

SOLUTIONS MANUAL



APPLIED NETWORKING LABS

Randall Boyle

APPLIED NETWORKING LABS:

A HANDS-ON GUIDE TO NETWORKING
AND SERVER MANAGEMENT

Solutions

Dr. Randall Boyle

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`, `-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 will tell you how packets are going to be routed depending on the destination IP address. It will 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 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 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 (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, with daily usage you won't notice any practical differences. There might be slight differences for one small file (FTP being faster) compared to multiple large files (HTTP being faster).

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

Answer: The binary mode (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 is 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. However, it could 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 that 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 (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.