LPI exam 202 prep: Network troubleshooting

Intermediate Level Administration (LPIC-2) topic 214

Skill Level: Intermediate

David Mertz (mertz@gnosis.cx)
Developer
Gnosis Software, Inc.

28 Jun 2006

In this tutorial, the last of a series of seven tutorials covering intermediate network administration on Linux®, David Mertz finishes preparing you to take the Linux Professional Institute Intermediate Level Administration (LPIC-2) Exam 202. This tutorial revisits earlier tutorials in the LPI 202 series, focusing on how to use the basic tools you've already covered to fix networking problems. The tool review is divided into two categories: configuration tools and diagnostic tools.

Section 1. Before you start

Learn what these tutorials can teach you and how you can get the most from them.

About this series

The Linux Professional Institute (LPI) certifies Linux system administrators at two levels: *junior level* (also called "certification level 1") and *intermediate level* (also called "certification level 2"). To attain certification level 1, you must pass exams 101 and 102; to attain certification level 2, you must pass exams 201 and 202.

developerWorks offers tutorials to help you prepare for each of the four exams. Each exam covers several topics, and each topic has a corresponding self-study tutorial on developerWorks.

- To prepare for certification level 1, see the developerWorks tutorials for LPI exams 101 and 102.

- To prepare for certification level 2, see the developerWorks tutorials for LPI exams 201 and 202.

View the entire set of developerWorks LPI tutorials.

For LPI exam 202, the seven topics and corresponding developerWorks tutorials are:

Table 1. LPI exam 202: Tutorials and topics

LPI exam 202 topic	developerWorks tutorial	Tutorial summary
Topic 205	LPI exam 202 prep (topic 205): Networking configuration	Learn how to configure a basic TCP/IP network, from the hardware layer (usually Ethernet, modem, ISDN, or 802.11) through the routing of network addresses.
Topic 206	LPI exam 202 prep (topic 206): Mail and news	Learn how to use Linux as a mail server and as a news server. Learn about mail transport, local mail filtering, mailing list maintenance software, and server software for the NNTP protocol.
Topic 207	LPI exam 202 prep (topic 207): DNS	Learn how to use Linux as a DNS server, chiefly using BIND. Learn how to perform a basic BIND configuration, manage DNS zones, and secure a DNS server.
Topic 208	LPI exam 202 prep (topic 208): Web services	Learn how to install and configure the Apache Web server, and learn how to implement the Squid proxy server.
Topic 210	LPI exam 202 prep (topic 210): Network client management	Learn how to configure a DHCP server, an NIS client and server, an LDAP server, and PAM authentication support. See detailed objectives below.
Topic 212	LPI exam 202 prep (topic 212): System security	Learn how to configure a router, secure FTP servers, configure SSH, and perform various other security administration tasks.
Topic 214	LPI exam 202 prep (topic 214): Network troubleshooting	(This tutorial) Review tools and commands that let you detect and solve networking problems. See detailed objectives below.

The Linux Professional Institute does not endorse any third-party exam preparation

material or techniques in particular. For details, please contact info@lpi.org.

About this tutorial

Welcome to "Network troubleshooting," the last of seven tutorials covering intermediate network administration on Linux. This tutorial re-examines the material covered in the first six tutorials on the Linux Professional Institute's 202 exam topics to give some general context for the entire series. Highlighted here are some of the tools you've previously covered -- `ifconfig`, `route`, `hostname`, `dmesg`, `netstat`, `ping`, `traceroute`, etc. -- with the focus on using those tools to fix problems.

As with the other tutorials in the developerWorks 201 and 202 series, this tutorial is intended to serve as a study guide and entry point for exam preparation, rather than complete documentation on the subject. Readers are encouraged to consult LPI's detailed objectives list and to supplement the information provided here with other material as needed.

is organized according to the LPI objectives for this topic. Very roughly, expect more questions on the exam for objectives with higher weight.

Table 2. Network troubleshooting: Exam objectives covered in this tutorial

LPI exam objective	Objective weight	Objective summary
2.214.7 Troubleshooting network issues	Weight 1	Identify and correct common network setup issues. This objective includes knowledge of locations for basic configuration files and commands.

Prerequisites

To get the most from this tutorial, you should already have a basic knowledge of Linux and a working Linux system on which you can practice the commands covered in this tutorial. This tutorial builds on material covered in the previous six tutorials in the LPI exam 202 series.

Other resources

As with most Linux tools, it is always useful to examine the manpages for any utilities discussed. Versions and switches might change between utility or kernel version or with different Linux distributions. For more in depth information, the Linux Documentation Project has a variety of useful documents, especially its HOWTOs. A variety of books on Linux networking have been published; I have found O'Reilly's *TCP/IP Network Administration*, by Craig Hunt to be quite helpful (find whatever edition is most current when you read this).

Section 2. Network configuration tools

About network troubleshooting

To troubleshoot a network configuration, you need to know how to use several of the tools discussed in this tutorial series; you also need to be familiar with the configuration files that affect network status and behavior. This tutorial summarizes the main tools and configuration files you should be familiar with for effective troubleshooting.

For simplicity, this tutorial groups the tools according to whether a given tool applies more to configuration of a network in the first place or to diagnosis of network problems. Of course, in practice those elements are rarely separate.

ifconfig

LPI exam 202 prep (topic 205): Networking configuration discusses `ifconfig` in greater detail. This utility both reports on the current status of network interfaces and lets you modify the configuration of those interfaces. In most cases, if *something* is wrong with a network -- like a particular machine does not appear to access the network at all -- running `ifconfig` with no options is usually the first step you should take. If this fails to report active interfaces, you can be pretty sure that the local machine itself has a configuration problem. "Active" in this case means that it shows an IP address assigned; in most cases, you should expect to see a number of packets in the RX and TX lines:

Listing 1. Using ifconfig

```
eth0    Link encap:Ethernet  HWaddr 00:C0:9F:21:2F:25
        inet addr:192.168.216.90  Bcast:66.98.217.255  Mask:255.255.254.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:6193735 errors:0 dropped:0 overruns:0 frame:0
        TX packets:6982479 errors:0 dropped:0 overruns:0 carrier:0
```

Attempting to activate an interface with something like `ifconfig eth0 up ...` is a good first step to try to see if an interface *can* be activated (in many cases, filling in additional options in the line).

route

LPI exam 202 prep (topic 205): Networking configuration discusses `route` in greater detail. This utility lets you both view and modify the routing tables currently in effect for a local machine and a local network. Using `route`, you may add and delete routes, set netmasks and gateways, and perform various other tweaking tasks.

For the most part, calls to `route` should be performed in initialization scripts, but in attempting to diagnose and fix problems, experimenting with routing options can help (you can copy successes to appropriate initialization scripts for later use).

hostname

This utility also has aliases to employ different aspects of the utility:

- `domainname`
- `nodename`
- `dnsdomainname`
- `nisdomainname`
- `ypdomainname`

You control these capabilities with switches to `hostname` itself.

`hostname` is used to either set or display the current host, domain, or node name of the system. These names are used by many of the networking programs to identify the machine. The domain name is also used by NIS/YP.

dmesg

The utility `dmesg` allows you to examine kernel log messages; it works in cooperation with `syslogd`. Any kernel process, including those related to networking, are best accessed using the `dmesg` utility, often filtered using other tools such as `grep`, as well as switches to `dmesg`.

Manually setting ARP

You almost never need or want to mess with automatically discovered ARP records. However, you may want to manually configure the ARP cache in debugging situations. The utility `arp` lets you do this. The key flag options in the `arp` utility are `-d` for delete, `-s` for set, and `-f` for set-from-file (default file is /etc/ethers).

For example, suppose that communication with a specific IP address on the local network is erratic or unreliable. One possible cause of this situation is if multiple machines are incorrectly configured to use the same IP address. When an ARP request is broadcast over the Ethernet network, it is not pre-determined which machine will respond first with an ARP reply. The end result might be that the data packets are delivered to one machine one time and to a different machine another time.

Using `arp -n` to debug the actual IP assignment is a first step. If you can determine that the IP address at issue does not map to the correct Ethernet device, that is a

strong clue about what is going on.

But beyond that somewhat random detection, you can force the right ARP mapping using the `arp -s` (or `-f`) option. Set an IP to map to the actual Ethernet device it should map to; manually configured mapping will not expire unless specifically set to do so using the `temp` flag. If a manual ARP mapping fixes the data loss problem, this is a strong sign the problem is over-assigned IP addresses.

Section 3. Network diagnostic tools

netstat

LPI exam 202 prep (topic 205): Networking configuration discusses `netstat` in greater detail. This utility displays a variety of information on network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. Among other things, `netstat` provides fairly detailed statistics on packets that have been handled in various ways.

The manpage for `netstat` provides information on the wide range of switches and options available. This utility is a good general-purpose tool for digging into details of the status of networking on the local machine.

ping

A good starting point in finding out if you can connect to a given host from the current machine (by either IP number or symbolic name) is the utility `ping`. As well as establishing that a route exists at all -- including the resolution of names via DNS or other means if a symbolic name is used -- `ping` gives you information on round-trip times that may be indicative of network congestion or routing delays. Sometimes `ping` will indicate a percentage of dropped packets, but in practical use you almost always see either 100 or 0 percent of packets lost by `ping` requests.

traceroute

The utility `traceroute` is a bit like a `ping` on steroids. Rather than simply report the fact that a route exists to a given host, `traceroute` reports complete details on all the hops taken along the way, including the timing of each router. Routes may change over time, either because of dynamic changes in the Internet or because of routing changes you have implemented locally. At a given moment though, `traceroute` shows you an actual followed path.

Listing 2. traceroute shows the actual followed path

```
$ traceroute google.com
traceroute: Warning: google.com has multiple addresses; using 64.233.187.99
traceroute to google.com (64.233.187.99), 30 hops max, 38 byte packets
 1  ev1s-66-98-216-1.ev1servers.net (66.98.216.1)  0.466 ms  0.424 ms  0.323 ms
 2  ivhou-207-218-245-3.ev1.net (207.218.245.3)  0.650 ms  0.452 ms  0.491 ms
 3  ivhou-207-218-223-9.ev1.net (207.218.223.9)  0.497 ms  0.467 ms  0.490 ms
 4  gateway.mfn.com (216.200.251.25)  36.487 ms  1.277 ms  1.156 ms
 5  so-5-0-0.mpr1.atl6.us.above.net (64.125.29.65)  13.824 ms  14.073 ms  13.826 ms
 6  64.124.229.173.google.com (64.124.229.173)  13.786 ms  13.940 ms  14.019 ms
 7  72.14.236.175 (72.14.236.175)  14.783 ms  14.749 ms  14.476 ms
 8  216.239.49.226 (216.239.49.226)  16.651 ms  16.421 ms  17.648 ms
 9  64.233.187.99 (64.233.187.99)  14.816 ms  14.913 ms  14.775 ms
```

host, nslookup, and dig

All three utilities -- `host`, `nslookup`, and `dig` -- are used for querying DNS entries; they largely overlap in their capabilities. Generally, `nslookup` provided enhancement to `host`, and `dig` in turn enhanced `nslookup` (though none of the three are exactly backward- or forward-compatible with the others). All the tools rely on the same underlying kernel facilities, so reported results should be consistent in all cases (except where level of detail differs). For example, each of the three is used to query google.com:

Listing 3. Using host, nslookup, and dig to query Google

```
$ host google.com
google.com has address 64.233.187.99
google.com has address 64.233.167.99
google.com has address 72.14.207.99

$ nslookup google.com
Server:         207.218.192.39
Address:        207.218.192.39#53

Non-authoritative answer:
Name:   google.com
Address: 64.233.167.99
Name:   google.com
Address: 72.14.207.99
Name:   google.com
Address: 64.233.187.99

$ dig google.com
; <<>> DiG 9.2.4 <<>> google.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46137
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             295     IN      A       64.233.167.99
google.com.             295     IN      A       72.14.207.99
google.com.             295     IN      A       64.233.187.99

;; Query time: 16 msec
;; SERVER: 207.218.192.39#53(207.218.192.39)
;; WHEN: Mon Apr 17 01:08:42 2006
;; MSG SIZE  rcvd: 76
```

Section 4. Network configuration files

/etc/network/ and /etc/sysconfig/network-scripts/

The directory /etc/network/ contains a variety of data about the current network on some Linux distributions, especially in the file /etc/network/interfaces. Various utilities, especially `ifup` and `ifdown` (or `iwup` and `iwdown` for wireless interfaces), are contained in /etc/sysconfig/network-scripts/ on some distributions (but the same scripts may live elsewhere instead on your distribution).

/var/log/syslog and /var/log/messages

Messages logged by the kernel or the `syslogd` facility are stored in the log files /var/log/syslog and /var/log/messages. LPI exam 201 prep (topic 211): System maintenance discusses system logging in greater detail. The utility `dmesg` is generally used to examine logs.

/etc/resolv.conf

LPI exam 202 prep (topic 207): Domain Name System discusses /etc/resolv.conf in greater detail. Generally, this file simply contains the information needed to find domain name servers. It may be configured either manually or via dynamic means such as RIP, DHCP, or NIS.

/etc/hosts

The file /etc/hosts is usually the first place a Linux system looks to attempt to resolve a symbolic hostname. You can add entries to either bypass DNS lookup (or sometimes YP or NIS facilities) or to name hosts that are not available on DNS, often because they are strictly names on the local network. See the examples in Listing 4.

Listing 4. /etc/hosts, the place to resolve symbolic hostnames

```
$ cat /etc/hosts
# Set some local addresses
127.0.0.1         localhost
255.255.255.255   broadcasthost
192.168.2.1       artemis.gnosis.lan
192.168.2.2       bacchus.gnosis.lan
# Set undesirable site patterns to loopback
127.0.0.1       *.doubleclick.com
127.0.0.1       *.advertising.com
127.0.0.1       *.valueclick.com
```

/etc/hostname and /etc/HOSTNAME

The file /etc/HOSTNAME (on some systems without the capitalization) is sometimes used for the symbolic name of the localhost as known on the network. However, use of this file varies between distributions; generally /etc/hosts is used exclusively on modern distributions.

/etc/hosts.allow and /etc/hosts.deny

LPI exam 201 prep (topic 209): File and service sharing and LPI exam 202 prep (topic 212): System security discusses the files /etc/hosts.allow and /etc/hosts.deny in greater detail. These configuration files are used for positive and negative access lists by a variety of network tools. Read the manpages on these configuration files for more information on the specification of wildcards, ranges, and specific permissions that may be granted or denied.

Beyond initial setup to enforce system security, you often want to examine the content of these when a connection fails that "just seems like" it should be working. Generally, examining access control issues comes after examining basic interface and routing information in a debugging effort. That is, if you cannot reach a particular host at all (or it cannot reach you), it does not matter whether the host has permissions to use the services you provide. But selective failures in connections and service utilization can often be because of access control issues.

Section 5. A final word

Take advantage of every resource

For the subjects addressed in this tutorial, possibly the best resource for further information is the rest of this tutorial series. Nearly all the topics addressed here are detailed further in previous tutorials.

Quite a few people have written step-by-step guides to fixing a broken Linux network. One that looks good is "Simple Network Troubleshooting." Debian's similar quick guide is "How To Set Up A Linux Network." Since tutorials come and go and are updated on different schedules as distributions and commands change, you can always search the Internet to find currently available sources.

Resources

Learn

- Review the entire LPI exam prep tutorial series on developerWorks to learn Linux fundamentals and prepare for system administrator certification.
- At the LPIC Program, find task lists, sample questions, and detailed objectives for the three levels of the Linux Professional Institute's Linux system administration certification.
- *TCP/IP Network Administration, Third Edition* by Craig Hunt (O'Reilly, April 2002) is an excellent resource on Linux networking.
- For more in-depth information, the Linux Documentation Project has a variety of useful documents, especially its HOWTOs.
- In the developerWorks Linux zone, find more resources for Linux developers.
- Stay current with developerWorks technical events and Webcasts.

Get products and technologies

- Order the SEK for Linux, a two-DVD set containing the latest IBM trial software for Linux from DB2®, Lotus®, Rational®, Tivoli®, and WebSphere®.
- With IBM trial software, available for download directly from developerWorks, build your next development project on Linux.

Discuss

- This list of more than 700 Linux User Groups around the world can help you find local and distance study groups for LPI exams.
- Check out developerWorks blogs and get involved in the developerWorks community.

About the author

David Mertz
David Mertz has been writing the developerWorks columns *Charming Python* and *XML Matters* since 2000. Check out his book *Text Processing in Python* . For more on David, see his personal Web page.

Trademarks

DB2, Lotus, Rational, Tivoli, and WebSphere are trademarks of IBM Corporation in the United States, other countries, or both.
Linux is a trademark of Linus Torvalds in the United States, other countries, or both.