Networking Troubleshooting Cheat Sheet

A handy cheat sheet covering essential networking troubleshooting commands, techniques, and concepts for network administrators and IT professionals.

Basic Network Troubleshooting Tools

Ping

Description:	Tests basic network connectivity by sending ICMP echo requests to a target host.
Command:	`ping <destination>`
Example:	`ping google.com` or `ping 192.168.1.1`
Troubleshooting Use:	Verify network connectivity, check for packet loss, and measure round-trip time.
Common Issues:	Destination unreachable, request timeout, high latency.
Solutions:	Check network configuration, verify DNS resolution, investigate network congestion or hardware issues.

Traceroute/Tracepath

Description:	Traces the route taken by packets to reach a destination, displaying each hop along the path.
Command:	`traceroute <destination>` (or `tracepath <destination>` on Linux)
Example:	`traceroute google.com`
Troubleshooting Use:	Identify network bottlenecks, locate points of failure, and map the network path.
Common Issues:	Hops timing out, unexpected routing paths, excessive latency at specific hops.
Solutions:	Investigate problematic hops, check firewall configurations, and review routing tables.

Nslookup/Dig

Description:	Queries DNS servers to obtain domain name or IP address information.
Command:	`nslookup <hostname>` or `dig <hostname>`
Example:	`nslookup google.com` or `dig google.com`
Troubleshooting Use:	Verify DNS resolution, check DNS records, and troubleshoot DNS-related issues.
Common Issues:	Incorrect DNS resolution, DNS server unreachable, incorrect DNS records.
Solutions:	Verify DNS server settings, check DNS records, and troubleshoot DNS server connectivity.

Advanced Network Analysis

Tcpdump/Wireshark

Description:	Packet capture and analysis tools used to inspect network traffic.
Command:	`tcpdump -i <interface> <filter>` or Wireshark GUI
Example:	`tcpdump -i eth0 port 80`
Troubleshooting Use:	Analyze network traffic, identify protocols, troubleshoot network performance issues, and detect security threats.
Common Issues:	Excessive traffic, unexpected protocols, suspicious activity, performance bottlenecks.
Solutions:	Filter traffic, analyze packet contents, and identify root causes of network issues.

Netstat/Ss

Description:	Displays network connections, routing tables, interface statistics, and masquerade connections.
Command:	`netstat -an` or `ss -an`
Example:	`netstat -an | grep :80`
Troubleshooting Use:	Identify listening ports, check connection states, and monitor network traffic.
Common Issues:	High number of connections, connections in CLOSE_WAIT state, unauthorized listening ports.
Solutions:	Investigate suspicious connections, identify resource-intensive processes, and secure listening ports.

Iperf/Nuttcp

Description:	Network bandwidth measurement tools used to test network throughput and performance.
Command:	`iperf -s` (server) and `iperf -c <server_ip>` (client)
Example:	`iperf -c 192.168.1.100`
Troubleshooting Use:	Measure network bandwidth, identify network bottlenecks, and evaluate network performance.
Common Issues:	Low bandwidth, high latency, packet loss.
Solutions:	Check network infrastructure, identify bandwidth-intensive applications, and optimize network configuration.

Common Network Issues and Solutions

IP Address Conflicts

Issue: Two or more devices are configured with the same IP address.

Symptoms: Intermittent connectivity issues, inability to access network resources.

Solutions:

- Use DHCP to dynamically assign IP addresses.
- Manually configure static IP addresses, ensuring each device has a unique address.
- Use `ping` to identify the conflicting IP address.
- Check ARP tables to determine the MAC address associated with the conflicting IP address.

DNS Resolution Problems

Issue: Inability to resolve domain names to IP addresses.

Symptoms: Cannot access websites by name, but can access them by IP address.

Solutions:

- Verify DNS server settings.
- Use `nslookup` or `dig` to query DNS servers.
- Flush the DNS cache using `ipconfig /flushdns` (Windows) or `sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder` (macOS).
- Check the host file for incorrect entries.

Gateway Issues

Issue: Devices are unable to communicate outside the local network.

Symptoms: Cannot access the internet, cannot ping external IP addresses.

Solutions:

- Verify the default gateway setting.
- Ensure the gateway device is reachable.
- Check the gateway device’s configuration.
- Traceroute to a known external IP address to identify the point of failure.

Wireless Network Troubleshooting

Signal Strength and Interference

Issue: Weak wireless signal or interference affecting network performance.

Symptoms: Slow connection speeds, intermittent disconnections, high latency.

Solutions:

- Check the wireless signal strength using a Wi-Fi analyzer tool.
- Identify sources of interference (e.g., microwave ovens, cordless phones).
- Move closer to the wireless access point.
- Change the wireless channel to avoid overlapping with other networks.

Authentication Problems

Issue: Inability to connect to the wireless network due to incorrect credentials or authentication failures.

Symptoms: Incorrect password error, authentication timeout.

Solutions:

- Verify the wireless password.
- Check the wireless security settings (e.g., WPA2, WPA3).
- Ensure the wireless client is configured to use the correct authentication method.
- Restart the wireless access point and client device.

DHCP Issues

Issue: Devices are unable to obtain an IP address from the DHCP server.

Symptoms: APIPA address (169.254.x.x), no internet access.

Solutions:

- Verify the DHCP server is running and reachable.
- Check the DHCP scope and lease time.
- Release and renew the IP address on the client device.
- Restart the DHCP server.