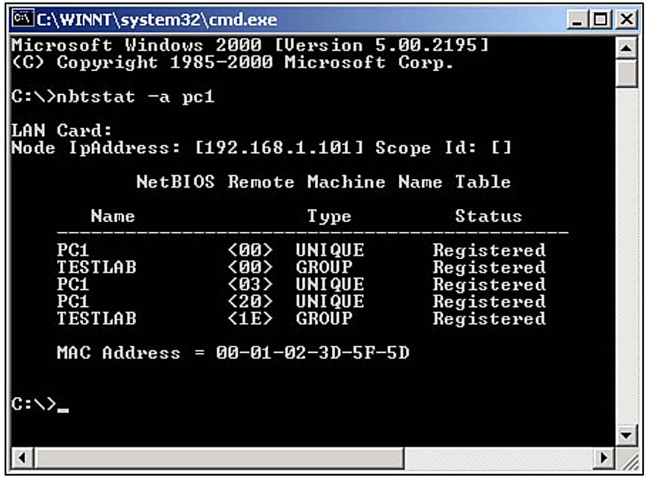
Services and Connections

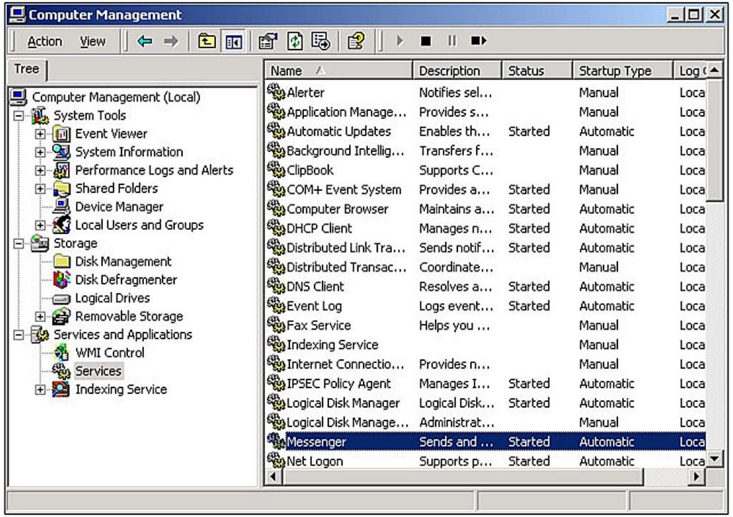
nbstat

1. Identify services with nbtstat (NetBIOS over TCP/IP Statistics).
    1. Access PC1. Make sure you are logged on as Administrator to the domain. You can verify this quickly by pressing Ctrl+Alt+Del.
    2. Open the command prompt and type nbtstat /?. This should give you a list of options with the nbtstat command. These include –a for accessing by NetBIOS names and –A for accessing by IP address. Try to memorize these different switches.
    3. Type nbtstat –a pc1. This reveals information like that shown in Figure 3.14.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>nbtstat -a pc1

LAN Card:
Node IpAddress: [192.168.1.101] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    PC1            <00>  UNIQUE      Registered
    TESTLAB        <00>  GROUP       Registered
    PC1            <03>  UNIQUE      Registered
    PC1            <20>  UNIQUE      Registered
    TESTLAB        <1E>  GROUP       Registered

    MAC Address = 00-01-02-3D-5F-5D


C:\>_
```

1. Notice the different line items. You have <00>, which is the hexadecimal ID for the Workstation service. You also have <03>, the ID for the Messenger service. Finally, you have the <20> ID for the Server service. These are the three basic services that all computers, servers and clients alike, use to transmit data across the network. There are others listed that deal with the domain. If one of the services is not listed, then you know that you will have to troubleshoot the system in question. It could have to do with what network the user logged in to, TCP/IP issues, or file corruption. Or it could be that the service is shut off. Let's take a look at the three main services from a graphical standpoint and show how they can be turned on and off.
2. Right-click My Computer and select Manage.
3. In the bottom-left area, click the plus (+) sign to expand the Services and Applications category.
4. Click the Services applet, as shown in Figure 3.15. Then select the Messenger service on the right side.



Name	Description	Status	Startup Type	Log (
Alerter	Notifies sel...		Manual	Loca
Application Manage...	Provides s...		Manual	Loca
Automatic Updates	Enables th...	Started	Automatic	Loca
Background Intellig...	Transfers f...		Manual	Loca
ClipBook	Supports C...		Manual	Loca
COM+ Event System	Provides a...	Started	Manual	Loca
Computer Browser	Maintains a...	Started	Automatic	Loca
DHCP Client	Manages n...	Started	Automatic	Loca
Distributed Link Tra...	Sends notif...	Started	Automatic	Loca
Distributed Transac...	Coordinate...		Manual	Loca
DNS Client	Resolves a...	Started	Automatic	Loca
Event Log	Logs event...	Started	Automatic	Loca
Fax Service	Helps you ...		Manual	Loca
Indexing Service			Manual	Loca
Internet Connectio...	Provides n...		Manual	Loca
IPSEC Policy Agent	Manages I...	Started	Automatic	Loca
Logical Disk Manager	Logical Disk...	Started	Automatic	Loca
Logical Disk Manage...	Administrat...		Manual	Loca
Messenger	Sends and ...	Started	Automatic	Loca
Net Logon	Supports p...	Started	Automatic	Loca

IPCONFIG

NAME

ipconfig -- view and control IP configuration state Go through the manual page and commands of ipconfig

https://man7.org/linux/man-pages/man8/ifconfig.8.html

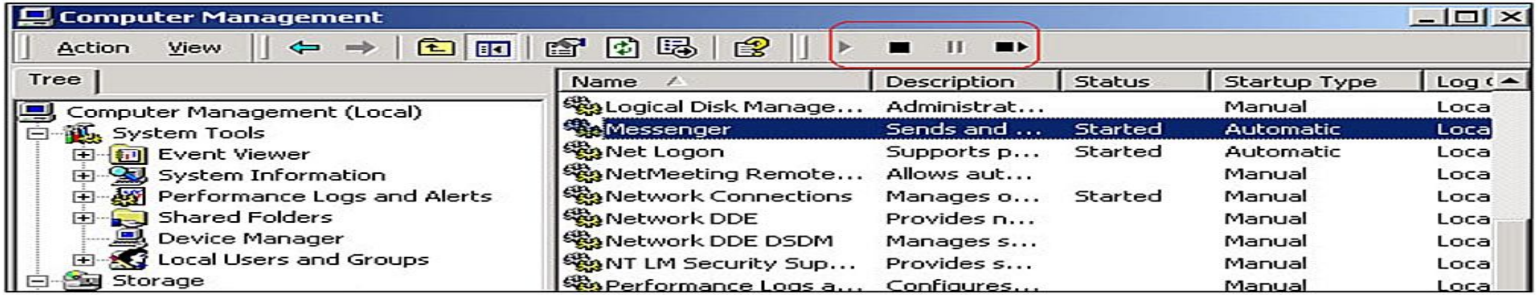
Questions

Questions:

1. Note down the name of some of the services.
2. IS the DHCP client service running?
3. Note down some services that started manually.
4. Use ipconfig to find out the IP address of the system
5. Find the MAC address of the system
6. How many interfaces are active in the system

Start and Stop the messenger service

1. **Although the Messenger service is very important to the system, it is not really considered one of the main services. This is because it is actually dependent on the Workstation service. Let's prove this now.**
    1. **Right-click the Messenger service and select Properties.**
    2. **Click the Dependencies tab. You will see that the Messenger service is indeed dependent on the Workstation service.**
    3. **Click the General tab. Notice that here you can start and stop the service as you see fit, as well as set how it will run at startup (or set it to not run at all).**
    4. **Close the Properties dialog box, but leave the Computer Management window open.**
    5. **There are several other ways to start and stop a service in the GUI and in the command prompt. For example, you can use the buttons at the top of the console window. You can also right-click the service and select Start/Stop, or you can use the net start and net stop commands in the command prompt.**



Computer Management (Local)
- System Tools
  - Event Viewer
  - System Information
  - Performance Logs and Alerts
  - Shared Folders
  - Device Manager
  - Local Users and Groups
- Storage

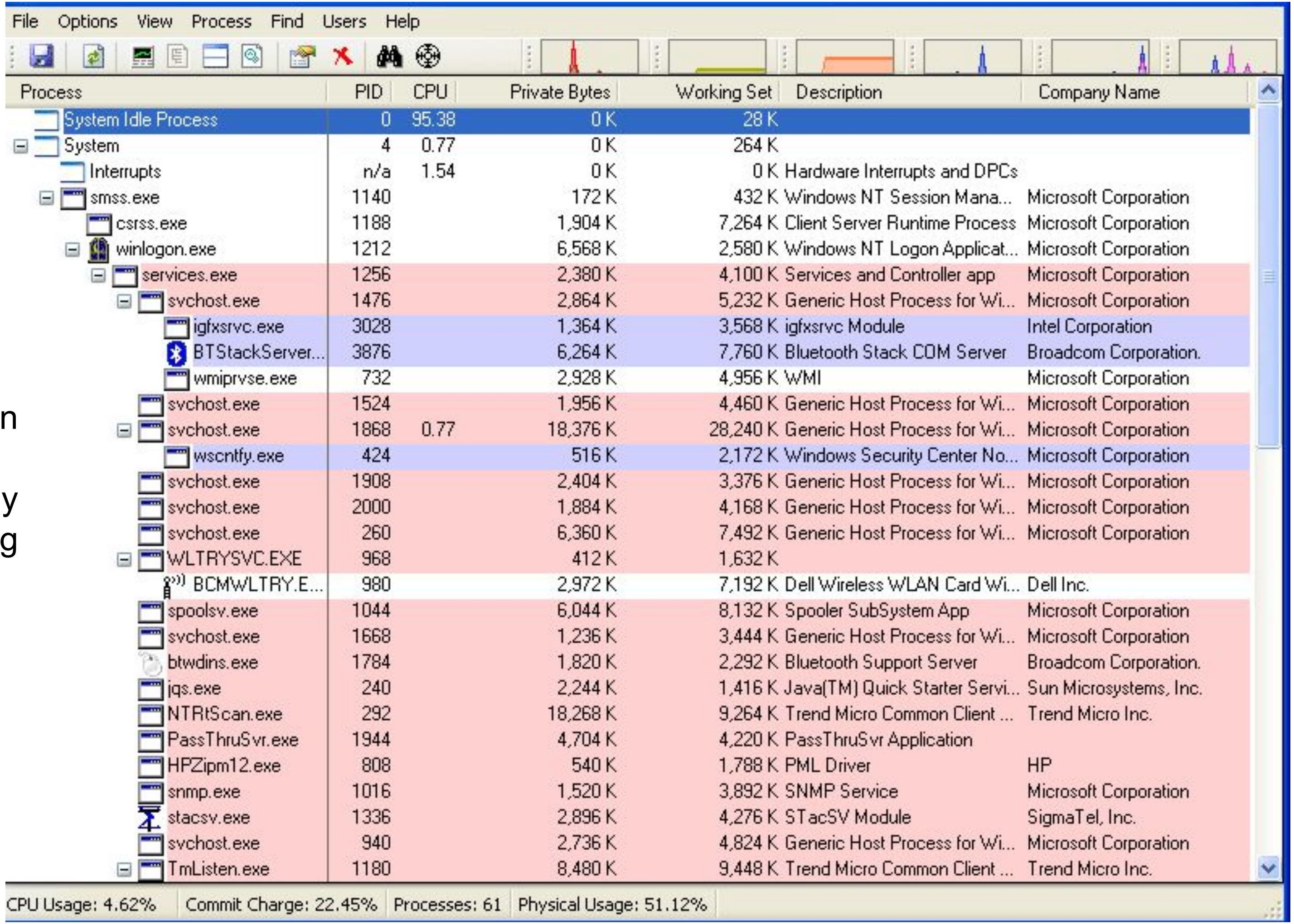
Name	Description	Status	Startup Type	Log (
Logical Disk Manage...	Administrat...		Manual	Loca
Messenger	Sends and ...	Started	Automatic	Loca
Net Logon	Supports p...	Started	Automatic	Loca
NetMeeting Remote...	Allows aut...		Manual	Loca
Network Connections	Manages o...	Started	Manual	Loca
Network DDE	Provides n...		Manual	Loca
Network DDE DSDM	Manages s...		Manual	Loca
NT LM Security Sup...	Provides s...		Manual	Loca
Performance Logs a...	Configures...		Manual	Loca

Sysinternals Process Explorer

Step-1 Download and Install Process VIEWER

https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer

Step 2. Open Process Explore by Double clicking the exe



Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	95.38	0 K	28 K		
System	4	0.77	0 K	264 K		
Interrupts	n/a	1.54	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	1140		172 K	432 K	Windows NT Session Mana...	Microsoft Corporation
csrss.exe	1188		1,904 K	7,264 K	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	1212		6,568 K	2,580 K	Windows NT Logon Applicat...	Microsoft Corporation
services.exe	1256		2,380 K	4,100 K	Services and Controller app	Microsoft Corporation
svchost.exe	1476		2,864 K	5,232 K	Generic Host Process for Wi...	Microsoft Corporation
igfxsrvc.exe	3028		1,364 K	3,568 K	igfxsrvc Module	Intel Corporation
BTStackServer...	3876		6,264 K	7,760 K	Bluetooth Stack COM Server	Broadcom Corporation.
wmiprvse.exe	732		2,928 K	4,956 K	WMI	Microsoft Corporation
svchost.exe	1524		1,956 K	4,460 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1868	0.77	18,376 K	28,240 K	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe	424		516 K	2,172 K	Windows Security Center No...	Microsoft Corporation
svchost.exe	1908		2,404 K	3,376 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	2000		1,884 K	4,168 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	260		6,360 K	7,492 K	Generic Host Process for Wi...	Microsoft Corporation
WLTRYSVC.EXE	968		412 K	1,632 K		
BCMWLTRY.E...	980		2,972 K	7,192 K	Dell Wireless WLAN Card Wi...	Dell Inc.
spoolsv.exe	1044		6,044 K	8,132 K	Spooler SubSystem App	Microsoft Corporation
svchost.exe	1668		1,236 K	3,444 K	Generic Host Process for Wi...	Microsoft Corporation
btwdins.exe	1784		1,820 K	2,292 K	Bluetooth Support Server	Broadcom Corporation.
jqs.exe	240		2,244 K	1,416 K	Java(TM) Quick Starter Servi...	Sun Microsystems, Inc.
NTRtScan.exe	292		18,268 K	9,264 K	Trend Micro Common Client ...	Trend Micro Inc.
PassThruSvr.exe	1944		4,704 K	4,220 K	PassThruSvr Application	
HPZipm12.exe	808		540 K	1,788 K	PML Driver	HP
snmp.exe	1016		1,520 K	3,892 K	SNMP Service	Microsoft Corporation
stacsv.exe	1336		2,896 K	4,276 K	STacSV Module	SigmaTel, Inc.
svchost.exe	940		2,736 K	4,824 K	Generic Host Process for Wi...	Microsoft Corporation
TmListen.exe	1180		8,480 K	9,448 K	Trend Micro Common Client ...	Trend Micro Inc.

CPU Usage: 4.62% Commit Charge: 22.45% Processes: 61 Physical Usage: 51.12%

Questions

Find the PID, CPU, Private bytes, working set, description, company name for the following processes

System

Csrss.exe

Smss.exe

wininit.exe

services.exe

svchost.exe

lsass.exe

Step 3: View Process Details

To view the details of a process, click on it in the list. You will see a detailed view of the process, including its name, ID, CPU usage, memory usage, and other details.

Step 4: Kill a Process

If you need to terminate a process, right-click on it in the list and select “Kill Process” from the context menu. You can also use the keyboard shortcut “Ctrl + D” to kill a process.

Step 5: Search for a Process

If you have a large number of processes running on your system, it can be difficult to find the process you are looking for. To search for a process, click on the “Find” menu and select “Find Handle or DLL”. In the search box, enter the name of the process you are looking for and click “Search”. Process Explorer will highlight the process in the list.

Step 6: Customize the Display

Process Explorer allows you to customize the display to show only the information you need. To customize the display, click on the “View” menu and select “Select Columns”. You can choose which columns to display, and the order in which they appear.

Sysinternals TCPVIEW

https://learn.microsoft.com/en-us/sysinternals/downloads/tcpview

Download TCPView from Microsoft’s Sysinternals website **here** in a zip file.

Extract the zip file and run the Tcpview.exe program to begin – a list of TCP/UDP connections is displayed along with the Process Name, Bytes Received/Sent and Remote Address etc.

The list is dynamic and presents a real time picture i.e. it changes as and when network connections are opened or closed.

By default, it updates every second but you can change the duration via View \ Update Speed in the menubar. IP addresses are resolved to their domain name versions.

Right clicking a Process presents several options:

- **Process Properties** – shows the filename and full path of the process so you can recognize or research unknown processes
- **End Process** – (for Advanced users), kill off a process if it is using too much data or is suspicious
- **Close Connection** – (for Advanced users), only available if the connection is Established
- **Whois** – opens in a separate window. See who owns the domain registered for a remote address
- **Copy** – copy the Process and associated details for pasting into a document or file. You can save the whole list by selecting File \ Save As from the menubar.