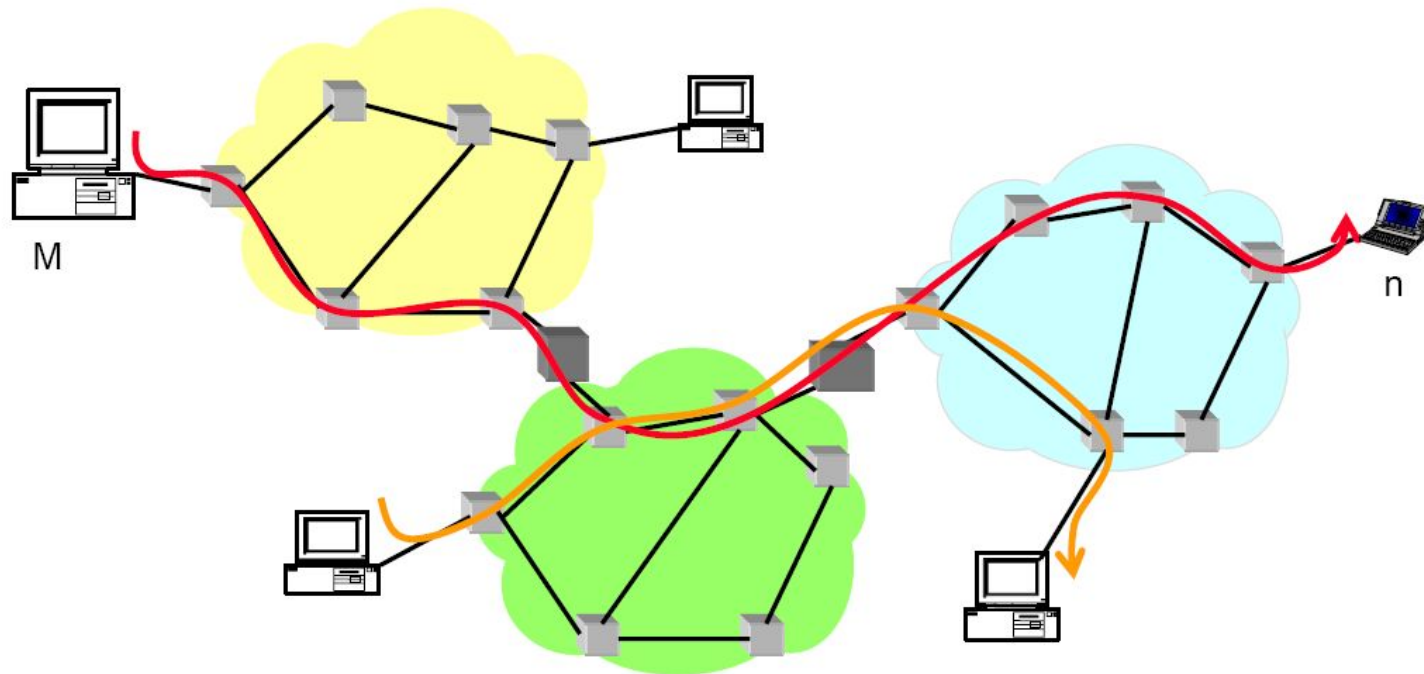# Computer Networks

Lab # 2

Networking Commands

Mohammad Ahsan Chishti
Assistant Professor
Computer Science & Engineering
NIT Srinagar

Basic Networking Commands

- How to detect if another machine is alive, the path to it, and resolve its DNS name to ip address, etc. …?

PING Command

- Ping is a basic Internet program that lets you verify that a particular IP address exists and can accept requests.

- The verb *ping means the act of using the ping utility or command. Ping is used diagnostically to ensure that a host computer you are trying to reach is actually operating.*

Various options available in the ping command:

- -t : repetitively send packets.

- -n: number of echo to be sent

- -l: sending buffer size [Max: 65500 bytes]

- -f: Dont fragment; If this option is provided, then the packet should not be fragmented and should be sent as it is.

- -r count: record route for count hops [3rd layer device]

- -j: loose source route [Optionally it can follow different route].

- -k: strict source route [MUST follow the route specified by us].

Note: For loopback address, you can ping it and get returns even when you are offline (not connected to any network).

If you don't get any valid replies, then there's a problem with the computer's Network settings.

Example:

- In order to send a packet to a host [192.168.230.1] with size of 60000 bytes each. We wish to send the packets repetitively.
  - ping -t -l 60000 192.168.230.1
- In order to send a packet with a size of 1000 bytes and don't permit fragmenting.
  - ping -f -l 2000 192.168.230.1
- In order to send a packet with a size of 1000 bytes and permit fragmenting.
  - ping -l 2000 192.168.230.1
- In order to use loose route to a destination.
  - ping –j 10.221.0.64 10.140.1.201
- In order to use strict route to a destination.
  - ping –k 10.221.0.64 10.140.1.201
    - • This will generate destination host unreachable message because this is not the first device that the ping will meet.
  - ping –k 172.16.0.253 10.140.1.201
    - • This will work fine because this is the first device that the ping will meet.

TRACERT Command

- If someone would like to know how he goes from his house to his office he could just tell the list of the crossroads where he passes.

- The same way we can ask the data sent over from your computer to the web server which way does it go, through which devices?

- We ask it by using the utility called traceroute.

- In most computers today you can use this tool from the command line: In UNIX machines it is called traceroute, in MS Windows machines it is called tracert.

Various options available in the tracert command:

- -d: Don't resolve addresses to hostnames.
- -h maximum_hops :Maximum number of hops to search for target
- -j host_list : Loose source router along host list.
- -w time-out : wait timeout milliseconds for each reply.

Example:

- • To check the options available in tracert,
  - tracert
- • To check the trace from your PC to a server
  - tracert 196.1.64.1
- • If you don't want the names of the PC or devices on the way,
  - tracert –d 196.1.64.1
- • To check the loose route trace from your PC to a server
  - tracert –j 10.221.0.64 10.140.1.201

PATHPING Command

- This command is used as IP trace utility and so it is similar to the tracert command.

- It has some extra features compared to tracert command.

- PATHPING [-n] [-h max_hops] [-g host-list] [-p period] [-q num_queries] [-w timeout] [-t] [-R] [-r] target_name

PATHPING [-n] [-h max_hops] [-g host-list] [-p period] [-q num_queries] [-w timeout] [-t] [-R] [-r] target_name

- -n Don't resolve addresses to hostnames
- -h max_hops Max number of hops to search
- -g host-list Loose source route along host-list
- -p period Wait between pings (milliseconds)
- -q num_queries Number of queries per hop
- -w timeout Wait timeout for each reply (milliseconds)
- -T Test each hop with Layer-2 priority tags
- -R Test if each hop is RSVP aware

Enhanced Ping

- TJPing is an excellent, widely acclaimed ping/lookup/traceroute utility for Win95/98/Me/NT/2000/XP.

- It's fully configurable, multithreaded, and is very fast.

- All configuration options, hosts, and interface settings are remembered from session to session.

- Users can log all results to the file of their choice.

A screen shot of the TJPing software is shown below:
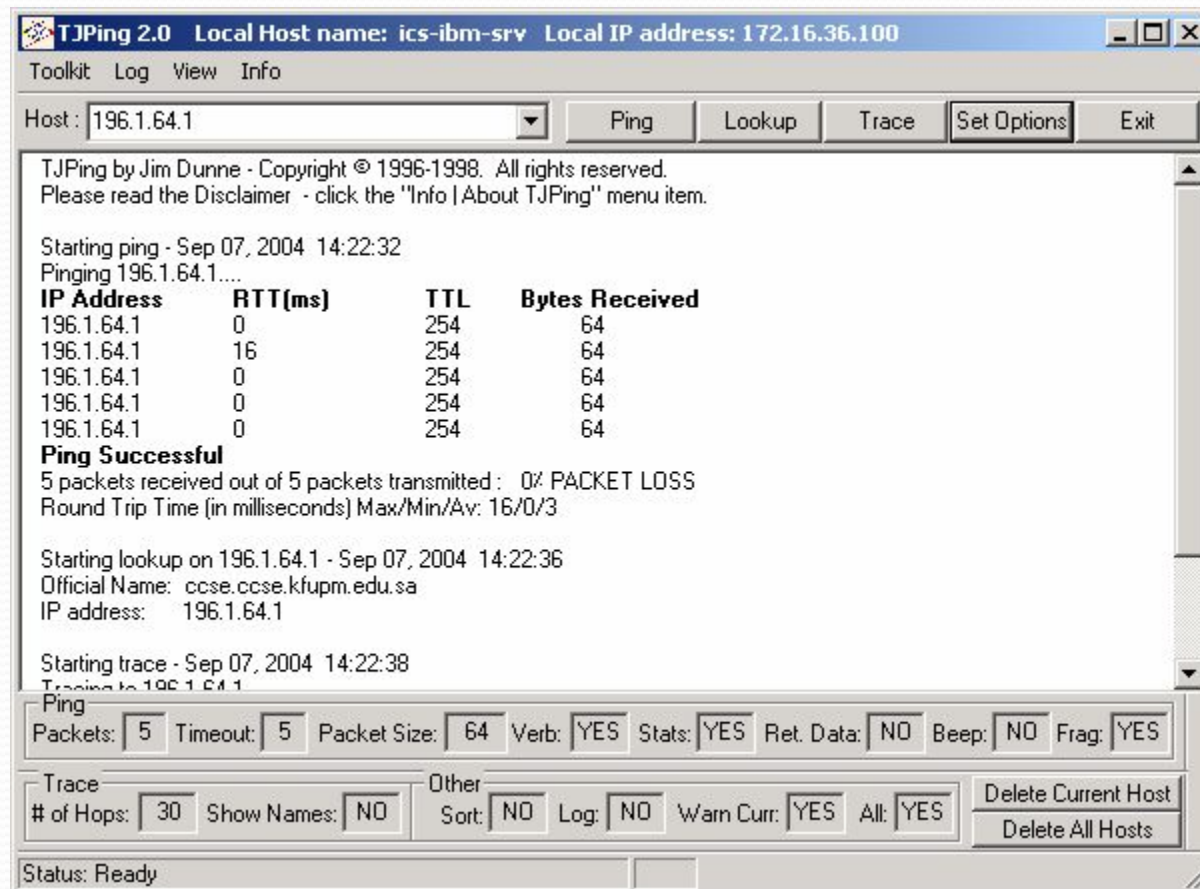
NETSTAT Command

● This command is used to get information about the open connections on your system (ports, protocols being used, etc.), incoming and outgoing data and also the ports of remote systems to which you are connected.

Various options available in the netstat command:

● -a :Displays all connections and listening ports.

● -e :Displays Ethernet statistics. This may be combined with the -s option.

● -n : Displays addresses and port numbers in numerical form.

● -p proto : Shows connections for the protocol specified by proto; proto may be TCP or UDP. If used with the -s option to display per-protocol statistics, proto may be TCP, UDP, or IP.

● -r : Displays the routing table.

● -s :Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.

Note: always use -a so as to see UDP packets also.

NetStat Live

- Have you ever wondered just how fast your network connection is?
- Not just how fast the modem is connected at, but how much data you can actually get?
- Does your internet connection sometimes seem slower than normal?
- NetStat Live is a small, easy to use TCP/IP protocol monitor which can be used to see your exact throughput on both incoming and outgoing data - whether you're using a modem, cable modem, DSL, or even local network!
- NSL doesn't just stop there, it lets you see how quickly your data goes from your computer to another computer on the internet;
- it even will tell you how many other computers your data must go through to get there!
- NSL also graphs your CPU usage of your system!
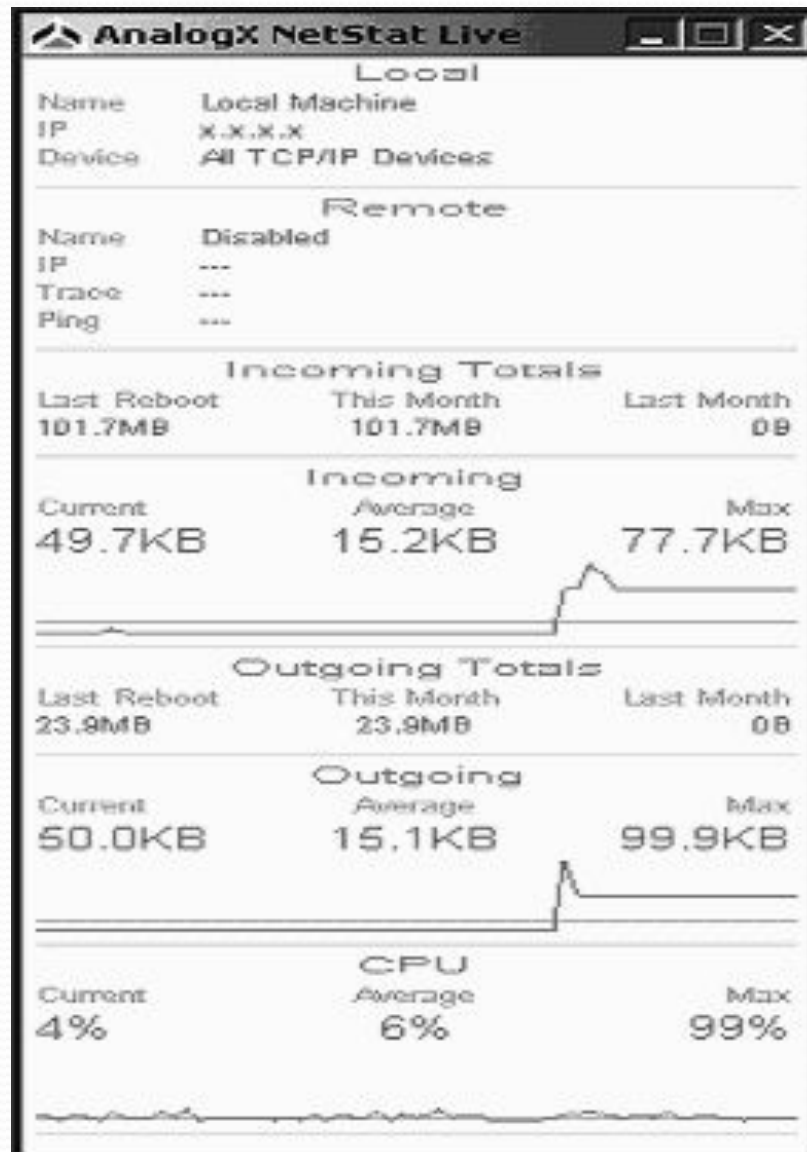
AT Command/schtasks

- This command is used to initiate any activity at a specific time.
- There are many options in at command but we will concentrate on very few which we would use for network related purposes.
- Use schtask instead for windows machine

Various options available in the **at command:**

- /i : interactive, which opens any window to show the pinging–[optional]
- /c : indicates command.
- AT [\\computername] [[id] [/DELETE] | /DELETE [/YES]]
- /every:date[,...] : Runs the command on each specified day(s) of the week or month. If date is omitted, the current day of the month is assumed.

Example:

● If we want to generate a ping at 13:15
at 13:15 /i cmd /c ping 192.168.232.2 -n 20

With interactive option, we don't need to give **cmd for general DOS commands.**
at 13:15 /i ping 192.168.232.2 –n 20

● If we want to generate a ping on a specific PC
at *pc_name* 13:15 /i cmd /c ping 192.168.234.245 -n 20

● If we want to generate ping with specific options.
at 11:03am cmd /c ping 192.168.230.1 -t -l 3000
at 5:15pm cmd /c ping 192.168.231.1 -t -l 15000

NET Command

- This command is used at the command prompt to display and control various network related activities. We would refer to only to a small set of the options available.

Various options available in the net command:
- net name : name of the PC
- net share : details about shared resources
- net start : to start a service
- net stop : to stop a service.
- net use : used to map a drive to the network path.

Example:

- • To create a share called "shared" for the "c:\ics432" directory
  - **net share shared=c:\ics432**

- • The computer would map the Z: drive to the network path //192.168.230.1/ics432 where c:\ics432 is already shared using the sharename 'shared'.
  - **net use z: \\192.168.230.1\shared**

- • To delete the mapped drive
  - **net use z: /DELETE**

- • To remove the sharing option
  - **net share shared /DELETE**

- • To send a text message to the computer with a host name of "ics-nwla1". If you receive an error, Start - Control Panel - Administrative Tools - Services. Make Messenger service automatic. Click the Start Service button.
  - **net send ics-nwla1 "ICS-NWLA1: A test message"**

- • To know the computer names that your computer can be sent messages TO
  - **net name**

- • To know about more options in net share command.[Similar applies to other options also]
  - **net share /?**

ROUTE Command

- This command manipulates network routing tables.
ROUTE [-f] [command [destination] [MASK netmask] [gateway]]

Various options available in the ROUTE command:
- -f : Clears the routing tables of all gateway entries. If this is used in conjunction with one of the commands, the tables are cleared prior to running the command.
  Command Specifies one of four commands
  - PRINT Prints a route
  - ADD Adds a route
  - DELETE Deletes a route
  - CHANGE Modifies an existing route
- Destination : Specifies the host to send command.
- MASK :If the MASK keyword is present, the next parameter is interpreted as the netmask parameter.
- Netmask :If provided, specifies a sub-net mask value to be associated with this route entry. If not specified, if defaults to 255.255.255.255.
- Gateway : Specifies gateway.

Example:

- • To display the routing table.
  - route PRINT

- To add a route a destination

- route add <destination> mask <subnetmask> <gateway> metric <number> IF <number>
  - -destination is the destination network or ip address [200.20.20.0].
  - -subnetmask is the subnet mask to be used [255.255.255.0].
  - -gateway is the next hop through which the packet goes [192.168.230.254].
  - -number after metric indicates the metric value [3].
  - -number after IF indicates interface number [0x2]

- **route add 200.20.20.0 mask 255.255.255.0 192.168.230.254 metric 3 if 0x2**

ARP Command

- The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol.

- The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer.

- ARP -s inet_addr eth_addr [if_addr]
- ARP -d inet_addr [if_addr]
- ARP -a [inet_addr] [-N if_addr]

Various options available in the ARP command:

- -a :Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

- -d :Deletes the host specified by inet_addr.
-
- -s : Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

- eth_addr : Specifies a physical address.

- if_addr : If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

Example:

- • To display the entries in ARP cache
  - arp -a

- • To delete an ARP entry in the cache
  - arp –d 192.168.230.1

IPCONFIG/IFCONFIG Command

● This command is used to get IP configurations present in your PC.

● IPCONFIG /all Display full configuration information.
● IPCONFIG /release [adapter] Release the IP address for the specified adapter.
● IPCONFIG /renew [adapter] Renew the IP address for the specified adapter.
● IPCONFIG /flushdns Purge the DNS Resolver cache. ##
● IPCONFIG /registerdns Refresh all DHCP leases and re-register DNS names. ##
● IPCONFIG /displaydns Display the contents of the DNS Resolver Cache. ##
● IPCONFIG /showclassid adapter Display all the DHCP class IDs allowed for adapter. ##
● IPCONFIG /setclassid adapter [classid] Modify the dhcp class id. ##
● ## works on Windows XP & 2K

Examples:

- \> ipconfig ... Show information.
- \> ipconfig /all ... Show detailed information
- \> ipconfig /renew ... renew all adapters
- \> ipconfig /renew EL* ... renew any connection that has its name starting with EL
- \> ipconfig /release *Con* ... release all matching connections,
- eg. "Local Area Connection 1" or

 "Local Area Connection 2"

NETSH Command

- Configure interfaces, routing protocols, filters, routes, RRAS.
- NETSH [-r *router name*] [*-a AliasFile*] [*-c Context*] [*Command | -f ScriptFile*]
- *context may be any of: DHCP,* **ip, ipx, netbeui, ras, routing, autodhcp, dnsproxy, igmp, mib, nat, ospf, relay, rip, wins.**
- Under Windows XP the available contexts are: AAAA, DHCP, DIAG, IP, RAS, ROUTING, WINS
- To display a list of commands that can be used in a context, type the context name followed by a space and a ? at the netsh> command prompt.
- e.g. netsh> **routing ?**

Examples:

- • Enter the netsh command.

netsh

- • Dump all the network information as a script to the screen. Can also be sent to a file by doing netsh dump > file.txt . This script can then be executed using the exec command.

netsh dump

- • Set the "Local Area Connection" to DHCP.

set address name="Local Area Connection" source=dhcp

- • Set the local address to Static.

set address local static 10.0.0.9 255.0.0.0 10.0.0.1 1

- • View network ip configuration. Below is an example of what may be seen.

netsh interface ip show config

Other Commands:

- telnet
- ssh
- Host
- Nslookup
- Dig
- Finger
- Wget
- ftp

Lab Work

1. Test the reach ability towards any server with all ping options enabled.
2. Find the route from your PC to CSC, NIT Srinagar
3. Find the route from your PC to Google server
4. Using the answers of the above, determine what is the first device your packet reaches to move from our network lab.
5. Use pathping with all the options
6. Install Tjping and repeat the exercises of Ping and Tracert commands
7. Show the output of netstat command with all options
8. Generate traffic to gateway using ping command [with various packet size options] and see how much of your outgoing interface is being used using Netstat Live
9. A network administrator wishes to check whether the sever present in his vicinity is reachable, at the start of the day [8:00am], Accomplish this task using at command.
10. Use net commands as show their usage.
11. Create a route entry in the routing table for your network with your gateway metric of 5.
12. Use ARP command with options on your PC.
13. Remove all the entries in the ARP cache and then generate a PING command to a specific PC on your network. Then, display all the entries in the ARP cache.
14. Show the TCP/IP configuration on your PC using **ipconfig /all.**
15. Get the information about the various interfaces present in your PC using netsh
16. Try all other commands and display screen shots.

Note:

- Screen Shots should be clear
- Each Screen shot should have your name in it
- Due Date: Next Lab
- Submit to: Miss Kiran

- Install OPNET IT Guru on your laptop and bring it along in your next lab.

- Have a wonderful weekend :)