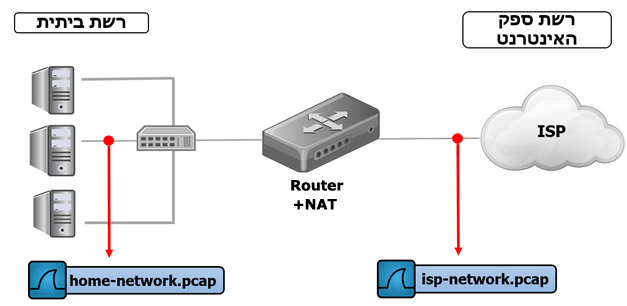
שיעור 11 – איך בונים רשת

**תרגיל: מעבדת NAT**

בתרגיל זה נכיר את פעולתו של רכיב ה-NAT מבפנים, בעזרת שתי הסנפות שנקבל ממקומות שונים ברשת.

**1. תמונת הרשת**

1. גלית פרשה כבלים, הקימה רשת ביתית והתחברה לספק האינטרנט "אינטרנט זהב".
2. גלית גלשה לאתר גוגל הנמצא בכתובת ה-IP: **64.233.169.104.**
3. בעזרת גמדי-רשת קטנים ושקופים, הוסנפה התעבורה בו זמנית בשני מקומות שונים ברשת, כפי שמסומן בתרשים הבא:

**2. חלק א' – ההסנפה ברשת הביתית**

1. פתחו את קובץ ההסנפה home-network.pcap בתוכנת Wireshark.
2. מהי כתובת ה-IP של גלית ברשת הביתית?

| 192.168.1.1 |
| --- |
| *תשובה* |

1. מהי כתובת ה-MAC של גלית?

| 00:22:68:0d:ca:8f |
| --- |
| *תשובה* |

1. האם אפשר לדעת ע"פ ההסנפות האם יש רכיב Switch ברשת של גלית? אם כן, כיצד? אם לא, מדוע?

| אי אפשר לדעת בגלל שהמחשב שלנו עונה לכל IP ששולח לו פאקטה. |
| --- |
| *תשובה* |

1. מהו ה-IP וה-MAC של ה-NAT של גלית? כתבו כיצד מצאתם את המידע וצרפו צילומי מסך רלוונטיים.



| בScreenshot אפשר לגלות את הMAC של הNAT בגלל שמחשב שנמצא ברשת פרטית של הבית שולח פקאטה למשתמש עצמו, והמכשיר היחיד שאליו יכולים לשלוח פקאטה למשתמש זה הNAT.  אז לפי הצילום מסך הip וmac של הNAT של הגלית זה: 74.125.91.113 ו00:22:6b:45:1f:1b. |
| --- |
| *תשובה* |

1. הציגו את כל הגלישה של גלית לאתר גוגל. כתבו פה את הפילטר שכתבתם / הפעולות שביצעתם:

| frame contains "Host: www.google" and http |
| --- |
| *תשובה* |

1. מצאו את לחיצת היד המשולשת של גלית עם אתר גוגל וצרפו צילום שלה.  
   זכרו! כדי לראות את כל תעבורת TCP בשיחה ספציפית השתמשו ב-Follow TCP Stream.



1. מהם ארבעת המאפיינים של ה-Socket בצד הלקוח (גלית)?

| Src IP = 192.168.1.1 Src Port = 4335  Dst IP = 64.233.169.104 Dst Port = 80 |
| --- |
| *תשובה* |

1. מי היה היעד המיידי (ה-Next Hop) אליו שלחה גלית את החבילות שיועדו בסופו של דבר לגוגל? כיצד גיליתם זאת?

| הראוטר, אפשר לגלות זאת דרך הMac כי הוא זהה לMac שידוע כבר שהוא של הראוטר. |
| --- |
| *תשובה* |

**3. חלק ב' – ההסנפה ברשת ספק האינטרנט**

1. פתחו את קובץ ההסנפהisp-network.pcap .
2. אתרו את אותה שיחת HTTP שדנו בה בסעיף הקודם. האם יש הבדלים במאפייני ה-Socket שכתבתם בסעיף 2-ו'? אם כן, הסבירו מהם ומדוע קיים שוני?

| כן, הip מקור השתנה כי כשהNat (בסיסי) שולח הודעות לרשת הוא משנה להודעה את הip בה הוא נשלח ממנה לIp חוקי לרשת. |
| --- |
| *תשובה* |

1. מהן שתי כתובות ה-IP שמחזיק ה-NAT שברשת הביתית? מהן שתי כתובות ה-MAC שלו?

| Ip:71.192.34.104  Mac:00:22:6b:45:1f:1c  Ip:192.168.1.100  Mac:00:22:6b:45:1f:1b |
| --- |
| *תשובה* |

1. כפי שלמדנו, רכיב NAT מחזיק בטבלה אשר מאפשרת לו לזהות שיחות שונות שעברו דרכו. מלאו את הטבלה בהתאם להסנפה שלנו:

| **טבלת NAT** | |
| --- | --- |
| **כתובת חיצונית + פורט** | **כתובת פנימית + פורט** |
| 71.192.34.104+4335 | 192.168.1.100+4335 |

1. האם ה-NAT מבצע החלפת פורטים? הסבירו כיצד אתם יודעים זאת.

| לא כי אפשר לדעת שהפורטים לא מוחלפים בגלל שבאותו שיחה עם אותן פאקטות הפורט לא משתנה אז הNAT לא מחליף בין הפורטים. |
| --- |
| *תשובה* |

1. בשתי ההסנפות, סמנו את בקשת ה-GET הראשונה ששלחה גלית בשיחה עם גוגל (זו השורה עם שדה ה-Length שהוא 689). במסך השכבות של Wireshark, הרחיבו בעזרת כפתור הפלוס את שכבת התעבורה (TCP) כך שיוצגו כל הפרטים. האם אתם מזהים הבדלים כלשהם בשדות ה-TCP בין שתי ההסנפות? כיצד תסבירו זאת?

| לא כי הדבר היחידי שאמור להשתנות בין כל פאקטה זה הIP ובגלל ששכבת התעבורה לא מכילה IP שום דבר בה לא משתנה. |
| --- |
| *תשובה* |

1. עשו אותו דבר בשכבת הרשת (IP). האם אתם מזהים הבדלים בין שתי ההסנפות? כיצד תסבירו זאת?

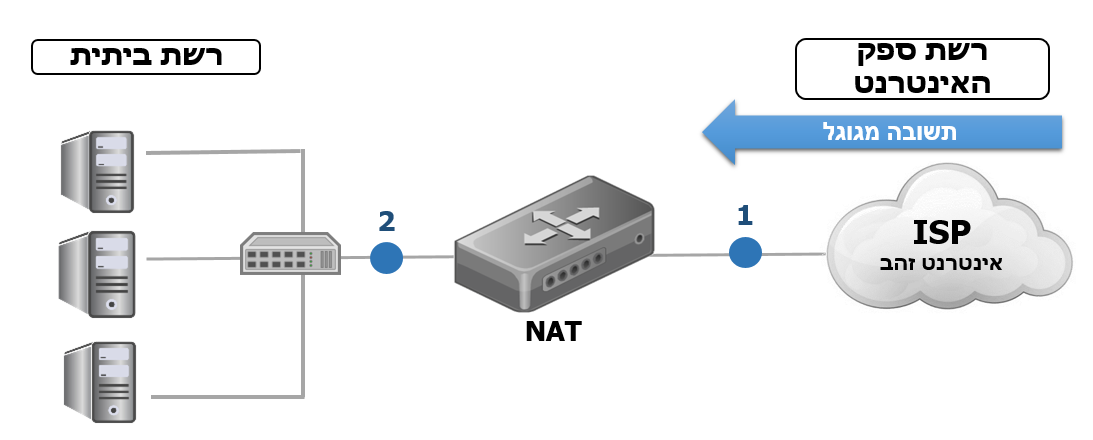
| כן, הIP משתנה לפי טבלת ההמרה של הNAT. |
| --- |
| *תשובה* |

1. **בונוס:** קראו באינטרנט כיצד מחושב שדה ה-Checksum של TCP. הסבירו מדוע הוא משתנה למרות שאף שדה בסגמנט TCP לא השתנה?

| ראשית, מחושבת סכום הבדיקה (Checksum) עם התחשבות ב-"Pseudo Header". ה-Pseudo Header אינו נשלח כחלק מהנתונים, אלא משמש אך ורק לצורך חישוב הסכום. הוא מכיל מידע מהשכבה העליונה (IP) כדי לוודא שהנתונים התקבלו במקום הנכון. |
| --- |
| *תשובה* |

המשך לתרגיל בדף הבא....

**3. חלק ג' – תשובה חוזרת מגוגל**

1. התשובה חזרה מגוגל. בתרשים מתוארות שתי נקודות בהן עצרנו את החבילה החוזרת מגוגל. ענו על השאלת הבאות:
2. עבור החבילה בנקודה 1 המסומנת בתרשים, מלאו את הפרטים הבאים:

| Src IP =64.223.169.104  Dst IP =71.192.34.104 Dst MAC =00:22:6b:45:1f:1c |
| --- |
| *תשובה* |

1. עבור החבילה בנקודה 2 המסומנת בתרשים, מלאו את הפרטים הבאים:

| Src IP =192.168.1.100 Src MAC =00:22:6b:45:1f:1b  Dst IP =192.168.1.1 Dst MAC =00:22:68:0d:ca:8f |
| --- |
| *תשובה* |

****