NETWORK MANAGEMENT

Linux Ubuntu Server Administration – VIDEOS

Two types of IP Addresses

1. Public
2. Private
3. Public – 5 CLASSES ipv4
   1. Class A: 1.0.0.1 176.255.255.254 (16 million hosts on

127 networks)

* 1. Class B: 128.1.0.1 191.255.255.254 (65,000 hosts on

16,000 networks)

* 1. Class C: 192.0.1.1 223.255.254.254 (254 hosts on 2

million networks)

* 1. Class D: 224.0.0.0 239.255.255.255 (multicasting)
  2. Class E: 240.0.0.0 254.255.255.254 (future/experiments)

1. Private – 3 CLASSES ipv4
   1. Class A: 10.0.0.0 10.255.255.253
   2. Class B: 127.16.0..0 172.31.255.255
   3. Class C: 192.168.0.0 192.168.255.255
2. Loopback IP 127.0.0.0 127.255.255.255

Subnet mask – 32 bit # used to convert ip #’s to network & host addresses.

Class A – 255.0.0.0

Class B – 255.255.0.0

Class C – 255.255.255.0

Network COMMANDS in linux

IFCONFIG

$ ifconfig – a # active.

$ ifconfig [interface]

NETSTAT

$ netstat | more

$ netstat –a #

$ netstat –at # tcp only.

$ netstat –au # udp only.

$ netstat –atl # listen to ports (tcp).

$ netstat –aul # listen to ports (udp).

$ netstat – s # status.

$ netstat – r # status.

$ netstat – rn # numbers only.

$ netstat – ie # list interfaces.

$ netstat – g # “mighty” cast info.

$ netstat – c # live stream monitor.

ROUTE – add gateway, block host, block entire network

$ route – n # the usual.

$ sudo route add default gw [192.168.128.1] # add default gateway.

$ sudo route add –host 10.0.2.14 reject # block host 10.0.2.14

$ sudo route add –net 10.0.2.0 netmask 255.255.255.0 reject # reject network.

TCPDUMP

$ sudo tcpdump –i [interface] # capture packets for interface.

$ sudo tcpdump –D

$ sudo tcpdump –c 5 –i [interface] # 5 times.

$ sudo tcpdump –A –i [interface] #

$ sudo tcpdump –XX –I [interface] # capture packets.

$ sudo tcpdump –w [filename] –i [interface] # create file of capture packets.

$ sudo tcpdump –r [filename] # read file of captured packets.

$ sudo tcpdump –i [interface] port ## # capture port ## only.

$ sudo tcpdump –i [interface] src [source ip] # capture source IP.

$ sudo tcpdump –i [interface] dst [dest’n ip] # capture destination IP.

NMAP

$ nmap –A –t4 scanme.nmap.org

NSLOOKUP

$ nslookup [domain name]

$ nslookup –query=mx [domain name] # mail server info.

$ nslookup –query=ns [domain name] # name servers.

$ nslookup –query=soa [dn] # startup information.

$ nslookup –query=any [domain] # ALL information.

$ nslookup [ip address] # reverse lookup.

$ nslookup # interactive

* set type=mx # mail.
* set type=nx
* set type=any

DIG

$ dig [domain name or IP]

$ dig [domain] +short

$ dig UBUNTU.COM mx +short

$ dig GOOGLE.COM ns

$ dig [ip]

HOST

$ host UBUNTU.COM

$ host –t mx GOOGLE.COM

$ host –a [domain name] # ‘A’ records of host

PING

$ ping [domain]

$ ping –c 5 # ping 5 time.

$ ping –I 7 # 7 milliseconds between pings.

$ ping – f 192.168.128.20 # I don’t know.

$ ping –I [ip number] # ip’s please.

$ ping –s 100 [www.google.com](http://www.google.com) # 100 bytes – packet size.

ARP

$ arp –v # verbose.

$ sudo arp –s [IP] [MAC ADDRESS]

$ sudo arp –d [IP] # remove.

TRACEROUTE

$ traceroute [www.google.com](http://www.google.com)

$ traceroute –d [www.google.com](http://www.google.com)

$ traceroute –p 30 # port 30.

$