דוח משוב לסטודנט

מזהה סטודנט	879332104277208938148519646446330857 13
תאריך בחינה	יום שבת, 24 במאי 2025
מזהה קורס	תקשורת באינטרנט (02360341/202402)
שם קורס	HW2
מרצה	tavran

ניקוד שאלות פתוחות	ציון מבחן מקורי	ציון מבחן סופי
98.00	98.00	**98.00**

סיכום

מספר שאלה	תיאור	ניקוד	ניקוד מירבי	שאלת בונוס
1	שאלה 1	20.00	20.00	0
2	שאלה 2	14.00	14.00	0
3	שאלה 3	62.00	66.00	0
4	שאלה 3 בונוס	2.00	5.00	1

תרגיל בית 2

20
(1)

האחראי על התרגיל: ערן, דוא"ל tavran@cs.technion.ac.il

תאריך הגשה:24.05.2025 ב-18:00

שאלה מס' 1 –

עיינו ב-RFC-2328 וענו על השאלות הבאות:

1. מבנה הנתונים של OSPF מייצג גרף מכוון. מהם צמתי הגרף ומה הן קשתות הגרף?

צמתי הגרף (Vertices):

- כל נתב (Router) הוא צומת.
- כל רשת היא גם צומת.

קשתות הגרף (Edges):

- קשת נמתחת בין שני נתבים אם הם מחוברים ישירות דרך רשת point-to-point.
- קשת בין נתב לרשת מצביעה על כך שלנתב יש ממשק ברשת הזו.

2. הסבירו מהו Stub network והסבירו מדוע בטבלה של מבנה הנתונים הקשר בין Stub network לנתב הוא חד כיווני.

Stub network היא רשת שמחוברת רק לנתב אחד, ואין דרכה תעבורת נתונים לנתבים אחרים. כלומר, כל התעבורה שנשלחת לרשת זו היא סופית, ולא נמשכת מעבר לה.

בגרף שמייצג את מבנה הנתונים של OSPF:

- Stub network מיוצגת כצומת (vertex) שיש לו רק קשתות נכנסות (incoming edges).
- כלומר, אפשר לשלוח מידע מהנתב לרשת, אך לא דרכה הלאה ולכן אין קשתות יוצאות מהרשת לצמתים אחרים. זה גם מסביר מדוע הקשר מהנתב לרשת מוצג כקשת חד-כיוונית בלבד.

3. הסבירו מה ההבדל בין Broadcast networks לבין NBMA networks ומדוע עבור רשתות מסוגים אלו **עם יותר מנתב אחד** במבנה הנתונים הקשר עם הנתבים הוא דו כיווני.

Broadcast networks מאפשרות שידור לכל המכשירים, ו־NBMA networks מאפשרות גישה מרובה ללא שידור. בשני הסוגים, כאשר יש יותר מנתב אחד, הרשת משמשת להעברת מידע בין הנתבים ולכן הקשר ביניהם לבין הרשת במבנה הנתונים של OSPF הוא דו-כיווני.

4. הסבירו מהו קשר point-to-point בין נתבים וכיצד הוא נשמר במבנה הנתונים.

קשר Point-to-Point בין נתבים הוא קישור ישיר בין שני נתבים בלבד, ללא רשת מתווכת שכוללת משתתפים נוספים.

איך זה נשמר במבנה הנתונים של OSPF:

במקרה של קשר Point-to-Point, נוצרות קשתות דו-כיווניות ישירות בין שני צמתים (הנתבים). כלומר, כל אחד מהנתבים מיוצג כצומת, ויש ביניהם קשתות לשני הכיוונים – מציין שהם יכולים לשלוח ולקבל זה מזה.

5. עיינו ב-section 3. הסבירו כיצד Autonomous systems גדולים מתמודדים עם התקורה הגדולה של מבנה הנתונים.

OSPF מתמודד עם התקורה על ידי חלוקת ה-Autonomous System לאזורים (Areas). כל אזור כולל קבוצה של רשתות ונתבים סמוכים, ומריץ עותק נפרד של אלגוריתם הניתוב מסוג Link-State.
לכל אזור יש מסד נתוני Link-State נפרד וגרף טופולוגי עצמאי, כך שניתן לנהל את המידע המקומי בתוך האזור בלבד, מבלי להחזיק את כל הטופולוגיה של ה-AS כולו.

כך מושגות שתי מטרות עיקריות:

1. צמצום כמות המידע שכל נתב צריך לעבד ולשמור.
2. בידוד טופולוגי – נתב בתוך אזור מסוים לא צריך לדעת את מבנה הרשת באזורים אחרים.

בנוסף, ניתוב מתבצע בשתי רמות:

- בתוך אזור – לפי מידע מקומי.
- בין אזורים – באמצעות נתבים מיוחדים המחברים בין אזורים (Area Border Routers).

כך OSPF תומך ב־scalability ומאפשר לנהל גם מערכות גדולות מבלי להעמיס את כל הנתבים במידע שאינו רלוונטי להם.

6. מהם 5 סוגי ההודעות הקיימים ב-OSPF? למה כל אחת מהן משמשת?

סוג	שם ההודעה	תפקיד/שימוש
1	**Hello**	גילוי ושמירה על קשר עם שכנים (neighbors). נשלחת תקופתית.
2	**Database Description**	סיכום תוכן מסד הנתונים – משמש להשוואה בין שכנים.
3	**Link State Request**	בקשת מידע חסר ממסד הנתונים (LSAs).
4	**Link State Update**	שליחת מידע מפורט (LSAs) – עדכון מסדי הנתונים.
5	**Link State Acknowledgment**	אישור קבלת עדכונים – מבטיח אמינות.

שאלה מס' 2 - 14) ICMP נק')

14
(2)

1. עיינו ב-RFC-792 והסבירו במקרים הבאים איזו חבילת ICMP (type+code) תשלח:

a. נתב קיבל חבילה שערך שדה ה-TTL שלה הוא 1 והוא לא היעד שלה.

ICMP packet	type	code	reason
Time Exceeded	11	0	The router decrements the TTL to 0, but it is not the destination of the packets so it sends back to the sender that the packet has exceeded the time to live.

b. נתב קיבל חבילה שגדולה יותר מה-MTU אבל דגל ה-DF של החבילה דלוק.

ICMP packet	type	code	reason
Destination Unreachable	3	4	The router cannot fragment the packet to fit the MTU because the DF flag is on, so it sends back “fragmentation needed and DF set”.

c. נתב קיבל חבילה אך החוצץ שלו לשליחת חבילות מלא.

ICMP packet	type	code	reason
Source Quench	4	0	The router sends that the buffer is full to the source because it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.

d. מחשב היעד קיבל חבילה שה-destination port שלה לא זמין.

ICMP packet	type	code	reason
Destination Unreachable	3	3	This type and code mean that the destination port is unreachable.

e. נתב מקבל חבילה ומזהה שכתובת המקור של החבילה והכתובת של ה-hop הבא שייכים לאותה רשת והוא מעוניין להודיע למחשב השולח שעדיף לו לשלוח את החבילה ישירות ל-hop הבא במקום דרכו.

ICMP packet	type	code	reason
Redirect Message	5	0	The router want to inform the sending host that a more direct path exists to the next hop on the same network.

f. נתב קיבל הודעת ping echo ומעוניין להחזיר תשובה.

ICMP packet	type	code	reason
Echo Reply	0	0	When receiving a valid Echo Request (ping), will typically respond with an Echo Reply to acknowledge receipt and indicate reachability.

g. הנתב קיבל חבילה שהרשת של כתובת היעד שלה לא מופיעה בטבלת הניתוב שלו.

ICMP packet	type	code	reason
Destination Unreachable	3	0	The router has no entry in its routing table to determine the

			next hop for the destination network so it sends “Network Unreachable”.

2. הסבר בקצרה את עקרון פעולת מנגנון הmtu discovery.

The MTU discovery mechanism is used for optimizing network efficiency and avoiding IP fragmentation, how it works:

basically the communicating parties try to find the MTU of the path that connects them, so the source host initiates communication with packets of different sizes that have the “DF” flag on, and as these packets traverse the network the routers along the path with smaller MTU than the packet’s size would send back an ICMP type 3 code 4 as explained in the previous part of Question 2 (2.1.b), upon receiving this message the source host reduces the assumed path MTU and retransmits the data with smaller packet size (DF flag also on), and so on, until the source host converges on the largest packet size that can traverse the path without being fragmented.

3. הסבר בקצרה את הקשר בין חבילת IP לחבילת ICMP.

IP (Internet Protocol) provides the fundamental addressing and routing for network data. ICMP (Internet Control Message Protocol) is a protocol that operates at the network layer and transmits control and error messages related to IP operations. ICMP packets are encapsulated as the data payload within IP packets. Network devices, such as routers and hosts, use ICMP to report issues like unreachable destinations or to perform network diagnostics. This feedback mechanism provided by ICMP is crucial for the proper functioning and management of IP-based networks.

מעבדת 66) mininet נק')

IP address - 192.168.56.102

שאלה 1: הסבירו בקצרה מהם ההבדלים בין נתב (router) למתג (switch)?

נתב - router	מתג - switch
מחבר בין רשתות שונות, כמו בין רשת ביתית לאינטרנט.	מחבר בין מכשירים באותה רשת מקומית (LAN).
מנתב תעבורה לפי כתובות IP.	מנתב תעבורה לפי כתובות MAC.
פועל בשכבה 3.	פועל בשכבה 2.

שאלה 2: התבוננו בהגדרות והסטטיסטיקות של הממשק h1-eth0 (interface בפלט של הפקודה ifconfig.:

```
mininet> h1 ifconfig
h1-eth0   Link encap:Ethernet  HWaddr 2e:cb:8a:58:d4:ba
          inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::2ccb:8aff:fe58:d4ba/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:558 (558.0 B)  TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

2.1 מה כתובת ה MAC של interface זה?

MAC address of the interface (HW addr): 2e:cb:8a:58:d4:ba

2.2 מהי כתובת ה IP של ה interface הזה? מה ה Subnetmask? כמה מקסימום hosts יכולים להיות ברשת זו?

IP address of the interface: 10.0.0.1

Subnet Mask: 255.0.0.0 -2

Max Number of Hosts: 2^24.(3)

פחות 2 כתובות שמורות בתוך הסאבנט

2.3 מהי כתובת ה IPV6 של ה interface הזה?

inet6 addr: fe80::88b3:98ff:feba:8c5e/64.

2.4 מה גודל המסגרת המקסימלי שה interface הזה יכול לשלוח ולקבל?

MTU: 1500 bytes.

2.5 מה משמעות השדה txqueuelen?

txqueuelen הוא פרמטר שמציין את אורך תור השליחה (transmit queue length) של ממשק רשת בלינוקס.

זהו מספר המקסימום של חבילות (packets) שיכולות להמתין לשליחה בממשק הרשת.

שאלה 3: הסבירו בקצרה מהו Loopback Interface , מה השימוש בו ומה אתם יכולים להגיד על כתובת ה IP שלו?

Loopback interface is an interface that connects a host with itself.

Its is used by the system to communicate with itself which could be important for things like testing, local services, and internal communication.

The IP address of lo is 127.0.0.1.

שאלה 4: הריצו את הפקודה ifconfig על h2 צרפו צילום מסך של הפלט. האם הפלט זהה לפקודת ifconfig שהרצנו על h1 ? מה משותף לכתובות ה ip של h1-eth1 ו h2-eth ?

```
mininet> h2 ifconfig
h2-eth0   Link encap:Ethernet  HWaddr 8a:b3:98:ba:8c:5e
          inet addr:10.0.0.2  Bcast:10.255.255.255  Mask:255.0.0.0
          inet6 addr: fe80::88b3:98ff:feba:8c5e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:558 (558.0 B)  TX bytes:648 (648.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

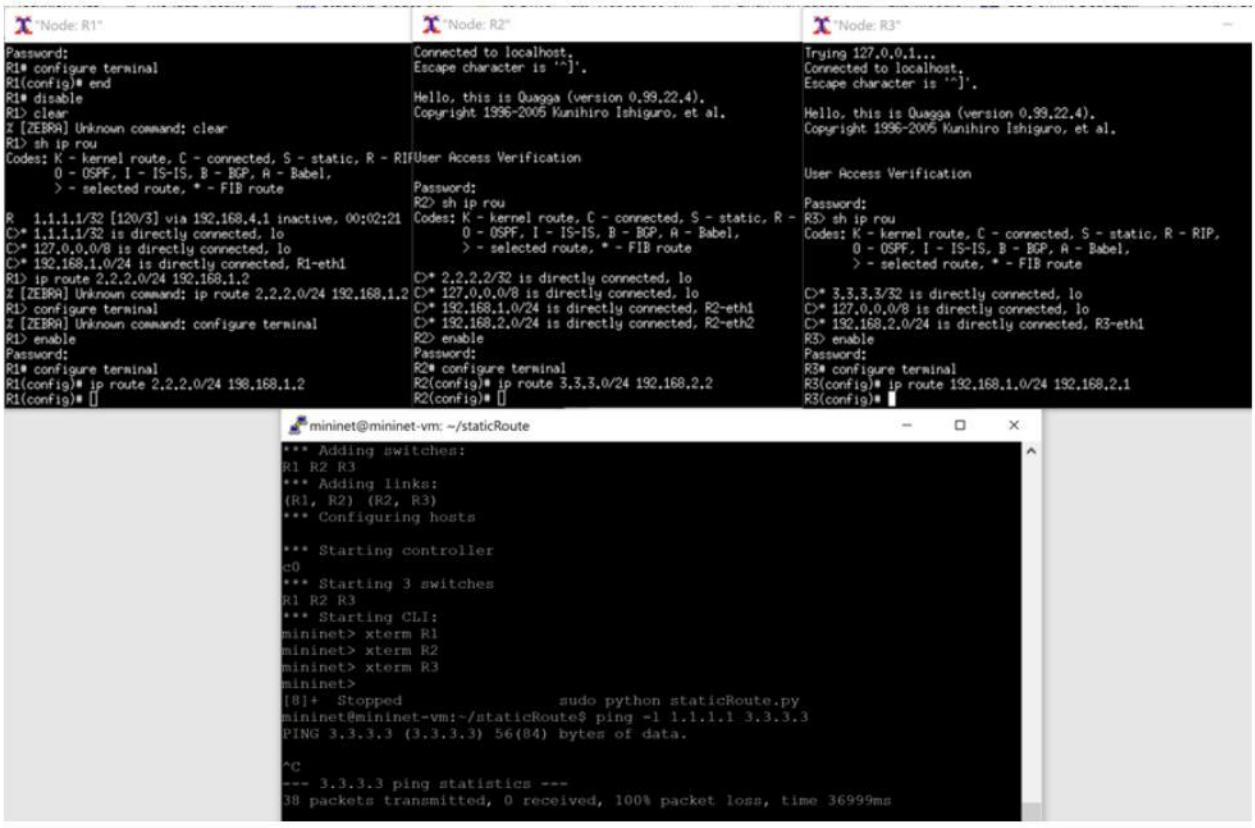
The output is pretty similar but it's not the same, basically since the hosts are different regardless of whether or not they share the same file system their MAC addresses are different, However, both hosts are in the same subnet but their IPs are different, so they start off with the same numbers since the subnet mask is 255.0.0.0 then they share the first 8 bits which are 10.0.0.0, but the rest of their IPs are different (coincidentally they are 0.0.1 and 0.0.2).

שאלה 5: רשמו את פקודות הניתוב הסטטי הסטטיים שהוספתם לכל ראוטר על מנת שהחבילות יעברו כהלכה.
צרפו את פלט פקודת ה ping לאחר הוספת הניתוב.

We opened 3 windows one for each router and we used the following commands:

router	command	meaning
R1	ip route 2.2.2.2/24 192.168.1.2	To reach anything in 2.2.2.0/24 R1 should forward messages to 192.168.1.2 (R2-eth1)
R2	ip route 3.3.3.0/24 192.168.2.2	To reach anything in 3.3.3.0/24 R2 should forward messages to 192.168.2.2 (R3-eth2)
R3	ip route 192.168.1.0/24 192.168.2.1	To reach anything in 192.168.1.0/24 R3 should forward messages to 192.168.2.1 (R2-eth2)

So basically we told R1 to forward to R2 which forwards to R3 - so R1 can now send packets to R3 which makes “ping -I 1.1.1.1 3.3.3.3” work as follows:



שאלה 6: מהם החסרונות העיקריים בשימוש בניתוב סטטי?

The main disadvantage of static routing is that it requires manual configuration by the network administrator, making it time-consuming and difficult to scale in large networks. It also lacks automatic updates, so routes do not adapt to changes or failures, making the network less resilient and less flexible overall.

שאלה 7: הסבירו בקצרה מה היא בעיית ה Count to Infinity ואיך Split horizon עוזר למנוע אותה.

The count to infinity problem occurs in distance vector routing when a router loses its connection to a destination but hasn’t yet updated its neighbors. It may receive a routing update from a neighbor claiming to have a shorter path—when in fact, that path loops back through the original router whose link has failed. As a result, routers continuously exchange incorrect routes, causing packets to loop or get stuck, and the cost to reach the destination keeps increasing until a better route is eventually found.

Split Horizon helps prevent this by not advertising a route back on the interface it was learned from, which stops routers from misleading each other with invalid paths.

שאלה 8: הסבירו בקצרה מה הוא מנגנון הpoisoned reverse.

It is an enhancment to Split Horizon, basically instead of simply not advertising a route back on the interface it was learned from, the router actively advertises that route with an infinite cost. This tells the neighbor not to use that route through the router, helping prevent routing loops and solving issues like the count to infinity problem.

שאלה 9: הסבירו בקצרה מה מנגנון ה-Triggered Updates ואיך הוא עוזר להתמודד עם בעיית ה Count to Infinity . מה החיסרון בשימוש במנגנון זה?

Triggered updates are a mechanism designed to speed up the resolution of the count to infinity problem. When a router detects a change in the network, it immediately sends an update to its neighbors—without waiting for the regular update interval. This is especially helpful in cases where the routing loop involves more than two routers, and split horizon alone isn't enough. By quickly spreading updated information, it helps the network converge faster and recover from failures.

The main disadvantage is that it can cause network congestion or update storms if many routers send triggered updates at the same time.

שאלה 10: הסבירו מהן המגבלות של פרוטוקול RIP.

1. Maximum hop count is 15 – Any route beyond 15 hops is considered unreachable, limiting RIP to small networks.
2. Slow convergence – RIP can take a long time to update the network after changes, especially in failure scenarios.
3. Count to infinity problem – RIP relies on incrementing hop counts to detect unreachable networks, which can lead to routing loops and delays.
4. Only uses hop count – RIP ignores other important metrics like delay, reliability, and network load, leading to suboptimal route choices.
5. Limited scalability – Due to its simplicity, RIP doesn’t scale well to large or complex network environments.

שאלה 11: מהו התפקיד של שדה ה-command בחבילות שנשלחות במסגרת פרוטוקול RIP?

The Command field in RIP packets defines the purpose of the datagram. It acts as a header that indicates whether the message is a request, response, or a special type like trace on, trace off, or reserved. This helps routers understand whether they should send routing information, update their tables, or perform a control action.

שאלה 12: כל כמה זמן בממוצע שולח R2 הודעת response?

About 15 seconds on average:

No.	Time	Source	Destination	Protoco	Lengtl	Info
1	0.000000000	192.168.1.2	224.0.0.9	RIPv2	66	Request
2	0.000059000	192.168.1.1	192.168.1.2	RIPv2	146	Response
3	0.005506000	192.168.1.2	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.9 for any sources
4	0.989901000	192.168.1.2	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.9 for any sources
5	1.528990000	192.168.1.2	224.0.0.9	RIPv2	186	Response
6	5.010724000	c6:65:d2:2d:7c:dd	06:60:0b:c8:28:03	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
7	5.010757000	06:60:0b:c8:28:03	c6:65:d2:2d:7c:dd	ARP	42	192.168.1.2 is at 06:60:0b:c8:28:03
8	24.55573900(	192.168.1.1	224.0.0.9	RIPv2	146	Response
9	25.53026500(	192.168.1.2	224.0.0.9	RIPv2	186	Response
10	50.56012500(	192.168.1.1	224.0.0.9	RIPv2	146	Response
11	61.53078300(	192.168.1.2	224.0.0.9	RIPv2	186	Response
12	83.57220900(	192.168.1.1	224.0.0.9	RIPv2	146	Response
13	94.54265400(	192.168.1.2	224.0.0.9	RIPv2	186	Response
14	112.5785350(	192.168.1.1	224.0.0.9	RIPv2	146	Response
15	123.5480530(	192.168.1.2	224.0.0.9	RIPv2	186	Response
16	147.5809470(	192.168.1.1	224.0.0.9	RIPv2	146	Response

שאלה 13: מעל איזה פרוטוקול נשלחת הודעה זו? לאיזה פורט?

Protocol : UDP. -2

(3)

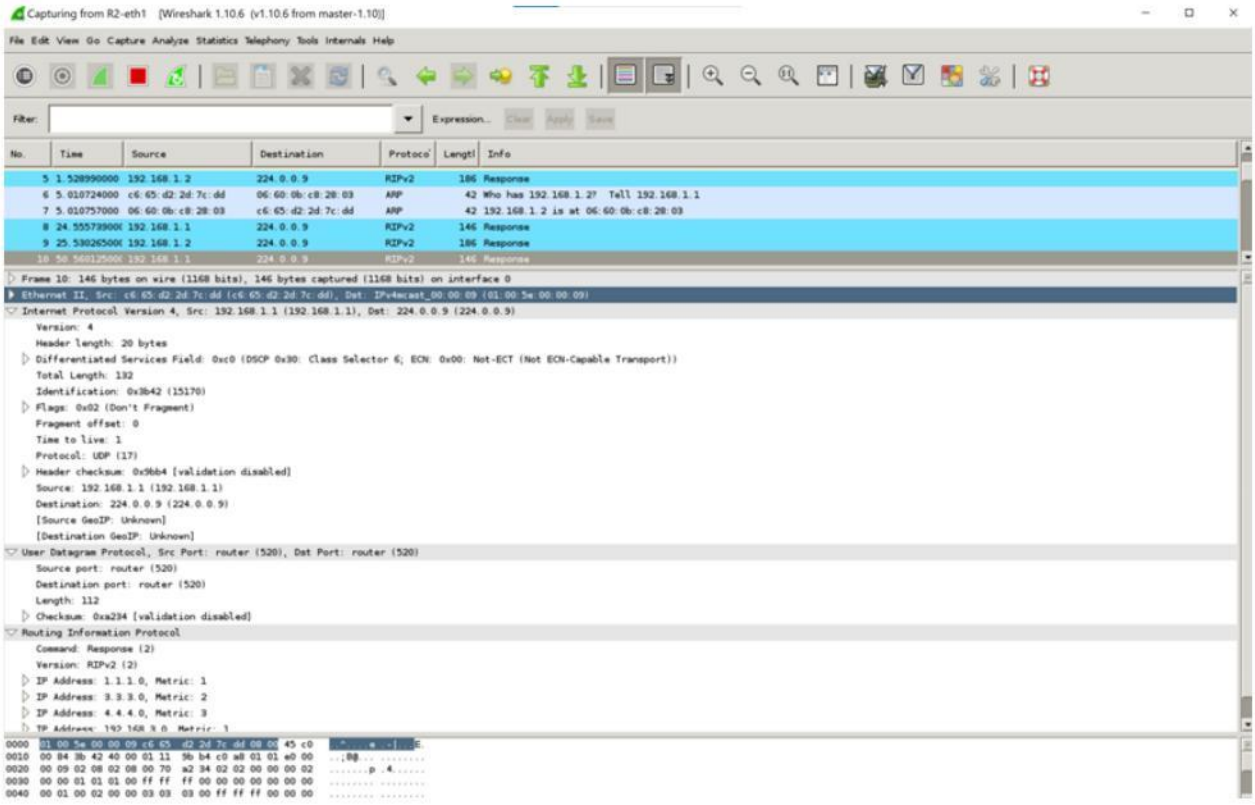
Port: 17.

פורט 520

שאלה 14: לאיזה כתובת IP נשלחת הודעה זו? מה מיוחד בכתובת זו? (חפשו בגוגל)

The dest IP address is 224.0.0.9: it is a multicast address used by RIP version 2 to send routing updates. It allows RIP routers to communicate efficiently by sending updates only to other RIP-enabled devices on the local network, rather than broadcasting to all hosts.

שאלה 15: פרטו איזה מידע מכילה כל הודעה כזו (מידע רלוונטי ל-RIP)? צרפו צילום מסך.



The key information in the RIP Response packet is the Metric field, which indicates the hop count—i.e., the number of routers a packet must pass through to reach a specific destination. This value helps routers build and update their routing tables based on the shortest path.

שאלה 16: מהי המטריקה שמייצגת אינסוף (המטריקה המקסימלית)? מה זה מעיד על אורך מסלול מקסימלי ברשת המשתמשת ב RIP בהנחה שמחיר כל קשת שלם?

The metric that represents infinity in RIP is 16.

This means that any route with a metric of 16 is considered unreachable.

Since RIP uses hop count as its metric and assumes the cost of each link is 1, this implies that the maximum path length in a RIP-based network is 15 hops. Any destination beyond 15 hops is not supported by the protocol.

שאלה 17: הסבירו כיצד בא לידי ביטוי מנגנון הTriggered Updates .

Triggered Updates is a mechanism in RIP where routers immediately send updates when they detect a change in the network, instead of waiting for the regular update interval. In your case, shortly after the link went down, the other routers quickly realized there was a better path to node 4. Thanks to Triggered Updates, they sent new response messages right away, updating their neighbors with the improved routing information. This sped up convergence and helped avoid routing issues.

Capturing from R2-eth1 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protoco	Lengt	Info
5	1.528990000	192.168.1.2	224.0.0.9	RIPv2	186	Response
6	5.010724000	c6:65:d2:2d:7c:dd	06:60:0b:c8:28:03	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
7	5.010757000	06:60:0b:c8:28:03	c6:65:d2:2d:7c:dd	ARP	42	192.168.1.2 is at 06:60:0b:c8:28:03
8	24.555739000	192.168.1.1	224.0.0.9	RIPv2	146	Response
9	25.530265000	192.168.1.2	224.0.0.9	RIPv2	186	Response
10	56.560125000	192.168.1.1	224.0.0.9	RIPv2	146	Response

```
▷ Frame 10: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
▶ Ethernet II, Src: c6:65:d2:2d:7c:dd (c6:65:d2:2d:7c:dd), Dst: IPv4mcast_00:00:09 (01:00:5e:00:00:09)
▽ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 224.0.0.9 (224.0.0.9)
    Version: 4
    Header length: 20 bytes
  ▷ Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 132
    Identification: 0x3b42 (15170)
  ▷ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 1
    Protocol: UDP (17)
  ▷ Header checksum: 0x9bb4 [validation disabled]
    Source: 192.168.1.1 (192.168.1.1)
    Destination: 224.0.0.9 (224.0.0.9)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▽ User Datagram Protocol, Src Port: router (520), Dst Port: router (520)
    Source port: router (520)
    Destination port: router (520)
    Length: 112
  ▷ Checksum: 0xa234 [validation disabled]
▽ Routing Information Protocol
    Command: Response (2)
    Version: RIPv2 (2)
  ▷ IP Address: 1.1.1.0, Metric: 1
  ▷ IP Address: 3.3.3.0, Metric: 2
  ▷ IP Address: 4.4.4.0, Metric: 3
  ▷ IP Address: 192.168.3.0, Metric: 1
```

```
0000  01 00 5e 00 00 09 c6 65  d2 2d 7c dd 08 00 45 c0   ..^....e .-|...E.
0010  00 84 3b 42 40 00 01 11  9b b4 c0 a8 01 01 e0 00   ..;B@... ........
0020  00 09 02 08 02 08 00 70  a2 34 02 02 00 00 00 02   .......p .4......
0030  00 00 01 01 01 00 ff ff  ff 00 00 00 00 00 00 00   ........ ........
0040  00 01 00 02 00 00 03 03  03 00 ff ff ff 00 00 00   ........ ........
```

בונוס:

כעת נחזיר את הלינק בין R2 ל R4, ב CLI של mininet הריצו את הפקודה

link R2 R4 up

ונפעיל את מנגנון הpoison reverse על הממשק R2-eth1, לשם כך נתחבר לdaemon של ripd על R2.

מתוך טרמינל של R2 הריצו את הפקודה:

telnet localhost ripd

עברו למצב קונפיגורציה (enable -> configure terminal) והריצו את הפקודות הבאות:

interface R2-eth1
ip rip split-horizon poisoned-reverse

סגרו את החלון, התבוננו בתעבורה על ממשק זה, וענו על השאלות הבאות:

שאלה 18: הסבירו כיצד בא לידי ביטוי מנגנון ה Poisoned Reverse ? צרפו צילום מסך של הודעת response שנשלחת ע"י R2 המעידה על כך שהמנגנון פועל.

שאלה 19: הסבירו מה ההבדל בין Poisoned Reverse ל Route Poisoning.

2
(4)

Route poisoning is the general technique of marking a bad route as unreachable by assigning it a metric of 16 in RIP.

Poisoned reverse is a specific application of this technique, where a router explicitly tells the neighbor it learned the route from not to use it to reach that destination — like saying, "don't go there through me!" This helps prevent routing loops.

https://en.wikipedia.org/wiki/Route_poisoning