APPLIED NETWORKING LABS:

A HANDS-ON GUIDE TO NETWORKING AND SERVER MANAGEMENT

Second Edition

Solutions

Dr. Randall Boyle

Jeffrey A. Clements

CONTENTS

CHAPTER 1: DOS COMMANDS

1.1 DOS BASICS

1. **Can you use the DIR command to show only executables? How?**

   Answer: You can use **dir /ad** to show only directories. You can use the command **dir *.exe** to see only executables.

2. **What happens if you start typing part of an existing file name and then press the Tab key?**

   Answer: It will complete the rest of the file name.

3. **Can you start programs from the command prompt? How?**

   Answer: Yes, you can start programs from the command prompt by typing in the name of the program. For example, you can type **explorer** to start a new Windows Explorer window.

4. **What happens if you drag-and-drop a file from Windows Explorer onto the DOS window?**

   Answer: It displays the complete path to that file.

1.2 IPCONFIG

1. **What is the practical difference between an IP address and a physical (MAC) address?**

   Answer: IP addresses help route packets as they move between networks. MAC addresses are used to pass packets across a single network. IP addresses on a packet won't change in transit, but a packet can have multiple frames with different MAC addresses. A host's MAC address won't change, but a host can switch IP addresses many times throughout a single day.

2. **What is the Default Gateway?**

   Answer: It's the computer that stands between you and the Internet.

3. **What do DNS servers do?**

   Answer: DNS servers will change domain names like www.Google.com into IP addresses.

4. **What is a subnet mask?**

   Answer: It tells you the size of your network and the number of hosts on your network.

1.3 PING

1. **Can you adjust the number of packets that are sent? How?**

   Answer: Yes, you use the –n option followed by the number of requests you'd like to send.

2. **What did the -t, -n, -l, and -r options do?**

   Answer: The -t option pinged the host until stopped. The -n option set the number of echo requests. The -l option adjusted the buffer size that was sent. The -r option recorded the route for count hops.

3. **Why would you experience packet loss?**

   Answer: There are many different reasons a packet could get lost: electromagnetic interference, power failure, faulty NICs, incorrectly configured networking equipment, solar flares, etc.

4. **Why would you want to send larger packets?**

   Answer: Sending larger packets would give you an idea of how packet size affects bandwidth, response times, fragmentation, etc.

1.4 TRACERT & PATHPING

1. **Why would you use the -d option?**

   Answer: It would not resolve addresses to host names.

2. **If you had several nodes "time out," how would the -w option help?**

   Answer: The -w option could be used to increase/decrease the time out option. This would tell you if the nodes were just slow or if they had completely failed.

3. **Why would a network administrator only want to see part of the route?**

   Answer: Being able to see specific network segments along an entire path would help a network administrator troubleshoot latency issues by identifying the problem segment along the path.

4. **How would the pathping results change if you didn't use -q 5 in the command?**

   Answer: If you hadn't used the -q 5 option, you would have sent many more queries (around 100).

1.5 NETSTAT

1. **How can netstat help you track the information coming in and out of your computer?**

   Answer: It can tell you which hosts are connected to your machine and which ports they are using.

2. **How can netstat help you diagnose network problems?**

Answer: It can give you network statistics and the status of each NIC.

3. **How would the routing table (`netstat -r`) be useful?**

   Answer: It would tell you how packets are going to be routed depending on the destination IP address. It would also tell you which IP address is assigned to a given NIC.

4. **Why would someone need different statistics for IP, IPv6, ICMP, TCP, UDP, etc.?**

   Answer: Each protocol can be used for a different purpose. A network administrator might want to know what types of traffic are flowing over his/her network. Knowing the types and quantities of each protocol may help solve a variety of network issues including faulty equipment, rogue machines, unapproved servers, compromised servers, etc.

1.6 NSLOOKUP

1. **Why are there multiple IP addresses associated with a single domain name (e.g., www.CNN.com and www.Google.com)?**

   Answer: This is done as a first step in load balancing requests sent to Google in order to increase availability and response time. Further load balancing is done at one of the Google clusters associated with that IP address.

2. **Why did Nslookup query fiber1.utah.edu instead of querying www.CNN.com directly?**

   Answer: Nslookup is designed to query the DNS server listed on the local host, not the remote Web server. It would need to query the DNS server to resolve the domain name (www.CNN.com) before it could even contact the CNN server.

3. **Why does www.Google.com use an alias?**

   Answer: Google likely has multiple name servers and/or multiple Web servers to handle the massive amount of requests. This would speed up overall response times and reduce congestion.

4. **How do domain names and IP addresses get registered?**

   Answer: ICANN manages the official assignment of domain names to IP addresses. You can get your domain name registered through a variety of companies (like www.GoDaddy.com) that will handle the registration process for you.

1.7 ARP

1. **Why do we need both MAC and IP addresses? Aren't IP addresses enough?**

   Answer: MAC addresses are necessary because any given host (e.g., your laptop) can receive multiple IP addresses throughout the day. A MAC address identifies a specific host on a single network, while an IP address is used to send/receive messages across multiple networks (i.e., the Internet).

2. **Where/when is your MAC address assigned?**

   Answer: It is assigned at the factory when the NIC is produced.

3. **Can you change your MAC address? How?**

   Answer: Yes, there is software that can temporarily change your MAC address. However, you can't change the address written into the hardware.

4. **What notation are MAC addresses written in?**

   Answer: MAC addresses use hexadecimal notation.

1.8 NET

1. **Could a network administrator reset an existing user's password using the `net user` command? How?**

   Answer: Yes, you would use a similar command shown in this example but with the "password" option.

2. **Why would a network administrator want to set up a network share?**

   Answer: Network shares are widely used to share files among users on the local network.

3. **What do the `net start` and `net stop` commands do?**

   Answer: The start/stop options can start/stop services. For example, you can use the net stop command to stop a printer service and then use net start to restart the printer service.

4. **When would a network administrator want to use the `net view` command?**

   Answer: The net view command would display a list of all domains, computers, and resources that are being shared by your computer (or a computer you specify).

1.9 FTP

1. **What would have happened if you had run the `mget *` command in interactive mode (i.e., without entering "prompt" first)?**

   Answer: It would not have transferred the files.

2. **Is transferring files with FTP faster than using HTTP?**

   Answer: No, you won't notice any practical differences with daily usage. There might be slight differences for one small file (i.e., FTP being faster) compared to multiple large files (i.e., HTTP being faster).

3. **What effect did the `binary` command have on the file transfer? Was it necessary?**

   Answer: The binary mode (or image mode) causes the sender to transfer all of the characters. Some FTP clients use ASCII mode in certain situations and would only transfer printable characters. This could render images, compressed files, and/or applications unreadable. It is recommended that binary mode be used for all transfers.

4. **Why did you use the `lcd` command?**

   Answer: The lcd command sets the local working directory for the FTP client.

1.10 CREATE A BATCH FILE

1. **What tasks do you think network administrators automate the most? Why?**

   Answer: It depends on their daily tasks. Backups, updates, disk management, reporting, and auditing are all common tasks.

2. **Could batch files be dangerous? How/Why?**

   Answer: A malicious custom batch file could cause a large amount of damage. It could be written to behave in the same manner as many of the more common viruses. It could automatically delete files, change system configurations, send/receive data, create unauthorized user accounts, and install unauthorized software.

3. **What does "REM" in the batch file stand for and what does it do?**

   Answer: It stands for remark and allows programmers to include comments about the code that won't be processed.

4. **Could you rename this shortcut and change the icon to use the same icon as one of your other shortcuts (i.e., make it look exactly like one of the other shortcuts)? How could you have fun with this?**

   Answer: Yes, you can rename the shortcut anything you want (including the names of icons already on your desktop) and change the icon to any one of your choosing. You can make it look exactly like any icon on your desktop. It could also have an alternative effect of your choosing. For example, instead of opening a Web browser, the shortcut could open the game Solitaire.

1.11 WINDOWS POWERSHELL

1. **Could you use the Invoke-Command to start a process on a remote computer?**

   Answer: Yes, the Invoke-Command can start/stop a process on a remote computer. This is useful for a network administrator who manages a large number of machines.

2. **What would you use the Measure-Object cmdlet for?**

   Answer: The Measure-Object cmdlet will give you basic statistics (e.g., count, average, sum, minimum, and maximum) for any object.

3. **Which cmdlet would you use to stop a service?**

   Answer: You would use the Stop-Service cmdlet.

4. **Pwd is an alias for which cmdlet?**

   Answer: Pwd stands for print working directory. It is an alias for Get-Location.

CHAPTER 2: WINDOWS UTILITIES

2.1 WINDOWS TASK MANAGER

1. **Can you send messages to other people on the same computer through Windows Task Manager?**

   Answer: Yes, you can use the Users tab to send messages to other people on the same computer. You select the other user and click the Send Message button.

2. **What key sequence allows you to switch users?**

   Answer: You can hold down the Windows key and press L. Then you click the Switch User button. You can also press Ctrl-Alt-Delete and then click Switch User.

3. **Why are there so few applications running yet so many processes running?**

   Answer: There are many processes running in the background that are started by default and may not be associated with an application you are currently running. Some of these are listening for certain events, while others are system processes that need to be running as part of your operating system.

4. **What happens if you press Ctrl-Alt-Del twice?**

   Answer: In prior versions of Windows (Windows 98 and earlier), it would perform a soft boot. From Windows 2000 through Windows 7, this will open the Windows Task Manager or Welcome Screen if you are not connected to a domain (done by pressing Ctrl-Alt-Del once). Pressing this key sequence twice will NOT soft boot current versions of the Windows OS.

2.2 WINDOWS REMOTE DESKTOP

1. **Can you remote into more than one computer at a time?**

   Answer: Yes, you can remote into many machines at the same time. A single network administrator can manage several dozen servers from a single console.

2. **Can you remote through a chain of multiple computers?**

   Answer: Yes, you can remote into and out of many computers.

3. **Can you copy files from a remote desktop and paste them to the local desktop?**

   Answer: Yes, you can enable file sharing between remote desktop connections. You can access remote printers, files, etc.

4. **What is the DOS command to start Remote Desktop? (Hint: Terminal Services)**

   Answer: MSTSC (Microsoft Terminal Server Client)

2.3 MSINFO32

1. **Can MSINFO32 tell you the model number of your network card?**

   Answer: Yes, it can give you the model number.

2. **Why would you want to know IRQs?**

   Answer: IRQs provide you with information about hardware components that are able to send requests directly to the CPU.

3. **Can you tell if your hard disks are formatted with FAT32 or NTFS? Does it matter?**

   Answer: Yes, MSINFO32 will tell you which type of formatting was used on your disks. This is important for many reasons. For example, FAT32 cannot handle single files larger than about 4 GB. If you are creating a single backup file from a typical computer, it will probably be larger than 4 GB and cannot be stored on a FAT 32 partition. It will need to be stored on a NTFS partition.

4. **What are environmental variables and why are they important?**

   Answer: Environmental variables are values related to the computer you are working on and will affect how your computer operates. For example, you will see values for the number of processors and the processor architecture. The value for your processor architecture will determine if your computer will need 32-bit software or 64-bit software.

2.4 BGINFO

1. **What DOS commands would you have to enter to get the information shown by BgInfo?**

   Answer: You can type MSINFO32 and IPCONFIG to get the system information and IP configuration information at the DOS prompt.

2. **Why would an administrator need to know the IP and MAC addresses for a given computer?**

Answer: Larger networks are managed virtually and filter out all packets from computers that are not registered by MAC addresses. A network administrator must know the MAC address for each machine in order to correctly administer the network and keep outside machines off internal systems. Knowing which MAC address has a given IP address can help manage a network. An administrator will know which machines are sending/receiving what information. Knowing both MAC and IP addresses are critical parts of diagnosing network problems.

3. **Why does this computer have three IP addresses and three MAC addresses?**

   Answer: It has one physical NIC with a factory-assigned MAC and two virtual NICs used by virtual computers. Each NIC was assigned an IP address.

4. **Can you change your MAC address?**

   Answer: Yes, you can get software that will change your MAC address. If you change your MAC address, and it accidentally matches another MAC address on your network, you will have connectivity problems.

2.5 PERFMON

1. **Can Performance Monitor look at past log files? How?**

   Answer: Yes, you can save the data you are collecting and open past log files by clicking on the Performance Monitor Properties button.

2. **Could you create a custom log to measure specific counters during a given period of time?**

   Answer: Yes, you can create a custom data collector to measure a variety of variables for any time period you specify.

3. **Why would a network administrator be interested in Pages/sec on a host?**

   Answer: The number of pages/sec on a host could indicate a low amount of memory.

4. **Can you set Performance Monitor to alert you if one of the counters passes a certain threshold?**

   Answer: Yes, you can create a new data collector set manually and select the Performance Counter Alert option. You can then select the counter(s) you want to monitor and specify the limit.

2.6 WINDOWS EVENT VIEWER

1. **Will these security logs track failed logon attempts? From remote machines?**

   Answer: Yes, they will track all failed logon attempts, even from remote machines.

2. **Will it track security events other than just logon/logoff events?**

   Answer: Yes, it tracks a variety of security events as defined by Microsoft.

3. **Can you use Event Viewer to view other logs?**

   Answer: Yes, Event Viewer is a "generic" program that will allow you to view a variety of different logs.

4. **Why is there a log that tracks which Microsoft office programs you use and how long you use them?**

   Answer: There is a log that will track when you use a MS Office product and how long you use it for. This log could be used to monitor user activities, or to identify unauthorized usage.

2.7 PROCESS EXPLORER

1. **Why are all of these processes started?**

   Answer: Some of them are system processes managing OS activities. Others are processes that start because you installed software that allowed them to start.

2. **Can you keep these processes from starting? How?**

   Answer: Yes, you can stop processes from starting through Start, Control Panel, Administrative Tools, Services, and then changing the settings for the process listed. You can also stop processes from starting by running the MSCONFIG command.

3. **Are there any processes you recognize or don't recognize?**

   Answer: Yes, it's likely that you may not recognize all of the processes listed.

4. **What do DLLs do and why are they associated with a specific process?**

   Answer: Dynamic-link libraries (DLLs) can contain code, data, or resources that may be shared by other programs. A given process may need specific components from a DLL to run.

2.8 PROCESS MONITOR

1. **Why do programs make so many read/writes to the hard drive?**

   Answer: There are a lot more background operations happening than most users are aware of. For example, Microsoft Word has a spell checking function running as you type. It also automatically saves your document at regular intervals. Each application will perform a variety of read/writes depending on their functionality.

2. **Can you stop programs from running or starting up?**

   Answer: Yes, you can stop programs from running. In the Control Panel, click on Administrative Tools, then Services, and then select the process you want to stop running. Double-click the service and then select the start up type as Disabled.

3. **Why are there so many entries for the registry? What is the registry?**

Answer: The Windows registry is basically a big database that stores settings and options for the operating system. Programs or hardware that need to access the registry will cause log entries for the registry.

4. **What is the difference between a process and a thread?**

   Answer: A thread can contain multiple processes. Processes mostly run independently, but threads are typically a subset of a single process. For example, you can press on the gas pedal and change the radio station at the same time. Both your hand and foot are completing different tasks but are part of the same body.

2.9 TEXT EDITOR (NOTEPAD)

1. **Why did the three different files (.txt, .rtf, and .doc) all look different when opened in Notepad?**

   Answer: The .rtf and .doc file types include additional formatting and meta information that the user will not see unless he or she opens the file with a text editor.

2. **Could a configuration file be affected if it were saved with a .doc extension?**

   Answer: Yes, the additional formatting added in by the .doc extension would make the configuration file inoperable.

3. **Can you open any file (including images) with Notepad?**

   Answer: Yes, you can open any type of file with a simple text editor. However, the contents may be unreadable.

4. **Why do so many programs still have help files and configuration files written with the .txt extension?**

   Answer: Help files and configuration files are written as text files because they can be read by anyone regardless of operating system or office suite. They also don't have any additional formatting that might interfere with the reading of the configuration file.

2.10 BACKUP & RECOVERY

1. **Can you start/stop tasks from the DOS prompt? How?**

   Answer: You can use the SCHTASKS command to start or stop a task.

2. **What utility would you use to restore a prior backup?**

   Answer: In Windows 7, you use the Backup and Restore utility. In Windows XP, you use the NTBackup utility.

3. **Could you back up your computer to an external hard drive attached to another computer?**

   Answer: Yes, you can back up all your files to an external hard drive or another internal hard drive.

4. **Could you automate the backup of an entire network to an off-site location?**

   Answer: Yes, many companies do weekly or daily backups of their critical systems to off-site locations. Most reputable data centers will offer these services. You can get hot, cold, and even warm sites through larger data centers.

2.11 HARDWARE DRIVER UPDATES

1. **Is it possible to get your hardware working with a generic driver?**

   Answer: Yes, in many cases a generic driver will work if you cannot find your specific driver. You may not get 100% functionality, but it will work until you can update with the correct driver.

2. **Do hardware manufacturers have to write different drivers for different operating systems? Why?**

   Answer: Yes, drivers are operating system specific in most cases.

3. **Why wouldn't your operating system come with all drivers for all hardware by default?**

   Answer: If it is a newer piece of hardware, it's likely that your operating system does not have that driver listed.

4. **Could a piece of hardware automatically install its own driver?**

   Answer: Yes, some pieces of hardware come with their own drivers onboard and can self-install. Windows 7 is much better at automatically installing and configuring software drivers than was Windows XP.

2.12 MSCONFIG

1. **Why do all of those processes have to be running at startup?**

   Answer: Some of the processes that are started by default do not have to be started. Software you install can designate a process to begin at startup. You can manually stop these services from starting and they can be started manually later.

2. **If you uninstalled some of those programs, would your computer seem to run faster? Why?**

   Answer: Yes, if you uninstall software that starts a service every time you boot, it could make your computer run faster because you would have more available memory. The amount of memory and processing time you could make available depends on the application you uninstall.

3. **What programs do you start each time you log in? Could you automate this process?**

Answer: This depends on the user. Most users check their email and use an Internet browser. You could have both an email client (e.g., Outlook) and a Web browser (e.g., Chrome) start every time you log in.

4. **What does the .INI extension mean?**

   Answer: The .INI extension is the standard file type for many configuration files.

2.13 IEXPRESS

1. **Can you add more than just .exe files to the list of installation files?**

   Answer: Yes, you can add any file type to the list of installation files. They will be written to the directory you specify.

2. **Why do some installations require you to reboot your computer?**

   Answer: They set variables and/or make changes to your registry. To take full effect, you need to reboot your computer.

3. **Give an example of when a network administrator might use this tool.**

   Answer: A network administrator might use this tool if he/she needs to install an antivirus or spyware client on several machines. There are many logical uses for this tool.

4. **In addition to the .exe file, another file was created. What is in this second file?**

   Answer: The second file is a Self-Extraction Directive (.sed) that stores information about the package you just created.