Services and Connections

Windows Services

- Press the Start (or) button.
- Type services.
- Click or tap the matching result.

OR

Use the Run dialog.

- Press the ⊞ Win+R keys simultaneously.
- Type services.msc.
- Press OK or hit ↵ Enter.

Questions

1. Note down the name of some of the services.
2. Note down some services that started manually.
3. Is the DHCP client service running?
4. Can you disable the messenger service?

netstat

Displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache. This command also allows a refresh of the NetBIOS name cache and the names registered with Windows Internet Name Service (WINS). Used without parameters, this command displays Help information.

Examples

To display both the Ethernet statistics and the statistics for all protocols, type:

```
netstat -e -s
```

To display the statistics for only the TCP and UDP protocols, type:

```
netstat -s -p tcp udp
```

To display active TCP connections and the process IDs every 5 seconds, type:

```
netstat -o 5
```

To display active TCP connections and the process IDs using numerical form, type:

```
netstat -n -o
```

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/netstat

Practice Questions

1. What is the local and foreign address of the established connections?
2. What are the different states of a tcp connection that you see?
3. What is the port number of the established connections?
4. Locate the connection mentioned in Question 3 and find it in wireshark. If it was a tcp connection can u locate the 3-way handshake for this established connection?

IPCONFIG

NAME

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

https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig

IPCONFIG

To display the basic TCP/IP configuration for all adapters, type:

```
ipconfig
```

To display the full TCP/IP configuration for all adapters, type:

```
ipconfig /all
```

To renew a DHCP-assigned IP address configuration for only the Local Area Connection adapter, type:

```
ipconfig /renew Local Area Connection
```

To flush the DNS resolver cache when troubleshooting DNS name resolution problems, type:

```
ipconfig /flushdns
```

To display the DHCP class ID for all adapters with names that start with Local, type:

```
ipconfig /showclassid Local*
```

To set the DHCP class ID for the Local Area Connection adapter to TEST, type:

```
ipconfig /setclassid Local Area Connection TEST
```

Practice Questions

Questions:

1. Write down the subnet mask of the local computer.
2. Write down the IP address of the default gateway of the local computer.
3. Find the MAC address of the system
4. How many interfaces are active in the system
5. Were you able to ping the IP address of your local gateway successfully?
6. Were you able to ping the IP address of your local DSN server successfully?

Traceroute

The TRACERT (in windows) diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, TRACERT uses varying IP Time-To-Live (TTL) values. Because each router along the path is required to decrement the packet's TTL by at least 1 before forwarding the packet, the TTL is effectively a hop counter. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer.

Use the Tracert Command

1. Open a command-line window like you did in Lab 1.
2. Type the command tracert /? and hit the <Enter> key on the keyboard.

Write down all the options available with tracert and what they do.

https://support.microsoft.com/en-gb/topic/how-to-use-tracert-to-troubleshoot-tcp-ip-problems-in-windows-e643d72b-2f4f-cdd6-09a0-fd2989c7ca8e

Practice Questions

Execute $tracert -d yahoo.com

1. How many hops is your machine away from yahoo.com? (Attach the output in the lab report)
2. Wait for a while and execute the same command again. Is the output the same as the first time? (Hint: no) Which hops are changed? Observe and compare the difference, and explain the reason

Sysinternals Process Explorer

Step-1 Download and Install Process VIEWER

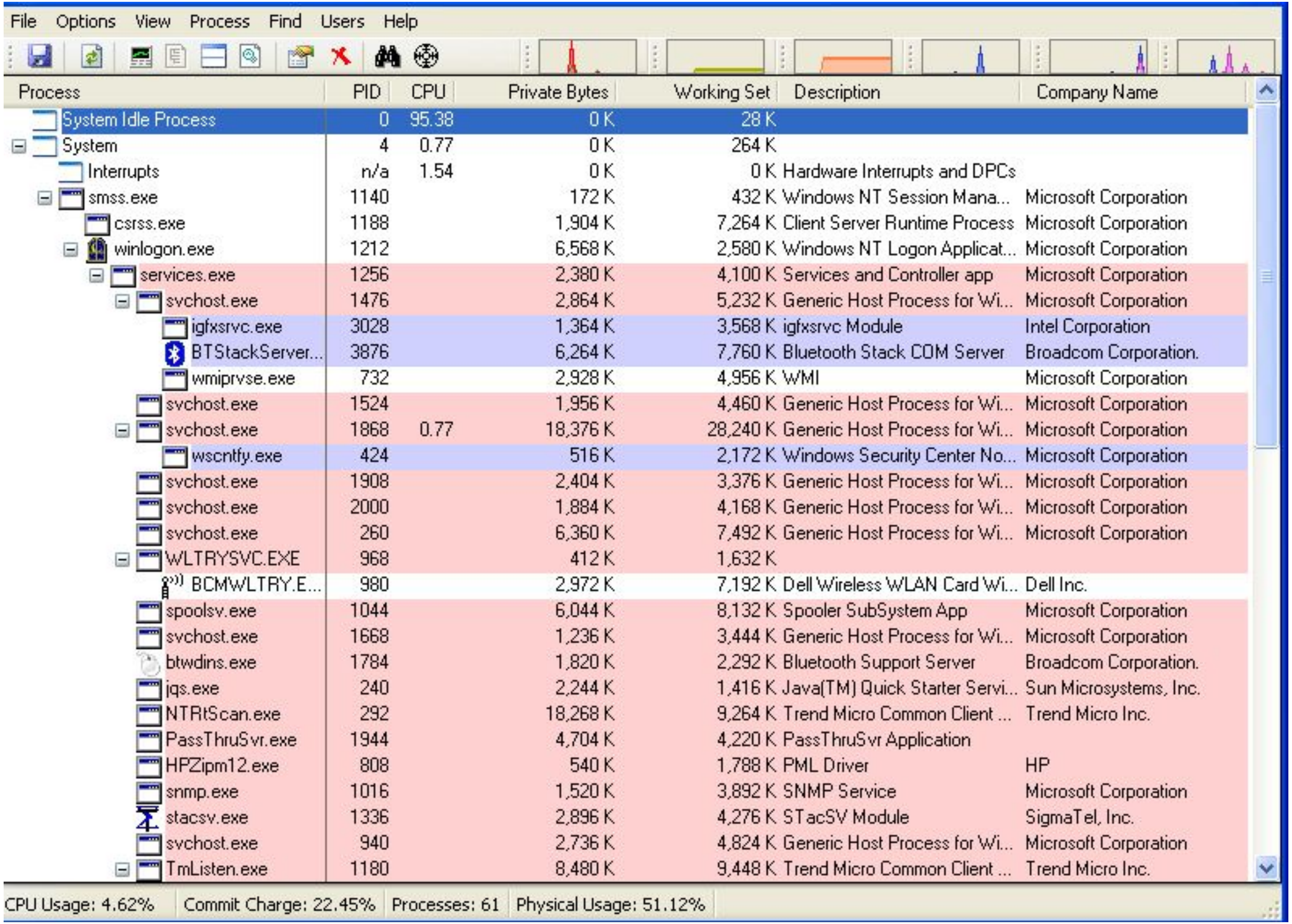
https://learn.microsoft.com/en-us/sysinternals/downloads/process-explorer

Process Monitor is an excellent troubleshooting tool from Windows Sysinternals that displays the files and registry keys that applications access in real-time. The results can be saved to a log file, which you can send it to an expert for analyzing a problem and troubleshooting it.

How to Use Process Monitor to Track Registry and File System Changes?

Step 1: Running Process Monitor & Configuring Filters

1. Download Process Monitor from Windows Sysinternals site.
2. Extract the zip file contents to a folder of your choice.
3. Run the Process Monitor application.
4. Include the processes that you want to track the activity on. For this example, you want to include Notepad.exe in the (Include) Filters.
5. Click Add, and click OK.
6. From the Options menu, click Select Columns.
7. Under “Event Details”, enable Sequence Number, and click OK.



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%

Step 2: Capturing Events

8. Open Notepad.
9. Switch to Process Monitor window.
10. Enable the “Capture” mode (if it’s not already ON). You can see the status of the “Capture” mode via the Process Monitor toolbar.
11. The highlighted button above is the “Capture” button, which is current disabled. You need to click that button (or use Ctrl + E key sequence) to enable capturing of events.
12. Cleanup the existing events list using Ctrl + X key sequence (Important) and start afresh.
13. Now switch to Notepad and try to reproduce the problem.
14. To reproduce the problem (for this example), try writing to HOSTS file (C:\Windows\System32\Drivers\Etc\HOSTS) and saving it. Windows offers to save the file (by showing the Save As dialog) with a different name, or in a different location. So, what happens under the hood when you save to HOSTS file? Process Monitor shows that exactly.
15. Switch to Process Monitor window, and turn off Capturing (Ctrl + E) as soon as you reproduce the problem. Important Note: Don’t take much time to reproduce the problem after enabling capturing. Similarly turn off capturing as soon as you finish reproducing the problem. This is to prevent Process Monitor from recording other unneeded data (which makes analysis part more difficult). You need to do all that as quickly as you can.

Step 3: Saving the Output

16. In the Process Monitor window, select the File menu and click Save.
17. Select Native Process Monitor Format (PML), mention the output file name and Path, save the file.
18. Right-click on the Logfile.PML file, click Send To, and choose Compressed (zipped) folder. This compresses the file by ~90%. Look at the graphic below.

Practice Questions

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

System

Csrss.exe

Smss.exe

wininit.exe

services.exe

svchost.exe

lsass.exe

Step 1 and 2 are same in slide 11

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.