HOMEWORK #6

Alexander Shender 328626114

Netanel Rotshild 204937841

Question 1.

First of all, X should receive an IP and Default Gateway IP (and DNS..) from DHCP. Two DHCP are available, so 2 of them will offer, but only 1 is accepted. Let’s say offer from DHCP2 is accepted.

Then, it will see that Y is not in its subnet, and send the request to the Default Gateway, which is R1 (figuring out its MAC first). R1 will see that the Y IP is in the local subnet, so it will send it directly to Y MAC, because R1 tables have the MAC address for Y.

Source	Phy. Net.	MAC src	MAC dst	IP src	IP dst	MAC frame payload
X	LAN1	MAC(X)	FF:FF:FF:FF:FF:FF	0.0.0.0	255.255.255.255	DHCP Discover
B1	LAN2	MAC(X)	FF:FF:FF:FF:FF:FF	0.0.0.0	255.255.255.255	DHCP Discover
DHCP2	LAN1	MAC(DHCP2)	FF:FF:FF:FF:FF:FF	IP(DHCP2)	255.255.255.255	DHCP Offer
DHCP1	LAN2	MAC(DHCP1)	FF:FF:FF:FF:FF:FF	IP(DHCP1)	255.255.255.255	DHCP Offer
B1	LAN1	MAC(DHCP1)	FF:FF:FF:FF:FF:FF	IP(DHCP1)	255.255.255.255	DHCP Offer
X chooses DHCP2 offer						
X	LAN1	MAC(X)	FF:FF:FF:FF:FF:FF	0.0.0.0	255.255.255.255	DHCP request
B1	LAN2	MAC(X)	FF:FF:FF:FF:FF:FF	0.0.0.0	255.255.255.255	DHCP request
DHCP2	LAN1	MAC(DHCP2)	FF:FF:FF:FF:FF:FF	IP(DHCP2)	255.255.255.255	DHCP ack
IP(X) allocation completed. IP(R1) is default gateway						
X	LAN1	MAC(X)	FF:FF:FF:FF:FF:FF	IP(X)	255.255.255.255	ARP request(Who has IP(R1)?)
B1	LAN2	MAC(X)	FF:FF:FF:FF:FF:FF	IP(X)	255.255.255.255	ARP request(Who has IP(R1)?)
R1	LAN2	MAC(R1)	MAC(X)	IP(R1)	IP(X)	ARP reply (MAC(R1_subnet1))
B1	LAN1	MAC(R1)	MAC(X)	IP(R1)	IP(X)	ARP reply (MAC(R1_subnet1))
X	LAN1	MAC(X)	MAC(R1_subnet1)	IP(X)	IP(Y)	IP_PACKET(DATA)
B1	LAN2	MAC(X)	MAC(R1_subnet1)	IP(X)	IP(Y)	IP_PACKET(DATA)
R1	LAN3	MAC(R1_subnet2)	MAC(Y)	IP(X)	IP(Y)	IP_PACKET(DATA)
Y receives message from X						

Question 2.

א) מומלץ לתקוף את הקו שמחבר בין $R1 \to R2$. זה מכיוון שמעבר למצב שכעת המסלול $R1 \to NET-1$ עובר דרך הקו $R3 \to R4$, בעל משקל של 200. קיים אפשרות השהייה נוספת ברגע שהקו נופל עלול לקראת מצב בו, לאחר מחיקת הכניסה מהטבלת ניתוב של $R1$, $R3$ ישלח ל$R1$ את הטבלה שלו וכעת כל אחד חושב שהניתוב האידיאלי עובר דרך השני. הם ימשיכו לעדכן אחד את השני עד למצב ש"העלות" לשדר $R3 \to NET-1$ דרך $R1$ יעלה יותר מ200. בשלב הזה $R3$ "מוצא" מסלול קל יותר דרך $R4$ והמערכת מתייצבת על המצב הזה.

אם היינו בוחרים לתקוף את קשת $R2 \to R4$ היה קורה מצב דומה בין $R1, R2$ אבל ההגעה למצב יציב הייתה מתרחשת בקפיצות של 2 (מהר יותר) בניגוד למקרה שתואר מקודם עם קפיצות של 1.

ב) במידה וכל התחנות משדרות את הDV באותו תדר, ההסתברות של שהתקפה תביא למצב "הלא טוב" הוא $\frac{1}{2}$ וההסתברות שתביא למצב ה"טוב" הוא $\frac{1}{2}$. זה מתוך ההבחנה כי בוחנים את המקרה בו קיים סיכוי ש$R3$ ישלח ל$R1$ את הDV שלו לפני ש$R1$ יספיק לשלוח את הDV המעודכן ל$R3$.

ג) לפני התקיפה, הרשת התייצבה על הטבלאות הבאות:

R3		
To Subnet	Via Router	Cost
Net-1	R1	7

R1		
To Subnet	Via Router	Cost
Net-1	R2	6

לאחר התקיפה הקו בין $R1 \to R2$ נופל. ו$R3$ ישלח ל$R1$ עדכון, כעת בטבלה יראה כך:

R1		
To Subnet	Via Router	Cost
Net-1	R3	7+1=8

לאחר מכן $R3$ יתעדכן ל:

R3		
To Subnet	Via Router	Cost
Net-1	R1	8+1=9

וכן הלאה וכן הלאה עד שהמסלול של $R3 \to R4$ יקבל תיעדוף בחציית ה200 במסלול $R3 \to R1$.
סה"כ איטרציות: 201-7=**194** איטרציות.

Question 3.

a.

The sketch is attached at the bottom of this report. B1 is a root port. Ports which have neither “d” nor “r” sign are disabled.

b.

B2 and B5 are placed at the same distance from B3, so we randomly assume that a message from B5 is received earlier than the one from B2.

The messages are received in the following order:

1. B3 sends: {B3, 0, B3} – B3 offers itself as a root
2. B3 receives: {B3, 1, B5} – B5 accepted B3 as a root because it has lower ID, and this is the BDPU message from B5. B3 sees that RootID is same as it’s own RootID, but B3 rootCost is lower than msg.rootCost, so it ignores this message. B3 declares itself designated on A.
3. B3 receives: {B2, 0, B2} – B2 didn’t accept B3 as a root. B2 offers itself as a root. B3 sees that msg.rootID is lower than B3 current rootID. B3 accepts B2 as root. rootCost is now 1 (portCost to B2). rootPort = port leading to B2.
4. B3 sends: {B2, 1, B3}
5. B3 receives: {B1, 1, B5} – B5 has acknowledged B1 as a root. Msg.RootID < rootID, so B3 changes: rootID = msg.RootID (1), rootCost = 1 + 1 = 2, rootPort = port leading to B5. rootCost > msg.rootCost, so B3 is not designated on A.
6. B3 receives: {B1, 1, B2} – B2 has also acknowledged B1 as a root port. But now:
    a. msg.rootID = rootID -> rootPort not changed
    b. rootCost = 2, msg.rootCost + portCost = 1+1 = 2 -> rootPort is not changed.
    c. rootCost = 2, msg.rootCost = 1, so port leading to C is not designated
7. B3 sends: {B1, 2, B3}
8. B3 receives: {B1, 1, B5} – nothing changed
9. B3 receives: {B1, 1, B2} – nothing changed
10. …

We end up with B3 having the following parameters:

RootID = 1, rootCost = 2, rootPort = <port to B5>, designatedOnLAN = {N/A}

NOTE: in the sketch in (a.), the rootPort from B3 leads to B2. This is equal, it depends on whether B3 receives packages from B2 earlier than B5. B2 and B5 have same rootCost, so the first to reach B3 will make B3's rootPort connected to itself.

c.

Since the tables are empty, each bridge will broadcast the message to add it's neighboring bridges/switches. So the message will be 'heard' on all the LANs in the network

d.

After the learning process, each bridge/switch knows on which port the computer on the A LAN network can be found. But because the computer on the I network never transmitted, no one knows where it's located (on which port). So the message will be broadcasted on the whole network again.

e.

Now, each bridge knows at which port the computer at LAN A can be reached. Message from H reaches B4, received message on the same port, on which it has received message from A, so it drops it. Message reaches B1 -> LAN D -> B5 -> LAN A -> Computer A. B1 learned before on which port A is located.

So It goes through 3 LANS: H, D, A

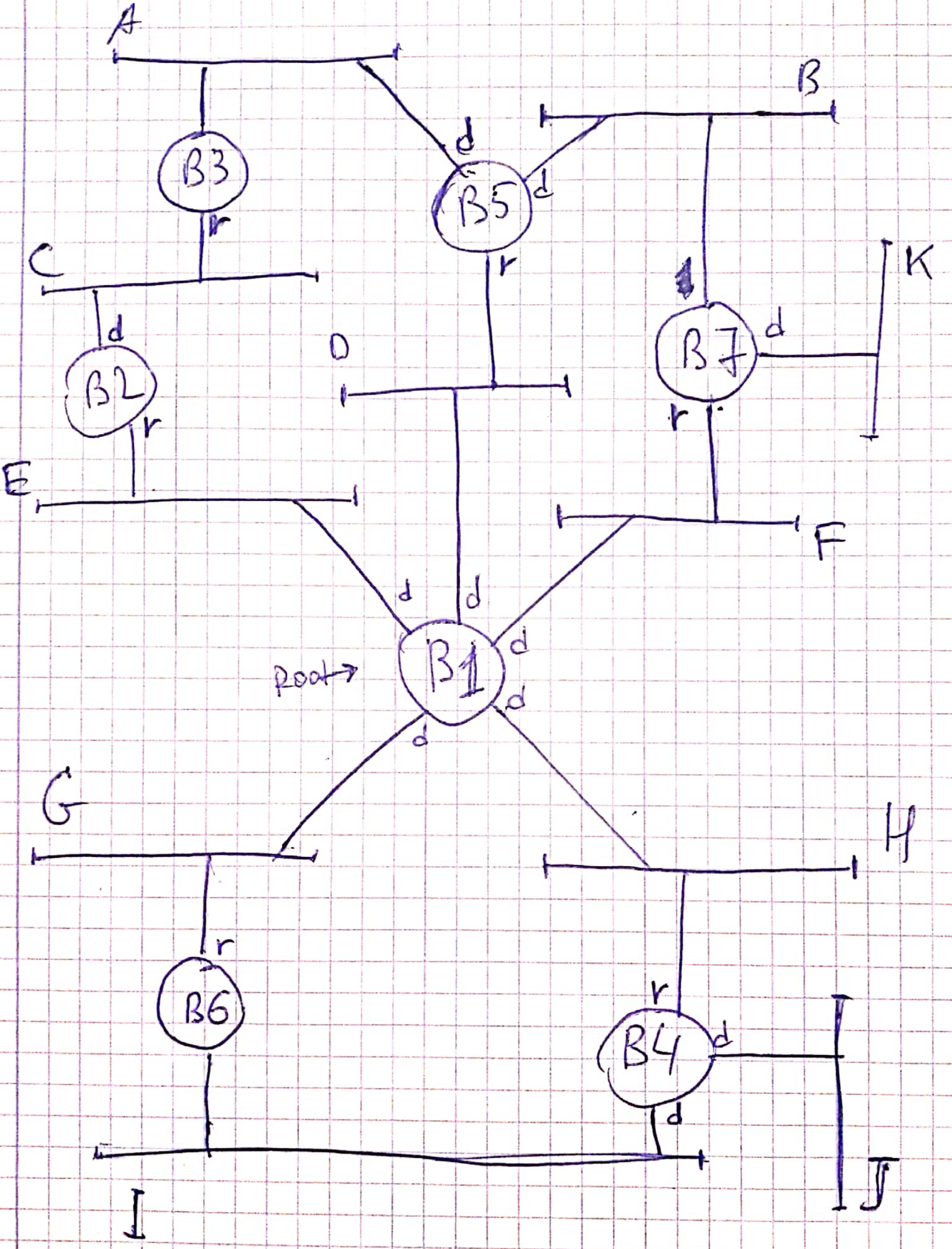
f.

First and foremost, STP algorithm is here to avoid loops. If it's not working correctly, loops will be created, which we will see here:

B4 stopped sending BPDU, so after a certain amount of time it will stop being the Designated Port for LAN I. And B6 will take its place. (B6 doesn't know B4 exists). Which means, now LAN I has 2 bridges, where it is on a designated port.

Let's imagine computer on LAN I sending packet to unknown computer on LAN B. Both B4 and B6 start broadcasting it. B1 also broadcasts it, and this broadcast is heard on BOTH B4 and B6. Which broadcast it again. And loop continues.

Even if stations on LAN I broadcast at 1% of the bandwidth, because of the loop, the packets stay permanently in the loop, which damages performance.


A
B
B3
d
B5
d
r
r
C
K
d
B7
d
B2
D
r
r
E
F
d
d
d
Root
B1
d
d
G
H
r
B6
r
B4
d
d
I
J