

## רשתות תקשורת - עבודה 2 תאורטי (:

### משימה 1:

א. בהתבסס על הדרישות המפורטות בשאלה , נציע את המבנה הבא עבור הפרוטוקול שלנו MyICMP:

- **Type** - סוג הבקשה ( 0 - ping response - 1 - ping req )
- **Received** - אם התקבלה תשובה - 0. אחרת אם היה - 1 - timeout.
- **currentT** - ערך השעון בזמן קבלת ההודעה .
- **srcIP** - כתובת IP או שם DNS למקור.
- **dstIP** - כתובת IP או שם DNS ליעד .
- **Checksum** - מנגנון לזיהוי שגיאות.

ב.

Client->Server

- לקוח שולח בקשת " ping req " לשרת.
- (ping req=1, currentT=s, srcIP, dstIP, CheckSum)

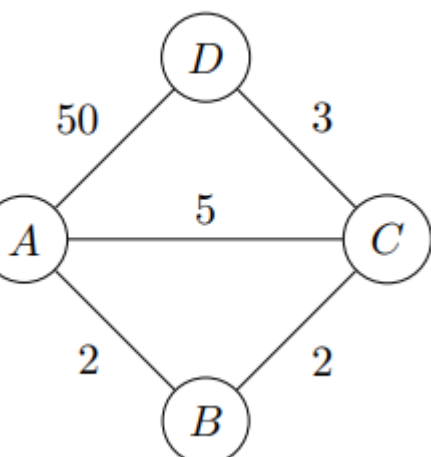
Server->Client

- שרת שולח "ping response" ללקוח
- (ping req, received , currentT=s, srcIP, dstIP, CheckSum)
- במידה ויש שגיאה נדע ע"י שדה received=1.

בס"ד

## משימה 2:

א:



נתונה טופולוגיית הרשת הבאה: בהינתן שאנו מריצים אלגוריתם vector distance עם reverse poisoned, מלאו בטבלה רק את התוצאה הסופית והסבירו בקצרה כיצד חושבה הטבלה.

A	B	C	D
0	2	4	7

הטבלה חושבה לפי אלגוריתם בלמן פורד תמיד צמצמתי שראיתי מסלול קצר יותר .

ב:

נתבים לא אמורים ליישם את פרוטוקולי שכבת ה-transport . הם אחראים להעברת מנות על סמך כתובת ה-IP של היעד ותחזוקת טבלאות ניתוב. נתבים אינם משמשים בדרך כלל להפעלת אפליקציות, שכן תפקידם העיקרי הוא להעביר מנות בין רשתות. עם זאת, ייתכנו חריגים שבהם נתבים יכולים להריץ יישומים או שירותים, במיוחד ברשתות ארגוניות או ספקי שירות, בהן נדרשות תכונות מתקדמות כגון חומות אש, VPNs או מערכות ניהול רשת.

- לדוגמה, לנתבים מסוימים עשויים להיות חומות אש מובנות או יכולות VPN הדורשות הפעלת יישומים או שירותים ספציפיים. לחלק מהנתבים עשויים להיות גם ממשקי ניהול המאפשרים למנהלי מערכת להגדיר ולנטר את ביצועי הנתב. בנוסף, ברשתות מוגדרות באמצעות תוכנה (SDN), הבקר עשוי לפעול על שרת איך לקיים אינטראקציה עם הנתבים והמתגים כדי לנהל את הרשת.

## משימה 3:

א) ישנם 4 לינקים :

בכל לינק נשלחות 2 הודעות לכל ראوتر שקיים חוץ מהשולח כמובן .  
נחשב את מספר ההודעות הכולל:

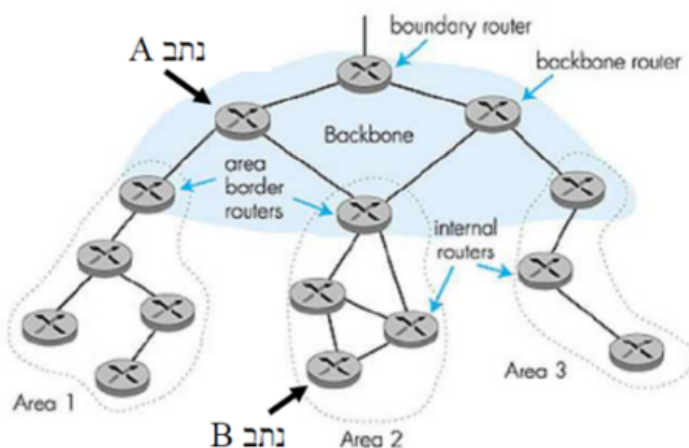
$32 = (5-1) * 4 * 2$  . ולכן כמות bytes של ההודעות הוא  $M * 32 \text{bytes}$

**(ב)** לוקח לכל הצמתים לקבל את האינפורמציה אחרי  $4T$  מאחר והמרחק הכי גדול בין שני צמתים הוא 4 לינקים וכמובן שנלך לפי מקרה קיצון .

**(ג)**

Step	Travel set	$D(B),p(B)$	$D(C),p(C)$	$D(D),p(D)$	$D(E),p(E)$
0	A	1A	$\infty$	$\infty$	$\infty$
1	AB	1A	2B	$\infty$	$\infty$
2	ABC	1A	2B	3C	$\infty$
3	ABCD	1A	2B	3C	4D
4	ABCDE	1A	2B	3C	4D

**(ד)** נתונה הרשת הבאה. כמה הודעות state link יגיעו לנתב במקרה של רשת אחת המריצה OSPF וכמה במקרה של OSPF היררכי כמו בתרשים? אותה שאלה לגביי נתב?? הסבירו את תשובתכם.



עבור A:

במצב ללא היררכיה - ברשת הנתונה יש 17 קשתות לכל קשת יש 2 הודעות לכן סה"כ עבור A יהיה 34 הודעות.  
במצב עם היררכיה - בתוך החלק של A יש 6 קשתות ולכן יהיה 12 הודעות .

עבור B:

במצב ללא היררכיה - ברשת הנתונה יש 17 קשתות לכל קשת יש 2 הודעות ולכן סה"כ נגיע ל 34.  
במצב עם היררכיה - בתוך החלק של B יש 5 קשתות ולכן יקבל 10 הודעות .

## בס"ד

### משימה 4:

פרוטוקול BGP

א. BGP - Border Gateway Protocol הינו פרוטוקול ניתוב וקטור של נתיב, מה שאומר שהוא אכן משדר מידע על כל המסלול ליעד, כולל נתיב AS. לכן BGP הוא אכן פרוטוקול ניתוב PV.

לגבי בעיית הספירה לאינסוף, היא עדיין יכולה להתרחש בגישה וקטורית של נתיב אם יש לולאות ניתוב. עם זאת, BGP נועד להימנע מניתוב לולאות על ידי אי קבלת מסלולים המכילים AS משלו בנתיב ה-AS, ועל ידי שימוש במנגנוני מניעת לולאות כגון כלל "split-horizon".

ב. האם BGP מבטיח ניתוב במסלולים קצרים ביותר? נמקו.  
מבטיח?? בהחלט לא (:

BGP אינו מיועד להבטיח ניתוב בנתיבים הקצרים ביותר. הוא נועד למצוא ולפרסם את הנתיב הטוב ביותר ליעד. בהתבסס על גורמים שונים כגון אורך נתיב, העדפת נתיב ומדיניות.

תהליך בחירת הנתיב ב-BGP כולל השוואת נתיבים מרובים ליעד בהתבסס על קבוצה של תכונות כגון אורך נתיב AS, סוג מוצא, העדפה מקומית. בקיצור BGP בוחר את הנתיב הטוב ביותר ליעד על סמך תכונות העדיפות הגבוהה ביותר.

לכן, הנתיב הטוב ביותר ב-BGP לא תמיד יהיה הנתיב הקצר ביותר מבחינת מספר הקפיצות או הנתיב הקצר ביותר מבחינת עיכוב ברשת. BGP לוקח בחשבון גורמים ומדיניות שונים שעלולים לגרום לנתיב שנבחר להיות ארוך יותר מהנתיב הקצר ביותר.

ג.

כן אפשר להריץ BGP בצורה היררכית, כלומר נחלק את AS למספר תת-AS, שכל אחד מפעיל מופע BGP משלו.

יכול לסייע בניהול רשתות גדולות ומורכבות על ידי הפחתת כמות המידע של BGP שצריך להחליף בין חלקים שונים של הרשת. על ידי חלוקת AS לתת-ASs, קונפדרציות BGP מפחיתות את כמות מידע ה-BGP שצריך להעביר בין חלקי הרשת השונים, מה שיכול לסייע בהפחתת העומס הכולל של עיבוד BGP על הנתבים ולשפר את המדרגיות הכוללת של ה-BGP.

עם זאת, חלוקות אלו ב BGP יכולות גם להכניס מורכבות נוספת ותקורה אדמיניסטרטיבית, מכיוון שמנהל הרשת צריך לנהל את תצורת ה-BGP עבור כל

תת-AS בנפרד. יתרה מכך, BGP אינו מבטיח ניתוב בנתיב הקצר ביותר בין שני צמתים כלשהם ברשת, שכן הקונפדרציות יכולות להציג נתיבי ניתוב לא אופטימליים בין חלקי הרשת השונים.

ד.

A יכול לנסות לשלוט בהתאם לכמה דרכים:  
להתאים מדדי ניתוב: A יכול להתאים את מדדי הניתוב, כגון אורך נתיב AS כדי להפוך את המסלולים לרשת X לאטרקטיביים יותר מהמסלולים המפורסמים על ידי ASs אחרים.

עמית עם ASs אחרים: A יכול להצפין עם ASs אחרים שיש להם קישוריות ישירה לרשת X. על ידי כך, A יכול להשפיע על החלטות הניתוב של ASs אלה ולנתב את התעבורה לרשת X דרך עצמה.

לסיכום האם ASs אחרים ינתבו את ההודעות שלהם ל-X (דרך A) תלוי במספר גורמים, כגון מדיניות הניתוב של ASs אלה, הזמינות של מסלולים חלופיים ואיכות השירות שמספק A. אם A מספק נתיב טוב יותר או ישיר יותר אל ASs, X, אחרים עשויים לבחור לנתב את התנועה שלהם דרך A. עם זאת, אם יש נתיבים חלופיים יעילים יותר או בעלי עלויות נמוכות יותר, ASs אחרים עשויים להעדיף להשתמש בהם במקום ניתוב דרך A.

**א.**

המוטיבציה למעבר לגישה ל-SDN (Software Defined Networking) מונעת מהצורך לרשתות זריזות וגמישות יותר שיכולות להסתגל במהירות למשתנים ודפוסי תעבורה. תשתית רשת מסורתית בנויה על חומרה ותוכנה שאינן גמישות וקשות לניהול. כל שינוי ברשת דורש התערבות ידנית (חומרה), אשר גוזלת זמן רב ונוטה לשגיאות. גישה זו גם מקשה על חידוש מהיר, שכן יש צורך לשלב שירותים ויישומים חדשים בתשתית הרשת, מה שעלול להימשך זמן רב.

SDN, לעומת זאת, מפריד בין מישור הבקרה למישור הנתונים, ומאפשר למנהלי רשת לנהל ולהגדיר את הרשת באופן מרכזי ממסוף תוכנה. זה מספק רמה גבוהה מפשט את ניהול הרשת ומאפשר גמישות וזריזות רבה יותר. על ידי שימוש בתוכנה לניהול הרשת, SDN מאפשר למנהלי מערכת להגדיר באופן פרוגרמטי התקני רשת, מדיניות ושירותים, מה שמקל על שילוב יישומים ושירותים חדשים ברשת.

בנוסף לזריזות וגמישות, SDN מציע גם אבטחה טובה יותר. לפלח תעבורה לזהות ולהגיב לאיומי אבטחה בזמן אמת. SDN מאפשר גם איזון עומסים דינמיים של תעבורה, שיכולים לשפר את ביצועי הרשת להפחית את העומס.

**לסיכום:** המוטיבציה למעבר לגישה ה-SDN היא ליצור רשתות **זריזות, גמישות וניתנות להרחבה** יותר שיכולות לענות על הצרכים המשתנים של העסק, לשפר את ביצועי הרשת **והאבטחה**, ולפשט את הניהול והניהול של הרשת.

**ב.**

רשת ה-4B של Google מתאימה במיוחד להטמעת SDN מכמה סיבות:

1. קנה מידה: הרשת של GOOGLE היא מהגדולות והמורכבות בעולם, עם אלפי מתגים ונתבים. ניהול רשת כה גדולה עם טכניקות רשת מסורתיות יכול להיות מאתגר, אבל SDN מציע יכולות ניהול ואוטומציה מרכזיות שמקלות בהרבה על הטיפול בה.
2. דפוסי תנועה: הרשת של גוגל נושאת כמות משמעותית של תעבורה פנימית בין מרכזי הנתונים והשירותים שלה. סוג זה של תעבורה יכול להיות מנוהל ביעילות עם SDN, המאפשר הנדסה ואופטימיזציה של תעבורה עדינה.
3. חדשנות: כחברה בחזית הטכנולוגיה, גוגל מתנסה כל הזמן בטכנולוגיות וגישות חדשות לרשת. SDN מציעה פלטפורמה גמישה לחדשנות, המאפשרת לגוגל לבדוק ולפרוס במהירות תכונות ושירותים חדשים.

מבחינת יישום, ארכיטקטורת ה-SDN של גוגל מורכבת מכמה שכבות:

1. שכבת יישומים: שכבה זו כוללת את השירותים והיישומים השונים הפועלים על גבי הרשת, כגון Gmail, Google Drive ו-Youtube. שירותים אלה יכולים למנף את SDN כדי לייעל את הביצועים שלהם ולשפר את חווית המשתמש.
  2. שכבת בקרה: שכבה זו אחראית לניהול ותזמור מרכזי של הרשת. שכבת השליטה ב-SDN של גוגל מבוססת על פרוטוקול OpenFlow, המאפשר שליטה עדינה בזרימות הרשת.
  3. שכבת תשתית: שכבה זו מורכבת מהתקני הרשת הפיזיים, כגון מתגים ונתבים. התקנים אלה מתוכננים באמצעות OpenFlow (כפי שלמדנו) ונמצאים בשליטה מרכזית של בקרת SDN.
- בסך הכל, הטמעת SDN של גוגל מאפשרת גמישות רבה יותר):

**בדיקה נעימה !!!**