第 2 章 基本概念

1、 目前在以太网最常见的接头是 RJ-45 接头，共 8 蕊，如图

而 RJ-45 接头又因为每条蕊线的对应不同而分为 568A 和 568B 接头，这两款接头的蕊线对应关系如表：（568A、568B）

表2-1 接头与蕊线的对应关系

接头名称	1	2	3	4	5	6	7	8
568A	白绿	绿	白橙	蓝	白蓝	橙	白棕	棕
568B	白橙	橙	白绿	蓝	白蓝	绿	白棕	棕

其中白绿指白绿色。目前实际使用的只有 1、2、3、6 蕊，一对用于传送，一对用于接收，其他的则是特殊场合会用到。但由于主机与主机连接以及主机与集线器连接时，所使用的网线引脚定义不同，对应网线又分为两种：

- 并行线：两边接头同为 568A 时称为并行线，用在连接主机网卡与集线器。（同为 568A、并行线）
- 跳线：一边为 568A 一边为 568B 的接头称为跳线，用在直接连接两台主机的网卡。（跳线）

568A：绿、蓝、橙、棕、白绿、白橙、白蓝、白棕

568B：橙、蓝、绿、棕、白橙、白绿、白蓝、白棕

2、 集线器、交换机和路由器：

- 集线器所有的输出端口分享集线器输入端口的带宽，属于共享媒介。（集线器、共享媒介）
- 交换机（Switch）具备自动寻址能力和交换作用，由于交换机根据所传递信息包的目的地址，将每一信息包独立地从源端口送至目的端口，避免了和其他端口发生碰撞，所以交换机所有的输出端口的带宽都等于输入端口的带宽（前提是不同时使用同一条线）。（交换机、具备自动寻址能力和交换作用）
- 当机器的数量达到一定数目时，使用集线器和交换机会既不安全，也会出现堵塞，所以可以使用路由器把较大的网络划分成一个小的子网。（路由器、划分为子网）

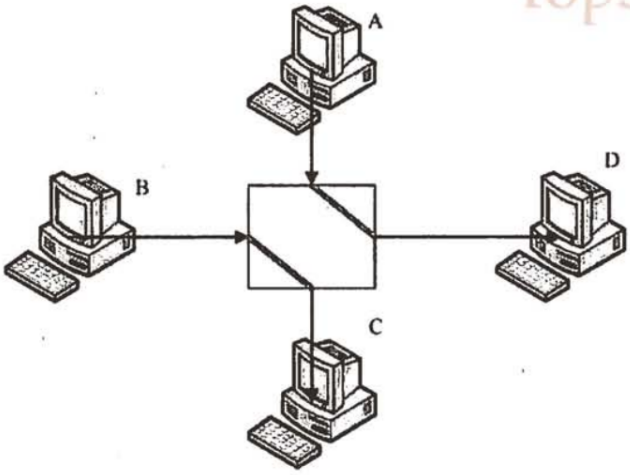


图 2-5　Switch 的带宽简介

如果所示，当数据从 A 传送到 D 时，使用交换机时并不会影响数据从 B 传送到 C。但是当数据同时从 A 和 D 传送到 C 时，也会发生和器一样的堵塞。

3、　全双工：可同时发送和接收数据。共享媒介（如集线器）不可能实现全双工。（全双工同时发送和接收、共享媒介不能全双工）

半双工：同一时间只能发送或者接收数据，不能同时进行。（半双工、同一时间只能接收或发送）

单工：任何时候只能发送或接收数据。（只能接收或发送）

4、　所谓结构化布线指的是将各个网络的组件划分成组，分别安装与布置到企业内部，这样，将来想要升级网络硬件或者移动某些网络设备时，只需要变化类似配线盘的机柜处，以及在末端的墙上预留孔与主机设备的连接就能够达到目的了。（结构化布线、划分为组）

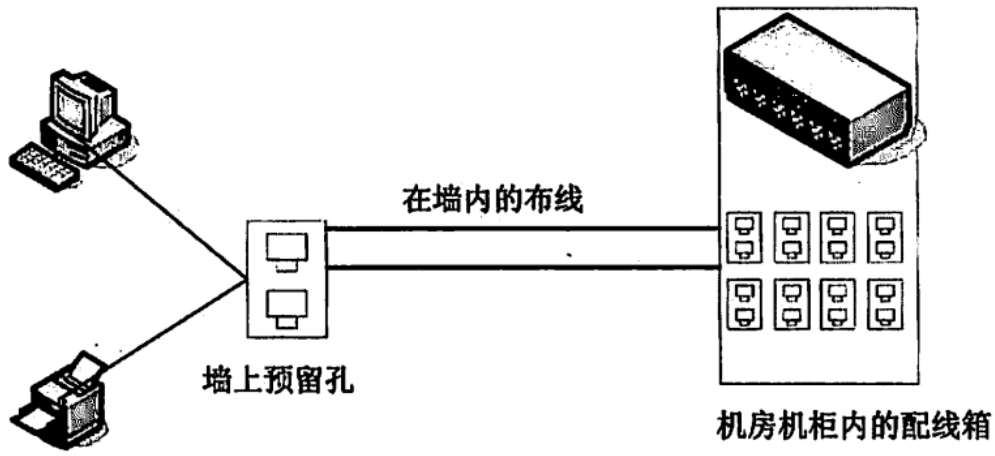
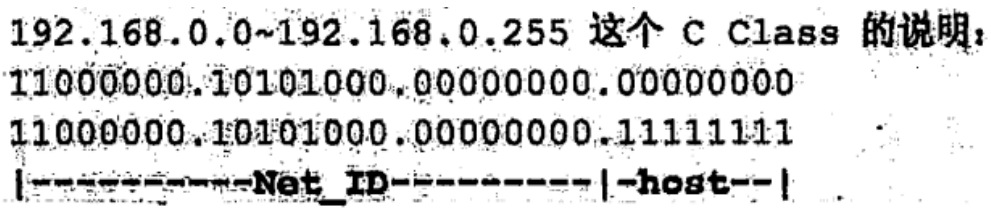


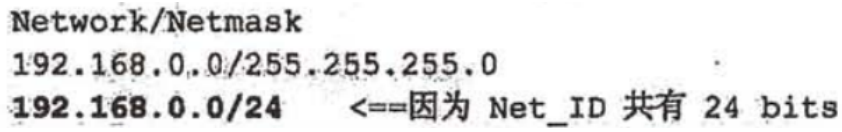
图 2-6　结构化布线简易图示

5、 在 IP 的 32bit 信息中，主要分为 Net_ID 和 HOST_ID 两个部分。（网络 ID、主机 ID）



6、 子网掩码的有几个字节为 0,表示有几个数字是 HOST_ID。（0 的数量就是主机 ID 的位数）

7、 由子网掩码可以推算出 Broadcast 的 IP，所以常常会有这样的写法：（网络 ID 位数、24 位）



8、 每台主机都会存在一个路由表，数据的传递将依据这个路由表进行传送。使用 route 命令查询路由表：（路由表、route 命令）

```
[root@linux ~]# route [-n]
```

-n：将主机名称以 IP 的方式显示。（-n、以 IP 方式显示）

```
lan@lan-Aspire-E1-571G:~$ route -n
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
0.0.0.0         192.168.1.1     0.0.0.0         UG    600    0        0 wlp3s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 wlp3s0
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlp3s0
```

U：代表该路由可用。（U、可用）

G：代表该网段需要经由 Gateway 来帮忙转发。(G、需要网关转发)

H：代表该行路由为一台主机。(H、是一台主机)

9、 在 Linux 环境下，各网络服务与端口号的对应默认项是写在/etc/services 文件内。不过如果是 Client 端的话，由于 Client 端口都是主动向 Server 端要数据，所以 Client 端就随机取一个大于 1024 且没有在用的端口号来进行连接。（服务与端口号对应默认在/etc/services）

10、 ICMP 全称是因特网信息控制协议，基本上是一个错误侦测与回报的机制，最大的功能就是可以确保我们的网络的连接状态与连接的正确性。（ICMP：错误侦测与回报的机制）

11、 最大传输单元（MTU）是指一种通信协议的某一层上面所能通过的最大数据包大小（以字节为单位）。设置该值可以防止由于数据包过大导致底层添加包头时数据出

错导致需要进行重组。如 TCP 层数据设置过大，IP 层就无法添加 IP 表头，需要对数据进行重组。（MTU：最大传输单元）

第 3 章 局域网架构简介与 linux 版本选择

1、 linux 主机直接连接到 internet 环境：

(1) 让 linux 与一般 pc 处于同等地位（同等地位，家庭用户，无防火墙）

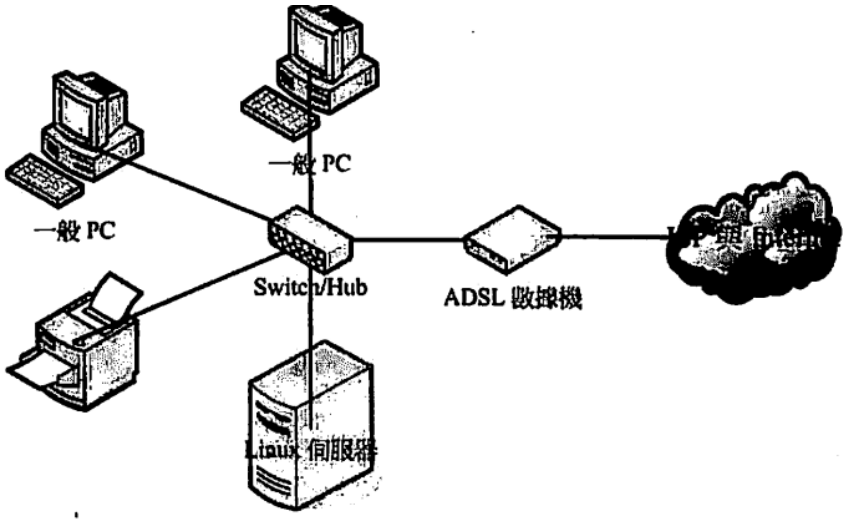


图 3-1 Linux 服务器取得 Public IP 的联机方式之一（具有多个可用 IP 情况）

优点：适合一般家庭用户。

缺点：没有防火墙，无法对网络进行访问控制，网管人员对进入客户端的数据包没有任何管理能力。不适合企业。

(2) 让 linux 与一般 PC 分开（分开多 IP，IP 分享器防火墙，易维护）

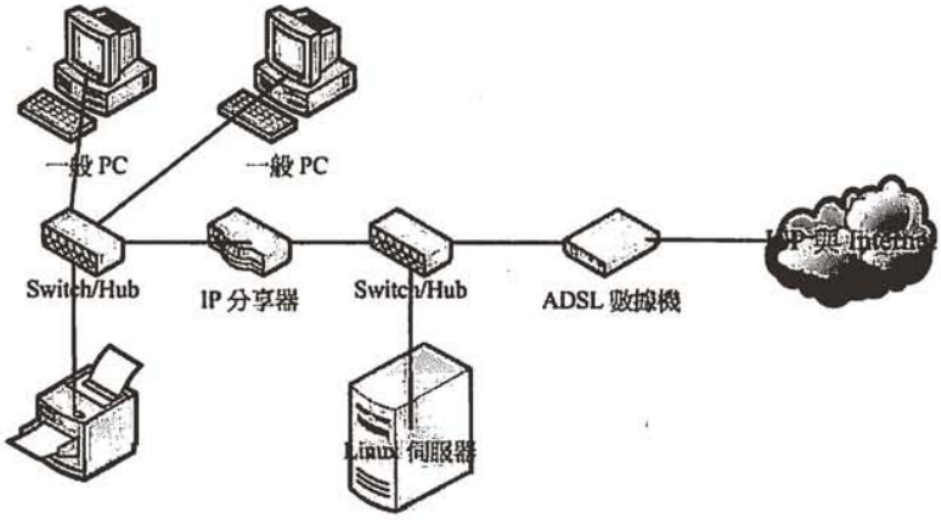


图 3-2 Linux 服务器取得 Public IP 的联机方式之二（具有多个可用 IP 情况）

有多个 Public IP 时，可以使用这种规则。linux 服务器提供 Internet 的 WWW 或 Mail 服务，拥有 Public IP，而且可以在 IP 分享器上设置防火墙规则，对主机有相当程序的管理，易于维护。

(3)　让 linux 直接管理 LAN（直接管理，单 IP，双网卡，做防火墙，宕机中断）

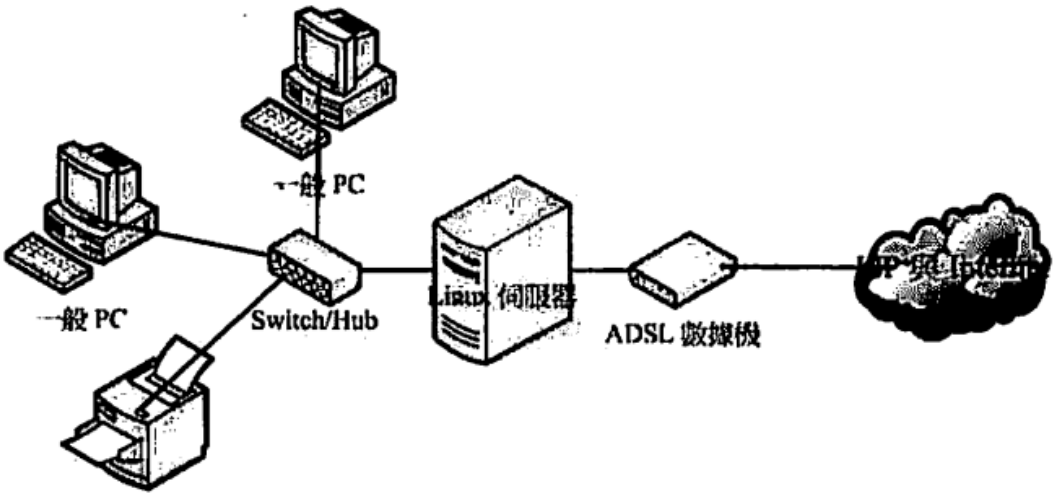


图 3-3　让 Linux 管理 LAN 的布线情况

优点：无论有多少 IP，特别是只有一个 Public IP 时，必须用这种方式。linux 作为 IP 分享器，必须具备两个网卡，分别对外、对内进行管理。linux 服务器还可以作为防火墙进行管理。

缺点：linux 宕机时，整个系统对外联系就中断了。此外，linux 的服务有些复杂，可能会造成维护上的困难。适合小型局域网。

2、　linux 主机放在 LAN 里面（LAN 里面，阻挡攻击，规则复杂）

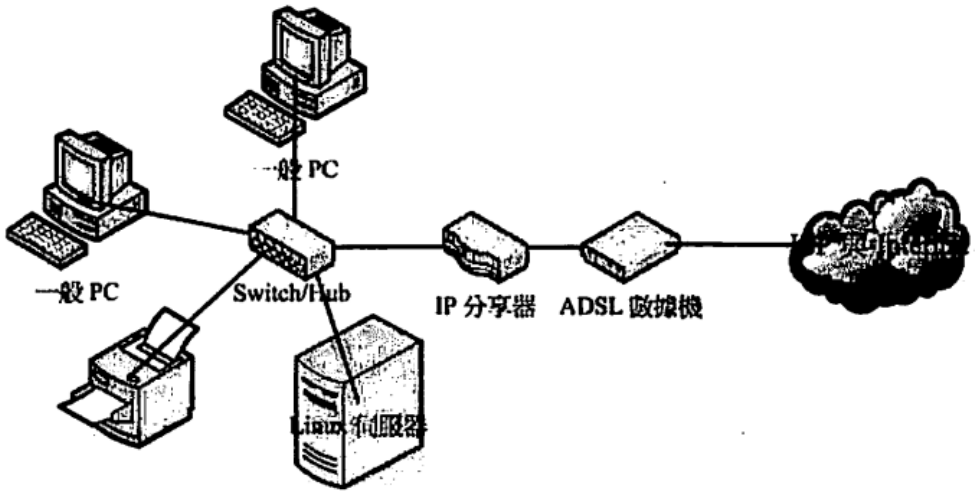


图 3-4　Linux 主机放在 LAN 里面的布线情况

优点：IP 分享器的防火墙功能可以为 linux 服务器阻挡攻击，比较安全。

缺点：由于涉及数据包转发，所以防火墙的规则变得相当复杂。

3、　网络组件名词：

- Node(节点)：连接在网络上的、具有网卡卡号的设备都可以是节点。（Node、有网卡的设备）

- Workstation(工作站)：没有对 Internet 提供网络服务，但是提供用户登录进行学术研究的高级主机，都可以称为工作站。

4、 无线网络最大的问题是“无线的安全性”。购买无线网络基地台时，注意它是否是“限制 MAC”，如此一来，至少可以锁网卡，只让指定的网卡可以使用您的无线基地台，增加安全性。（限制 MAC、只让指定的网卡使用）

第 4 章 连上 Internet

1、 dmesg 命令用于显示开机信息。（dmesg、开机信息）

2、 lspci 命令显示所有的 pci 设备信息。pci 是一种总线，而通过 pci 总线连接的设备就是 pci 设备了。如今，我们常用的设备很多都是采用 pci 总线了，如：网卡、存储等。（lspci、pci 设备）

3、 lsmod 命令用于查看已经加载的模块。通常会 lsmod | grep 来查看指定的模块是否已经加载以使用模块提供的功能支持。（lsmod、查看已经加载的模块）

4、 depmod 命令用于分析可载入模块的相依性。（depmod 命令、分析模块的相仿性）

5、 modprobe 命令用于智能地向内核中加载模块或者从内核中移除模块。 modprobe 会根据 depmod 所产生的相依关系，决定要载入哪些模块。若在载入过程中发生错误，在 modprobe 会卸载整组的模块。

6、 与网络相关的文件：

(1) /etc/sysconfig/network：主要功能在于设置主机名称及能否启动 Network。设置后务必重启。

(2) /etc/sysconfig/network-scrips/ifcfg-etho：设置网卡参数的文件，里面可以设置 Network、IP、Netmask、Broadcast、Gateway、开机时的 IP 取得方式（DHCP、Static）、是否在开机的时候启动等等。ifcfg-etho 是第一块网卡，ifcfg-eth1 是第二块网卡，依此类推。

(3) /etc/modprobe.conf：开机时用来设置加载内核模块的文件就是 modprobe.conf。

(4) /etc/resolv.conf：设置 DNS IP 的文件。这个文件设置错误可能导致能 ping 通 IP 但输入网址却上不了网。

(5) /etc/hosts：记录计算机的 IP 对应主机的名称或者主机的别名。

(6) /etc/services：记录架构在 TCP/IP 上的所有协议，包括 HTTP、FTP、SSH、Telnet 等服务所定义的端口数，都是在这个文件中规定的。

(7) /etc/protocols：定义 IP 数据包协议的相关数据，包括 ICMP、TCP、UDP 等方面的数据包协议的定义等。

7、 网络方面的启动指令：

(1) /etc/init.d/networking restart：一口气重新启动整个网络参数。它会主动去读取所有的网络设置文件。

(2) ifup etho(ifdown eth0)：启动或者关闭某个网络接口。

8、 要拨号连接上网时，可以使用 rp-pppoe 软件。

第 5 章 linux 常用的网络命令

1、 ip 命令基本上是集合了 ifconfig 与 route 这两个命令。

- ip link 可以设置与设备有关的设置，包括 MTU 以及该网络接口的 MAC 等，当然也可以启动或关闭某个网络接口。（ip link：设备有关）

```
[root@linux ~] ip link show
```

- ip address 主要在设置与 IP 有关的各项参数，包括 netmask、broadcast 等。（ip address：IP 有关）
- ip route 主要是路由的观察与设置。（ip route：路由）

2、 下面两个命令需要有无线网卡才能使用：

- iwlist: 利用无线网卡进行无线 AP 的检测与取得相关的数据。（iwlist：无线网卡、检测和取得数据）
- iwconfig：设置无线网卡的相关参数。（iwconfig：无线网卡参数）

3、 使用 dhClient 命令可以快速的将网络设置为使用 DHCP 协议。

4、 traceroute 命令可以追踪两台主机之间通过的各个节点通信状态的好坏，用于检查网络环境。如果 5 秒内听不到回应，屏幕上就会出现一个“*”，告知该节点没有响应。但有些防火墙或主机可能会将 traceroute 命令的 ICMP 数据包扔掉，有些 Gateway 本来就不支持 traceroute 的功能。（traceroute：追踪节点状态）

```
lan@lan-Aspire-E1-571G:~$ traceroute -n www.baidu.com
traceroute to www.baidu.com (111.13.100.91), 30 hops max, 60 byte packets
 1  192.168.1.1  1.808 ms  1.754 ms  1.811 ms
 2  172.18.90.1  6.881 ms  6.955 ms  7.056 ms
 3  120.196.168.105  51.976 ms  32.540 ms  49.838 ms
 4  183.233.35.5  29.848 ms 183.233.35.45  25.684 ms 183.233.35.5  29.830 ms
 5  120.196.243.225  29.812 ms  29.810 ms  29.801 ms
 6  221.183.13.65  29.792 ms 221.183.38.161  45.365 ms 221.183.19.13  45.347 ms
 7  * * 221.176.15.209  88.180 ms
 8  221.183.19.50  86.259 ms  74.997 ms 221.183.18.134  77.141 ms
 9  111.13.98.249  72.470 ms * *
10  111.13.98.249  77.499 ms 111.13.98.253  77.259 ms  74.759 ms
11  111.13.108.1  66.027 ms * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
lan@lan-Aspire-E1-571G:~$
```

5、 Netstat 命令用于显示各种网络相关信息、如网络连接、路由表、接口状态 、多播成员等等。（netstat、网络相关信息）

6、 host 命令可以用来查出某个主机名称的 IP。（host、查出某个主机名称的 IP）

7、 nslookup 命令和 host 基本上是一样的，用来作为 IP 与主机名称对应的检查，同样使用/etc/resolv.conf 这个文件作为 DNS 服务器的来源选择。

8、 可以通过 Telnet、SSH 或者 FTP 等协议来进行远程主机的登录。（telnet、ssh 或 ftp、远程主机的登陆）

- Telnet

```
[root@linux ~]# Telnet [host|IP] [port]

范例一：连接到成大梦之大地这个 BBS 站
[root@linux ~]# Telnet bbs.dorm.ncku.edu.tw
bbs.ccns.ncku.edu.tw ⊙
⊙ 140.116.250.3 [DreamBBS Ver.040223]
欢迎光临。系统负载：0.16 0.16 0.16 [负载正常]
```

- 使用 FTP 登录后，可以使用 help(或问号？)来查询可用的命令。
- LFTP 命令和 FTP 命令非常类似，同样可以使用 help 来显示出可以执行的命令。还过 LFTP 多了书签功能，而且使用了类似 Bash 的指令功能。

9、 lynx 及 wget 是文本界面的浏览器，是在文本界面下上网浏览的好工具。

- lynx 最大的功能是查阅 linux 本机上面以 HTML 语法写成的文件信息。

```
[root@linux ~]# lynx http://www.kernel.org
```

- wget 是一个下载文件的工具，它支持 HTTP，HTTPS 和 FTP 协议。（lynx 浏览，wget 下载。）

10、 数据包捕获功能：

(1) tcpdump：分析数据包的流向，监听数据包的内容。如果使用的传输数据是明文，则在 Router 上可能被人家监听到。（tcpdump、监听数据包的内容）

```
范例一：以 IP 与 Port Number 捉下 eth0 这个网卡上的数据包，持续 3 秒
[root@linux ~]# tcpdump -i eth0 -nn
```

(2) ethereal：网络流量分析软件，分为文本界面与图形界面，文本界面的用法与 tcpdump 类似。

11、 nc，有的系统将执行文件改名为 netcat，可用来取代 telnet 进行某些服务端口的检测工作。

第 7 章 主机基本安全之一：限制 linux 对外连接的端口

1、 nmap 命令：通过网络的测试软件辅助，可测试非本机上的其他网络主机，但这有违法之嫌。（nmap 命令、测试软件辅助）

```
[root@linux ~]# nmap 192.168.10.0/24
```

第 10 章 认识网络安全

1、 Dos 攻击：客户端利用 3 次握手，发送一个 SYN，要求服务器打开一个端口，但却丢弃响应数据并重复发送 SYN，服务器就会一直在空等并开启大量端口空等，等到主机全部端口启用完毕，系统就完了。（Dos 攻击、利用 3 次握手、丢弃响应数据）

2、 网管人员必备技巧与任务：

- 了解什么是需要保护的内容
- 预防黑客入侵
- 主机环境安全化
- 防火墙规则的制订
- 实时维护主机
- 良好的教育训练
- 完善的备份计划

3、 入侵恢复工作

(1) 立即拔除网络线

(2) 分析日志文件信息，找到可能的入侵途径

(3) 重要数据备份

(4) 重新安装

(5) 软件的漏洞修补

(6) 关闭和修补不需要的服务

(7) 数据恢复与恢复服务设置

(8) 连上 Internet

第 11 章 linux 防火墙与 NAT 主机

1、 防火墙分为硬件防火墙和软件防火墙。硬件防火墙由厂商设计好的主机硬件，以提供数据包过滤机制为主，并将其他功能拿掉。软件防火墙本身就是保护网络安全的一套软件，例如，iptables 与 TCP Wrappers 都可以称为软件防火墙。

2、 linux 系统上防火墙的主要类别：

- IP Filter(数据包过滤机制)：利用 TCP/IP 数据包表头的 IP 来源、端口号等数据进行过滤，以判断该数据包是否能进入本机取得本机资源。如 iptables。
- Proxy(代理服务器)

3、 防火墙的一般部署方法与过滤技巧：

(1) 单一 linux 主机兼任防火墙功能，这类防火墙通常至少需要有两个接口，将可信任的内部网段与不可信任的外部 Internet 分开，所以可以分别设置两个网络接口的防火墙规则。

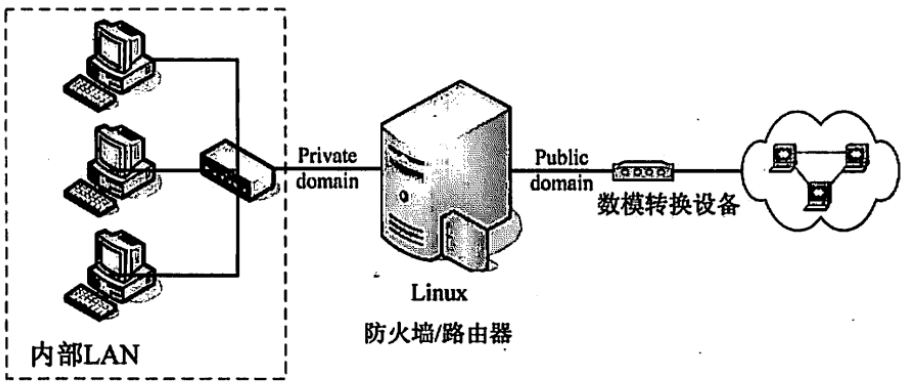


图 11-2 单一 Linux 防火墙主机

(2) 单一 linux 防火墙，但 LAN 内另设防火墙：保证某些特殊的设备。

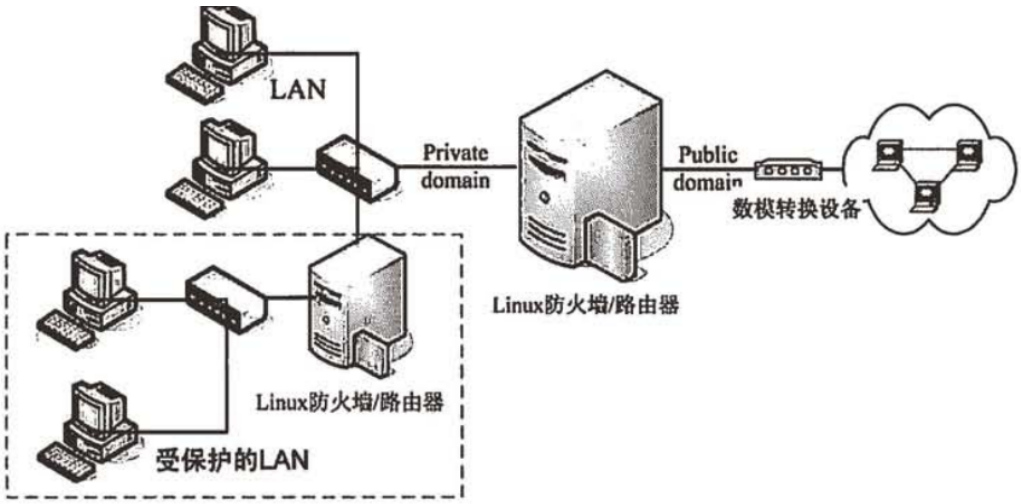
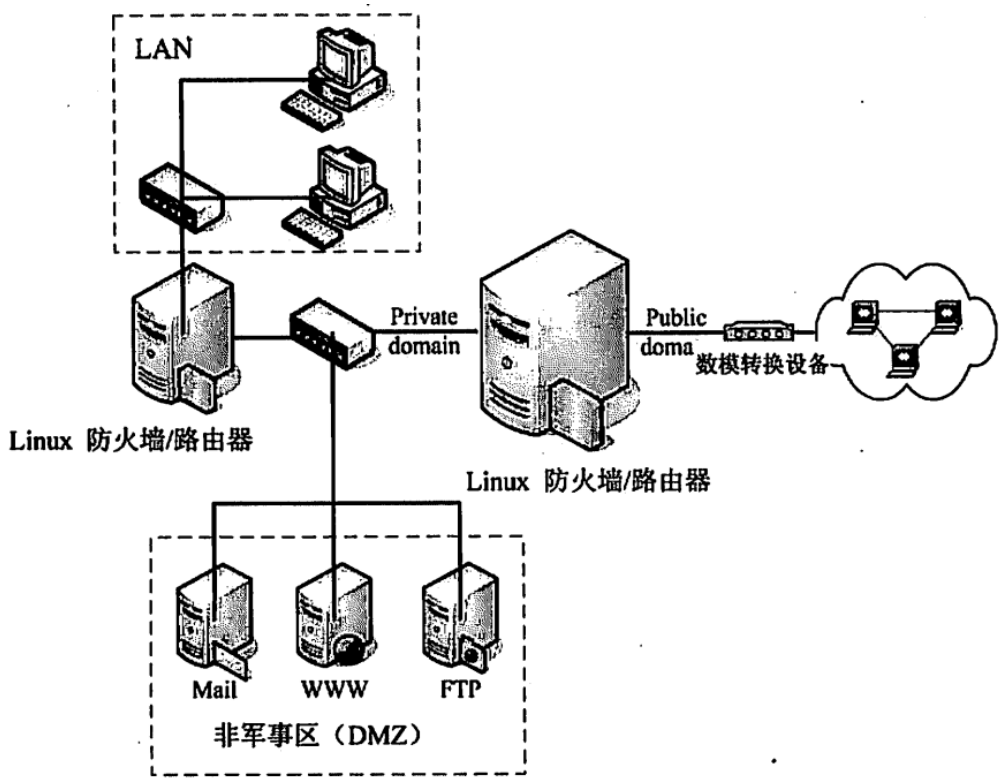


图 11-3　单一 Linux 防火墙主机，但 LAN 内另设防火墙

(3)　在防火墙后端的主机设置，适合大型企业，但设置上有一定的难度。



4、　iptables 至少可以有下面这几种阻止数据包的方式：

(1)　拒绝让 internet 的数据包进入 linux 主机的某些 port

(2)　拒绝让带有某些特殊标记的数据包进入，如带 SYNC 的主动联机的标记

(3)　拒绝某些来源 IP 的数据包进入

(4)　分析硬件地址来提供服务

5、 防火墙的使用限制

(1) 防火墙不能有效阻止病毒或木马程序

(2) 防火墙对于来自内部LAN的攻击无能为力

6、 iptables至少有3个默认table（filter、nat、mangle），较常用的是本机的filter表格，这也是默认表格，另一个则是后端主机的nat表格。如果安装linux时选择让系统自动建立防火墙，则系统有个默认的防火墙规则。（iptables、3个默认table、filter、nat、mangle）

7、 本机的防火墙规则：

(1)

```
[root@linux ~]# iptables [-t tables] [-L] [-nv]
参数:
-t : 后面接 table，例如 nat 或 filter，若省略此项目，则使用默认的filter
-L : 列出目前的 table 的规则
-n : 不进行IP与HOSTNAME的反查，显示信息的速度会快很多。
-v : 列出更多的信息，包括通过该规则的数据包总个数、相关的网络接口等

范例：列出 filter 表格的3条链的规则
[root@linux ~]# iptables -L -n
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

(2) 清除规则：

```
[root@linux ~]# iptables [-t tables] [-FXZ]
参数:
-F : 清除所有的已定规则
-X : 除掉所有用户“自定义”的链(应该说的是tables)
-Z : 将所有的 chain 的计数与流量统计都归零
```

8、 当数据包不在我们设置的规则之内时，该数据包通过与否，以Policy的设置为准。

```
[root@linux ~]# iptables [-t nat] -P [INPUT,OUTPUT,FORWARD] [ACCEPT,DROP]
参数：
-P ：定义策略( Policy )。注意，这个P为大写
ACCEPT ：该数据包可接受
DROP   ：该数据包直接丢弃，不让 Client 端知道为何被丢弃
```

9、 简单地说，NAT 是内部 LAN 主机的 IP 共享器。通过修改数据包的来源 IP 和目的 IP 实现多台主机同时通过一条 ADSL 网络联机到 Internet 上。注意：NAT 主机一定是路由器，但因为 NAT 主机会修改表头数据，因此与单纯转发数据包的路由器不同。

第 13 章 远程联机服务器 Telnet/SSH/VNC/XDCMP/RSH

1、 通常情况下，因特网服务的主机不要开放联机服务。

2、 由于 telnet 是明文传输，所以使用时需要注意一些事项：（telnet、明文传输）

(1) 以受限的配置文件来规范联机的 IP

(2) root 不能直接以 telnet 登录 linux 主机

(3) 加上防火墙 iptables

(4) 加上防火墙/etc/hosts.allow 机制

(5) 非必要时不要启动 telnet

3、 SSH 通过对联机数据包加密的技术来进行数据传递，它可以用来取代 Internet 上较不安全的 finger、R Shell、talk 及 Telnet 等联机模式。SSH 协议默认状态下本身提供两个服务器功能：一个是类似 Telnet 的远程联机使用 shell 的服务器，亦即是俗称的 SSH，SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议；另一个是类似 FTP 服务的 sftp-Server，可以提供更安全的 FTP 服务。

4、 公钥和私钥：公钥是公开的，任何人都可获得；私钥是私有的，只能自己拥有。如要实现安全登录的话，首先需要在客户端向服务器端请求登录页面时，服务器生成公钥和私钥，然后将公钥随登录页面一起传递给客户端浏览器，当用户输入完用户名密码点击登录时，登录页面中的 JavaScript 调用非对称加密算法对用户名和密码用用公钥进行加密。然后再提交到服务器端，服务器端利用私钥进行解密，再跟数据库中的用户名密码进行比较，如果一致，则登录成功，否则登录失败。（公钥加密、私钥解密、随登陆页面一起传递）

5、 使用以下命令来启动 SSH 服务：（sshd restart、启动 ssh 服务）

```
[root @ linux ~] # /etc/init.d/sshd restart
```

daemon，也就是守护进程。 daemon 服务程序一般以 d 结尾。（daemon、守护进程、以 d 结尾）

注意：rcn.d 目录下面的文件都是软链接，指向 init.d 目录的文件，而这个 init.d 目录存放可执行文件。n 是数字 0～6，表示运行级别。init.d 里面的脚本包含了完整的 start、stop、status、reload 等参数，推荐使用。

6、 SSH 在 linux Client 端使用的是 SSH 命令，通常使用方法如下：

- 直接登录到对方主机的方法：（直接登陆、ssh）

```
1．直接登录到对方主机的方法：
[root@linux ~]# ssh account@hostname
```

- 不登录对方主机，直接在对方主机执行命令的方法：（不登陆、直接执行命令）

```
2．不登录对方主机，直接在对方主机执行命令的方法：
[root@linux ~]# ssh dmtsai@localhost date
```

注意：其中的 account 指的是登录用户，hostname 指登录地址，如

不指定用户：

```
ssh 192.168.0.11
```

指定用户：

```
ssh -l root 192.168.0.11
```

```
ssh root@192.168.0.11
```

7、 使用 sftp 程序使用 SSH 的 FTP 功能。

```
[root@linux ~]# sftp dmtsai@localhost
Connecting to localhost...
dmtsai@localhost's password: <== 这里请输入密码啊。
sftp> <== 这里就是在等待您输入ftp命令的地方了。
```

8、 scp 命令在两个主机之间复制文件，它比 sftp 更简单。这个命令和 cp 很相像。（scp、复制文件）

```
1. 将数据由本机上传到远程主机上去
[root@linux ~]# scp /etc/crontab dmtsai@localhost:/home/dmtsai/
dmtsai@localhost's password: <== 这里请输入密码啊。
crontab                   100%  620     0.6KB/s   00:00
# 这个例子的作用是将本机目录的/etc/crontab文件传送给 dmtsai这个用户，
# 而这个用户在"localhost"那台主机上。
# 仔细看一下，会有一个传输数据的信息跑出来。
```

9、 所有的SSH相关的设置都放在/etc/ssh/sshd_config里。

10、 不要开放SSH的登录权限给所有Internet上的主机。

第14章 NFS服务器

1、 NFS（网络文件系统）：不同的机器、不同的操作系统之间可以彼此共享文件。适合小公司或学校单位内部unix like机器共享文件。但是windows主机与linux主机之间的沟通，还是以SAMBA为好。

2、 NFS使用的端口是随机选择的，惟一的限制是小于1024。那么，客户端如何知道服务器使用哪个端口呢？答案是使用远程过程调用RPC。

远程过程调用（RPC）服务最主要的功能就是指定每个NFS功能所对应的端口号，并且传递该信息给客户端，让客户端可以连接到正确的端口上去。NFS启动时随机取数个端口并主动向RPC注册，然后RPC固定使用111端口来监听客户端的需求并应答客户端正确的端口。注意，启动NFS之前，RPC要先启动，否则NFS无法向RPC注册。另外，RPC若重启，原来注册的端口数据会丢失。RPC必须先于NFS启动，否则NFC会注册失败。（RPC、指定每个NFS功能所对应的端口号）

3、 NFS、NIS都是RPC Server的一种。

4、 NFC客户端使用root账号登录文件系统时，默认情况下会被主动的压缩成为匿名者；当客户端的UID在服务器端不存在时，也会被压缩成匿名者。

5、 以CentOS 4.x为例，要设置好NFS服务器，需要两个软件：

(1) NFS主程序：nfs-utils

(2) RPC主程序：portmap

6、 NFS最主要的几个文件：

(1) /etc/exports：NFS的主要配置文件，但系统并没有默认值，所以一开始这个文件不一定存在，可使用vi自行建立。

(2) /usr/sbin/exportfs：维护NFS共享资源的命令，我们可以利用这个命令重新共享/etc/exports变更的目录资源、将NFS Server共享的目录重新共享等等。

(3) /usr/sbin/showmount：这是另一个重要的NFS命令，exportfs用在NFS Server端，而showmount则主要用在Client端。这个命令可以用来观察NFS服务器共享出来的目录资源。

(4) /var/lib/nfs/*tab：日志文件都放在/var/lib/nfs目录里。

7、 NFS服务器的架设也很简单，先编辑好主要配置文件/etc/exports，再启动portmap（RPC主程序），然后启动nfs，NFS服务器就架设成功了。

8、 /etc/exports文件的配置很简单，每一行最前面是要共享出来的目录，然后是这个目录可以依照不同的权限共享给不同的主机。

```
[root@linux ~]# vi /etc/exports
/tmp        192.168.1.0/24(ro)  localhost(rw)   *.ev.ncku.edu.tw(ro,sync)
# [共享目录] [第一台主机(权限)]   [可用主机名]       [可用通配符]
```

9、 在NFS服务器设置妥当之后，我们可以先自行测试一下是否可以联机。具体做法就是利用showmount这个命令来查阅：

```
[root@linux ~]# showmount [-ae] [hostname|IP]
参数:
-a ：显示目前主机与客户端的NFS联机共享状态
-e ：显示某台主机的/etc/exports所共享的目录数据
```

10、 在NFS的安全性上，需要在以下几方面多加注意：

(1) 利用iptables做大范围联机的限制

(2) 利用tcp Wrappers限制

(3) 使用/etc/exports设置更安全的权限

(4) 更安全的partition规划

11、 远程NFS服务器的挂载

(1) 开启portmap和nfslock

```
[root@linux ~]# /etc/init.d/portmap start
[root@linux ~]# /etc/init.d/nfslock start
# 一般来说，系统默认会启动portmap，不过鸟哥之前关闭过，所以要启动
# 另外，如果服务器端启动nfslock的话，客户端也要启动才能生效
```

注意：nfslock进程用于给文件加锁，保持文件同步。

(2) 建立挂载目录

```
[root@linux ~]# mkdir -p /home/nfs/public
```

(3) 使用 mount 命令直接挂载 NFS 的文件系统

```
[root@linux ~]# mount -t nfs 192.168.0.2:/home/public /home/nfs/public
# 注意一下挂载的语法。「 -t nfs 」用于指定文件系统类型
# IP:/dir 则是指定某一台主机的某个目录
```

一般来说，如果 NFS 服务器只是提供个人数据，不需要可执行、SUID 与装置文件，那么时可以指定权限

```
[root@linux ~]# mount -t nfs -o nosuid,noexec,nodev,rw \
> 192.168.0.2:/home/public /home/nfs/public
```

如何使 NFS 在开机时就挂载？修改/etc/fstab：

```
[root@linux ~]# vi /etc/fstab
192.168.0.2:/home/public  /home/nfs/public  nfs  nosuid,noexec,nodev,rw,
bg,soft,rsize=32768,wsize=32768   0   0
# 注意。上面的设置是同一行的，不要搞错了。
```

12、 autofs 服务用于让客户端在使用 NFS 时才挂载，使用完毕后，让 NFS 自动卸载。autofs 可以预先定义好客户端预计挂载服务器端的哪些上层目录，及相关的对应 NFD 服务器共享目录。当我们在客户端要使用/home/nfs/public 的数据时，autofs 才会去挂载，5 分钟内没有使用该目录下的数据后自动删除。autofs 的主要配置文件为/etc/auto.Master。在/etc/auto.nfs(auto.nfs 文件的文件名可以在/etc/auto.Master 中自行设置)里则可以定义出每个目录欲挂载的远程服务器目录。

(1) 建立配置文件/etc/auto.Master：这个文件很简单，只要有默认目录及数据对应文件即可。

```
[root@linux ~]# vi /etc/auto.Master
/home/nfs  /etc/auto.nfs

[root@linux ~]# mkdir /home/nfs
# 注意。此时/home/nfs内并没有其他的目录存在。
```

注意：/home/nfs 是挂载到哪个目录，/etc/auto.nfs 是配置文件

(2) 建立数据对应文件内的信息：挂载目录由/etc/auto.nfs 文件指定，这个文件是不存在的，由自行设置，格式如下：

```
[本地端目录] [-挂载参数] [服务器所提供的目录]
参数:
[本地端目录] : 指的就是在/etc/auto.Master内指定的目录的下一级目录
[-挂载参数] : 就是前一小节提到的 rw,bg,soft 等等的参数，可有可无;
[服务器所提供的目录] : 例如192.168.0.2:/home/public等

[root@linux ~]# vi /etc/auto.nfs
public  -rw,bg,soft,rsize=32768,wsize=32768 192.168.0.2:/home/public
testing -rw,bg,soft,rsize=32768,wsize=32768 192.168.0.2:/home/test
temp    -rw,bg,soft,rsize=32768,wsize=32768 192.168.0.2:/tmp
# 参数部分，只要最前面加个 - 符号即可。
```

第 15 章 NIS 服务器

1、 NIS 最大的用途在于向客户端用户提供信息查询，例如，用户的账号、密码、UID、默认目录、shell 等等，都可以通过 NIS 服务器来查询。因此，一般在高性能运算计算机中，如果想要让所有的机器都拥有相同的账号密码，通常使用 NIS 提供身份验证，配合 NFS 提供所需要磁盘空间。也就是让一台主机管理所有主机账号，其余主机在有用户登录时才到这台主控服务器上查询相关的账号。（NIS 提供信息查询）

2、 Master/Slave 主从架构：一般来说用在数据库集群比较多，主要是实现读写分离。对于数据库应用而言基本上是读大于写，因此由 Master 服务器负责增、删、改操作，由 Slave 负责读操作（也就是 SELECT），Master 一般只有一台，而 Slave 可以有好多台。Slave 与 Master 之间会有心跳数据包（一般数据库服务器会提供配置）。当 Master 有数据写入时 Master 会将数据同步至各 Slave 上。（主写从读）

3、 在较大型企业环境中，NIS 服务器使用 Master/Slave 主从架构，避免单一的一台 NIS 服务器宕机时出现的风险。Master NIS 服务器提供系统管理者制作的数据库，Slave NIS 保存数据库副本，Master NIS 服务器修改数据库时同步到 Slave NIS 服务器，并以此提供其他客户端的查询。客户端向整个网段请求用户数据的响应时，Master 和 Slave 皆可回答。

4、 NIS Client 有登陆需求时，会先查询其本机的/etc/passwd、/etc/shadow 等文件。在本机找不到相关账号信息时，才开始向整个 NIS 网段的主机查询，无论是 Master 还是 Slave，都可以响应，基本上是先响应者优先。

5、 根据说明，我们的 NIS 环境大致上需要设置的基本组件有以下 3 种：

(1) NIS master Server：将文件建成数据库，并提供 Slave Server 来更新

(2) NIS slave Server：以 Master Server 的数据库作为本身的数据库来源

(3) NIS Client：向 Master/Server 请求登录者的验证数据。

第 20 章　SAMBA 服务器

1、　　SAMBA 服务器用于在 windows 和 unix 之间共享数据，NFS 只能用于 unix 之间共享数据。

第 21 章 vsFTPd 文件服务器

1、　　FTP 使用明文传输，vsFTPd 相比 FTP 而言要安全。

第 22 章 NTP 时间服务器

1、　　NTP 时间服务器用于将本地 BIOS 内部时间和国际标准时间同步。它分成 NTP 服务器和客户端，如果只对单台主机时间同步，则不需要架设 NTP，直接使用 NTP 客户端。