Anonymous ID

Answer sheet 1 of 2 for the NETMET 2020-2021 final exam

Multiple choice questions

M1	M4	M7
M2	M5	M8
M3	M6	M9

Short answer questions

S1

S2

S3

Anonymous ID

Answer sheet 2 of 2 for the NETMET 2020-2021 final exam

Multiple choice questions

M10	M13	M16
M11	M14	M17
M12	M15	M18

Short answer questions

S4

S5

S6

NETMET 2020-2021
Final exam – 16 February 2021
Duration: 1 ½ hours

Allowed: English dictionary or bilingual dictionary (printed books only, with no written notes)

Not allowed: Documents, computers, pocket calculators, mobile phones, etc.

Answer sheet and anonymous ID

The first sheet of paper in this exam is your answer sheet. It bears an anonymous ID number. This number, recorded on the attendance sheet for the exam, provides the connection between your answer sheet and your identity.

Please do not write your name on the answer sheet.

You will submit only the answer sheet at the end of the exam.

Multiple-choice questions numbered M1, M2, … (1 point each)

The multiple-choice questions each have four possible answers: A, B, C, and D.

A fifth choice X indicates "no answer". Mark your answers by writing A, B, C, D, or X in the box alongside the question number.

For each multiple-choice question, there is only one correct answer.

- Correct answer = 1 point
- Incorrect answer = ½ a point subtracted
- No answer = 0 (no points gained, none lost either)

Because of the penalty for an incorrect answer, it is not in your interest to make a random guess.

If there is ambiguity, and we cannot tell which answer you have provided, we will need to mark the answer as incorrect.

Short answer questions numbered S1, S2, … (1 point each)

Please use the space provided in which to write your answers to the short answer questions.

Additional remarks

Do not hesitate to raise your hand with any questions you might have. Best wishes for a successful exam!

Multiple choice questions for Answer Sheet 1

M1. Network operators often need to identify the application that generates the traffic traversing their networks. Port-based identification is simple and fast. Which statement best describes why port-based identification is not sufficient for identifying applications today?

A. IP-level encryption (e.g., IPSec) blocks port-based identification.
B. Many applications use non-standard ports.
C. Applications may hide by using another's application port number.
D. All of the above.

M2. Which of the following statements is false?

A. The network telescope can only detect denial of service attacks that use randomly spoofed source addresses.
B. The network telescope can detect worms because it receives a large fraction of the probes to infect hosts.
C. The network telescope can detect malicious port scans.
D. None of the above.

M3. Select the false statement.

A. Network anomaly detection is ideal to watch for high volume attacks.
B. Network intrusion detection is the only method to detect denial of service attacks.
C. The network telescope can detect the scanning of worms.
D. Network intrusion detection systems can look for malicious commands in traffic.

M4. Say that the result of a round-trip time measurement between X and Y is RTT(X,Y) and that delay(X,Y) is a function that returns the speed of light delay between locations X and Y. Which of the potential tests below are useful to identify measurement errors?

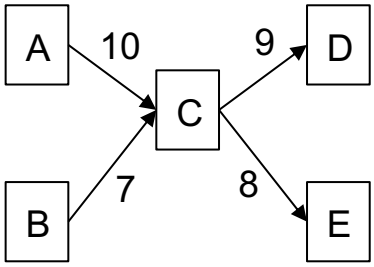
i. RTT(X,Y) < 1 second
ii. RTT(X,Y) > delay(X,Y)
iii. RTT(X,Y) < 0

A. All tests are useful to identify measurement errors.
B. Only test iii is useful to identify measurement errors.
C. Tests ii, iii are useful to identify measurement errors.
D. None of these tests will help identify measurement errors.

M5. Select the true statement about measuring network traffic with interface counts.

A. One advantage of measuring traffic with interface counts is that it eliminates the risk of missing data.
B. One disadvantage of interface counts is that it is not universally supported.
C. One advantage of interface counts is that it has little performance impact on routers and it requires little storage needs.
D. None of the above

M6. In the topology below, nodes represent routers in a small network and links are annotated with the byte count in MB during a 5-minute interval (note that links are directed according to traffic flow). Select the true statement about the traffic matrix of this network.



A. There is only one possible traffic matrix for this network and it is represented in the following table:

	D	**E**
A	4	6
B	5	2

B. We cannot infer the traffic matrix from these measurements. If we use SNMP to collect byte counters from router A, then we will be able to find the traffic matrix.
C. We cannot infer the traffic matrix from these measurements. If we use Netflow to collect flow statistics from router A, then we will be able to find the traffic matrix.
D. None of the above.

M7. Select the true statement about anonymization of packet traces.

A. A two-way hash function (using the same seed) is a good approach to anonymize identifiers if people may want to get back to the individuals in the dataset.
B. One-way hashing of identifiers will prevent attackers from identifying individuals in the dataset.
C. One-way hashing is an example of a semi-lossy transformation.
D. All of the above.

M8. The following table represents an anonymized dataset. Select the true statement.

Zipcode	Age	Disease
476**	2*	Heart Disease
476**	2*	Heart Disease
478**	2*	Flu
478**	2*	Flu
4790*	≥40	Heart Disease
4790*	≥40	Flu

A. This dataset is 3-anonymous.
B. This dataset is 2-diverse.
C. If we know the quasi-identifier of one of the patients in this dataset, we cannot know their disease.
D. None of the above.

M9. Refer to the example iperf output below to select the true statement.

```
$ iperf3 -u -t 10 -b 100Mbit --get-server-output -c 192.168.1.174
Connecting to host 192.168.1.174, port 5201
[  4] local 192.168.1.231 port 51069 connected to 192.168.1.174 port 5201
[ ID] Interval           Transfer     Bandwidth       Total Datagrams
[  4]   0.00-1.00   sec  10.8 MBytes  90.2 Mbits/sec  1379
[  4]   9.00-10.00  sec  12.0 MBytes   100 Mbits/sec  1532
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth       Jitter    Lost/Total Datagrams
[  4]   0.00-10.00  sec   118 MBytes  99.0 Mbits/sec  0.839 ms  2034/15114 (13%)
[  4] Sent 15114 datagrams
Server output:
Accepted connection from 192.168.1.231, port 58542
[  5] local 192.168.1.174 port 5201 connected to 192.168.1.231 port 51069
[  5]   0.00-1.00   sec  7.05 MBytes  59.2 Mbits/sec  1.190 ms  226/1129 (20%)
[  5]   9.00-10.00  sec  11.4 MBytes  95.9 Mbits/sec  2.670 ms  74/1537 (4.8%)
```

A. During the first second of the test, the server received 90.2 Mbps.
B. The host 192.168.1.174 is running an iPerf client.
C. This call is performing a UDP test
D. None of the above statements are true.

Short answer questions for Answer Sheet 1

S1. Define what l-diversity is. Identify 1 limitation of l-diversity, and mention how t-closeness overcomes this limitation. Does t-closeness guarantee privacy?

S2. Define the difference between Temporal and Spatial Anomaly Detection. Given an example of an anomaly that requires both temporal and spatial correlation to identify the cause of the anomaly.

S3. Why is it challenging to measure packet capture using interface counts? In the event of an under-constrained problem, describe two ways to add more constraints.

Multiple choice questions for Answer Sheet 2

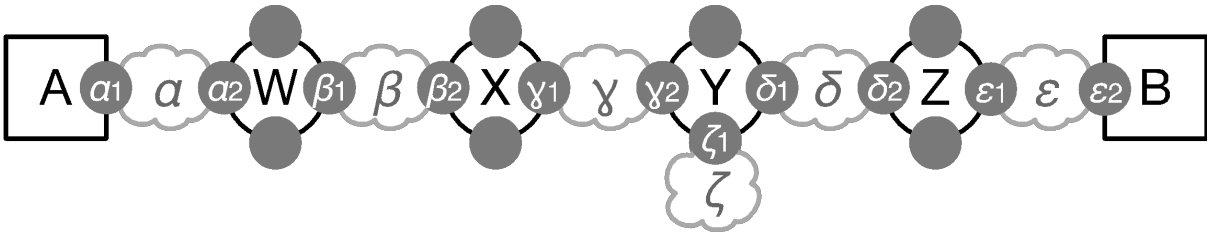
M10. What is an example of direct probing?
A. Ping with the Timestamp option
B. Ping without the Timestamp option
C. Traceroute
D. None of the above

M11. Which is an example of indirect probing?
A. Ping with the Timestamp option
B. Ping without the Timestamp option
C. Traceroute
D. None of the above

M12. Which is an example of hybrid direct and indirect probing?
A. Ping with the Timestamp option
B. Ping without the Timestamp option
C. Traceroute
D. None of the above

M13. In latency measurements, what is the order of magnitude of propagation delays for packets travelling across a country the size of France?
A. Nanoseconds
B. Microseconds
C. Milliseconds
D. Seconds

M14. Suppose a traceroute from A to B in the topology below elicits responses from interfaces α_2, β_2, ζ_1, δ_2, and ε_2.



Which network does the traceroute fail to reveal anything about?
A) β
B) γ
C) ζ
D) δ

M15. At which layers of the network stack are queueing delays encountered?
A. application
B. TCP/UDP
C. IP
D. MAC & PHY

M16. Using the GeoPing geolocation method, when geolocating a target X from vantage points A and B, using landmarks Y and Z, X is:

A. On a line between Y and Z
B. At either Y or Z
C. In the intersection of disks centered at Y and at Z
D. At a branching point between traceroutes A-X, A-Y, ad A-Z, or B-X, B-Y, and B-Z

M17. Using the Street-Level geolocation method, when locating a target X using vantage point A and landmark B, X is:

A. On a line between A and B
B. At either A or B
C. In the intersection of disks centered at A and at B
D. At the branching point between traceroutes A-X and A-B

M18. What type of packet is used for classic pings?

A. DNS
B. BGP
C. TCP
D. ICMP

Short answer questions for Answer Sheet 2

S4. Describe, with a diagram and a short description, the Shortest Ping method for geolocation, mentioning the circumstances under which it works best.

S5. Name three ways of calculating distances between points on the surface of the earth, and describe when you might want to use each one for the purposes of geolocation.

S6. How can we measure one-way delays?