



DES352: Networking Laboratory

Midterm Mock Exam

curated by The Peanuts

Name ID Section Seat No

Conditions: Semi-closed Book

Directions:

1. This exam contains 17 pages (including this one). If yours has fewer, you've experienced packet loss. Please send an ARP request to your TA.
2. Write your name clearly at the top.
3. Show your work. Partial credit is real, this isn't binary classification.
4. Answers must be written in English. Binary, hexadecimal, or IPv6 notation will not be graded (though we appreciate your commitment to the cause).
5. You may use one A4 paper (both sides, print ok) as cheat sheet.

*For solution, **click here**.*

Part I: Multiple Choice Questions (25 points)

Choose the best answer for each question. Each question is worth 1 point.

1. You are in directory `/home/student/Documents` and want to go to `/home/student/Pictures`. Which command would NOT work?

- a) `cd ../Pictures`
- b) `cd /home/student/Pictures`
- c) `cd ~/Pictures`
- d) `cd Pictures`

2. What will happen if you run `ls -l /etc > output.txt` twice in a row?

- a) The file will contain the output twice (appended)
- b) The file will contain only the second output (overwritten)
- c) An error will occur
- d) The file will be empty

3. Which command will count the number of lines in a file named `data.txt`?

- a) `wc data.txt`
- b) `wc -l data.txt`
- c) `cat data.txt | wc -l`
- d) Both b and c

4. In a shell script, what is the value of \$0?

- a) The first argument passed to the script
- b) The name of the script itself
- c) The exit status of the last command
- d) The number of arguments

5. You ping a host with `ping -c 5 -s 1000 192.168.1.1`. How many bytes will each ICMP echo reply show in the output?

- a) 1000 bytes
- b) 1008 bytes
- c) 1028 bytes
- d) 1020 bytes

6. After running a command that produces both output and errors, you want to save ONLY the errors to a file. Which command does this?

- a) `command > errors.txt`
- b) `command 2> errors.txt`
- c) `command >> errors.txt`
- d) `command | errors.txt`

7. What happens when you run `uniq file.txt` without sorting first?

- a) It removes all duplicate lines from the file
- b) It removes only adjacent duplicate lines
- c) It returns an error
- d) It sorts the file first automatically

8. You have a running process in the foreground. You press CTRL-Z. What is the state of the process?

- a) Terminated
- b) Running in background
- c) Stopped (paused)
- d) Running in foreground

9. When you ping 8.8.8.8 from your computer at 192.168.1.100, what MAC address will be in the destination field of the Ethernet frame?

- a) MAC address of 8.8.8.8
- b) MAC address of your default gateway
- c) MAC address of your computer
- d) Broadcast MAC address (ff:ff:ff:ff:ff:ff)

10. You run `ifconfig eth0 down` and then immediately run `ping 192.168.1.1`. What happens?

- a) Ping works normally
- b) Ping fails with “Network is unreachable”
- c) Ping works but slower
- d) The interface automatically comes back up

11. In Wireshark, which filter shows packets where either the source or destination is 192.168.1.10?

- a) `ip.src == 192.168.1.10 && ip.dst == 192.168.1.10`
- b) `ip.addr == 192.168.1.10`
- c) `ip == 192.168.1.10`
- d) `ip.src == 192.168.1.10 || ip.dst == 192.168.1.10`

12. You capture packets with `tcpdump -i eth0 -c 100 tcp`. How many packets will be captured if only 80 TCP packets pass through but 200 UDP packets also pass through?

- a) 80 packets
- b) 100 packets
- c) 200 packets
- d) 280 packets

13. Your ARP cache already has an entry for 192.168.1.50. You ping this IP. Which statement is TRUE?

- a) An ARP broadcast will be sent first
- b) An ARP unicast will be sent first
- c) No ARP packets will be sent
- d) The ARP entry will be deleted first

14. What is the total size of a ping packet when you run `ping -s 50 npwitk.com`?

- a) 50 bytes
- b) 58 bytes (50 + 8 ICMP header)
- c) 78 bytes (50 + 8 ICMP + 20 IP header)
- d) 92 bytes (50 + 8 ICMP + 20 IP + 14 Ethernet header)

15. In a shell script, which comparison should you use: `if [$count -gt 10]` or `if [$count > 10]`?

- a) Both are correct and equivalent
- b) First one (using `-gt`) for numeric comparison
- c) Second one (using `>`) for numeric comparison
- d) Neither is correct

16. You see TTL=117 in a ping response. The original TTL was likely 128. How many routers (hops) did the packet pass through?

- a) 11 hops
- b) 117 hops
- c) 128 hops
- d) Cannot determine

17. Which Wireshark filter will show TCP packets that are NOT going to port 80?

- a) `tcp && port != 80`
- b) `tcp && !tcp.port == 80`
- c) `tcp.port != 80`
- d) Both b and c

18. What does mtr do that ping and traceroute don't?

- a) Shows real-time continuous statistics
- b) Uses ICMP packets
- c) Shows packet loss percentage
- d) Both a and c

19. You run `tcpdump -i eth0 -w capture.dump icmp`. What gets saved to the file?

- a) Human-readable text of ICMP packets
- b) Binary data of ICMP packets only
- c) Binary data of all packets
- d) Nothing (wrong syntax)

20. In a routing table, you see two routes: `192.168.1.0/24` and `192.168.1.128/25`. You ping `192.168.1.150`. Which route is used?

- a) `192.168.1.0/24` (broader range)
- b) `192.168.1.128/25` (more specific)
- c) Default route
- d) Either one randomly

21. What is the difference between `jobs` and `ps aux`?

- a) `jobs` shows only current shell's jobs, `ps aux` shows all processes
- b) They are identical
- c) `jobs` shows all processes, `ps aux` shows current shell only
- d) `jobs` requires `sudo`, `ps aux` doesn't

22. You want to append text to a file but redirect errors to /dev/null. Which is correct?

- a) `command >> file 2> /dev/null`
- b) `command > file 2>> /dev/null`
- c) `command 2> /dev/null >> file`
- d) Both a and c

23. When does `nslookup` return a “Non-authoritative answer”?

- a) When the DNS server is not the official source
- b) When the query fails
- c) When using cached DNS data
- d) Both a and c

24. You execute `ping -c 3 -i 2 192.168.1.1`. How long will it take minimum (assuming instant replies)?

- a) 3 seconds
- b) 4 seconds (2 intervals between 3 packets)
- c) 6 seconds
- d) 2 seconds

25. In `tcpdump` output, what does “length 64” refer to?

- a) Total packet size including all headers
- b) Only the data payload size
- c) Frame size on the wire
- d) IP packet size excluding Ethernet header

Part II: Short Answer Questions (15 points)

Provide concise answers for each question. Write commands exactly as you would type them in the terminal.

1. (1.5 points) Write a SINGLE command that creates a directory called `backup` and immediately navigates into it.

2. (1.5 points) Write a command to find all files in your current directory that contain the word “error” (case-insensitive) and save the matching lines to `errors.log`.

3. (2 points) Write a command to list all processes owned by user “student” and display only the PID and command name columns.

4. (1 point) Write a command to bring job number 2 from background to foreground.

5. (2 points) Write a command to configure interface `eth1` with IP address `10.0.0.5` and netmask `255.255.255.0` in a single command.

6. (1.5 points) Write a ping command that sends exactly 20 packets with 512 bytes of data, waiting 0.5 seconds between each packet, to IP 8.8.8.8.

7. (1.5 points) Write a command to delete a specific MAC address entry from the ARP cache. The IP address is 192.168.1.100.

8. (2 points) Write a tcpdump command to capture packets on interface eno1, filter for port 443 (HTTPS), capture exactly 50 packets, and save to https_traffic.pcap.

9. (1 point) Write a Wireshark display filter that shows only ARP reply packets (not requests).

10. (1 point) Write a Wireshark filter to show packets where the source is 192.168.1.0/24 subnet AND destination port is 80.

11. (1.5 points) Write a command to trace the route to **www.npwitk.com** using ICMP packets instead of UDP (requires sudo).

Part III: Problem-Solving and Explanation Questions (10 points)

Show all work and explain your reasoning clearly.

Problem 1 (3 points)

You run the command `cat file1.txt file2.txt > file1.txt`. Explain what happens and why this is a problem. What is the correct approach if you want to combine both files and save the result in `file1.txt`?

Problem 2 (2 points)

A student writes this shell script:

```
1 #!/bin/bash
2 count = 5
3 if [ $count -gt 3 ]
4 then
5     echo "Count is greater than 3"
6 fi
```

The script produces errors. Identify ALL the errors and provide the corrected version.

Problem 3 (3 points)

You capture network traffic between two computers and see the following sequence:

1. ARP Request: Who has 192.168.1.50?
2. ARP Reply: 192.168.1.50 is at aa:bb:cc:dd:ee:ff
3. ICMP Echo Request to 192.168.1.50
4. ICMP Echo Reply from 192.168.1.50
5. ARP Request: Who has 192.168.1.50?
6. ARP Reply: 192.168.1.50 is at aa:bb:cc:dd:ee:ff

Why would the second ARP request (step 5) happen even though the MAC address was already learned in step 2? Provide at least TWO possible reasons.

Problem 4 (2 points)

Given this routing table on a computer with IP 10.0.5.100:

Destination	Gateway	Genmask	Flags	Iface
0.0.0.0	10.0.5.1	0.0.0.0	UG	eth0
10.0.5.0	0.0.0.0	255.255.255.0	U	eth0
172.16.0.0	10.0.5.50	255.255.0.0	UG	eth0

(a) Where will a packet destined for 172.16.20.100 be sent first, and why?

(b) What is unusual about this routing table configuration? Explain.

Problem 5 (Bonus: 3 points)

You're troubleshooting network connectivity. You can successfully ping your default gateway (192.168.1.1), but you cannot ping 8.8.8.8 (Google DNS). However, when you run `tracert 8.8.8.8`, you see:

```
1  192.168.1.1    1.234 ms    1.190 ms    1.156 ms
2  * * *
3  * * *
4  * * *
```

- (a) Why can you ping the gateway but not 8.8.8.8?

- (b) Why does `tracert` show the gateway (hop 1) but then asterisks for all subsequent hops?

- (c) What are TWO different approaches to get more information about the path to 8.8.8.8?

Problem 6 (Bonus: 2 points)

In Wireshark, you apply the filter `tcp.port == 80`. You expect to see only HTTP traffic, but you also see many packets with destination port 443 (HTTPS). Explain why this happens and write the correct filter that shows ONLY traffic where port 80 is involved.