



Tips & Tricks

 [Click To Print](#)

Tips & Tricks

December 2007 • Vol.7 Issue 12

Page(s) 97-98 in print issue

Warm Up To Penguins

The Down & Dirty Details Of Linux Network Configuration, Part II

You've read the first part of this series, and you're fairly comfortable with how to set up an Ethernet interface on a local subnet. Now you're ready to jump into the big, wide, wonderful Internet.

(Remember that the premise of this series is that although GUI-based network configuration is great, you can't always depend on it. So in this article, we'll continue to look at what you can do from the command line.)



Continuing with the sample network we used last time, we've gone as far as getting our system (on 192.168.1.178) to ping to the local broadband router (at 192.168.1.1) successfully. The 192.168.1 class C subnet, along with the 10. class A subnet and the 172.16 class B subnet are referred to as private subnets. By definition, Internet backbone routers will not route them. Private subnets are used solely for configuring LANs behind some kind of router that does address translation (commonly referred to as NAT).

In this case, the router at 192.168.1.1 acts as a gateway. As we mentioned, we've already determined that we can ping the router from our machine. However, there are two additional steps we need to do to communicate with the rest of the Internet.

■ Get Your Kicks On Route 66

First, you need to let your local system know that 192.168.1.1 is the gateway. To do that temporarily (for example, when making a quick repair), you use the route command.

To begin, let's see what the output of route looks like if you run it with no arguments.

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

```
Kernel IP routing table
```

```
Destination Gateway Genmask Flags Metric Ref Use Iface
```

```
192.168.1.0 * 255.255.255.0 U 0 0 0 eth0
```



What you're looking at is called a routing table, and in very advanced networking situations, it can be used to send traffic to specific subnets over specific interfaces, usually to even out bandwidth usage. However, few but the largest data centers will ever use it for that. The above example looks a little complicated but isn't that bad. What it's telling us is that anything intended for the 192.168.1.0 subnet (that is to say, any address that begins with 192.168.1) should be transmitted over the eth0 Ethernet interface. That makes sense, because that's the interface that we configured to talk to that subnet.

Here, you'll see the

All we want to do is tell the system what the default gateway is. The default gateway is the one

***routing table stating
that we've established
a default gateway at
192.168.1.1.***

that gets any Internet traffic that hasn't been assigned a specific gateway. At the command line, we typed **route add default gw 192.168.1.1** and pressed ENTER. We issued a route command again, and the output changed to:

Kernel IP routing table

```
Destination Gateway Genmask Flags Metric Ref Use Iface
```

```
192.168.1.0 * 255.255.255.0 U 0 0 0 eth0
```

```
default 192.168.1.1 0.0.0.0 UG 0 0 0 eth0
```

Here, we're essentially telling the router to add a default gateway with an address of 192.168.1.1. If you look at the routing table after the command is run, you'll see there's a new routing that sends all traffic to the gateway router if it doesn't belong on the local subnet.

After you've done this, you should be able to ping systems on the Internet by IP address. However, you still won't be able to access them by their host name because you haven't set up a DNS resolver. Again, DNS configuration can become pretty hairy in corporate and data center environments, but for the rest of us, it's very simple.

Your ISP should have provided you with primary and secondary (and sometimes tertiary) DNS servers. These will be specified as IP addresses, because it would be hard to look them up by host name when you don't have DNS running yet. If you're running things from the command line, the file you want to play with is `/etc/resolv.conf`. At the command line, we typed **more /etc/resolv.conf**. Our system produced the following output:

```
nameserver 192.168.1.1
```

All this does is tell the system that it should go to 192.168.1.1 to resolve its DNS requests. In this case, that's the gateway router; the router we're using does proxy DNS forwarding, sending any DNS requests it receives on to the nameservers (the IP addresses your ISP provides for its DNS servers) that it was configured to use (usually via DHCP). If your router doesn't do this or you want to use the ISP's nameservers, you need to edit the `/etc/resolv.conf` file, adding a line for each nameserver your ISP gives you, starting with the primary server. You'd use the following format: "nameserver 192.168.1.1," where "nameserver" is the specific IP address your ISP provides.

To test that you configured things correctly, you can try pinging some remote host by its domain name. We used the command **ping www.ieee.org**. If everything works, you should see the site you pinged returning bytes of data, followed by the time it took to receive the data. If you don't have things configured right, you'll get the following friendly message:

```
ping: unknown host www.ieee.org
```

■ Can You Dig It?

Sometimes it's nice to find out some things about a domain (such as a Web site's IP address). The old standby for making a DNS query used to be a tool called `nslookup`, but it's been largely overshadowed by a new and more powerful tool called `dig`. The simplest way to use `dig` is to type **dig** followed by a host name. For example, if you wanted to dig the IEEE, you'd type **dig www.ieee.org** and press ENTER. We did just this and received the following output:

```
; <<>> DiG 9.3.4 <<>> www.ieee.org
```

```
:: global options: printcmd
```

```
:: Got answer:
```

```
:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26875 ;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0,
```

ADDITIONAL: 0

:: QUESTION SECTION:

;www.ieee.org. IN A

:: ANSWER SECTION:

www.ieee.org. 0 IN CNAME www.ieee.org.edgesuite.net.

www.ieee.org.edgesuite.net. 21600 IN CNAME a165.g.akamai.net.

a165.g.akamai.net. 20 IN A 62.41.81.56

a165.g.akamai.net. 20 IN A 62.41.81.10

:: Query time: 48 msec

:: SERVER: 192.168.1.1#53(192.168.1.1)

:: WHEN: Tue Sep 18 23:52:30 2007

:: MSG SIZE rcvd: 130

This is actually pretty easy to understand if you ignore anything preceded by semicolons. CNAME (canonical host name), which means that a host name is an alias for another, tells us that www.ieee.org is actually an alias for www.ieee.org.edgesuite.net. In turn, this is an alias for a165.g.akamai.net. That host name resolves to two different IP addresses, both on the 62.41.81 subnet. This is a round robin DNS; it's a way of balancing load between two Web servers by splitting the requests between two different machines on different IP addresses. If you want to see this taken to an extreme, try running dig on www.cnn.com.

■ Without A Trace

The last tool we'll cover this month is traceroute. This tool is very useful if you are having trouble connecting to a remote host and want to troubleshoot it. For example, let's assume we couldn't connect to or successfully ping eBay, but dig tells us that there's a valid DNS record for the site. Therefore, there must be a problem somewhere along the way, and traceroute can pinpoint it. At the command line, we typed **traceroute www.ebay.com** and pressed ENTER. We received:

traceroute to www.ebay.com (66.135.214.176), 30 hops max, 40 byte packets

1 192.168.1.1 (192.168.1.1) 0.447 ms 1.563 ms 1.551 ms

2 12.39.144.19 (12.39.144.19) 4.657 ms 4.661 ms 6.875 ms

3 P0-2.LCR-02.CNCDNH.verizon-gni.net (130.81.38.54) 6.865 ms 9.474 ms

9.461 ms

4 130.81.28.76 (130.81.28.76) 11.759 ms 11.761 ms 14.278 ms

5 0.so-2-2-0.XL2.BOS4.ALTER.NET (152.63.16.13) 24.289 ms 24.264 ms

26.522 ms

```
6 0.so-6-0-3.XT2.SAC1.ALTER.NET (152.63.0.190) 96.586 ms 89.891 ms
89.661 ms
7 POS7-0.GW5.SAC1.ALTER.NET (152.63.52.157) 92.287 ms 92.298 ms 92.282 ms
8 * * *
9 * * *
10 * * *
```

This output shows every network hop that a connection to eBay needs to make. If you start seeing lines that are all asterisks, this means that things aren't getting through that link. So, in this case, we can guess that alter.net is having some kind of connectivity problem. There's not much you can do at this point, but at least you'll know that the problem doesn't lie with your system.

Next month, we'll show you the files that are responsible for configuring your network, discuss DHCP a bit, and cover some Wi-Fi networking information. ■

James Turner

Infinite Loop A Dog's Life For Movie Pirates

Humans may have an ear for music or an eye for talent, but in Malaysia, a pair of black labs have acquired a nose for DVDs. More specifically, the two canines have been trained by the government to detect illegal copies by sniffing out chemicals used to produce DVDs. So far, the pair has found 1.6 million illegal DVDs, representing a would-be loss of over \$6 million. Man's best friend has now become one of Hollywood's best friends.

cnews.canoe.ca/CNEWS/WeirdNews/2007/08/20/4432261-ap.html