A sysadmin's daily task involve managing servers and the data center's network. Following utilities and commands would help a sysadmin manage networks using linux from basic to advanced level.

Ping	
As the name suggests, ping is used to check the end-to-end connectivity between the system that you are pinging it to from your system. It uses ICMP Echo packets that travel back when a ping is successful. This might be a very first step to check any system/network connectivity. Ping can be with IPv4 and IPv6 addresses both. To know more about IP addresses and how to get your system's IP, refer to the article: https://opensource.com/article/18/5/how-find-ip-address-linux	
IPv4- ping <ip address>/<fqdn>	fqdn stands for fully qualified domain name, this can be your website-name.com or your server like server-name.company.com
IPv6- ping6 <ip address>/<fqdn>	
Also, you can use it to resolve names of websites to their corresponding IP address.	
Traceroute	
This is a nice utility for tracing the full network path from your system to other. Ping check's the end-to-end connectivity, traceroute utility tell you all the router IPs which come in the path when you try to reach the end system/website/server. Usually it is the second step after ping for any network connection debugging.	
traceroute <ip address>/<fqdn>	
Telnet	
Use this to telnet to any server.	
telnet <ip address>/<fqdn>	
Netstat	
Network statistics (netstat) utility is used to troubleshoot network connection problems with ability to check interface/port statistics, routing tables, protocol stats, etc. Any sysadmin's must-have tool!	
netstat -l	shows the list of all the ports which are in listening mode
netstat -a	shows all ports, to specify only tcp use '-at' (for udp use '-au')
netstat -r	provides routing table
netstat -s	provides summary of statistics for each protocol
netstat -i	displays TX/RX packet statistics for each interface
Nmcli	
A very good utility for managing network connections,configurations,etc. It can be used to control Network Manager and modify network configuration details of any device.	
nmcli device	lists all devices on the system
nmcli device show <interface>	shows network related details of the specified interface
nmcli connection	to check connection of the device
nmcli connection down <interface>/nmcli connection up <interface>	this command shuts/starts the specified interface
nmcli con add type vlan con-name <connection-name> dev <interface> id <vlan-number> ipv4 <ip/cidr> gw4 <gateway-ip>	this commmand adds a vlan interface with the specified vlan number, ip and a gateway to a particular interface
Routing	
There are many commands to check and configure routing. Some useful ones and their short description is as shown below:	
ip route	shows all the current routes configured for respective interfaces.
route add default gw <gateway-ip>	to add a default gateway to the routing table
route add -net <network ip/cidr> gw <gateway ip> <interface>	to add a new network route to the routing table. There are many other routing parameters like adding a default route, default gateway, etc.
route del -net <network ip/cidr>	to delete a particular route entry from the routing table.
ip neighbor	this shows the current neighbor table. It can be used to add/change/delete new neighbors.
arp	this is another similar utility like ip neighbor. It maps IP address of a system to its corresponding MAC (Media Access Control) address. In networking, ARP stands for Address Resolution Protocol.

Tcpdump

Linux provides many packet capturing tools like tcpdump, wireshark, tshark etc. They are used to capture the network traffic in packets which are transmitted/received and hence very useful for a sysadmin to debug any packet loss or related issues. For CLI enthusiasts, tcpdump is a great tool and for GUI users Wireshark is a great utility to capture and analyze packets. Tcpdump is a linux built-in utility to capture network traffic. It can be used to capture/show traffic on specific ports, protocols, etc.

tcpdump -i <interface-name>	shows live packets from the specified interface. Packets can be saved in a file by the adding '-w' flag & name of the output file to the command ex- tcpdump -w <output-file.> -i <interface-name>
tcpdump -i <interface> src <source-ip>	to capture packets from a particular source IP
tcpdump -i <interface> dst <destination-ip>	to capture packets from a particular destination IP
tcpdump -i <interface> port <port-number>	to capture traffic for a specific port number like 53, 80, 8080, etc.
tcpdump -i <interface> <protocol>	to capture traffic for a particular protocol like tcp, udp, etc.

Iptables

this is a firewall-like packet filtering utility which can allow/block certain traffic. The scope of this utility is very wide so we will discuss few of the useful ones.

iptables -L	lists all existing iptables rules
iptables -F	delete all the existing rules

The below commands allow traffic from the specified port number to the specified interface:

iptables -A INPUT -i <interface> -p tcp –dport <port-number> -m state –state NEW,ESTABLISHED -j ACCEPT

iptables -A OUTPUT -o <interface> -p tcp -sport <port-number> -m state – state ESTABLISHED -j ACCEPT

To allow loopback access to the system:

iptables -A INPUT -i lo -j ACCEPT

iptables -A OUTPUT -o lo -j ACCEPT

Nslookup

this tool is used to obtain IP address mapping of a website/domain and vice versa. It can also be used to obtain information on your DNS server, all DNS records of the website, shown in one of the examples below. Similar tool to nslookup is dig (Domain Information Groper) utility.

nslookup <website-name.com>	this command shows the IP address of your DNS server in Server field and below that it gives the IP address of the website you are trying to reach
nslookup -type=any <website-name.com>	shows all the available records for the specified website/domain

Network/Interface Debugging

To troubleshoot interface connectivity or related network issues, here is a quick summary of the necessary commands/files.

netstat	utility for network statistics
ss	utility for dumping socket statistics
nmap <ip-address>	to scan network ports, discover hosts, MAC address detection, much more. Stands for Network Mapper.
ip addr/ifconfig -a	command to provide IP addresses and related info of all the interfaces of a system
ssh -vvv user@<ip/domain>	used to ssh to another server with the specified ip/domain and username. The '-vvv' flag provides "triple-verbose" details of the processes going on while ssh'ing to the server
ethtool -S <interface>	to check the statistics for a particular interface
ifup <interface>/ifdown <interface>	to start/shut the specified interface
systemctl restart network	to restart network service for the system
/etc/sysconfig/network-scripts/<interface-name>	interface configuration file used to set IP, network, gateway, etc. for the specified interface. DHCP mode can be set here.
/etc/hosts	this file contains custom host/domain to IP mappings
/etc/resolv.conf	used to specify DNS nameserver IP of the system
/etc/ntp.conf	used to specify NTP server domain

