# Linux Academy: Network Topics – Course Notes http://linuxacademy.com

**Video One – hostname**

- Ubuntu
  - /etc/hostname
- CentOS or other RPM based distributions
  - /etc/sysconfig/network
- Hostname command
  - Will allow a change of hostname on the system *during the current session only*
  - The next reboot will revert the hostname back to the default configured in the files above
- uname
  - another command that will provide hostname information, universal across distributions – will also provide kernel version and platform (32bit or x64)
- Changing a hostname
  - In addition to the above distribution specific files
  - /etc/hosts
    - Many times a localhost reference will exit in the 'hosts' file
    - Ubuntu consideration:
      - 127.0.1.1 hostname
      - This is used as a local 'callback' hostname value on versions of Ubuntu after 10.04, is expected by some applications and can cause significant network delays on local network based applications if it does not exist
      - Can cause the system call 'getHostByName()' to return an error locally without

**Video Two – Interface Management (ifconfig/ifup/ifdown)**

- ifconfig up/down
  - -a summary listing of all interfaces
  - ifconfig [interface] up/down
    - [interface] can be ppp, serial, ethernet, vpn, etc
      - up or down will only work on already running and/or already configured interfaces
- Managing all interfaces at one time
  - ifup/ifdown –a (or –all) will perform the appropriate activate/deactivate on all interfaces
    - *CAUTION:* This includes the 'lo' or loopback interface. Taking this interface offline more than momentarily, especially within Xwindows will cause strange results
- Interface configuration – distribution differences
  - Ubuntu (or Debian based distributions)
    - /etc/network/interface
      - Sample static configuration for eth0
        - auto eth0
        - iface eth0 inet static
        - address 192.168.0.130
        - netmask 255.255.255.0
        - network 192.168.0.0
        - broadcast 192.168.0.255
        - gateway 192.168.0.1
        - dns-nameservers 192.168.0.1

- CentOS (or RPM based distributions)
  - /etc/sysconfig/network-scripts
  - 'ls –al ifcfg*' will list all configuration scripts for each interface available (i.e. ifcfg-eth0 for Ethernet '0')
  - Sample configuration:
    - DEVICE=eth0
    - BOOTPROTO=static
    - ONBOOT=yes
    - HWADDR=00:50:56:bc:00:71
    - IPADDR=192.168.1.195
    - NETMASK=255.255.255.0
    - GATEWAY=192.168.1.1
    - TYPE=Ethernet

**Video Three – Route**

- Several ways to review system routing
  - netstat –rn
  - route or route –n
    - return identical results (-n skips IP/name resolution and is faster, -r on netstat specifically asks for 'routing')
- Managing gateways
  - Add a default gateway
    - sudo route add default gw 192.168.1.1
  - Remove a default gateway
    - sudo route del default gw 192.168.1.1
  - Reject access to a host/network despite having a route
    - sudo route add –host 192.168.1.5 reject
      - ping will now report 'network unreachable' despite a default route to that network being available
    - Remove the previous rejection
      - sudo route del –host 192.168.1.5
  - Add access to a network with no default gateway OR using a different gateway than default
    - sudo route add –net 172.10.1.0 netmask 255.255.255.0 gw 192.168.1.1
      - will route all network traffic from the 172.10.1.0 network (with that netmask) through IP 192.168.1.1 – note that IP must itself be routable in the current routing scheme

**Video Four – Resolv.conf**

- Distribution independent location
  - /etc/resolv.conf
- CentOS (RPM based distributions)
  - Simply editing the resolv.conf file and adding dns servers will carry changes between sessions
- Ubuntu (Debian based distributions)
  - resolv.conf can be changed with an edit to the file, but will exist for the current session only, it is dynamically built during each boot from an existing configuration

- /etc/resolvconf/resolvconf.d
  - files will be ‘head’ ‘base’ and possibly ‘tail’
  - these contain anything from the specific configurations and documentation to end user warnings
  - created by a script called ‘resolvconf”
    - recreate the resolv.conf executing ‘resolvconf –u’ which will read and concatenate the existing ‘head’, ‘base’ and ‘tail’ files to create the system resolv.conf
- Sample configuration
  - # Warning – Changes directly to this file are good for current session only (Ubuntu)
  - # Warning – Changes directly to this file are permanent (CentOS)
  - nameserver 8.8.8.8
  - nameserver 208.67.222.222
  - domain localdomain.com
  - [optional]
    - options timeout:1 (one second timeout per DNS query before dropping)
    - search local.local (overridden if ‘domain’ exists as above)
    - options attempts: 1 (one attempt per DNS server to resolve name)

**Video Five – Nsswitch.conf**

- File is a list of system databases and name service configurations
- Associated with ‘nscd’ name service caching service
  - ‘nscd’ does NOT have to be installed, and often is not
  - if it is, ‘ncsd’ must be restarted to be sure the ‘nsswitch.conf” changes are reread immediately
    - sudo /etc/init.d/nscd restart
  - ‘ncsd’ can speed up name resolution when network performance is not optimal
- Determines the order in which name resolution happens, by default, local host file resolution is checked (/etc/hosts), if name/IP is not there, DNS is next, etc.
  - In /etc/nsswitch.conf, determined by following line:
    - hosts db files nisplus nis dns
    - this tells the system “when answering a name request, check internal DB (nscd cache), local files (/etc/hosts), nisplus (network information service), nis (same) and then DNS
  - We can force DNS to be the primary method of name resolution with a simple change
    - hosts dns db files nisplus nis
  - On systems where ‘nscd’ is not installed, this change is immediate as the configuration file is referenced during each call to ‘getHostByName()’ (an internal function called during every name/IP lookup)
  - On systems where ‘ncsd’ IS installed, the change may not be immediate depending on system load and processes in flight/locked during change – executing a restart flushes that cache and forces a read of that configuration
- Authentication to the system can be controlled through this file as well, by adding values to the fields called ‘passwd’, ‘group’ and ‘shadow’ you can control what systems or methods user authentication uses:
  - mysql – will attempt to use a mysql database configured to look up users
  - ldap – will perform an ldap lookup of that user and password
  - sss – will attempt to use a Active Directory configured to log in a user

    - ker – kerberos server user lookup
        - configuration of these specific services are topics covered in other/future tutorials, but knowing what they mean will help you recognize systems that have these configurations in place

**Video Six – Ping**

- ICMP
    - Internet Control Message Protocol
    - Stateless, protocol used to relay query messages
- Simple ping
    - ping host/ip/website
    - sends a specifically formatted 56byte ICMP packet and expects a specifically formatted 64byte packet in return
    - commonly blocked at firewalls
    - each response attempts to do a reverse DNS lookup from the responding IP
    - normal ping show performance information for each packet, stopping the ping will display a summary including total packets sent, average response time and total time spent in transit of all packets as well as the % of packets returned/lost
- Options
    - -a Audible: will beep on some terminals, flash on others, be ignored on some depending on the terminal configuration and operating system version
    - -A Adaptive: fast flood of packets, packets sent in sequence not waiting for a response before sending next request – must be run as 'sudo' or 'root'
    - -c Count: sent '#' of packets and stop, displaying summary
    - -f Flood: commonly referred to as a 'ping flood' but also viewed as a DoS tactic (Denial of Service), will send as many packets out to the destination host or IP as the network interface will handle
    - -I Interval: each request will be delayed by 'N' seconds
    - -n Numeric: return IP information only, do not attempt to do DNS lookups
    - -D Timestamp: will print a date/timestamp (in milliseconds since the epoch) with each line
    - -q Quiet: nothing is printed during packet transmission, only summary information is printed once stop – mainly used in conjunction with the '-c' parameter (above)
    - -w Deadline: only wait 'N' seconds between each SEND for an ACK before moving on
    - -v Verbose: gives more transmission information than just SEND/ACK

**Video Seven – Hosts**

- Universal location regardless of distribution
    - /etc/hosts
- Contains hosts and corresponding IPs as well as 'localhost' designation
    - CentOS (RPM based distributions) will contain '127.0.0.1 localhost' only
    - Ubuntu (Debian based distributions) will also contain '127.0.1.1 hostname'
        - Used as local loopback reference to the hostname by multiple applications, including some network X Windows apps
- Comments are typical '#' preceded
- Default DNS search order controlled by configuration in /etc/nsswitch.conf and is 'local files first, external DNS after'
- Any name can be assigned to your local IP or local host in /etc/hosts for testing purposes

- Can also be used as a simple ACL (Access Control List) to deny access to unwanted IPs (by redirecting to localhost) or domains (by redirecting to local system)