Some commands to look at:

- traceroute <hostname or ip>
    - The format of each line is as follows:
        - Hop RTT1 RTT2 RTT3 Domain Name [IP Address]
- ping <hostname or ip>
- df -kh
    - Display file system disk space usage in bytes and human readable format
- df -a
    - Display all file system disk space usage
- cat /proc/cpuinfo
    - Shows processor info
- mount
    - Use the mount command to mount a shared NFS directory from another machine:
        - mount -F nfs [-o mount-options] server:/directory /mount-point
        - Example:
            - mkdir /misc/local
            - mount -F nfs shadowman.example.com:/misc/export /misc/local
- dmesg
    - writes kernel info to stdout
    - Useful with less: dmesg | less
    - http://www.linfo.org/dmesg.html
- lspci
    - Lists detailed information about all PCI buses and devices in the system.
    - PCI is peripheral component interconnect protocol.
- lsusb
    - Like lspci, but shows usb connected devices.
- lshw
    - List hardware
- ipconfig   // Windows
    - Shows ip settings info
- ipconfig /all   // Windows
- ifconfig   // Linux
    - ifconfig <interface name>
    - ifconfig <interface name> up
    - ifconfig <interface name> <ip addr> up
    - ifconfig <interface name> <netmask> up
- arp -a
    - Displays the content of the ARP cache.
- arp -d <ip addr>
    - Deletes the entry with the IP address IPAddress.

- ps aux
  - "a" lists all processes on a terminal, including those of other users.
  - "x" lists all processes without controlling terminals.
  - "u" adds a column for the controlling user for each process.
- nslookup
  - http://techgenix.com/Using-NSLOOKUP-DNS-Server-diagnosis/
- host <ipaddress> or <hostname>
- sudo su -

Some stuff to know about:

- **DHCP vs Static IPs**
  - Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.
- **IP addresses, Subnetting, Netmasks**
  - http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html
  - http://www.subnet-calculator.com/
- **Gateway address**
  - The gateway operates at the network layer (Layer 3) of the OSI Model. The gateway is used when transmitting packets. When packets are sent over a network, the destination IP address is examined. If the destination IP is outside of the network, then the packet goes to the gateway for transmission outside of the network. The gateway is on the same network as end devices. The gateway address must have the same subnet mask as host devices. Each host on the network uses the same gateway.
  - The gateway should have a static address, as changing the address would cause packets not to be delivered. The gateway is typically assigned either the highest or lowest network address. This is not a requirement, but many organizations use a consistent addressing scheme to facilitate network planning.
- **Broadcast address**
  - A logical address at which all devices connected to a multiple-access communications network are enabled to receive datagrams. A message sent to a broadcast address is typically received by all network-attached hosts, rather than by a specific host.
  - The broadcast address for an IPv4 host can be obtained by performing a bitwise OR operation between the bit complement of the subnet mask and the host's IP address. In other words, take the host's IP address, and set to '1' any bit positions which hold a '0' in the subnet mask.

    - *Example:* For broadcasting a packet to an entire IPv4 subnet using the private IP address space 172.16.0.0/12, which has the subnet mask 255.240.0.0, the broadcast address is 172.16.0.0 | 0.15.255.255 = 172.31.255.255.
    - A special definition exists for the IP broadcast address 255.255.255.255. It is the broadcast address of the zero network or 0.0.0.0, which in Internet Protocol standards stands for this network, i.e. the local network. Transmission to this address is limited by definition, in that it is never forwarded by the routers connecting the local network to other networks.
- **DNS and DNS servers**
    - The **Domain Name System** (DNS) is a technology standard for managing names of public Web sites and other Internet domains. DNS technology allows you to type names into your Web browser like lifewire.com and your computer to automatically find that address on the Internet.
    - A **DNS server** is any computer registered to join the Domain Name System.
    - Computers on your home network locate a DNS server through their Internet connection setup properties.
    - Internet providers supply their customers the public IP addresses of primary and backup DNS servers, which are normally automatically set on a home network gateway device via DHCP. Alternatively, a home network administrator may also elect to use one of the free Internet DNS services.
    - *You can find the current IP addresses of your DNS server configuration via several methods*:
        - on the configuration screens of a home network router
        - on the TCP/IP connection properties screens in Windows Control Panel (if configured via that method)
        - from ipconfig or similar command line utility
- **DNS Records**
    - DNS stands for Domain Name System, which is the largest digital database in the world, containing information about every website on the internet. Every web site online has an IP address that is its actual internet location, and this number is used to locate the web site within the database. The data that tells the web server how to respond to your input is known as the DNS records, or zone files.
    - DNS records are basically mapping files that tell the DNS server which IP address each domain is associated with, and how to handle requests sent to each domain. When someone visits a web site, a request is sent to the DNS server and then forwarded to the web server provided by a web hosting company, which contain the data contained on the site.
    - Various strings of letters are used as commands that dictate the actions of the DNS server, and these strings of commands are called DNS syntax. Some DNS records syntax that are commonly used in nearly all DNS record configurations are A, AAAA, CNAME, MX, PTR.
- **Virtual machines and Hypervisors**

    - Specialized software, called a **hypervisor**, emulates the PC client or server's CPU, memory, hard disk, network and other hardware resources completely, enabling virtual machines to share the resources.
    - Advantages:
        - The hypervisor can emulate multiple virtual hardware platforms that are isolated from each other, allowing virtual machines to run Linux and Windows Server operating systems on the same underlying physical host.
        - Virtualization limits costs by reducing the need for physical hardware systems.
        - Virtual machines more efficiently use hardware, which lowers the quantities of hardware and associated maintenance costs, and reduces power and cooling demand.
        - They also ease management because virtual hardware does not fail. Administrators can take advantage of virtual environments to simplify backups, disaster recovery, new deployments and basic system administration tasks.
    - Disadvantages:
        - Virtualization does, however, require more bandwidth, storage and processing capacity than a traditional server or desktop if the physical hardware is going to host multiple running virtual machines.
        - There are some risks to consolidation, including overtaxing resources or potentially experiencing outages on multiple VMs due to one physical hardware outage.
- **Bridged adapter vs NAT**
    - **Bridged mode** basically means that the virtual network adapter in the virtual machine is bridged to the production network and the virtual machine operates as if it exists directly on the production network.
    - If NAT was used, each VM using NAT would use the host’s IP address, instead of its own.
    - http://techgenix.com/nat-vs-bridged-network-a-simple-diagram-178/
    - Set the network adapter to be "bridged" so the network traffic is visible on the 192.168.26 network.
- **Windows Server and Windows Server Manager**
- **Domains**
    - A domain name is an identification string that defines a realm of administrative autonomy, authority or control within the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS). Any name registered in the DNS is a domain name.
- **Windows Domain Services**
- **Domain Controllers**
    - As defined by Microsoft, in Active Directory server roles, computers that function as servers within a domain can have one of two roles: member server or domain controller.

    - Abbreviated as DC, domain controller is a server on a Microsoft Windows or Windows NT network that is responsible for allowing host access to Windows domain resources.
    - The domain controllers in your network are the centerpiece of your Active Directory directory service. It stores user account information, authenticates users and enforces security policy for a Windows domain.
- **Join a pc to a domain**
    - Just add the domain name to the domains the pc is a member of.
    - The domain controller will have a set up a user account with a username and a password the pc can authenticate to the domain with.
- **RDP**
- **Find pc hardware info**
- **Active Directory**
    - Active Directory will store information about organizations, sites, systems, users, shares, and just about any other network object that you can imagine.
    - A directory, in the most generic sense, is a comprehensive listing of objects.
    - Active Directory is similar to a phone book in several ways, and it is far more flexible.
    - Active Directory can be replicated between multiple domain controllers, so no single system is critical. In this way, the crucial data stored within Active Directory is both redundant and load-balanced.
- **Routers and Routing Tables**
    - https://technet.microsoft.com/en-us/library/cc958823.aspx
    - *When an IP packet is to be forwarded, the routing table is used to determine:*
        - The forwarding or next-hop IP address.
        - The interface to be used for the forwarding.
    - ***IP Routing Table Entries***
        - Network ID.
            - The network ID or destination corresponding to the route. The network ID can be class-based, subnet, or supernet network ID, or an IP address for a host route.
        - Network Mask.
            - The mask that is used to match a destination IP address to the network ID.
        - Next Hop.
            - The IP address of the next hop.
        - Interface.
            - An indication of which network interface is used to forward the IP packet.
- **Switches**
    - Switches occupy the same place in the network as hubs. Unlike hubs, switches examine each packet and process it accordingly rather than simply repeating the signal to all ports.

    - Switches map the Ethernet addresses of the nodes residing on each network segment and then allow only the necessary traffic to pass through the switch.
- **VPNs**
    - A remote-access VPN uses a public telecommunication infrastructure like the internet to provide remote users secure access to their organization's network.
    - A VPN client on the remote user's computer or mobile device connects to a VPN gateway on the organization's network.
    - The gateway typically requires the device to authenticate its identity. Then, it creates a network link back to the device that allows it to reach internal network resources -- e.g., file servers, printers and intranets -- as though it was on that network locally.
- **OSPF**
    - Routers connect networks using the Internet Protocol (IP), and OSPF (Open Shortest Path First) is a router protocol used to find the best path for packets as they pass through a set of connected networks.
    - OSPF is designated by the Internet Engineering Task Force (IETF) as one of several Interior Gateway Protocols (IGPs) -- that is, protocols aimed at traffic moving around within a larger autonomous system.
- **BGP**
    - BGP (Border Gateway Protocol) is protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers. BGP directs packets between autonomous systems (AS) -- networks managed by a single enterprise or service provider.
- **Finding redundant paths in a network**
- **SSH**
    - A network protocol that provides strong authentication and secure encrypted data communications between two computers connecting over an insecure network such as the Internet.
- **X Windows Display**
    - X's network protocol is based on X command primitives. This approach allows both 2D and (through extensions like GLX) 3D operations by an X client application which might be running on a different computer to still be fully accelerated on the X server's display.
- **NFS**
    - The Network File System (NFS) is a client/server application that lets a computer user view and optionally store and update files on a remote computer as though they were on the user's own computer.
    - The NFS protocol is one of several distributed file system standards for network-attached storage (NAS).
    - NFS allows the user or system administrator to mount (designate as accessible) all or a portion of a file system on a server.
    - The portion of the file system that is mounted can be accessed by clients with whatever privileges are assigned to each file (read-only or read-write).

    - NFS uses Remote Procedure Calls (RPC) to route requests between clients and servers.

Subnet Calculator

- http://www.subnet-calculator.com/