



Introduction to Practical IP Networking

Rik Wade

rik@rikwade.com

WYLUG 9/Feb/2004



What We'll Cover

- Files
- Tools
- Procedures



Files

- /etc is your friend
- Scripts: /etc/init.d/ or /etc/rc.d/init.d/
- Networking: /etc/network (Debian)
 - /etc/sysconfig/networking/ (RedHat)
- Local hosts: /etc/hosts
- DNS resolution: /etc/resolv.conf
- inetd: /etc/xinetd.conf or /etc/inetd.conf
 - xinetd uses /etc/xinetd.d/
- etc. (pun intended)



/etc/init.d

- Contains scripts to start services
- IP networking is one of those services
- Startup script pulls information from networking configuration files
- Brings up interfaces and installs routes



Networking Configuration

- if-up, if-down and if-only-I-understood
 - /etc/network/ (Debian)
 - /etc/sysconfig/networking/ (RedHat)
 - /etc/sysconfig/network-scripts/ (RedHat)
- if-up: bringing the interface UP
- if-down: taking the interface DOWN
- if-cfg: configuration parameters
 - IP address, netmask, name, onboot etc.
- Debian is easier: /etc/network/interfaces



Networking Configuration

- **Debian**

```
# /etc/network/interfaces - configuration file for ifup(8),ifdown(8)
# The loopback interface
auto lo
iface lo inet loopback

# The first network card
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.10
netmask 255.255.255.0
gateway 192.168.1.1
```



Networking Configuration

- RedHat

```
bash-2.05a$ cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
IPADDR=192.168.1.2
NETMASK=255.255.255.0
ONBOOT=yes
```



DNS Resolution

- `/etc/hosts`
 - `127.0.0.1 localhost`
 - `192.168.1.2 mybox.localnet mybox`
- `/etc/resolv.conf`
 - Where to go to resolve domain names
 - `search localnet`
 - `nameserver 195.92.195.94`
 - `nameserver 195.92.195.95`



(x)inetd

- If you don't need it, turn it off...please
- Starts services (willy nilly)
- Basic control using `hosts.allow` and `hosts.deny` – no substitute for IPTables
- Better to run services explicitly bound to a port and shut down `inetd` e.g. an FTP Server



Tools

- We will now look at:
 - Configuration commands
 - ifconfig, ip
 - Debug commands
 - ping, traceroute, arp
 - Advanced commands
 - tcpdump, netstat, nmap



Configuration

- **ifconfig**

- `ifconfig eth0 192.168.1.2 netmask 255.255.255.0`
- `route add default gateway 192.168.1.1`

- **ip addr add**

- `ip addr add 192.168.1.2/24 brd 192.168.1.255 dev eth0`

- **ip route add**

- `ip route add default via 192.168.1.1 dev eth0`

- **man ip:** ip - show / manipulate routing, devices, policy routing and tunnels



IP Address Configuration

- RFC1918 <http://www.ietf.org/rfc/rfc1918.txt>
 - Private addressing for non-public networks. Use these at home!

10.0.0.0	-	10.255.255.255	(10/8 prefix)
172.16.0.0	-	172.31.255.255	(172.16/12 prefix)
192.168.0.0	-	192.168.255.255	(192.168/16 prefix)

- Use NAT on your router/gateway to the Internet
- Linux IPTables can be used to NAT and Firewall
- Your ISP will assign your router a public IP address



Debug

- ARP (address resolution protocol)
<http://www.ietf.org/rfc/rfc826.txt>
- Discover MAC address for a given IP address

```
debian:/root# arp -an
```

```
? (192.168.1.1) at 00:60:5C:BC:09:15 [ether] on eth0
```

```
? (192.168.1.21) at 00:A0:CC:D0:B0:87 [ether] on eth0
```

```
debian:/root# tcpdump -i eth0 arp
```

```
18:08:36.727610 arp who-has 192.168.1.254 tell 192.168.1.10
```

```
18:08:36.728257 arp reply 192.168.1.254 is-at 0:b:6b:38:9:93
```



Debug

- ping 192.168.1.1

- debian:~# ping 192.168.1.1
- PING 192.168.1.1 (192.168.1.1): 56 data bytes
- 64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=2.7 ms
- 64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=2.5 ms

- ping <dns server of your ISP>

- debian:~# ping 195.92.195.92
- PING 195.92.195.92 (195.92.195.92): 56 data bytes
- 64 bytes from 195.92.195.92: icmp_seq=0 ttl=61 time=44.4 ms
- 64 bytes from 195.92.195.92: icmp_seq=1 ttl=61 time=44.9 ms

- ping www.google.com

- debian:~# ping www.google.com
- PING www.google.akadns.net (216.239.59.104): 56 data bytes
- 64 bytes from 216.239.59.104: icmp_seq=0 ttl=244 time=77.4 ms
- 64 bytes from 216.239.59.104: icmp_seq=1 ttl=244 time=74.7 ms



Debug

- **traceroute 195.92.195.92**

```
debian:~# traceroute -n 195.92.195.92
traceroute to 195.92.195.92 (195.92.195.92), 30 hops max, 38
  byte packets
 1  192.168.1.1    2.589 ms  2.642 ms  2.239 ms
 2  195.92.168.35  35.108 ms 35.885 ms 35.811 ms
 3  195.92.168.2   35.785 ms 34.702 ms 35.861 ms
 4  195.92.195.92  36.631 ms 35.671 ms 35.566 ms
```

- **traceroute www.google.com**
 - To verify that DNS is working



Advanced

- **Tcpdump, a leatherman...**(with many sharp blades)

```
debian:~# tcpdump -n -i eth0 icmp
```

```
tcpdump: listening on eth0
```

```
13:20:07.743209 192.168.1.10 > 192.168.1.1: icmp: echo request  
(DF)
```

```
13:20:07.745823 192.168.1.1 > 192.168.1.10: icmp: echo reply (DF)
```



Advanced

- **Tcpdump, a leatherman...**(with many sharp blades)

```
debian:~# tcpdump -n -i eth0 host 192.168.1.1 and port 80
```

```
tcpdump: listening on eth0
```

```
13:11:23.273096 192.168.1.10.1026 > 192.168.1.1.80: SWE  
2742861373:2742861373(0) win 5840 <mss 1460,sackOK,timestamp  
6110623 0,nop,wscale 0> (DF) [tos 0x10]
```

```
13:11:23.275815 192.168.1.1.80 > 192.168.1.10.1026: R 0:0(0) ack  
2742861374 win 0
```

```
2 packets received by filter
```

```
0 packets dropped by kernel
```



Advanced

- **Tcpdump, a leatherman...**(with many sharp blades)

```
debian:~# tcpdump -n -i eth0 host 195.92.195.94 and port 53
tcpdump: listening on eth0
13:16:43.496037 192.168.1.10.1358 > 195.92.195.94.53: 35665+ A?
www.deja.com. (30) (DF)
13:16:43.755849 195.92.195.94.53 > 192.168.1.10.1358: 35665 4/9/9
CNAME[|domain] (DF)
```

```
2 packets received by filter
```

```
0 packets dropped by kernel
```



Advanced

```
debian:~# netstat --listening --tcp
```

```
Active Internet connections (only servers)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	*:864	*:*	LISTEN
tcp	0	0	*:printer	*:*	LISTEN
tcp	0	0	*:time	*:*	LISTEN
tcp	0	0	*:netbios-ssn	*:*	LISTEN
tcp	0	0	*:daytime	*:*	LISTEN
tcp	0	0	*:imap2	*:*	LISTEN
tcp	0	0	*:sunrpc	*:*	LISTEN
tcp	0	0	*:www	*:*	LISTEN
tcp	0	0	*:auth	*:*	LISTEN
tcp	0	0	*:1012	*:*	LISTEN
tcp	0	0	*:ftp	*:*	LISTEN
tcp	0	0	*:ssh	*:*	LISTEN
tcp	0	0	*:telnet	*:*	LISTEN
tcp	0	0	*:8888	*:*	LISTEN
tcp	0	0	*:smtp	*:*	LISTEN
tcp	0	0	*:microsoft-ds	*:*	LISTEN



Advanced

```
debian:~# netstat --tcp --listening --program
```

```
Active Internet connections (only servers)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program
tcp	0	0	*:864	*:*	LISTEN	264/famd
tcp	0	0	*:printer	*:*	LISTEN	9209/lpd
tcp	0	0	*:time	*:*	LISTEN	405/xinetd
tcp	0	0	*:netbios-ssn	*:*	LISTEN	382/smbd
tcp	0	0	*:daytime	*:*	LISTEN	405/xinetd
tcp	0	0	*:imap2	*:*	LISTEN	405/xinetd
tcp	0	0	*:sunrpc	*:*	LISTEN	178/portmap
tcp	0	0	*:www	*:*	LISTEN	463/apache
tcp	0	0	*:auth	*:*	LISTEN	405/xinetd
tcp	0	0	*:1012	*:*	LISTEN	
406/rpc.statd						
tcp	0	0	*:ftp	*:*	LISTEN	421/proftpd
tcp	0	0	*:ssh	*:*	LISTEN	392/sshd
tcp	0	0	*:telnet	*:*	LISTEN	405/xinetd
tcp	0	0	*:8888	*:*	LISTEN	268/perl
tcp	0	0	*:smtp	*:*	LISTEN	373/master
tcp	0	0	*:microsoft-ds	*:*	LISTEN	382/smbd



Advanced

- ~~nmap www.google.com~~
- nmap 192.168.1.1

```
debian:~# nmap 192.168.1.1
```

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-08  
13:22 GMT
```

```
Interesting ports on fluffy.localnet (192.168.1.1):
```

```
(The 1658 ports scanned but not shown below are in state: closed)
```

```
PORT      STATE SERVICE
```

```
23/tcp    open  telnet
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 12.665  
seconds
```



Advanced

```
debian:~# nmap 192.168.1.2
```

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-08  
13:22 GMT
```

```
Interesting ports on puppy.localnet (192.168.1.2):
```

```
(The 1653 ports scanned but not shown below are in state: closed)
```

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
777/tcp	open	unknown
3389/tcp	open	ms-term-serv
5000/tcp	open	UPnP

```
Nmap run completed -- 1 IP address (1 host up) scanned in 0.805  
seconds
```



Advanced

```
debian:~# nmap 192.168.1.x
```

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-08 13:37 GMT
```

```
Interesting ports on hostX.localnet (192.168.1.x):
```

```
(The 1643 ports scanned but not shown below are in state: closed)
```

PORT	STATE	SERVICE
13/tcp	open	daytime
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
37/tcp	open	time
80/tcp	open	http
111/tcp	open	rpcbind
113/tcp	open	auth
139/tcp	open	netbios-ssn
143/tcp	open	imap
445/tcp	open	microsoft-ds
515/tcp	open	printer
864/tcp	open	unknown
1012/tcp	open	unknown
8888/tcp	open	sun-answerbook

```
Nmap run completed -- 1 IP address (1 host up) scanned in 3.945 seconds
```



Advanced

```
debian:/# nmap -O 192.168.1.1
```

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-08  
14:13 GMT
```

```
Interesting ports on fluffy.localnet (192.168.1.1):
```

```
(The 1658 ports scanned but not shown below are in state: closed)
```

```
PORT      STATE SERVICE
```

```
23/tcp    open  telnet
```

```
Device type: router
```

```
Running: Cisco IOS 12.X
```

```
OS details: Cisco router running IOS 12.1.5-12.2.13a
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 14.203  
seconds
```



Advanced

```
debian:/etc/network# nmap -O 192.168.1.x
```

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-02-08 14:16 GMT
```

```
Interesting ports on puppy.localnet (192.168.1.x):
```

```
(The 1653 ports scanned but not shown below are in state: closed)
```

PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
777/tcp	open	unknown
3389/tcp	open	ms-term-serv
5000/tcp	open	UPnP

```
Device type: general purpose
```

```
Running: Microsoft Windows 95/98/ME|NT/2K/XP
```

```
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Professional  
or Advanced Server, or Windows XP, Microsoft Windows 2000 Server SP3
```

```
Nmap run completed -- 1 IP address (1 host up) scanned in 2.484 seconds
```



FIN

- References:
- Linux Documentation Project
 - <http://en.tldp.org>
- TCPDump Homepage
 - <http://www.tcpdump.org>
- Nmap Homepage
 - <http://www.insecure.org>
- Lots of Traceroute tools
 - <http://www.traceroute.org>
- Linux Network Administrator's Guide
 - <http://en.tldp.org/LDP/nag/node1.html>