第 1 章

Linux 网络设置与基础服务

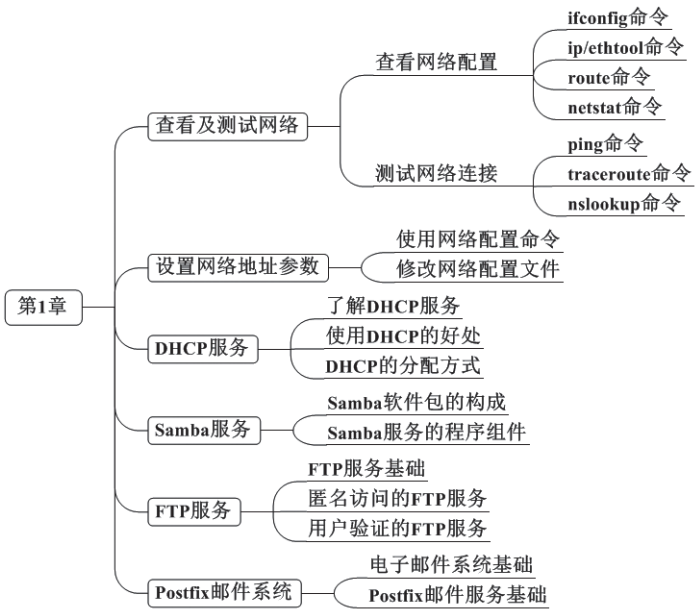
技能目标

- 学会查看及测试网络
- 学会设置网络地址参数
- 了解 DHCP、Samba、FTP、Postfix 服务

本章导读

之前大家已经学习了 Linux 系统的基本管理命令和技巧，为进一步学习 Linux 网络服务打下了基础。从本章开始，我们将陆续开始学习 Linux 系统的网络设置、文件服务、域名解析等在网络服务器方面的应用。

知识服务



1.1 查看及测试网络

查看及测试网络配置是管理 Linux 网络服务的第一步，本节中将学习 Linux 系统中的网络查看及测试命令，其中讲解的大多数命令以普通用户权限就可以完成操作。

1.1.1 查看网络配置

1. 使用 ifconfig 命令查看网络接口地址

主机的网络接口卡（网卡）通常称为“网络接口”。在 Linux 系统中，使用 ifconfig 命令可以查看网络接口的地址配置信息。

（1）查看活动的网络接口设备

当 ifconfig 命令不带任何选项和参数时，将显示当前主机中已启用（活动）的网络接口信息。例如，直接执行 ifconfig 命令后可以看到 eth0、lo 这两个网络接口的信息。这里要注意，CentOS 7 之前的网卡命名采用 eth0、eth1 等，而 CentOS 7 版本采用了一致的网络设备命名（Consistent Network Device Naming），该命名是与物理设备本身相关的。常见的其他网卡命名例如 eno16777736，表示板载的以太网设备（板载设备索引编号为 16777736）。但也可以将默认的网卡命名修改成 eth0、eth1 的形式，参见本章的知识服务。

```
[root@localhost ~]# ifconfig

eth0      flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
```

```
        inet 192.168.4.11  netmask 255.255.255.0  broadcast 192.168.4.255
        ……                          // 省略部分内容

        ……                          // 省略部分内容

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
      inet 127.0.0.1  netmask 255.0.0.0
        ……                          // 省略部分内容
```

在上述输出结果中，eth0 对应为第 1 块物理网卡，lo 对应为虚拟的回环接口。

- eth0：第 1 块以太网卡的名称。“eth0”中的“eth”是“ethernet”的缩写，表示网卡类型为以太网，数字“0”表示第 1 块网卡。如果有多个物理网卡，则第 2 块网卡表示为“eth1”，第 3 块网卡表示为“eth2”，以此类推。
- lo：“回环”网络接口，“lo”是“loopback”的缩写，它并不代表真正的网络接口，而是一个虚拟的网络接口，其 IP 地址默认是“127.0.0.1”。回环地址通常仅用于对本机的网络测试。

如果想要查看所有网络接口信息，只需要在 ifconfig 命令后面加上 -a 选项即可，即 ifconfig -a。

（2）查看指定的网络接口信息

当只需要查看其中某一个网络接口的信息时，可以使用网络接口的名称作为 ifconfig 命令的参数（不论该网络接口是否处于激活状态）。例如，执行“ifconfig eth0”命令后可以只查看网卡 eth0 的配置信息。

```
[root@localhost ~]# ifconfig eth0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.4.11  netmask 255.255.255.0  broadcast 192.168.4.255
      inet6 fe80::250:56ff:fe81:2986  prefixlen 64  scopeid 0x20<link>
      ether 00:50:56:81:29:86  txqueuelen 1000  (Ethernet)
      RX packets 5638126  bytes 457742188 (436.5 MiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 72986  bytes 5962876 (5.6 MiB)
      TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

从上述命令显示的结果中，可以获知 eth0 网卡的一些基本信息，如下所述。

- ether：表示网络接口的物理地址（MAC 地址），如“00:50:56:81:29:86”。网络接口的物理地址通常不能更改，是网卡在生产时确定的全球唯一的硬件地址。
- inet：表示网络接口的 IP 地址，如“192.168.4.11”。
- broadcast：表示网络接口所在网络的广播地址，如“192.168.4.255”。
- netmask：表示网络接口的子网掩码，如“255.255.255.0”。

除此以外，还能够通过“TX”“RX”等信息了解到通过该网络接口发送和接收的数据包个数、流量等更多属性。

2. 使用 ip/ethtool 命令查看网络接口

ip/ethtool 与 ifconfig 命令相同，也是参看网络接口的命令。但与 ifconfig 相比，ip/ethtool 命令的功能更强大，它不仅仅可以查看网络接口的基本信息，还可以查看更深层的内容，如查看网络接口的数据链路层、网络层信息和网络接口的速率、模式等信息。其中常用的命令有：

- ip link：查看网络接口的数据链路层信息。
- ip address：查看网络接口的网络层信息。
- ethtool eth0：查看指定网络接口的速率、模式等信息。

3. 使用 route 命令查看路由表条目

Linux 系统中的路由表决定着从本机向其他主机、其他网络发送数据的去向，是排除网络故障的关键信息。直接执行 route 命令可以查看当前主机中的路由表信息，在输出结果中，Destination 列对应目标网段的地址，Gateway 列对应下一跳路由器的地址，Iface 列对应发送数据的网络接口。

```
[root@localhost ~]# route
Kernel IP routing table
Destination  Gateway      Genmask        Flags  Metric  Ref  Use  Iface
192.168.4.0  *            255.255.255.0  U      0       0    0    eth0
default      192.168.4.1  0.0.0.0        UG     0       0    0    eth0
```

当目标网段为“Default”时，表示此行是默认网关记录；当下一跳为“*”时，表示目标网段是与本机直接相连的。例如，从上述输出信息中可以看出，当前主机与 192.168.4.0/24 网段直接相连，使用的默认网关地址是 192.168.4.1。

若结合“-n”选项使用，可以将路由记录中的地址显示为数字形式，这可以跳过解析主机名的过程，在路由表条目较多的情况下能够加快执行速度。例如，执行“route -n”命令后，输出信息中的“*”地址将显示为“0.0.0.0”，默认网关记录中的“default”也将显示为“0.0.0.0”。

```
[root@localhost ~]# route -n
Kernel IP routing table
Destination  Gateway      Genmask        Flags  Metric  Ref  Use  Iface
192.168.4.0  0.0.0.0      255.255.255.0  U      0       0    0    eth0
0.0.0.0      192.168.4.1  0.0.0.0        UG     100     0    0    eth0
```

4. 使用 netstat 命令查看网络连接情况

通过 netstat 命令可以查看当前系统的网络连接状态、路由表、接口统计等信息，是了解网络状态及排除网络服务故障的有效工具。以下是 netstat 命令常用的几个选项。

- -a：显示当前主机中所有活动的网络连接信息（包括监听、非监听状态的服务端口）。
- -n：以数字的形式显示相关的主机地址、端口等信息。
- -r：显示路由表信息。

- -l：显示处于监听（Listening）状态的网络连接及端口信息。
- -t：查看 TCP 协议相关的信息。
- -u：显示 UDP 协议相关的信息。
- -p：显示与网络连接相关联的进程号、进程名称信息（该选项需要 root 权限）。

通常使用“-anpt”组合选项，以数字形式显示当前系统中所有的 TCP 连接信息，同时显示对应的进程信息。结合命令管道使用“grep”命令，还可以在结果中过滤出所需要的特定记录。例如，执行以下操作可以查看本机中是否有监听“TCP 80”端口（即标准 FTP 服务）的服务程序，输出信息中包括 PID 号和进程名称。

```
[root@localhost ~]# netstat -anpt | grep ":80"
tcp6       0      0 :::80                   :::*                    LISTEN      15613/httpd
```


1.1.2 测试网络连接

1. 使用 ping 命令测试网络连通性

使用 ping 命令可以向目的主机持续地发送测试数据包，并显示反馈结果，直到按 Ctrl+C 组合键后中止测试，并显示最终统计结果。例如，以下操作将测试从本机到另一台主机 192.168.4.110 的连通性情况，连接正常时会收到返回的数据包。

```
[root@localhost ~]# ping 192.168.4.110
PING 192.168.4.110 (192.168.4.110) 56(84) bytes of data.
64 bytes from 192.168.4.110: icmp_seq=1 ttl=128 time=0.694 ms
64 bytes from 192.168.4.110: icmp_seq=2 ttl=128 time=0.274 ms
……                          // 按 Ctrl+C 组合键中止执行

--- 192.168.4.110 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1162ms
rtt min/avg/max/mdev = 0.274/0.484/0.694/0.210 ms
```

运行 ping 测试命令时，若不能获得从目标主机发回的反馈数据包，则表示在本机到目标主机之间存在网络连通性故障。例如，若看到“Destination Host Unreachable”的反馈信息，则表示目的主机不可达，可能目标地址不存在或者主机已经关闭；若看到“Network is unreachable”的反馈信息，则表示没有可用的路由记录（如默认网关），无法达到目标主机所在的网络。

```
[root@localhost ~]# ping 192.168.4.123
PING 192.168.4.123 (192.168.4.123) 56(84) bytes of data.
From 192.168.4.11 icmp_seq=2 Destination Host Unreachable
From 192.168.4.11 icmp_seq=3 Destination Host Unreachable
……                          // 省略部分内容
```

当网络中存在影响通信过程稳定性的因素（如网卡故障、病毒或网络攻击等）时，使用 ping 命令测试可能会频繁看到“Request timeout”的反馈结果，表示与目标主机间的连接超时（数据包响应缓慢或丢失）。除此以外，当目标主机有严格的防火墙限

制时，也可能收到发回“Request timeout”的反馈结果。

2. 使用 traceroute 命令跟踪数据包的路由途径

使用 traceroute 命令可以测试从当前主机到目的主机之间经过了哪些网络节点，并显示各中间节点的连接状态（响应时间）。对于无法响应的节点，连接状态将显示为“*”。例如，通过以下操作结果可以看出，从本机到目标主机 192.168.7.7 之间，中间需跨越一个路由器 192.168.4.1。

```
[root@localhost ~]# traceroute 192.168.7.7
traceroute to 192.168.7.7 (192.168.7.7), 30 hops max, 40 byte packets
 1  (192.168.4.1)  7.740 ms  15.581 ms  15.881 ms
 2  (192.168.7.7)  19.652 ms  19.995 ms  19.942 ms
```


traceroute 命令能够比 ping 命令更加准确地定位网络连接的故障点（中断点），执行速度也因此会比 ping 命令稍慢。在网络测试与排错过程中，通常会先使用 ping 命令测试与目的主机的网络连接，如果发现网络连接有故障，再使用 traceroute 命令跟踪查看是在哪个中间节点存在故障。

3. 使用 nslookup 命令测试 DNS 域名解析

当域名解析出现异常时，将无法使用域名的形式访问网络中的 Web 站点、电子邮件系统等服务。nslookup 命令是用来测试域名解析的专用工具，使用时只要指定要解析的目标域名作为参数即可。例如，执行“nslookup www.google.com”命令后，nslookup 程序将提交查询请求，询问站点 www.google.com 对应的 IP 地址是多少。

```
[root@localhost ~]# nslookup www.google.com
Server:         202.106.0.20                    // 所使用的 DNS 服务器
Address:        202.106.0.20#53

Non-authoritative answer:                       // 以下为 DNS 解析的反馈结果
Name:   www.google.com
Address: 173.194.127.51
……                                              // 省略部分内容
```

若能够成功反馈要查询域名的 IP 地址，则表示域名解析没有问题，否则需要根据实际反馈情况来判断故障原因。例如，若出现“…… no servers could be reached”的信息，表示不能连接到指定的 DNS 服务器；若出现“…… can't find xxx.yyy.zzz: NXDOMAIN”的信息，表示要查询的域名不存在。

```
[root@localhost ~]# nslookup www.google.com
;; connection timed out; trying next origin
;; connection timed out; no servers could be reached
```

1.2 设置网络地址参数

从本节开始将学习如何来修改 Linux 主机的各种网络地址参数。在 Linux 主机中，

手动修改网络配置包括两种最基本的方法。

- 临时配置：通过命令行直接修改当前正在使用的网络地址，修改后立即可以生效。这种方式操作简单快速、执行效率高，一般在调试网络的过程中使用。但由于所做的修改并没有固定地存放在静态的文件中，因此当重启 network 服务或重启主机后将会失效。
- 固定配置：通过配置文件来存放固定的各种网络地址，需要重启 network 服务或重启主机后才会生效。这种方式操作上相对要复杂一些，但相当于“永久配置”，一般在需要为服务器设置固定的网络地址时使用。

1.2.1 使用网络配置命令

1. 使用 ifconfig 命令修改网卡的地址、状态

ifconfig 命令不仅可以用于查看网卡配置，还可以修改网卡的 IP 地址、子网掩码，也可以绑定虚拟网络接口、激活或停用网络接口。

（1）修改网卡的 IP 地址、子网掩码

需要设置网卡的地址时，命令格式如下所示。

```
ifconfig 网络接口名称 IP 地址 [ netmask 子网掩码 ]
```

或者

```
ifconfig 网络接口名称 IP 地址 [/ 子网掩码长度 ]
```

通常后一种方式用得更多一些。当不指定子网掩码时，将使用 IP 地址所在分类的默认子网掩码。指定新的 IP 地址和子网掩码以后，原有的地址将会失效。例如，执行以下操作可以将网卡 eth0 的 IP 地址设置为 192.168.168.1，子网掩码长度为 24。

```
[root@localhost ~]# ifconfig eth0 192.168.168.1/24
```

或者

```
[root@localhost ~]# ifconfig eth0 192.168.168.1 netmask 255.255.255.0
```

（2）禁用、激活网络接口

需要临时禁用或者重新激活指定的网络接口时，需要结合“down”“up”开关选项。网络接口被禁用以后，将无法使用该网络接口与其他主机进行连接。例如，执行以下操作将会禁用网卡 eth1。

```
[root@localhost ~]# ifconfig eth1 down
```

（3）为网卡绑定虚拟接口

在对服务器网络进行调试的过程中，有时候需要临时在同一个网卡上使用一个新的 IP 地址，但是又不能覆盖原有 IP 地址而导致服务程序不可用。这时可以为网卡绑定一个虚拟的网络接口，然后再为虚拟接口设置新的 IP 地址（相当于一块网卡配多个

IP 地址）。

例如，执行以下操作可以为网卡 eth0 添加一个虚拟接口 eth0:0，并将这个虚拟接口的 IP 地址设置为 172.17.17.17。虚拟接口的 IP 地址和网卡原有的 IP 地址都可以正常使用。

```
[root@localhost ~]# ifconfig eth0:0 172.17.17.17
[root@localhost ~]# ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.0.58  netmask 255.255.255.0  broadcast 10.0.0.255
        inet6 fe80::250:56ff:fe81:2986  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:81:29:86  txqueuelen 1000  (Ethernet)
        RX packets 5647402  bytes 458488057 (437.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 74294  bytes 6128830 (5.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0:0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.17.17.17  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 00:50:56:81:29:86  txqueuelen 1000  (Ethernet)
```

可以根据需要添加更多的虚拟接口，如“eth0:1”“eth0:2”等。

2. 使用 route 命令添加、删除静态路由记录

route 命令不仅可以用于查看路由表信息，还可用来添加、删除静态的路由表条目，其中当然也包括设置默认网关地址（默认网关记录是一条特殊的静态路由条目）。

（1）添加、删除到指定网段的路由记录

通过“route add”操作可以添加路由记录，结合“-net”选项指定目标网段的地址，结合“gw”选项指定下一跳路由器的 IP 地址。例如，若要使本机访问另一个网段 192.168.3.0/24 的数据包都发给 192.168.4.254，可以执行以下操作。需要注意的是，默认网关的 IP 地址应该与本机其中一个接口的 IP 地址在同一个网段内。

```
[root@www ~]# route add -net 192.168.3.0/24 gw 192.168.4.254        // 添加静态路由
[root@www ~]# route -n                                              // 确认添加的路由条目
Kernel IP routing table
Destination   Gateway         Genmask         Flags   Metric   Ref   Use   Iface
192.168.4.0   0.0.0.0         255.255.255.0   U       0        0     0     eth0
192.168.3.0   192.168.4.254   255.255.255.0   UG      0        0     0     eth0
```

通过“route del”操作可以删除路由记录，只要结合“-net”选项指定对应路由记录中目标网段的地址即可。例如，执行以下操作可以删除前面添加到 192.168.3.0/24 网段的静态路由条目。

```
[root@www ~]# route del -net 192.168.3.0/24
[root@www ~]# route -n
Kernel IP routing table
```

```
Destination  Gateway     Genmask         Flags  Metric  Ref  Use  Iface
192.168.4.0  0.0.0.0     255.255.255.0   U      0       0    0    eth0
```

（2）添加、删除默认网关记录

添加、删除默认网关记录时，与添加、删除静态路由记录的命令格式类似，但指定目标网段时只需简单地使用“default”表示即可，无须再使用“-net”选项指明网段地址。例如，执行以下操作将先删除已有的到 192.168.4.1 的默认网关记录，再添加到 192.168.4.254 的默认网关记录。

```
[root@www ~]# route del default gw 192.168.4.1        // 删除默认网关记录 192.168.4.1
[root@www ~]# route add default gw 192.168.4.254      // 添加新的默认网关记录 192.168.4.254
```

需要注意的是，在同一个主机的路由表中只应有一条默认网关记录。若同时存在多条默认网关记录，可能会导致该主机的网络连接出现故障。

1.2.2 修改网络配置文件

当需要为 Linux 服务器设置固定的网络地址时，若还是用 ifconfig 等网络命令来进行设置，将会大大降低服务器运行的可靠性。若要使 Linux 主机在重启系统以后仍然能够使用相同的网络配置，那么直接修改配置文件是最好的方法。

下面将分别介绍最常见的几个网络配置文件。

1. 网络接口配置文件

网络接口的配置文件默认位于目录“/etc/sysconfig/network-scripts/”中，文件名格式为“ifcfg-XXX”，其中“XXX”是网络接口的名称。例如，网卡 eth0 的配置文件是“ifcfg-eth0”，回环接口 lo 的配置文件是“ifcfg-lo”。

```
[root@localhost ~]# ls /etc/sysconfig/network-scripts/ifcfg-*
/etc/sysconfig/network-scripts/ifcfg-eth0
/etc/sysconfig/network-scripts/ifcfg-lo
```

在网卡的配置文件 ifcfg-eth0 中，可以看到设置静态 IP 地址的部分内容如下。

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=192.168.4.1
NETMASK=255.255.255.0
GATEWAY=192.168.4.2
```

上述各配置项的含义及作用如下。

- DEVICE：设置网络接口的名称。
- ONBOOT：设置网络接口是否在 Linux 系统启动时激活。
- BOOTPROTO：设置网络接口的配置方式，值为“static”时表示使用静态指定的 IP 地址，为“dhcp”时表示通过 DHCP 的方式动态获取地址。
- IPADDR：设置网络接口的 IP 地址。

- NETMASK：设置网络接口的子网掩码。
- GATEWAY：设置网络接口的默认网关地址。

2. 启用、禁用网络接口配置

在 CentOS 6 系统中，当修改了网络接口的配置文件以后，若要使新的配置生效，可以重新启动 network 服务或者重启主机。默认情况下，重启 network 服务将会先关闭所有的网络接口，然后再根据配置文件重新启用所有的网络接口。

```
[root@localhost ~]# service network restart
```

CentOS 7 系统使用命令 systemctl restart network.service 重新启用所有的网络接口。

如果只是想禁用、启用某一个网络接口（而不是所有接口），可分别使用两个接口控制脚本 ifdown、ifup。例如，执行以下操作将会先关闭 eth0 网卡，然后再根据配置文件启用 eth0 网卡。

```
[root@localhost ~]# ifdown eth0
[root@localhost ~]# ifup eth0
```

3. 主机名称配置文件

在 CentOS 6 系统中，若要修改 Linux 系统的主机名，可以修改配置文件 /etc/sysconfig/network。在此文件中，“HOSTNAME”行用于设置主机名，而“NETWORKING”行用于设置 IPv4 网络的默认启用状态。例如，执行以下操作可以将主机名由默认的 localhost.localdomain 改为 www.kgc.cn。

```
[root@localhost ~]# vi /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=www.kgc.cn
```

之前已经学习过，CentOS 7 版本中的主机名配置文件变为 /etc/hostname 文件，而 systemd 的命令 hostnamectl 用于修改此文件信息。

4. 域名解析配置文件

（1）指定为本机提供 DNS 解析的服务器地址

/etc/resolv.conf 文件中记录了本机默认使用的 DNS 服务器的地址信息，对该文件所做的修改将会立刻生效。Linux 系统中最多可以指定 3 个（第 3 个以后的将被忽略）不同的 DNS 服务器地址，优先使用第 1 个 DNS 服务器。例如，执行以下操作可以指定默认使用的两个 DNS 服务器地址分别位于 202.106.0.20 和 202.106.148.1。

```
[root@localhost ~]# vi /etc/resolv.conf
search localdomain
nameserver 202.106.0.20
nameserver 202.106.148.1
```

resolv.conf 文件中的“search localdomain”行用来设置默认的搜索域（域名后缀）。例如，当访问主机“localhost”时，就相当于访问“localhost.localdomain”。

（2）本地主机映射文件

/etc/hosts 文件中记录着一份主机名与 IP 地址的映射关系表，一般用来保存经常需要访问的主机的信息。当访问一个未知的域名时，先查找该文件中是否有相应的映射记录，如果找不到再去向 DNS 服务器查询。

例如，若在 /etc/hosts 文件中添加“119.75.218.70 www.baidu.com”的映射记录，则当访问网站 www.baidu.com 时，将会直接向 IP 地址 119.75.218.70 发送 Web 请求，省略了向 DNS 服务器解析 IP 地址的过程。

```
[root@localhost ~]# cat /etc/hosts
127.0.0.1 localhost localhost.localdomain  localhost4 localhost4. localdomain4
…… // 省略部分内容
119.75.218.70     www.baidu.com
```

对于经常访问的一些网站，可以通过在 /etc/hosts 文件添加正确的映射记录，减少 DNS 查询过程，从而提高上网速度。当然，若添加了错误的映射记录，则可能会导致网站访问出现异常。另外，正因为 hosts 文件只保存在本地，所以其中的映射记录也只适用于当前主机，而无法作用于整个网络。

1.3 DHCP 服务

1. 了解 DHCP 服务

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是由 Internet 工作任务小组设计开发的，专门用于为 TCP/IP 网络中的计算机自动分配 TCP/IP 参数的协议。DHCP 服务避免了因手动设置 IP 地址所产生的错误，同时也避免了把一个 IP 地址分配给多台工作站所造成的地址冲突。DHCP 提供了安全、可靠且简单的 TCP/IP 网络设置，降低了配置 IP 地址的负担。DHCP 的网络结构如图 1.1 所示。

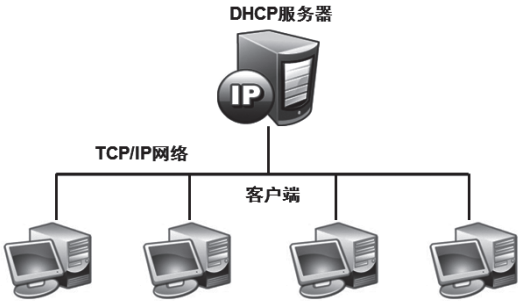


图 1.1 DHCP 网络结构

2. 使用 DHCP 的好处

Internet 是目前世界上用户最多的服务之一，有几亿人在使用 Internet。由于上网

时间的不确定性以及使用人员的技术水平不同，为每位用户分配一个固定的 IP 地址，不仅造成了 IP 地址的浪费，也会为 ISP 服务商带来高额的维护成本。而使用 DHCP 服务则有以下好处。

- 减少管理员的工作量。
- 避免输入错误的可能。
- 避免 IP 地址冲突。
- 当网络更改 IP 地址段时，不需要再重新配置每个用户的 IP 地址。
- 提高了 IP 地址的利用率。
- 方便客户端的配置。

3. DHCP 的分配方式

DHCP 的典型应用模式如下：在网络中架设一台专用的 DHCP 服务器，负责集中分配各种网络地址参数（主要包括 IP 地址、子网掩码、广播地址、默认网关地址、DNS 服务器地址）；其他主机作为 DHCP 客户机，将网卡配置为自动获取地址，即可与 DHCP 服务器进行通信，完成自动配置过程。

在 DHCP 的工作原理中，DHCP 服务器提供了三种 IP 地址分配方式：自动分配（Automatic Allocation）、手动分配（Manual Allocation）和动态分配（Dynamic Allocation）。

- 自动分配是当 DHCP 客户机第一次成功地从 DHCP 服务器获取到一个 IP 地址后，就永久地使用这个 IP 地址。
- 手动分配是由 DHCP 服务器管理员专门指定 IP 地址。
- 动态分配是当 DHCP 客户机第一次从 DHCP 服务器获取到 IP 地址后，并非永久地使用该地址，而是在每次使用完后，DHCP 客户机就会释放这个 IP 地址，供其他客户机使用。

关于 DHCP 的更多内容请访问课工场观看相关视频。

1.4 Samba 服务

在 Windows 网络环境中，主机之间进行文件和打印机共享是通过微软公司自己的 SMB/CIFS 网络协议实现的。SMB（Server Message Block，服务消息块）和 CIFS（Common Internet File System，通用互联网文件系统）协议是微软的私有协议，在 Samba 项目出现之前，并不能直接与 Linux/UNIX 系统进行通信。

Samba 是著名的开源软件项目之一，它在 Linux/UNIX 系统中实现了微软的 SMB/CIFS 网络协议，从而使得跨平台的文件共享变得更加容易。在部署 Windows、Linux/UNIX 混合平台的企业环境时，选用 Samba 可以很好地解决不同系统之间的文件互访问题。

1. Samba 软件包的构成

在 CentOS 6.5 系统的 DVD 安装光盘中可以找到与 Samba 相关的几个软件包，主要包括服务端软件 samba、客户端软件 samba-client，用于提供服务端和客户端程序的公共组件 samba-common。

大部分软件包已经随 CentOS 6.5 系统默认安装好了，用户可以查询系统中 samba 相关软件包的安装情况。

```
[root@localhost ~]# rpm -qa | grep "^samba"
samba-common-3.6.9-164.el6.x86_64
samba-client-3.6.9-164.el6.x86_64
samba4-libs-4.0.0-58.el6.rc4.x86_64
samba-winbind-clients-3.6.9-164.el6.x86_64
samba-winbind-3.6.9-164.el6.x86_64
samba-3.6.9-164.el6.x86_64
```

2. Samba 服务的程序组件

Samba 服务器提供 smbd、nmbd 两个服务程序，分别完成不同的功能。其中，smbd 负责为客户机提供服务器中共享资源（目录和文件等）的访问；nmbd 负责提供基于 NetBIOS 协议的主机名称解析，以便为 Windows 网络中的主机进行查询服务。

安装好 samba 软件包以后，在 CentOS 系统中会添加名为 smb 和 nmb 的标准系统服务，管理员可以通过 service 工具来控制 Samba 服务的启动与终止。

```
[root@localhost ~]# service smb start
启动 SMB 服务 :                                    [ 确定 ]
启动 NMB 服务 :                                    [ 确定 ]
[root@localhost ~]# service nmb start
```

使用 netstat 命令可以验证服务进程状态，其中 smbd 程序负责监听 TCP 协议的 139 端口（SMB 协议）、445 端口（CIFS 协议），而 nmbd 服务程序负责监听 UDP 协议的 137 ～ 138 端口（NetBIOS 协议）。

```
[root@localhost ~] # netstat  -anptu | grep "mbd"
tcp    0    0 0.0.0.0:139           0.0.0.0:*    LISTEN   6306/smbd
tcp    0    0 0.0.0.0:445           0.0.0.0:*    LISTEN   6306/smbd
tcp    0    0 :::139                :::*         LISTEN   6306/smbd
tcp    0    0 :::445                :::*         LISTEN   6306/smbd
udp    0    0 192.168.4.255:137     0.0.0.0:*             6310/nmbd
udp    0    0 192.168.4.11:137      0.0.0.0:*             6310/nmbd
udp    0    0 0.0.0.0:137           0.0.0.0:*             6310/nmbd
udp    0    0 192.168.4.255:138     0.0.0.0:*             6310/nmbd
udp    0    0 192.168.4.11:138      0.0.0.0:*             6310/nmbd
udp    0    0 0.0.0.0:138           0.0.0.0:*             6310/nmbd
```

关于 Samba 的更多内容请访问课工场观看相关视频。

1.5 FTP 服务

1.5.1 FTP 服务基础

FTP（File Transfer Protocol，文件传输协议）是典型的 C/S 结构的应用层协议，需要由服务端软件、客户端软件两个部分共同实现文件传输功能。关于 FTP 服务，可以从以下几个方面进行了解。

1. FTP 连接及传输模式

FTP 服务器默认使用 TCP 协议的 20、21 端口与客户端进行通信。20 端口用于建立数据连接，并传输文件数据；21 端口用于建立控制连接，并传输 FTP 控制命令。根据 FTP 服务器在建立数据连接过程中的主、被动关系，FTP 数据连接分为主动模式和被动模式，两者的含义及主要区别如下。

- 主动模式：服务器主动发起数据连接。首先由客户端向服务端的 21 端口建立 FTP 控制连接，当需要传输数据时，客户端以 PORT 命令告知服务器“我打开了某端口，你过来连接我”，于是服务器从 20 端口向客户端的该端口发送请求并建立数据连接。
- 被动模式：服务器被动等待数据连接。如果客户机所在网络的防火墙禁止主动模式连接，通常会使用被动模式。首先由客户端向服务端的 21 端口建立 FTP 控制连接，当需要传输数据时，服务器以 PASV 命令告知客户端“我打开了某端口，你过来连接我”，于是客户端向服务器的该端口（非 20）发送请求并建立数据连接。

客户端与服务器建立好数据连接以后，就可以根据从控制连接中发送的 FTP 命令上传或下载文件了。在传输文件时，根据是否进行字符转换，分为文本模式和二进制模式。

- 文本模式：又称为 ASCII（American Standard Code for Information Interchange，美国信息交换标准码）模式，这种模式在传输文件时使用 ASCII 标准字符序列，一般只用于纯文本文件的传输。
- 二进制模式：又称为 Binary 模式，这种模式不会转换文件中的字符序列，更适合传输程序、图片等非纯文本字符的文件。

使用二进制模式比文本模式更有效率，大多数 FTP 客户端工具可以根据文件类型自动选择文件传输模式，而无需用户手工指定。

2. FTP 用户类型

使用 FTP 客户端软件访问服务器时，通常要用到一类特殊的用户账号，其用户名

为 ftp 或 anonymous，提供任意密码（包括空密码）都可以通过服务器的验证，这样的用户称为“匿名用户”。匿名用户一般用于提供公共文件的下载，如提供一些免费软件、学习资料下载的站点。

除了不需要密码验证的匿名用户以外，FTP 服务器还可以直接使用本机的系统用户账号来进行验证，这些用户通常被称为“本地用户”。在 CentOS 6.5 系统中，匿名用户也有对应的本地系统用户账号“ftp”，但对于 vsftpd 服务来说，本地用户指的是除了匿名用户以外的其他系统用户。

有些 FTP 服务器软件还可以维护一份独立的用户数据库文件，而不是直接使用系统用户账号。这些位于独立数据库文件中的 FTP 用户账号，通常被称为“虚拟用户”。通过使用虚拟用户，将 FTP 账户与 Linux 系统账户的关联性降至最低，可以为系统提供更好的安全性。

3. FTP 服务器软件的种类

在 Windows 系统中，常见的 FTP 服务器软件包括 FileZilla Sener、Serv-U 等，而在 Linux 系统中，vsftpd 是目前在 Linux/UNIX 领域应用十分广泛的一款 FTP 服务软件，本课程将以 vsftpd 进行讲解。

vsftpd 服务的名称来源于“Very Secure FTP Daemon”，该软件针对安全特性方面做了大量的设计。除了安全性以外，vsftpd 在速度和稳定性方面的表现也相当突出。根据 ftp.redhat.com 服务器反映的数据，vsftpd 可以支持 15000 个用户并发连接。

4. FTP 客户端工具的种类

最简单的 FTP 客户端工具莫过于 ftp 命令程序了。Windows 系统和 Linux 系统默认都自带有 ftp 命令程序，可以连接到 FTP 服务器进行交互式的上传、下载通信。

除此以外，还有大量的图形化 FTP 客户端工具。Windows 中较常用的包括 CuteFTP、FlashFXP、LeapFTP、Filezilla 等，在图形化的客户端程序中，用户通过鼠标和菜单即可访问、管理 FTP 资源，而不需要掌握 FTP 交互命令，因此使用户的操作更加简单、易于使用。

还有一些下载工具软件，如 FlashGet、Wget 等，包括大多数网页浏览器程序，都支持通过 FTP 协议下载文件，但因不具备 FTP 上传等管理功能，通常不称为 FTP 客户端工具。

1.5.2 匿名访问的 FTP 服务

访问匿名 FTP 服务器时，不需要密码验证，任何人都可以使用，非常方便。当需要提供公开访问的文件下载资源（如 ftp.redhat.com），或者让用户上传一些不需要保密的数据资料时，可以选择搭建匿名 FTP 服务器。

1. 准备匿名 FTP 访问的目录

在 CentOS 6.5 系统中，FTP 匿名用户对应的系统用户为 ftp，其宿主目录 /var/ftp/

也就是匿名访问 vsftpd 服务时所在的 FTP 根目录。基于安全性考虑，FTP 根目录的权限不允许匿名用户或其他用户有写入权限（否则访问时会报 500 错误）。

为了后续测试方便，可以在 /var/ftp/ 目录下创建一个用于下载的测试文件。例如，执行以下操作创建一个压缩包文件作为测试。

```
[root@localhost ~]# tar zcf /var/ftp/vsftpdconf.tar.gz /etc/vsftpd/
```

/var/ftp/ 目录下默认设置了一个名为 pub 的子文件夹，可以在匿名访问 FTP 时供上传文件使用。执行以下操作可以使匿名用户 ftp 对该目录拥有写入权限，以便上传数据。


```
[root@localhost ~]# chown ftp /var/ftp/pub/
[root@localhost ~]# ls -ld /var/ftp/pub/
drwxr-xr-x. 2 ftp root 4096 2 月 13 /var/ftp/pub/
```

2. 开放匿名用户配置并启动 vsftpd 服务

配置 vsftpd 服务时，是否开放匿名 FTP 访问取决于配置项“anonymous_enable”，只要将其设为“YES”，即表示允许匿名用户访问，反之表示禁用。启用匿名用户后，默认情况下只具有读取权限，匿名用户可以完成目录列表、下载文件等基本的 FTP 任务。

若要进一步放开权限，允许匿名用户上传文件，则需要开放更多的配置。主要涉及以下几个配置项，分别对应不同的 FTP 操作权限。

- write_enable：用于启用 / 禁止 vsftpd 服务的写入权限，是全局性的选项，不管是匿名用户、本地用户还是虚拟用户，若要允许其上传，都必须启用此配置项。
- anon_upload_enable：用于允许 / 禁止匿名用户在现有的可写入目录中上传文件。
- anon_mkdir_write_enable：用于允许 / 禁止匿名用户在现有的可写目录中创建文件夹，即上传目录。
- anon_other_write_enable：用于允许 / 禁止匿名用户的其他写入权限，包括删除、改名、覆盖等操作。

上述四个配置项，应根据匿名 FTP 服务器的实际应用需求来选择设置。若只要求能够上传文件，则只需启用“write_enable”和“anon_upload_enable”就足够了；若还要求能够上传文件夹，则需进一步启用“anon_mkdir_write_enable”。只有在希望匿名用户能够对上传的文件和目录进行覆盖、删除等管理操作时，才需要启用“anon_other_write_enable”。

例如，若要设置 vsftpd 服务器提供匿名访问，允许匿名用户上传、下载，但禁止使用删除操作，可以参考以下步骤修改配置文件。

```
[root@localhost]# vi /etc/vsftpd/vsftpd.conf
anonymous_enable=YES                    // 允许匿名用户访问
local_enable=NO                         // 若不需启用本地用户，可将此项设为 NO
```

```
write_enable=YES                    // 开放服务器的写权限
anon_umask=022                      // 设置匿名用户上传数据的权限掩码
anon_upload_enable=YES              // 允许匿名上传文件
anon_mkdir_write_enable=YES         // 允许匿名用户创建目录
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=YES
pam_service_name=vsftpd
userlist_enable=YES                 // 因未启用本地用户 , 可将用户列表功能禁用
tcp_wrappers=YES
```

在上述配置内容中，还使用了“anon_umask”配置项，此配置项用于设置匿名用户所上传文件或目录的权限掩码。权限掩码的作用与子网掩码的作用有点类似，用于去掉特定的权限。例如，若上传权限掩码设为 022，则所上传的文件或目录将减去 022 对应的这部分权限（Group 和 Other 的 w 权限），实际结果是所上传文件的默认权限为 644、目录的实际权限为 755。

确认配置无误后，就可以启动 vsftpd 服务了，使用 netstat 命令可以确认监听状态。

```
[root@localhost vsftpd]# service vsftpd start
为 vsftpd 启动 vsftpd:                [ 确定 ]
[root@localhost vsftpd]# netstat -anpt | grep "vsftpd"
tcp     0     0 0.0.0.0:21     0.0.0.0:*       LISTEN      8989/vsftpd
```

3. 测试匿名 FTP 服务器

配置好 vsftpd 并启动服务以后，就可以使用 FTP 客户端工具进行验证了。Windows 主机中可以直接在“我的电脑”地址栏内输入 URL 地址访问，如“ftp://192.168.4.11”。在 Linux 的字符界面中，可以使用 ftp 命令进行测试。例如，执行以下操作可以匿名登录到 FTP 服务器 192.168.4.11（ftp 命令需要安装 ftp-0.17-54.el6.x86_64.rpm 包）。

```
[root@localhost ~]# ftp 192.168.4.11
Connected to 192.168.4.11 192.168.4.11.
220 (vsFTPd 2.2.2)
Name (192.168.4.11:root): ftp       // 用户名为 ftp 或 anonymous
331 Please specify the password.
Password:                           // 密码可任意输入 , 或直接回车
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>                                // 成功登录后的操作提示符
```

成功登录 FTP 服务器以后，将进入到显示“ftp>”提示符的交互式操作环境。在此操作界面中，可以执行实现各种 FTP 操作的交互指令（执行？或 help 命令可查看指

令帮助）。例如，以下操作过程依次展示了列表查看、下载文件、上传文件等相关的操作。

```
ftp> ls                                    // 查看 FTP 服务器中的内容
227 Entering Passive Mode (192,168,4,11,69,105)
150 Here comes the directory listing.
drwxr-xr-x    5 14       0            4096 Feb 12 2013 pub
-rw-r--r--    1 0        0            2639 Jun 20 20:44 vsftpdconf.tar.gz
226 Directory send OK.
ftp> lcd /opt                              // 将本地目录切换到 /opt/
Local directory now /opt
ftp> get vsftpdconf.tar.gz                 // 将文件下载到本地（/opt/ 目录）
……                                         // 省略部分内容
ftp> lcd /root                             // 将本地目录切换到 /root/
Local directory now /root
ftp> cd pub                                // 将 FTP 目录切换到 /pub/
250 Directory successfully changed.
ftp> put install.log                       // 将文件上传到服务器（/pub/ 目录）
……                                         // 省略部分内容
ftp> ls                                    // 查看所上传文件的权限
227 Entering Passive Mode (192,168,4,11,29,225)
150 Here comes the directory listing.
-rw-r--r--    1 14       50           37039 Jun 20 23:03 install.log
226 Directory send OK.
ftp> quit                                  // 断开 ftp 连接并退出
221 Goodbye.
[root@localhost ~]#
```

在已经知道要下载文件的完整 URL 地址的情况下，用户也可以使用 wget 命令工具直接下载文件，省去了交互式的登录过程。

```
[root@localhost ~]# wget ftp://192.168.4.11/vsftpdconf.tar.gz
--2014-06-26 07:25:29--  ftp://192.168.4.11/vsftpdconf.tar.gz
           => 'vsftpdconf.tar.gz'
正在连接 192.168.4.11:21... 已连接 .
正在以 anonymous 登录 ... 登录成功 !
==> SYST ... 完成 .    ==> PWD ... 完成 .
==> TYPE I ... 完成 .  ==> 不需要 CWD.
==> SIZE vsftpdconf.tar.gz ... 2639
==> PASV ... 完成 .    ==> RETR vsftpdconf.tar.gz ... 完成 .
长度 :2639 (2.6K)( 非正式数据 )
100%[======================================>] 2,639       --.-K/s   in 0s
2014-06-26 07:25:29 (6.95 MB/s) - 'vsftpdconf.tar.gz' 已保存 [2639]
```

1.5.3 用户验证的 FTP 服务

vsftpd 可以直接使用 Linux 主机的系统用户作为 FTP 账号，提供基于用户名 / 密

码的登录验证。用户使用系统用户账号登录 FTP 服务器后，将默认位于自己的宿主目录中，且在宿主目录中拥有读写权限。

1. 基本的本地用户验证

使用基本的本地用户验证，只需打开 local_enable、write_enable 两个配置项。为了提高上传文件的权限，可以将权限掩码设为 077（仅宿主用户拥有权限）。若还希望将所有的宿主目录禁锢在其宿主目录中，可以添加 chroot_local_user 配置项，否则用户将能够任意切换到服务器的 /var/、/etc/、/boot/ 等宿主目录以外的文件夹，这样一来便存在安全隐患。

```
[root@localhost ~]# vi /etc/vsftpd/vsftpd.conf
local_enable=YES
write_enable=YES
local_umask=077
chroot_local_user=YES
…… // 省略部分内容
[root@localhost ~]# service vsftpd reload
关闭 vsftpd:                                    [ 确定 ]
为 vsftpd 启动 vsftpd:                          [ 确定 ]
```

在访问要求用户验证的 FTP 服务器时，如果使用 URL 地址的形式，必须指定 FTP 账号名称，如访问“ftp://laya@192.168.4.11”，可以根据提示输入密码进行验证，当然也可以在 URL 地址中直接指定密码，如访问“ftp://laya:123456@192.168.4.11”。

通过 ftp 命令访问 FTP 服务器时，只需输入正确的用户名、密码验证即可。例如，以下操作将以系统用户 laya 登录到 FTP 服务器 192.168.4.11，并进行上传文件测试。

```
[root@localhost ~]# ls > uptest.txt                  // 创建用于上传的测试文件
[root@localhost ~]# ftp 192.168.4.11
Connected to 192.168.4.11(192.168.4.11).
220 (vsFTPd 2.2.2)
Name (192.168.4.11:root): laya                       // 以 laya 用户登录
331 Please specify the password.
Password:                                            // 以 laya 用户的密码验证
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put uptest.txt                                  // 将文件上传到服务器
……                                                   // 省略部分内容
ftp> ls                                              // 查看上传文件的权限
227 Entering Passive Mode (192,168,4,11,136,45)
150 Here comes the directory listing.
-rw-------    1 507      507           167 Jun 26 23:48 uptest.txt
226 Directory send OK.
ftp> quit
221 Goodbye.
```

2. 使用 user_list 用户列表文件

当 vsftpd 服务器开放了“local_enable”配置项以后，默认情况下除 root 外的所有的系统用户都可以登录到此 FTP 服务器。若只希望对一小部分系统用户开放 FTP 服务，则需要开放用户列表控制的相关配置项，其中主要包括 userlist_enable、userlist_deny。例如，执行以下操作后 vsftpd 服务器将只允许 laya、vanko、hunter 这三个用户登录。

```
[root@localhost ~]# vi /etc/vsftpd/user_list          // 添加以下三行，并清空其他内容
laya
vanko
hunter
[root@localhost]# vi /etc/vsftpd/vsftpd.conf
……                                                   // 省略部分内容
userlist_enable=YES                                  // 启用 user_list 用户列表文件
userlist_deny=NO                                     // 不禁用 user_list 列表中的用户
[root@localhost]# service vsftpd reload              // 重新加载 vsftpd 服务的配置
```

关于 vsftpd 的更多内容请访问课工场观看相关视频。

1.6 Postfix 邮件系统

1. 电子邮件系统基础

（1）邮件系统角色、邮件协议

Internet 网络中的电子邮件系统并不是一个孤立的体系。除了需要 DNS 服务器提供邮件域的解析，通过 Web 服务器提供邮箱操作界面以外，邮件收取、传递等功能也是由不同的组件来提供的。

- 邮件系统的角色

在实现电子邮件收发的完整系统中，根据各组件所处的位置、承担的功能不同，可以分为不同的角色。

MTA（Mail Transfer Agent，邮件传输代理）：一般被称为邮件服务器软件。MTA 软件负责接收客户端软件发送的邮件，并将邮件传输给其他的 MTA 程序，是电子邮件系统中的核心部分。Exchange 和 Sendmail、Postfix 等服务器软件都属于 MTA。

MUA（Mail User Agent，邮件用户代理）：一般被称为邮件客户端软件。MUA 软件的功能是为用户提供发送、接收和管理电子邮件的界面。在 Windows 平台中常用的 MUA 软件包括 Outlook Express、Outlook、Foxmail 等，在 Linux 平台中常用的 MUA 软件包括 Thunderbird、Kmail、Evolution 等。

MDA（Mail Delivery Agent，邮件分发代理）：MDA 软件负责在服务器中将邮件分发到用户的邮箱目录。MDA 软件相对比较特殊，它并不直接面向邮件用户，而是在后台默默地工作。有时候 MDA 的功能可以直接集成在 MTA 软件中，因此经常被忽略。

通过邮件系统中的角色划分可以看出，电子邮件系统与其他 C/S（Client/Server，

客户端 / 服务器）模式的网络应用一样，包括独立的客户端和服务器端软件。

- 邮件通信协议

在电子邮件通信过程中，邮件传递、收取是最基本的两个功能，应用于不同角色的软件之间。其中，最常用的三种邮件协议如下所述。

SMTP（Simple Mail Transfer Protocol，简单邮件传输协议）：主要用于发送和传输邮件。MUA 使用 SMTP 协议将邮件发送到 MTA 服务器中，而 MTA 将邮件传输给其他 MTA 服务器时同样也使用 SMTP 协议。SMTP 协议使用的 TCP 端口号为 25。对于支持发信认证的邮件服务器，将会采用扩展的 SMTP 协议（Extended SMTP）。

POP（Post Office Protocol，邮局协议）：主要用于从邮件服务器中收取邮件。目前 POP 协议的最新版本是 POP3。大多数 MUA 软件都支持使用 POP3 协议，因此该协议应用最为广泛。POP3 协议使用的 TCP 端口号为 110。

IMAP（Internet Message Access Protocol，互联网消息访问协议）：同样用于收取邮件。目前 IMAP 协议的最新版本是 IMAP4。与 POP3 相比较，IMAP4 协议提供了更为灵活和强大的邮件收取、管理功能。IMAP4 协议使用的 TCP 端口号为 143。

只有电子邮件客户端和服务器同时支持 SMTP 和 POP/IMAP 协议，才能够实现完整的邮件发送和收取功能。

（2）常见的邮件服务器软件

当用户在享受电子邮件带来的便利的时候，往往看到的只是邮件系统的“品牌”，而忽视了邮件系统的“幕后英雄”——邮件服务器软件。例如，使用 163 邮箱的用户可能并没有想过，网易公司的邮件服务器是使用什么软件搭建的。然而，对于企业邮件系统的管理员来说，则必须熟练掌握邮件服务器软件的配置和管理。

邮件服务器软件的种类并不是很多，常见的主要包括以下几种。

- 商业邮件系统

Exchange：Windows 系统中最著名的邮件服务器软件，也是微软公司的重量级产品，可以与活动目录等应用很好地结合在一起。当使用 Windows 服务器平台构建电子邮件系统时，Exchange 自然就成为首选。

Notes/Domino：由 IBM 公司出品的商业电子邮件和办公协作软件产品，其功能丰富、强大，集成性较好且提供跨系统平台的支持，给用户提供了广泛的选择。多应用于一些高校、政府部门、银行等较大型的企业单位。

- 开源邮件系统

Sendmail：对于运行在 UNIX/Linux 环境中的邮件服务器，Sendmail 无疑是资格最老的，目前仍然有许多企业的电子邮件系统是使用 Sendmail 进行搭建的。Sendmail 运行的稳定性较好，但安全性欠佳。

Qmail：另一款运行在 UNIX/Linux 环境中的邮件服务器，比 Sendmail 具有更好的执行效率，且配置、管理更加方便，很多商用电子邮件系统都采用 Qmail 作为服务器。

Postfix：同样是运行在 UNIX/Linux 环境中的邮件服务器，Postfix 由 Wietse 负责开发，其目的是为 Sendmail 提供一个更好的替代产品。Postfix 在投递效率、稳定性、

服务性能及安全性等方面都有相当出色的表现。

2. Postfix 邮件服务基础

Postfix 邮件服务器采用了模块化的设计，由许多个不同的程序集合而成，分别用于实现不同的功能。

关于 Postfix 的更多内容请访问课工场观看相关视频。

本章总结

- 使用 ifconfig 命令可以查看、配置网络接口的属性。
- 使用 route 命令可以查看、管理主机的路由表记录。
- 使用 ping 和 traceroute 命令可以测试主机的网络连接。
- 配置文件 ifcfg-eth0、network、hosts、resolv.conf 等可分别用于设置主机的 IP 地址、主机名、域名映射、DNS 服务器地址等参数。
- FTP 的主动模式是由服务端先发起数据连接，被动模式是由客户端先发起数据连接。
- 邮件系统所包含的角色有 MTA、MUA、MDA。电子邮件通信过程中最常用的三种邮件协议是 SMTP、POP、IMAP。

本章作业

1. 列举 Linux 系统中的主要网络配置文件并说明其作用。

2. 修改配置文件，将当前主机的 IP 地址改为 172.16.16.11，主机名改为 dhcpsvr。

3. 为网卡 eth0 添加两个虚拟接口 eth0:0、eth0:1，其对应的 IP 地址分别为 192.168.7.7/24、192.168.8.8/24。

4. 使用 vsftpd 搭建匿名 FTP 服务器，允许匿名用户上传文件到 upload 目录下，并能够在 upload 目录下执行创建文件夹、删除文件、重命名文件等操作。

5. 用课工场 APP 扫一扫，完成在线测试，快来挑战吧！