Network Troubleshooting

Part I

LinuxTrainingAcademy.com

Network Troubleshooting

Part II

What You Will Learn

- ping
- traceroute / tracepath
- netstat
- tcpdump
- telnet

Testing Connectivity with Ping

Format:

```
ping HOST
ping -c COUNT HOST
```

Example:

```
ping -c 3 google.com
```

```
$ ping -c 3 google.com
PING google.com (216.58.2.7) 56 bytes of data.
64 bytes from 216.58.2.7: icmp_seq=1 ttl=53 time=20.1 ms
64 bytes from 216.58.2.7: icmp_seq=2 ttl=53 time=20.2 ms
64 bytes from 216.58.2.7: icmp_seq=3 ttl=53 time=23.9 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time
2004ms
rtt min/avg/max/mdev = 21.489/22.924/24.154/1.111 ms
```

```
$ ping -c 3 google.com
PING google.com (216.58.2.7) 56 bytes of data.
From 216.58.2.7 icmp_seq=1 Destination Host Unreachable
From 216.58.2.7 icmp_seq=2 Destination Host Unreachable
From 216.58.2.7 icmp_seq=3 Destination Host Unreachable

--- google.com ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet
loss, time 2002ms
pipe 3
```

```
$ ping -c 3 10.0.2.2
PING 10.0.2.2 (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2: icmp_seq=1 ttl=63 time=0.272 ms
64 bytes from 10.0.2.2: icmp_seq=2 ttl=63 time=0.103 ms
64 bytes from 10.0.2.2: icmp_seq=3 ttl=63 time=0.202 ms

--- 10.0.2.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time
2001ms
rtt min/avg/max/mdev = 0.103/0.192/0.272/0.070 ms
```

```
# traceroute -n google.com
traceroute to google.com (216.58.2.7), 30 hops
max, 60 byte packets
Diagnosing Network Connections 413
 1  10.0.2.2  0.296 ms  0.178 ms  0.220 ms
 2  192.168.1.1  2.529 ms  2.713 ms  2.630 ms
 3  72.14.237.231  23.750 ms  22.087 ms
12.122.132.137  22.701 ms
 4  216.58.216.78  20.549 ms 12.250.16.30  22.904
ms 216.58.216.78  20.724 ms
```

```
$ tracepath -n google.com
 1?: [LOCALHOST]   pmtu 1500
 1:  10.0.2.2      0.470ms
 1:  10.0.2.2      0.649ms
 2:  192.168.1.1   2.147ms asymm 64
...
```

The `netstat` Command

-n Display numerical addresses and ports.

-i Displays a list of network interfaces.

-r Displays the route table. (netstat -rn)

-p Display the PID and program used.

-l Display listening sockets. (netstat -nlp)

-t Limit the output to TCP (netstat -ntlp)

-u Limit the output to UDP (netstat -nulp)

```
[jason@linuxsvr ~]$ netstat -i
Kernel Interface table
Iface    MTU  RX-OK RX-ERR RX-DRP RX-OVR  TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0    1500   3975      0      0 0        2627      0      0      0 BMRU
lo     65536      8      0      0 0           8      0      0      0 LRU
[jason@linuxsvr ~]$ netstat -rn
Kernel IP routing table
Destination Gateway     Genmask         Flags   MSS Window  irtt Iface
0.0.0.0     10.0.2.2    0.0.0.0         UG        0 0          0 eth0
10.0.2.0    0.0.0.0     255.255.255.0   U         0 0          0 eth0
[jason@linuxsvr ~]$ sudo netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address  State   PID/Program
name
tcp        0      0 0.0.0.0:22     0.0.0.0:*        LISTEN  943/sshd
tcp        0      0 127.0.0.1:25   0.0.0.0:*        LISTEN  1313/master
```

Packet sniffing with `tcpdump`

tcpdump

-n Display numerical addresses and ports.

-A Display ASCII (text) output.

-v Verbose mode. Produce more output.

-vvv Even more verbose output.

```
$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
19:25:49.639495 IP linuxsvr.ssh > 10.0.2.2.64440: Flags [P.], seq 3312803324:3312803408, ack 2443835, win 40880, length 84
19:25:49.639586 IP linuxsvr.ssh > 10.0.2.2.64440: Flags [P.], seq 84:120, ack 1, win 40880, length 36
19:25:49.639750 IP 10.0.2.2.64440 > linuxsvr.ssh: Flags [.], ack 84, win 65535, length 0
19:25:49.639763 IP 10.0.2.2.64440 > linuxsvr.ssh: Flags [.], ack 120, win 65535, length 0
$ sudo tcpdump -Anvvv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
19:44:27.067530 IP (tos 0x10, ttl 64, id 5120, offset 0, flags [DF], proto TCP (6), length 64)
    10.0.2.44.37534 > 10.0.2.15.80: Flags [P.], cksum 0xfe34 (incorrect -> 0xce40), seq 1:13, ack 1, win 683, options [nop,nop,TS val 1585227 ecr 1584441], length 12
E..@..@.@.(............P..>.:........4.....
..0K..-9GET /about
```

```
telnet HOST_OR_IP PORT_NUMBER
```

```
$ telnet google.com 80
Trying 216.58.2.7...
Connected to google.com.
Escape character is '^]'.
GET /
HTTP/1.0 200 OK
^]
telnet> quit
closed.
```

Summary

- ping
- traceroute / tracepath
- netstat
- tcpdump
- telnet