Networking Cheat Sheet for Platform Engineers

Abul Hasan Fahad

May 1, 2025

1 Diagnose First: Network Down or Misconfigured?

Before jumping to theory, test from the CLI:

```
# Test DNS
$ dig google.com +short

# Ping external and internal targets
$ ping 8.8.8.8        # Is IP reachable?
$ ping google.com     # Is DNS working?

# Check routing
$ ip route show

# Check active interfaces
$ ip addr show

# Default gateway
$ ip route | grep default
```

If DNS fails, check `/etc/resolv.conf`. If routes are missing, re-check your DHCP or static config.

2 Understand the Flow: What Talks to What?

Everything in Linux uses the same TCP/IP stack. Think layers:

- **Layer 1-2 (Ethernet)**: MAC address, switches, ARP
- **Layer 3 (IP)**: IP addressing, routing
- **Layer 4 (TCP/UDP)**: Ports, connections
- **Layer 7 (Apps)**: HTTP, SSH, DNS

3 Who's Using the Network? (Processes and Ports)

```
# Show all listening services
$ ss -tulnp

# What process owns a port?
$ lsof -i :8080

# Connections in/out
$ netstat -antp | grep ESTABLISHED
```

4 Create or Watch Network Traffic

Use these to troubleshoot or test services.

Netcat: The Swiss Army Knife

```
# Listen on port 9999
$ nc -l 9999

# Connect to a port
$ nc <target-ip> 9999
```

Curl: Test HTTP Services

```
$ curl -I http://localhost:8080
```

Tcpdump: See the Wire

```
# Capture traffic on eth0
$ sudo tcpdump -i eth0 -nn port 80
```

5 Firewall Rules: Are You Blocking Yourself?

```
# See iptables rules
$ sudo iptables -L -v -n

# Allow incoming SSH
$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

For persistent rules, use `iptables-save` and `iptables-restore` or modern `nftables`.

6 Traceroute and DNS: Diagnosing Remote Issues

```
# Trace network path
$ traceroute google.com

# DNS resolution test
$ dig google.com
$ dig @8.8.8.8 google.com
```

If traceroute fails early, the issue is likely local or at your ISP. Late failures = remote server or upstream block.

7 Quick Tips and Reminders

- Always check loopback: `ping 127.0.0.1`
- DNS problems? Try `dig` or `host`
- New services not reachable? Check `ss -tuln` and firewall
- Use `netcat` to simulate services quickly
- Want to sniff traffic? `tcpdump` is your friend

Further Reading

- M. W. Lucas, *Networking for Systems Administrators*
- Julia Evans' zines (`https://jvns.ca/zines/`)
- Linux man pages: `man ip`, `man ss`, `man tcpdump`