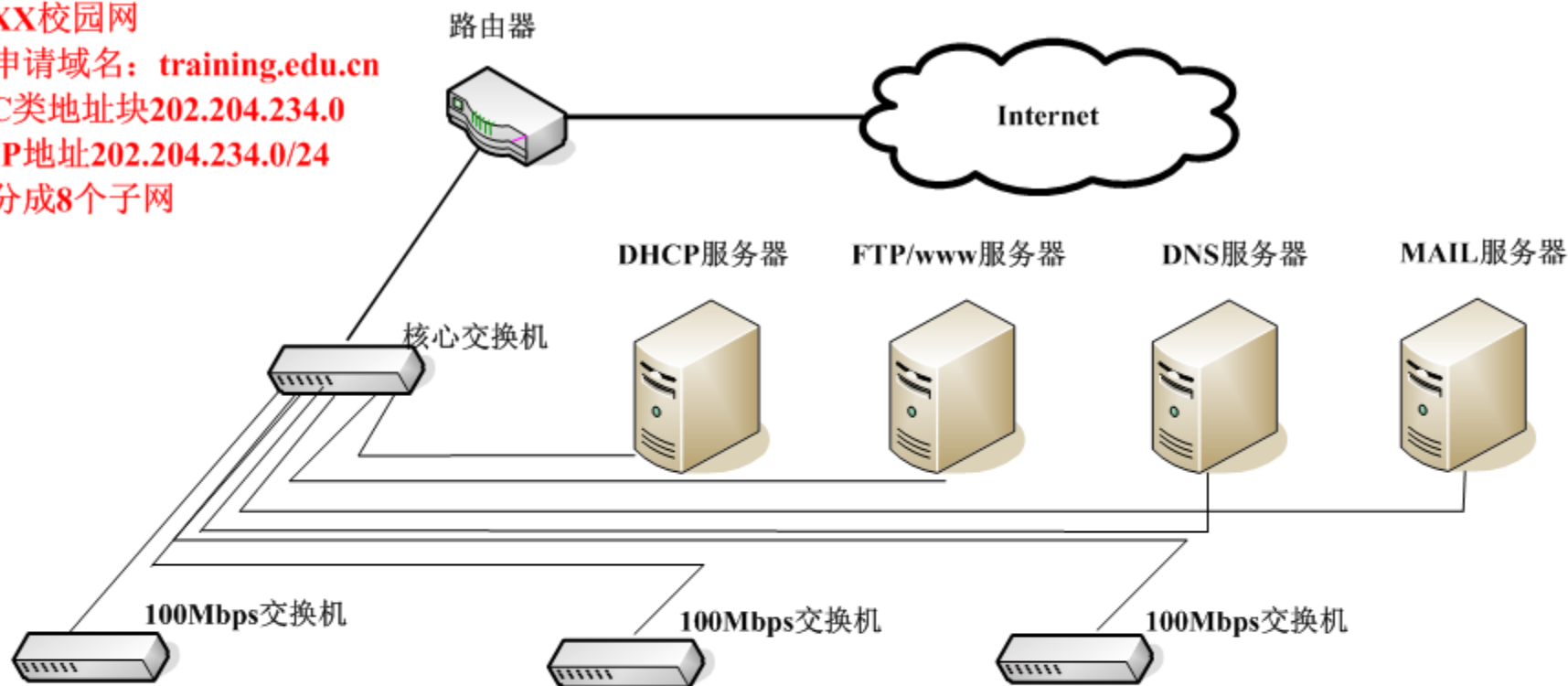
**XX校园网**

申请域名: **training.edu.cn**

C类地址块**202.204.234.0**

IP地址**202.204.234.0/24**

分成**8个子网**



要求:

- 1) www服务器的网页根目录是/orange, 用户网页目录/public,
- 2) 目录/orange/vlan100只允许202.204.234.0/27网段使用。
- 3) NFS只允许202.204.234.0/27网段使用

Mail服务器: mail.training.edu.cn, 202.204.234.4/27

FTP/www服务器: www.training.edu.cn, 202.204.234.3/27

DNS服务器: dns.training.edu.cn, 202.204.234.2/27

NFS服务器: nfs.training.edu.cn, 202.204.234.33/27

DHCP服务器: dhcp.training.edu.cn, 202.204.234.6/27

网络掩码: 255.255.255.224

# 1. 网络配置

---

- **网络接口设备：计算机中连接网络的设备。**
- **Linux的网络配置通常有两种方式：**
  - **直接修改配置文件**
  - **通过系统提供的软件或工具来修改**
- **前者要求对相关的系统文件非常熟悉。**

# 相关系统文件 (1)

---

## (1) /etc/inetd.conf

- 该文件告诉inetd监听的服务名称、套接字类型、所使用的协议、等待/非等待标记、执行用户、服务程序路径、服务程序运行参数。

- 示例:

```
# <service_name> <sock_type> <proto>  
  <flags> <user> <Server_path> <args>  
  
ftp    stream  tcp    nowait  root  
  /usr/sbin/tcpd  proFTP  
  
telnet  stream  tcp    nowait  root  
  /usr/sbin/tcpd  telnetd
```

# 相关系统文件 (2)

---

## (2) /etc/rc.d/rc.inet1和/etc/rc.d/rc.inet1.conf

- 网卡的初始化设置，定义了主机的一系列网络环境，包括IP地址、子网掩码，以及网关。

- 示例：

**IPADDR[0]=" 192.168.1.2"          #网卡IP地址**

**NETMASK[0]=" 255.255.255.0" #子网掩码**

**USE\_DHCP=" "          #是否使用DHCP服务**

**DHCP\_HOSTNAME[0]=" " #DHCP服务器的主机名**

**GATEWAY=" 192.168.1.1"          #默认的网关地址**

# 相关系统文件 (3)

---

## (3) /etc/HOSTNAME

- 用于保存完整的主机名和域名
- 程序和变量从此文件获取主机名。
- 示例：

**server1.computer.edu.cn**

# 相关系统文件 (4)

---

## (4) /etc/host.conf

- ❑ order hosts, bind
- ❑ 在查询主机名时先查hosts文件，如没有则向DNS服务器查询。
- ❑ multi on
- ❑ 表示hosts中指定的主机可以有多个IP地址。



# 相关系统文件 (5)

---

## (5) `etc/hosts`

- 记录IP地址与主机名Hostname之间的对应关系
- 示例:

**127.0.0.1localhost**

**192.168.1.2server1.computer.deu.cnserver1**

**192.168.1.1server0.computer.edu.cnserver0**

# 其它相关系统文件

---

## (6) `/etc/resolv.conf`

- 记录当前操作系统的域名以及DNS的IP地址。示例：  
`searchcomputer.edu.cn`  
`nameServer222.214.218.1`

## (7) `/etc/hosts.allow`和`/etc/hosts.deny`

- 控制远程用户的访问，前者列出了允许从远程访问本机的主机和用户，后者列出了禁止从远程访问本机的主机和用户。

## (8) `/etc/services`

- 存放服务名称和端口号的对照表，基本不用编辑。

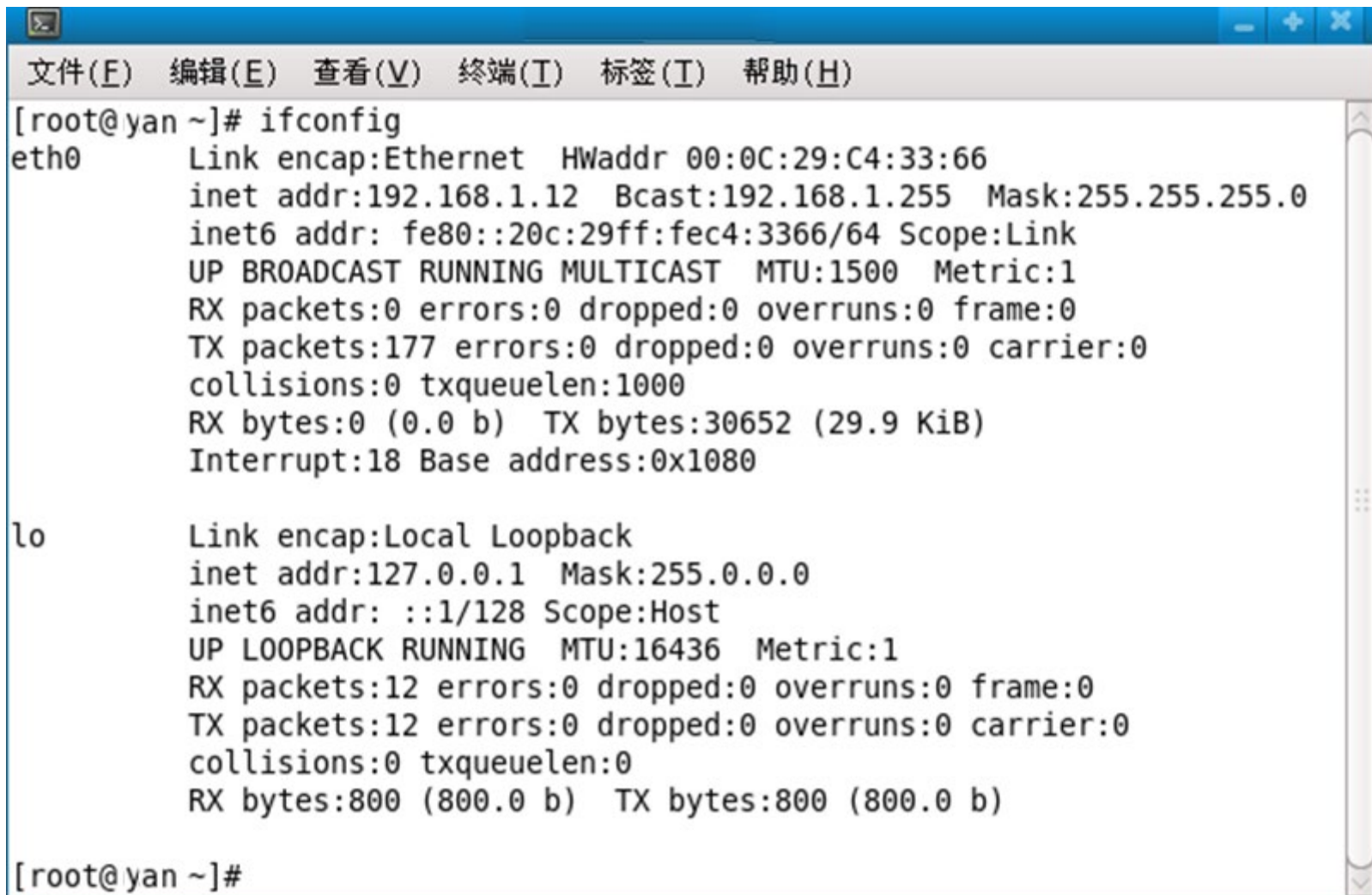
# 常用网络命令

---

- **ifconfig**
- **ping**
- **traceroute**

# ifconfig命令

## 查看当前的网络配置信息



```
[root@yan ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:C4:33:66
          inet addr:192.168.1.12  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec4:3366/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:177 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:30652 (29.9 KiB)
          Interrupt:18 Base address:0x1080

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:800 (800.0 b)  TX bytes:800 (800.0 b)

[root@yan ~]#
```

# ifconfig命令 (续)

---

## □ 配置网卡，示例：

```
# ifconfig eth0 192.168.1.2 192.168.1.255 255.255.255.0
```

## □ 给同一网卡绑定两个IP地址，示例：

```
# ifconfig eth0:0 192.168.1.2 192.168.1.255 255.255.255.0
```

```
# ifconfig eth0:1 192.168.2.2 192.168.1.255 255.255.255.0
```

## □ 关闭/启动网卡，修改网卡MAC地址

```
# ifconfig eth0 down
```

```
# ifconfig eth0 hwether 00:AA:BB:CC:DD:EE
```

```
# ifconfig eth0 up
```

## □ 部署/删除IPV6

```
# ifconfig eth0 inet6 add 3ffe:ffff:0:f101::1/64
```

```
# ifconfig eth0 inet6 del 3ffe:ffff:0:f101::1/64
```

# ping命令

---

- 用来测试网络是否连通，测试主机是否在线。
- 常用ping命令来测试网络是否连通，步骤如下：

- 测试本机网络操作系统是否正常工作

**[yan@主机名]\$ ping 127.0.0.1**

**[yan@主机 名]\$ ping localhost**

- 测试本机网络接口是否正常

**[yan@主机名]\$ ping 192.168.1.2**

**假设本机IP 地址为192.168.1.2**

**如果返回正常信息，则表示本机网卡正常。**

# ping命令 (续)

---

- 测试与本地局域网中网关或其它主机的连通性

[yan@主机名]\$ ping 192.168.1.1

假设本机所在网关地址192.168.1.1

[yan@主机名]\$ ping 192.168.1.10

假设本机所在网络其它主机地址192.168.1.10

- 测试与远程网络中的网关或其它主机的连通性

[yan@主机名]\$ ping 192.168.2.1

[yan@主机名]\$ ping 192.168.2.10

- 测试DNS服务器是否正常

[yan@主机名]\$ ping www.dhu.edu.cn

# traceroute命令

---

- 向目的地址发送的数据包每经过一个网关或路由器，就返回一行信息。
- 最后可知到达目的地址需要经过多少网关或路由。
- 示例如下：

**[yan@主机名]\$ traceroute www.dhu.edu.cn**



# OpenSSH

---

## □ 远程访问

早期命令名称	升级版	命令功能
rcp	scp	远程文件拷贝复制
rlogin	ssh	远程注册
telnet	ssh	远程登录
FTP	sFTP	文件传输

# OpenSSH (续)

---

- ❑ **sFTP和scp都是OpenSSH软件自带的命令。**
- ❑ **SSH 可以确保两个网络 and 系统之间交换数据的机密性和完整性，其主要的优点是通过使用公共密钥加密进行服务器身份验证。**
- ❑ **OpenSSH 是 SSH 协议的开源实现，可以进行远程登录和备份并通过scp或sFTP进行远程文件传输等等。**
- ❑ **OpenSSH提供了服务端后台程序和客户端工具，用来加密远程控件和文件传输过程中的数据。SSH默认端口是TCP 22。**

# 几个重要的配置文件

---

- **/etc/ssh/sshd\_config: OpenSSH 服务器配置文件**
- **/etc/ssh/ssh\_config: OpenSSH 客户端配置文件**
- **~/.ssh/: 用户独立的 ssh 配置目录**
- **~/.ssh/authorized\_keys或者  
~/.ssh/authorized\_keys: 公钥 (RSA or DSA)**
- **/etc/nologin: 如果该文件存在, 则只允许 root 帐号  
登录**
- **/etc/hosts.allow和/etc/hosts.deny: 访问控制定  
义**

# 提高服务器端安全性的策略

---

- ❑ 如果工作站或者笔记本不需要OpenSSH服务，那么就禁用SSHD服务。
- ❑ SSH 协议版本1有很多漏洞和安全问题，应该避免使用SSH-1，可通过在 `sshd_config` 文件中配置如下信息来启用SSH-2: Protocol 2。
- ❑ 限制用户访问SSH。默认所有系统用户都可以通过SSH登录，只需要用密码或者公钥即可。通过 `sshd_config` 文件中的 `AllowUsers` 和 `DenyUsers` 来设置可访问SSH服务的用户名单。

# 提高服务器端安全性的策略（续）

---

- ❑ **配置空闲登出的超时间隔。** 如果长时间没有任何动作的话，可通过设置空闲超时时间来让登录的用户自动登出，以避免一些不必要的ssh会话连接。
- ❑ **禁止 root 帐号通过SSH登录。** 没必要让root帐号通过ssh登录，可通过正常用户登录后然后执行su或者sudo来执行root权限的操作，可在sshd\_config中禁用 root 帐号登录。
- ❑ **防火墙处理SSH 端口#22。** 需要在防火墙规则中打开22端口，除非服务器只允许通过局域网访问。

## 2. Web服务器

---

- **Linux系统中最常使用的Web服务器是Apache HTTP Server。**
- **Apache HTTP Server是Apache软件基金会有一个开放源码的网页服务器，可以在大多数计算机操作系统中运行。**
- **官网： <http://httpd.apache.org/>**

# Apache HTTP Server

---

## □ 服务器安装

**# sudo apt-get install Apache2**

## □ 服务器启动与关闭

- Apache服务的守护程序名称为httpd。
- 命令: **/etc/init.d/httpd [ start|stop|...]**
- start: 启动Web服务器
- stop: 正常停止Web服务器
- Reload: 重新读取更改后的配置文件
- restart: 重启服务器
- status: 检测Web服务器是否在运行

# 服务器配置

---

- Apache服务器的主要配置文件是httpd.conf，一般默认安装在目录/etc/httpd/conf下。该文件由一些配置项构成。

**listen 192.168.1.2:80**

- 指定Apache在哪个TCP端口进行侦听，HTTP服务默认端口为80。
- 如果指定服务端口为8080，那么在客户端的浏览器中可以使用如下URL：

**http://www.mypage.com:8080**



# 服务器配置 (续)

---

## □ user与group

- 用于设置Apache运行时的权限。
- Apache服务器在启动时需要使用root权限。
- 为了防止黑客攻击，系统在服务启动后将Apache运行时的权限切换到一个低级的用户权限。
- User Apache
- Group Apache

# 服务器配置 (续)

---

## □ **ServerRoot**

- 指定Apache配置文件和日志文件所在的目录。
- 系统默认的安装目录是 “/etc/httpd”。
- 管理员要对这个目录的文件进行维护和管理。

# 服务器配置 (续)

---

## □ **ServerName**

- 允许管理员设置一个不同于Apache服务器主机名的“别名”。

## □ **DocumentRoot**

- 指存放网页的根文档目录。
- Apache2.2.10默认的根文档目录是“/var/www/HTML”。
- 用户可以根据需要改变根文档目录的位置

# 安装与配置实例

---

- **开发需求：**在一台具有Linux系统并安装有Apache服务器的机器上，发布自己的个人主页。

**(1) 编写主页文件。**使用各种网页设计工具以及各种脚本语言制作个人网页，建议将首页文件命名为index.htm或index.HTML。

```
<html>
```

```
<head><title>欢迎访问我的个人主页</title></head>
```

```
<body>
```

```
<p align="center">XX的个人主页</p>
```

```
</body>
```

```
</html>
```

# 安装与配置实例（续）

---

**(2) 部署主页文件。将网页文件复制到Linux系统中Apache服务器指定的根文档目录中。**

# 安装与配置实例（续）

---

**(3) 修改Apache的配置。根据自己的需要，修改配置文件/etc/httpd/conf/httpd.conf。**

在文件末尾添加如下代码：

```
NameVirtualHost 192.168.1.2:80  
<VirtualHost 192.168.1.2:80>  
ServerName server1.dhu.edu.cn  
ServerAdmin root@ server1.dhu.edu.cn  
DocumentRoot /home/yan/www/HTML  
customlog logs/access_log combined  
errorlog logs/error_log  
</ VirtualHost>
```

---

# 安装与配置实例（续）

---

**(4) 重新启动Apache服务器，使新的配置生效。**

**`/etc/init.d/httpd restart`**

**(5) 在客户机浏览器中输入url检测主页是否能够看到。**

**`http://192.168.1.2`**

**(6) 客户机浏览器中输入url，检测主页是否能够看到。**

**`http://server1.dhu.edu.cn`**

### 3. FTP服务器

---

- 在Linux下实现FTP服务的软件很多，最常见的有vsFTPD、WU-FTPD、ProFTP等。
- vsFTPD是一个功能强大的FTP服务器，能运行在大部分的Unix和Linux操作系统上。



# FTP服务器安装

---

- ❑ **[root@主机名]# sudo apt-get install vsFTP**
- ❑ **这个命令会在/var/cache/apt/archives的位置拷贝一个vsFTPd-版本号.deb的包，install命令会从这个包开始安装。**
- ❑ **安装完成后，没有修改配置的情况下，在/usr/sbin下会有vsFTPd文件，用于启动服务；在/etc下有vsFTPd.conf文件，用于配置服务；在/var/log下有vsFTPd.log文件，用于记录FTP的日志。**

# 服务器启动与关闭

---

- ❑ 与Apache类似，vsFTPD是vsFTP的守护程序，负责监听客户的请求。
- ❑ **[root@主机名]# /etc/init.d/FTPd start/stop/status**
- ❑ 或者，**[root@主机名]# service vsFTPD start/stop/restart**
- ❑ 或者，**[root@主机名]# sudo /usr/sbin/vsFTPD**

# 服务器配置

---

## □ vsFTP的配置文件

- `/etc/vsFTPD/vsFTPD.conf`
- `/etc/vsFTPD/FTPusers`
- `/etc/vsFTPD/user_list`

# vsFTPD主要配置项

---

- ❑ **anonymous\_enable=YES#允许匿名登录**
- ❑ **local\_enable=YES#允许本地用户登录**
- ❑ **write\_enable=YES#开放本地用户的写权限**
- ❑ **local\_umask=022#本地用户文件掩码为022，即新建文件权限为755**
- ❑ **dirmessage\_enable=YES#切换目录时，显示该目录的信息**
- ❑ **xferlog\_enable=YES#激活上传和下载日志**
- ❑ **connect\_from\_port\_20=YES#使用FTP数据端口20的连接请求**
- ❑ **xferlog\_std\_format=YES#使用标准的xFTPd sferlog日志格式**
- ❑ **pam\_service\_name=vsFTPD#设置PAM认证服务的配置文件名称**
- ❑ **userlist\_enable=YES#与vsFTPD.user\_list配置文件有关**
- ❑ **listen=YES#是否允许vsFTPD运行在独立启动模式**
- ❑ **tcp\_wrappers=YES#使用tcp\_wrapper作为主机访问控制方式**

# 安装与配置实例

---

- **开发需求：**在一台具有Linux系统并安装有vsFTPD服务器的机器上，创建FTP目录。
- **目录upload：**匿名用户可以上传文件或目录，但是不能下载或更新文件或目录。
- **目录download：**匿名用户可以下载文件或目录，不能上传和修改文件或目录。
- **用户yan**可以对upload和download目录下的文件或目录做任何操作。

# 安装与配置实例（续）

---

步骤如下：

## （1）新建目录并设置其权限

```
[root@主机名]# mkdir /var/FTP/upload
```

```
[root@主机名]# chmod -R 777 /var/FTP/upload
```

```
[root@主机名]# mkdir /var/FTP/download
```

```
[root@主机名]# chmod -R 777 /var/FTP/download
```

# 安装与配置实例（续）

---

## (2) 修改配置文件/etc/vsFTPD/vsFTPD.conf

**anonymous\_enable=YES** //允许匿名访问，这是匿名服务器必须的

**write\_enable=YES** //全局配置可写

**no\_anon\_password=YES** //匿名用户login时不询问口令

**anon\_umask=077** //匿名用户上传的文件权限是-rw----

**anon\_upload\_enable=YES** //允许匿名用户上传文件

**anon\_mkdir\_write\_enable=YES** //允许匿名用户建立目录

**anon\_other\_write\_enable=YES** //允许匿名用户具有建立目录，上传之外的权限，如重命名，删除

**dirmessage\_enable=YES** //当使用者转换目录，则会显示该目录下的.message信息

**xferlog\_enable=YES** //记录使用者所有上传下载信息

**xferlog\_file=/var/log/vsFTPD.log** //将上传下载信息记录到/var/log/vsFTPD.log中

# 安装与配置实例（续）

---

**xferlog\_std\_format=YES //日志使用标准xferlog格式**

**idle\_session\_timeout=600 //客户端超过600s没有动作就自动被服务器踢出**

**data\_connection\_timeout=120 //数据传输时超过120s没有动作被服务器踢出**

**chown\_uploads=YES**

**chown\_username=daemon //上传文件的属主**

**FTPd\_banner=Welcome to d-1701.com FTP service. //FTP欢迎信息**

**anon\_max\_rate=80000 //设定匿名用户最大传输速度为80KBytes/s**

**check\_shell=NO //不检测SHELL**



# 安装与配置实例（续）

---

## （3）本地测试搭建好的匿名用户方式

□ [root@主机名]# **FTP 127.0.0.1**

## （4）远程客户端测试

□ **FTP://192.168.1.2**

## 4. Samba服务器

---

- Samba能够为选定的Unix或Linux目录（包括所有子目录）建立网络共享。
- 使得Windows用户可以像访问普通Windows下的文件夹那样来通过网络访问这些Unix或Linux目录。

# Samba简介

---

- ❑ **Samba是遵循GNU GPL的自由软件**
- ❑ **从1992年，为所有使用SMB/CIFS的客户端（如DOS和Windows、OS2、Linux、Unix）提供安全、稳定和快速文件和打印服务。**
- ❑ **Windows 2000、Windows XP、Windows NT、Windows 95、OS/2 Warp Connect和OS/2 Warp 4客户端在连接Samba服务器并使用共享服务时不需要安装额外的软件。**
- ❑ **官网：<http://www.Samba.org/>**

# Samba服务器安装

---

## □ 安装命令:

- **[root@主机名]# rpm -ivh Samba-3.0.rpm -f - -nodeps**
- **[root@主机名]# rpm -ivh Samba-client-3.0.33.rpm -f --nodeps**
- **[root@主机名]# rpm -ivh Samba-common-3.0.33.rpm -f --nodeps**

## □ 查询命令:

- **[root@主机名]# rpm -qa | grep Samba**
- **Samba服务器所依赖的所有服务器都已安装好。**

# Samba服务器启动与关闭

---

- 核心配置文件为smb.conf
- shell命令：
  - [root@主机名]# service smb start
  - [root@主机名]# service smb stop
  - [root@主机名]# service smb restart

# Mail服务器

---

## (1) Postfix

- **Postfix在性能上大约比sendmail快三倍，一台运行Postfix的PC机每天可以收发上百万封邮件。**
- **Postfix与sendmail兼容，从而使sendmail用户可以很方便地迁移到Postfix。**
- **Postfix被设计成在重负荷之下仍然可以正常工作，当系统运行超出了可用的内存或磁盘空间时，Postfix会自动减少运行进程的数目；当处理的邮件数目增长时，Postfix运行的进程不会跟着增加。**

# Mail服务器 (续)

---

## (2) ExtMail

- **Extmail是国内唯一活跃开发的中文开源邮件系统软件。**
- **最早诞生于2004年底，2005年9月正式发布。**
- **从最初的WebMail逐步发展成完整的邮件系统，并最早发布集成ExtMail的定制版Linux系统EMOS，极大地简化了安装设置，将用户从大量源码包和杂乱的文档中解放出来。**

# DNS服务器

---

## □ DNS：域名服务系统

### (1) 主域名服务器 (Master Server)

- 主要完成域内主机名及其相关信息的管理、更新和维护。
- 一个DNS服务器通常包括四类数据库：根域、正向解析域、反向解析域和反向回数、解析域。



# DNS服务器 (续)

---

## (2) 辅助域名服务器 (Slave Server)

- 当主、辅DNS服务器同时存在时，DNS数据库的信息管理、更新和维护在主DNS服务器完成。
- 辅DNS的进程初次启动时，向主DNS服务器请求并下载域内的数据库信息，此后，辅DNS服务器定期向主DNS服务器发出请求，并比较两者数据库文件的最后修改日期，若相同则无需更新，否则自动下载并更新。

# DNS服务器（续）

---

## （3）缓存域名服务器

- 缓存服务器是利用服务器缓存来存储从上级域或其它DNS域收到的信息，一直到信息过期或作废为止，缓存DNS服务器对任何分区都没有代理权限。
  - 。
- 它只控制查询，并向有权限的DNS服务器请求需要的信息。它不管理和维护任何DNS数据库的信息。

# 本章小结

---

- **Linux就是依靠互联网才迅速发展起来的，因此Linux系统最重要的功能之一是强大的网络功能。**
- **远程访问是Linux服务器使用中必不可少的操作。**
- **OpenSSH 是 SSH 协议的开源实现，已经成为很多发行版自带的工具软件。**
- **Linux支持的网络服务非常丰富，特别是Apache HTTP服务器、FTP 服务器、Samba服务器、Mail服务器、DNS服务器，以及DHCP服务器。**