Lab 1

Sunday, January 31, 2021 1:56 PM

ping:
MAC Colon-separated hexadecimal + Port number
Time required to transmit and get reply from destination

Look-back address(127.0.0.1)(self): <1ms
TTL (Time to leave transmission)
If you want to use applications on local system
Client and server application on same machine
Special addresses
ICMP internet control massive protocol
Network layer

netstat: network statistics

-e
How many bytes sent, received
3 transmissions:
unicast 1 sender 1 receiver
Multicast: 1 sender multiple receiver
Broadcast: all receivers
Protocols: mobile: GSM
Packets transferred according to protocol
Packets without protocol are suspicious/malicious

Without -e:
Want to see which messages transmitted with which protocol, state of transmission, who is sender and receiver

arp:
Address resolution protocol: for converting logical (IP) to physical address (MAC)

Entries of ARP cache (temp. memory)
Comes from LAN (ethernet) card, network provides processor (logical to physical translation happens on machine)

Machine gets IP address statically or dynamically
Static through Reverse Address?
Dynamic through DNCP

hostname:
Useful to get name of host

tracert:
Trace route from sender to destination,
Hop in between machines: between sender and receiver, n machines.
shows a max of 30 hops
At each hop, it will connect 3 times
Request time out: skip the hop
If not connected, it will try to connect through another machine
Shows IP, DNS, physical address of the destination

ipconfig: gives you how many different adapters and their configurations that are connected to the system

Configuration of your network
Active LAN cards (and configs)

nbtstat: diagnostic tool for NetBIOS over TCP/IP

Computer boots from BIOS mem
Network boots from NetBIOS

-c: netbios status
Ethernet - wired LAN card
Wifi - wireless ethernet/LAN card

Host assigns IP address
After lifetime, new IP address may be assigned

Entries in a cache table

Dynamic IP assignment
(limited IP addresses, may be given to another system)

nslookup: lookup + diagnose DNS

DNS: matches IP address to a name
Contacts DNS server

Without argument: of your machine
With argument (DNS):

route: device routing table
Every device finds route from source to destination
route PRINT: routing table currently stored in routing cache

pathping: trace route + ping (availability)

Ping uses ICMP protocol
On every hop, 32 byte message sent (100 messages transmitted) max 30 hops

getmac: get physical address of your machine on a windows computer

IP addresses (formats):
Dotted decimal: 127.0.0.1
(max 2^8=255.255.255.255, each segment of 8 bits: *IPv4 only*)
MAC/Physical: 1001:A45B:3ADC:984E::78(colon-separated hex digits-->48bits)
78-->port address (16 bits)
DNS Name: google.com