1.112.3
TCP/IP configuration and troubleshooting
Weight 7

Linux Professional Institute Certification — 102

Angus Lees `gus@inodes.org`   Geoffrey Robertson
`ge@ffrey.com`   Nick Urbanik `nicku@nicku.org`

This document Licensed under GPL—see section 16

2005 July

Outline

Context

Objective

Resources

Configuring network
interfaces

Adding routes with
route

netstat

Troubleshooting Tools

hostname

nsswitch.conf

/etc/networks

/etc/hosts

/etc/host.conf

/etc/resolv.conf

Debugging DNS

DHCP

License Of This
Document

Topic 112 Networking Fundamentals [14]
Where we are up to

1.112.1 Fundamentals of TCP/IP [4]

1.112.3 **TCP/IP configuration and troubleshooting [7]**

1.112.4 Configure Linux as a PPP client [3]

Description of Objective
1.112.3 TCP/IP configuration and troubleshooting

Candidates should be able to view, change and verify configuration settings and operational status for various network interfaces. This objective includes manual and automatic configuration of interfaces and routing tables. This especially means to add, start, stop, restart, delete or reconfigure network interfaces. It also means to change, view or configure the routing table and to correct an improperly set default route manually. Candidates should be able to configure Linux as a DHCP client and a TCP/IP host and to debug problems associated with the network configuration.

Key files, terms, and utilities include: I
1.112.3 TCP/IP configuration and troubleshooting

/etc/HOSTNAME or /etc/hostname — a text file holding the hostname

/etc/hosts — a file mapping IP addresses ↔ hostnames

/etc/networks — an obsolete file that maps only classful network addresses ↔ names

/etc/host.conf — an obsolete file replaced by nsswitch

/etc/resolv.conf — configuration file used when system looks up a name or address

/etc/nsswitch.conf — name service switch configuration file: determines how system looks up name and various other things

ifconfig — a command to show and configure network interfaces

route — a command to show and configure network routes

dhcpcd, dhcpclient, pump — DHCP clients

Key files, terms, and utilities include: II
1.112.3 TCP/IP configuration and troubleshooting

host — a program to query and debug DNS servers

hostname (domainname, dnsdomainname) — commands to show the hostname, and NIS domain settings

netstat — a command that shows what service is listening on what port

ping — sends ICMP ECHO_REQUEST to hosts, displays time it takes to get an answer

traceroute — command to show the path that a network connection takes, showing routes along the way

tcpdump — packet sniffer command that displays the contents of packets received on a network interface

the network scripts run during system initialization.

TCP/IP Configuration and Troubleshooting
Resources of Interest

Linux Networking HOWTO by Joshua Drake : `http://tldp.org/HOWTO/Net-HOWTO/index.html`

Linux Ethernet-Howto by Paul Gortmaker : `http://tldp.org/HOWTO/Ethernet-HOWTO.html`

ifconfig – Low level network config

Network interface configuration
$ **sudo ifconfig eth0 192.168.7.26 netmask
255.255.255.0 broadcast 192.168.7.255** ↩
$ **sudo ifconfig eth0 down** ↩

route – Low level network config

```
$ sudo route add –net 192.168.7.0 netmask
255.255.255.0 dev eth0 ↩
$ sudo route add default gw 192.168.7.1 ↩
```

View routing table: $ `route -n` ↩

Ports in use	`netstat -a -u -t`
Routing table	`netstat -r`
Interfaces	`netstat -i`
Multicast groups	`netstat -g`
Masqueraded connections	`netstat -M`
Statistics	`netstat -s`

Network debugging

ping

- ► Try to bounce an ICMP packet off a host
- ► Good for reachability, round trip delay, packet loss

traceroute

- ► Show the network path to a particular host
- ► Good for testing routing problems, "which ISP screwed up"

tcpdump

- ► Dump raw network traffic
- ► Exceptional for diagnosing network problems involving a particular host

Outline

tcpdump again

tcpdump is your friend, learn to use it

```
$ sudo tcpdump -i ppp0 not port ssh
tcpdump: listening on ppp0
21:54:32.913475 10.0.128.107.1024 > 10.0.128.97.domain:  20147+ A?
  fatso.urnet.com.au. (36) (DF)
21:54:33.102745 10.0.128.97.domain > 10.0.128.107.1024:  20147* 1/3/3
 (178) (DF)
21:54:33.103766 10.0.128.107 > 203.26.250.2: icmp: echo request (DF)
21:54:33.352745 203.26.250.2 > 10.0.128.107: icmp: echo reply
21:54:34.102912 10.0.128.107 > 203.26.250.2: icmp: echo request (DF)
21:54:34.302745 203.26.250.2 > 10.0.128.107: icmp: echo reply
21:56:09.908636 10.0.128.107.1068 > 203.26.250.2.www:
 S 1245080954:1245080954(0) win 5840 <mss 1460,sackOK,timestamp
 5047727 0,nop,wscale 0> (DF) [tos 0x10]
21:56:10.052743 203.26.250.2.www > 10.0.128.107.1068:
 S 3633684004:3633684004(0) ack 1245080955 win 5792 <mss
 1460,sackOK,timestamp 409734147 5047727,nop,wscale 0> (DF)
21:56:10.052869 10.0.128.107.1068 > 203.26.250.2.www: . ack 1 win 5840
 <nop,nop,timestamp 5047742 409734147> (DF) [tos 0x10]
21:56:12.977510 10.0.128.107.1068 > 203.26.250.2.www: P 1:2(1) ack 1
 win 5840 <nop,nop,timestamp 5048034 409734147> (DF) [tos 0x10]
```

/etc/HOSTNAME or /etc/hostname

- System scripts set the hostname from one of these files during boot, using the **hostname** command.
- **dnsdomainname**, **ypdomainname**, **nisdomainname** and **domainname** are variations on **hostname**

- **domainname** gives the NIS domainname, **NOT the DNS domain**

/etc/nsswitch.conf

"Name Service Switch" configuration

```
passwd:         compat
group:          compat
shadow:         compat

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

/etc/networks

- Labels for network addresses
- Only supports class A, B or C addresses (not CIDR)
- Rarely used or kept up to date `localnet 192.168.1.0`

/etc/hosts

- ▶ Hostname to IP address mapping, mostly superseded by DNS
- ▶ Still matters before DNS is running

```
127.0.0.1 localhost
192.168.1.1 cat.pasture.com.au cat

# The following lines are desirable for IPv6 capable hosts

::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

/etc/host.conf — Resolver configuration

- ▶ Various keywords to tweak non-DNS-specific resolver behaviour
- ▶ Rarely modified; most options no longer relevant
- ▶ See $ **man host.conf** ↩

```
order hosts,bind
multi on
```

/etc/resolv.conf — DNS configuration

- ▶ DNS configuration for resolver
- ▶ Nameserver defaults to `127.0.0.1`, search suffix defaults to DNS domain name

```
search pasture.com.au
nameserver 10.0.128.97
```

Outline

Debugging DNS with `host`

- ▶ **host** performs various DNS queries

  host *[options]* hostname *[server]*

- ▶ Common options:

                  -v verbose
                  -l list all hosts in a domain (using AXFR)
                  -t query type ("-t any" is useful)

DHCP

- ▶ "Dynamic Host Control Protocol" configures networking details, DNS, etc automatically by querying a "DHCP server"
- ▶ Various DHCP clients:

  dhcpclient Comes with ISC DHCP server, highly configurable

  dhcpcd

  pump Simple DHCP client written by RedHat

  udhcpc Very small DHCP client

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

Topics Covered

License Of This Document