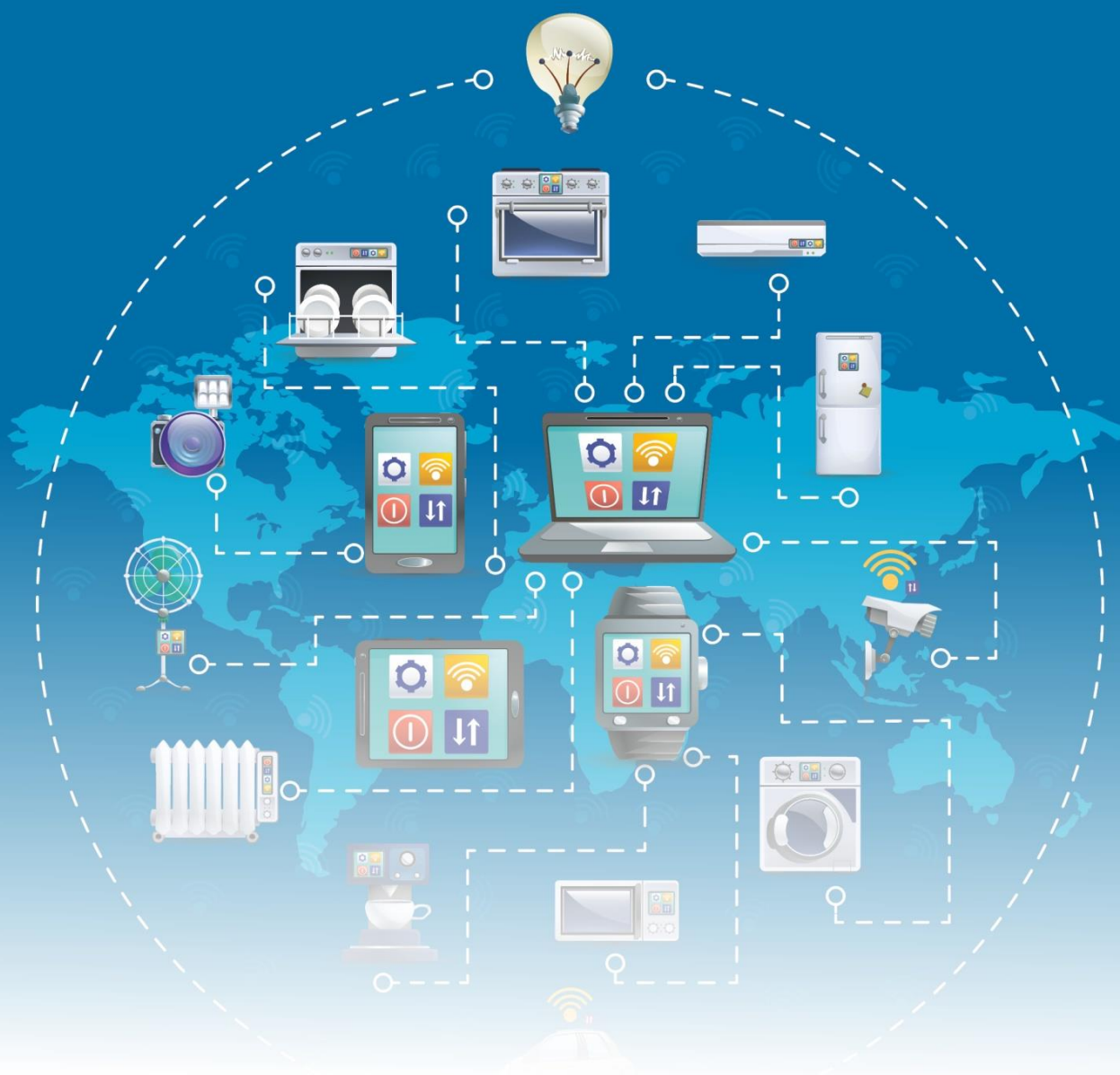


מדיניות ציבורית מומלצת לפרישת פרוטוקול IPv6 בישראל



נחקר ונכתב על ידי: ערן גרף (2017)

בקרה ועריכה: יורם הכהן ונעם אלון

הוער על ידי: לביא שיפמן, דני רוזן, פרופ' טל ז'רסקי, אדי אהרונוביץ',

אריאל בינה, ווסים אבו-סאלם, רבין ישרזדה, מיטל גרייבר-שוורץ

מדיניות ציבורית מומלצת לפרישת פרוטוקול IPv6 בישראל

I SBN 978-965-92622-2-9



נחקר ונכתב על ידי: ערן גרף (2017)

בקרה ועריכה: יורם הכהן ונעם אלון

הוער על ידי: לביא שיפמן, דני רוזן, פרופ' טל ז'רסקי, אדי אהרונוביץ',

אריאל בינר, ווסים אבו-סאלם, רבין ישחזדה, מיטל גרייבר-שוורץ

1. תקציר מנהלים

רשת האינטרנט (או בשמה העברי: מרשתת) הוקמה לפני כ- 47 שנים על ידי הסוכנות לפרוייקטי מחקר מתקדמים במשרד ההגנה של ארצות הברית¹. בתחילת שנות ה-90 של המאה ה-20, עם פתיחתה של האינטרנט לפעילות מסחרית, הפכה האינטרנט למערכת תקשורת מחשבים גלובלית שבה אנשים וגופים מרחבי העולם וממגזרים שונים יכולים לחלוק ולשתף מידע ביניהם. האינטרנט התפתחה רבות בשנים האחרונות והפכה לזירת תקשורת גלובלית בה מתקיימים שימושים רבים, כגון: הפצת מידע ותוכנות, קבצים, דואר אלקטרוני, תקשורת טלפונית, רשתות חברתיות, הוראה וחינוך, מסחר אלקטרוני, ניהול עסקים ועוד תחומים נוספים רבים.

כדי לאפשר זאת, רשת האינטרנט מבוססת על פרוטוקול טכנולוגי של תקשורת בין מחשבים IP (Internet Protocol). לכל מחשב או ציוד קצה שמחובר לאינטרנט יש כתובת מספרית ייחודית הידועה בשם כתובת IP. כתובת זו משמשת לצורך ניתוב המידע מהשולח למקבל בין ציודי הקצה השונים. פרוטוקול האינטרנט הרווח והנפוץ כיום בשימוש הינו מגרסה 4 ונקרא IPv4. על בסיסו ניתן להקצות כתובות IP לכ-4.3 מיליארד מחשבים וציודי קצה ייחודיים שיחוברו לאינטרנט².

אולם, כמות ציוד הקצה המחובר לאינטרנט, כבר היום, עולה על כמות הכתובות הייחודיות הקיימות בפרוטוקול IPv4. על כן נוצר מחסור קשה בכתובות IP בפרוטוקול IPv4. לפיכך, כבר בשנות ה-90 התחילו בפיתוח של פרוטוקול חדש - אשר נקרא IPv6 - שאמור היה לפתור, בין היתר, את המחסור הצפוי שזוהה במאגר כתובות ה-IP. במסגרת הפרוטוקול החדש ניתן להקצות כ-340 טריליון טריליון כתובות אינטרנט (3.4×10^{38}) ייחודיות, והוא זמין ליישום מאמצע שנות ה-2000.

¹ <http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet>

² בפועל, ניתן לחבר יותר ציודי קצה, בשל היכולת לשתף כתובת IP בין ציודי קצה רבים לצורך חיבורם לאינטרנט, למשל באמצעות הפעלת NAT (Network Address Translation).

במחקר שנערך לצורך כתיבת מסמך זה נמצא כי המומחים תמימי דעים כי בשנים הבאות רשת האינטרנט תעבור ברובה ל-IPv6, עד לדעיכתו המוחלטת של פרוטוקול ה-IPv4. מעבר זה צפוי לבטל המחסור בכתובות IP מגרסה IPv4, אשר חונק את התפתחות האינטרנט והתחרותיות בה, ופוגע בחווית השירות של המשתמשים השונים. בנוסף, אימוץ IPv6 עתיד לסייע בקידום התפתחויות טכנולוגיות משמעותיות ובראשם לאפשר פרישת סנסורי IoT – Internet of Things, המחייבים כמות גדולה ביותר של כתובות IP ייחודיות.

מנגד, המחקר מצא כי המעבר לשימוש בפרוטוקול IPv6 אינו פשוט ומהיר, ועשוי להתארך לכדי יותר מעשור. לצד זאת, הקושי העיקרי עימו יש להתמודד כדי להטמיע את הפרוטוקול החדש הוא התנגדותם של בעלי עניין רבים, משיקולים כלכליים, כמו גם משיקולים נוספים דוגמת סיבוכיות ניהול רשתות התקשורת, וסוגיות אבטחת מידע וסייבר. **מסיבות אלה, המשותף למרבית המדינות שהתקדמו באימוץ הפרוטוקול הוא מעורבות כלשהי של המדינה/רגולטור בתחום.**

על פי ממצאי המחקר, מדינת ישראל טרם החלה בביצוע צעדים לאימוץ פרוטוקול IPv6 (הגם שמשרד התקשורת החל לבחון הנושא) ומשתרכת מאחור ביחס למדינות אחרות בעולם, אשר זיהו במעבר מנוע צמיחה פוטנציאלי של המשק. זאת ועוד, למרות שקיימים גופים רבים שיכולים לסייע לקידום הנושא בישראל ובהם גופי הממשלה, ספקי התקשורת, גופי האקדמיה, חברות מסחריות והציבור - לא התקיימה עד לאחרונה כל יוזמה מרכזית בנושא, וניכר בבירור העדר עניין משמעותי בנושא של רוב השחקנים המרכזיים במגזרים הציבוריים והעסקיים. זאת, באופן שעלול לפגוע ביכולת של ישראל להמשיך לעמוד בחזית הטכנולוגיה והחדשנות העולמית, ומעמיד אותה כבר עתה בנחיתות למול מדינות אליהן היא משווה עצמה.

מסמך זה נכתב על ידי איגוד האינטרנט הישראלי (ע"ר) במטרה לבחון ולשקף את סטטוס מימוש פרוטוקול IPv6 בישראל, להמליץ על מדיניות ותהליכים אשר נדרשים להטמעתו באופן מוצלח ומהיר במרחב האינטרנט הישראלי, ולהניע תהליכים אלה.

להלן עיקרי ההמלצות של איגוד האינטרנט הישראלי:

איגוד האינטרנט הישראלי ממליץ כי קובעי המדיניות בישראל יכירו במעבר ל-IPv6 כיעד לאומי, ובתאם יקבעו תוכנית אסטרטגית רב-שנתית להשלמת המעבר. האיגוד ממליץ שהתוכנית תקבע יעד ביניים של העלאת השימוש ב-IPv6 בישראל ל-40% מכלל תעבורת האינטרנט בישראל עד שנת 2022, והשלמת ההטמעה (100%) תוך כעשור. להחלטה זו תהא השפעה דרמטית על מוכנותו של המשק הישראלי לפיתוחים הטכנולוגיים המרכזיים באינטרנט.

איגוד האינטרנט הישראלי ממליץ להקים כוח משימה (task force) מאוחד לקידום פרישת IPv6 בישראל. האיגוד ממליץ שבראשות כוח המשימה יעמוד נושא משרה בכיר בשירות המדינה, כגון מנכ"ל משרד התקשורת או ראש מערך הסייבר הלאומי, ותפקידו יהיה:

- להוציא לפועל את התוכנית הלאומית למעבר ל-IPv6;
- לנטר ולמדוד את התקדמות התהליך על ידי כלל השחקנים במשק;
- להוות מוקד ידע עבור המשק הישראלי בנושא.

עוד ממליץ האיגוד שכוח משימה זה ידווח לוועדת המדע והטכנולוגיה של הכנסת על בסיס עיתי על אודות התקדמות התוכנית.

איגוד האינטרנט הישראלי ממליץ שהמשרדים והגופים המדינתיים שהם בעלי עניין בסוגיה (ומפורטים במסמך) יגבשו מסמך מדיניות בתחומם עד 31 דצמבר 2018. עוד ממליץ האיגוד שמסמכי מדיניות אלה, יחד עם התוכנית האסטרטגית שתגובש, ירוכזו למסמך אחוד שישמש כמסמך אב לאומי לתהליך.

איגוד האינטרנט הישראלי ממליץ שהגישה הבסיסית לתהליך תהיה הסדרה עצמית של השוק הפרטי, ולשם כך האיגוד ממליץ למשרד התקשורת ו/או כוח המשימה הלאומי לתכנן מנגנון שישלב בין רגולציה (רזה) לתמריצים לשוק הפרטי. זאת, תוך העברת כלל השירותים הממשלתיים לפרוטוקול IPv6.

תוכן עיניינים

1.	תקציר מנהלים.....	3
2.	פרוטוקולי האינטרנט IPv4 ו-IPv6.....	9
א.	מהו פרוטוקול האינטרנט ולשם מה הוא נועד?.....	9
ב.	פרוטוקול IPv4.....	10
(1	היסטוריה.....	10
(2	מגבלת הכתובות בפרוטוקול IPv4.....	11
(3	תמונת מצב כלל עולמית של הקצאת כתובות IPv4.....	12
(4	הרחבת יכולת השימוש בכתובות IPv4 באמצעות טכנולוגיית NAT.....	15
(5	תמונת מצב הקצאת כתובות IPv4 בישראל.....	16
(6	צמיחתו של שוק מסחר בכתובות IPv4.....	17
ג.	פרוטוקול IPv6.....	18
(1	יתרונותיו של פרוטוקול IPv6.....	18
(2	גישות למעבר טכנולוגיות מ-IPv4 ל-IPv6.....	19
3.	תמונת תהליכי מעבר ל-IPv6 בעולם.....	22
א.	גישות של המדינות המובילות במעבר ל-IPv6.....	25
(1	אירופה.....	25
(2	צפון אמריקה.....	27
(3	אסיה.....	29
(4	ארגונים בין-לאומיים.....	31
4.	החסמים המונעים מעבר לשימוש ב-IPv6.....	32
א.	רשת רב-ציידית רבת גורמים.....	32
ב.	מרכיבי העלויות של מעבר ל-IPv6.....	33
(1	רשת כפולה.....	33
(2	מנהור (Tunneling).....	34
(3	הכשרות והסבות.....	34
(4	עסקים קטנים.....	34
ג.	סיכונים טכנולוגיים.....	35
(1	דו-קיום בין שתי הגירסאות.....	35
(2	המשכיות השירות.....	35
(3	סיכוני אבטחת מידע.....	36

36.....	האם ניתן להמיר את כל כתובות האינטרנט ביום אחד?	ד.
36.....	האם יש צורך בתקינה אחידה לשלב המעבר?	ה.
37.....	תמריצים מוכחים למעבר ל-IPv6	5.
37.....	רגולציה	א.
37.....	תחרות	ב.
38.....	העצמת הפעילות של חברות גלובליות	ג.
38.....	פגיעות לאיומי סייבר	ד.
38.....	ROI (החזר השקעה)	ה.
39.....	מפת בעלי העניין הרלוונטיים להטמעת IPv6 בישראל	6.
39.....	ממשלה	א.
39.....	1) משרד התקשורת	
40.....	2) מערך הסייבר הלאומי	
41.....	3) רשות התקשוב הממשלתי	
41.....	4) חשב כללי	
42.....	5) משרד הבטחון	
42.....	6) משרד הכלכלה	
43.....	7) רשות החדשנות	
43.....	8) המיזם הלאומי "ישראל דיגיטלית"	
44.....	9) הרשות להגנת הפרטיות (לשעבר רמו"ט)	
44.....	ב. כנסת	
44.....	1) ועדת מדע וטכנולוגיה	
45.....	2) ועדת הכלכלה	
45.....	ג. מגזר עסקי	
46.....	1) ספקי התשתית הפיזית	
47.....	2) ספקי הגישה לאינטרנט (ISP)	
49.....	3) ספקי התשתית והגישה הסלולריים	
50.....	4) ספקי ציוד תקשורת	
51.....	5) ספקי תוכן ישראלים	
51.....	6) חברות גלובליות	
52.....	7) מגזר שלישי - איגוד האינטרנט הישראלי	

53.....	סיכום – תמונת מצב שימוש ומעבר ל- IPv6 בישראל	ד.
56.....	מדיניות מוצעת לקידום והטמעת IPv6 בישראל	7.
56.....	הגדרת המעבר ל- IPv6 כיעד לאומי בתחום התקשורת בישראל	א.
56.....	הקמת כוח משימה (Task Force) לאומי	ב.
58.....	אימוץ גישה המשלבת בין הסדרה עצמית לרגולציה רכה	ג.
58.....	מדיניות לאומית רב מימדית	ד.
58.....	1) משרד התקשורת	
59.....	2) מערך הסייבר הלאומי	
59.....	3) הרשות לאבטחת מידע	
60.....	4) הממונה על התקשוב הממשלתי	
60.....	5) הרשות לחדשנות	
60.....	6) ישראל דיגיטלית	
60.....	7) הרשות להגנת הפרטיות	
61.....	ה. איגוד האינטרנט הישראלי	
63.....	נספח א' - טבלת מדינות מובילות בהקצאת IPv6	
67.....	נספח ב' - הקצאת כתובות IPv4 בחלוקה לאזורים	
69.....	נספח ג' - שיטות טכנולוגיות עיקריות להמרה מפרוטוקול IPv4 לפרוטוקול IPv6	
70.....	נספח ד' - מקורות מידע נוספים להרחבה	

2. פרוטוקולי האינטרנט IPv4 ו-IPv6

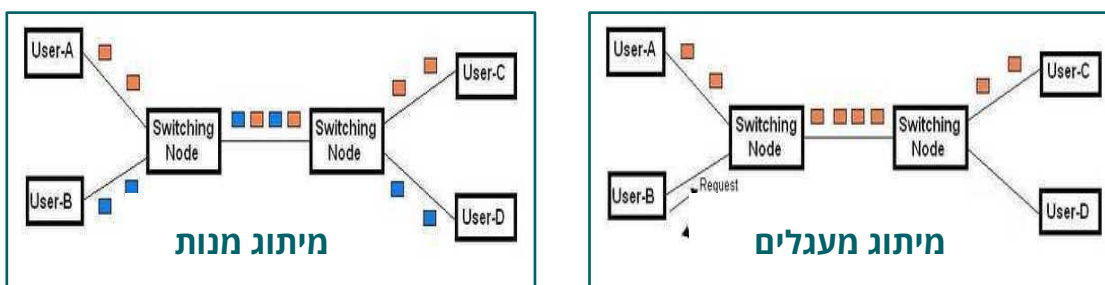
רוב האוכלוסייה אינה מבינה את המשמעות של פרוטוקול האינטרנט וחשיבותו לפעולתה של המרשתת (להלן, אינטרנט). ללא פעולה תקינה של פרוטוקול זה לא ניתן להעביר מידע, לבצע מסחר אלקטרוני, לשחק משחקי מחשב וליהנות מהתועלות הרבות של האינטרנט. אילולא פרוטוקול האינטרנט, האינטרנט לא היה עובד!.

א. מהו פרוטוקול האינטרנט ולשם מה הוא נועד?

בתחילת דרכה של תקשורת המחשבים, על מנת להעביר מידע ממחשב אחד למשנהו נדרש חיבור פיזי ישיר בין המחשבים. ככל שהתרבו המחשבים, הרצון לקישוריות בין המחשבים יצר בעיות בהעברת המידע באופן פיזי. פיתוח פרוטוקול התקשורת, העומד בבסיסה של האינטרנט היווה, קפיצה משמעותית ומהותית ליכולת תקשורת בין-מחשבתית והעברת מידע.

התפתחות זו נולדה על בסיס תיאורית העברת חבילות מידע אשר ידועה בשם מיתוג מנות (Packet switching), שהוצעה במקום תהליכי העברת מידע באופן ישיר הידועים בשם מיתוג מעגלים (circuit switching). טכניקת מיתוג המנות מאפשרת העברת מידע ממחשב אחד לאחר ללא חיבור פיזי ישיר בין המחשבים, באופן שכל חבילת מידע ("מנה") המועברת ממחשב אחד מכילה את הכתובת של המחשב הנמען.

איור 2.1: הדגמה של ההבדל בין מיתוג מעגלים למיתוג מנות



לקוח מתוך RF Wireless World

בשיטה זו, ניתוב המידע ברשת התקשורת (routing) מתבצע בהתאם לאלגוריתמים שיוזעים כיצד ולכן לנתב את המידע. המנה מכילה, לבד מהמידע אותו היא נדרשת להעביר, מידע נוסף כגון כתובת המקור, כתובת היעד, מספרה הסידורי של המנה ונתוני בקרה, כך שהרשת תוכל לנתב את המנה ליעד הנכון. לא כל המנות המרכיבות הודעה אחת יעברו בהכרח באותו מסלול

בדרך מהמקור ליעד, אולם המחשב המקבל את המידע יידע לחבר אותו בסדר הנכון כדי שיתקבל בשלמותו.

רשתות הפועלות בשיטת מיתוג מנות בנויות בטופולוגית אריג (Mesh). טופולוגית אריג כוללת צמתים רבים שדרךם העברת המידע תנוטב בסופו של דבר אל היעד. יכולת הגיבוי של התשתיות המובנית במתאר זה, מאפשרת אמינות גבוהה ביותר של העברת המידע.

בהיבט הטכנולוגי, מיתוג המנות מוגדר בשכבה הרביעית (שכבת תעבורה) של מודל 7 השכבות OSI (Open System Interconnection). בשכבה השלישית (שכבת הרשת) נוספות למנות תגיות הנקראות Header, ובהן מצוינות, כאמור, כתובות המקור והיעד ופרטים רלוונטיים אחרים.

איור 2.2: מודל שבע השכבות OSI



הגרסה הראשונה של פרוטוקול זה נקראת פרוטוקול גרסה 4 (IPv4), והיא זו העומדת בבסיס האינטרנט כפי שאנו מכירים ומשתמשים בה היום.

ב. פרוטוקול IPv4

(1) היסטוריה

בסוף שנות ה-60 של המאה הקודמת נוצר הצורך לקשר רשתות שונות של גופים שונים, בעיקר אוניברסיטאות ומרכזי מחקר, להעברת מידע ביניהם. בהתאם, הסוכנות לפרויקטי מחקר מתקדמים, ARPA (Advanced Research Project Agency), ארגון השייך לממשלת ארה"ב, החלה לפתח, החל משנת 1968, רשת בשם ARPANET, אשר הדרישות הבסיסיות בהן התבקשה לעמוד היו יכולת להעברת קבצים, התחברות מרחוק ושימושי דואר אלקטרוני. בבסיס הטכנולוגיה של הרשת שפותחה עמד פרוטוקול בקרת רשת (NCP Network Control Protocol), שהיווה הבסיס לפיתוחו של הפרוטוקול המוכר כיום ברשת האינטרנט

TCP/IP (Transmission Control Protocol). השימוש הראשון של ARPANET בפרוטוקול זה היה בשנת 1971.

בשנת 1973 החל פרוייקט לפיתוח פרוטוקולי שכבת רשת חדשים. הדרישות שאופיינו לפרוטוקולי השכבה כללו: עצמאות של טכניקות רשת בסיסיות ומבנה מבוסס ארכיטקטורה של קישוריות אוניברסלית בכל רחבי הרשת, מקצה לקצה. בשנת 1981 נקבע הפרוטוקול הסטנדרטי הראשון שנקרא - TCP/IP⁴, עליו מבוססת האינטרנט, כפי שמוכרת לנו, וככל הנראה רוב רשתות התקשורת בעולם כיום.

2) מגבלת הכתובות בפרוטוקול IPv4

פרוטוקול IPv4 מורכב מסדרה של 32 ספרות של אפס (0) ואחד (1), כאשר כל ספרה נקראת סיבית (bit). כתובת IPv4 מכילה שילובים שונים של 32 הביטים, ועל כן IPv4 מאפשר כ-4.3 מיליארד כתובות אפשריות³. לשם הנוחות, מקובל לייצג ערך זה כארבעה מספרים עשרוניים. כל אחד בין 0 ל-255⁴. מספרים אלה נקראים אוקטטים⁵, כיוון שגודל כל אחד מהם הוא 8 סיביות. לדוגמה - 192.168.0.1 הוא הייצוג הנפוץ של הכתובת הבינארית - 10000001 00000000 00000000 10101000.

מכיוון שטווחים מסויימים של כתובות במסגרת הפרוטוקול שמורים למטרות מיוחדות, מספר הכתובות השמישות בפועל קטן יותר, ועומד על כ-4 מיליארד כתובות. כמות כתובות זו, בראשית השימוש באינטרנט, נשמעה רבה ומספקת לכל השימושים, אך ברבות השנים נוצר מחסור בכתובות ברמה העולמית. זאת, בעיקר עקב ההחלטה לפתוח את האינטרנט לשימוש של כלל המגזרים בעולם ולכלל האוכלוסייה (כזכור, בתחילה הרשת נועדה לצרכים מקצועיים בלבד), ההתקדמות הטכנולוגית המשמעותית וחיבור מגוון רחב ורב של ציודי קצה לאינטרנט, כגון מחשבים ניידים, מחשבים ניידים, טלפונים סלולריים, מחשבי כף יד, אביזרי ניווט, שעונים, אביזרי צילום וכד'.

³ מספר הכתובות האפשריות הינו - $2^{32}=4,294,967,296$.

⁴ $2^8=256$.

⁵ הוא שם לקבוצה הבנויה משמונה מרכיבים.

3) תמונת מצב כלל עולמית של הקצאת כתובות IPv4

הקצאת כתובות האינטרנט מנוהלת ברמה העולמית על ידי ארגון IANA, תחתיו קיימים 5 ארגוני גג איזוריים למרשם והקצאה RIR (Regional Internet Registry) המחולקים לחמישה אזורים גיאוגרפיים עולמיים:

1. RIPE NCC – כולל את מדינות אירופה וחלקים מהמזרח התיכון, ובתוכם ישראל.

2. ARIN – כולל את מדינות צפון אמריקה.

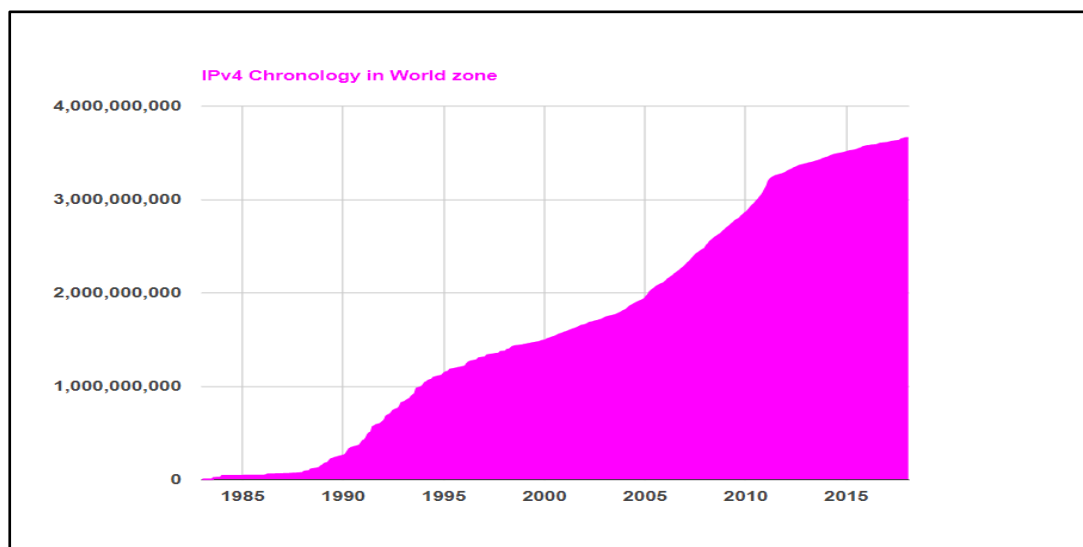
3. LACNIC – כולל את מדינות אמריקה הלטינית, אזור האיים הקריביים ודרום אמריקה.

4. APNIC – כולל את מדינות אסיה ואוקיאניה (ובכלל זאת אזור אוסטרליה וניו זילנד).

5. AFRINIC – כולל את מדינות אפריקה.

כפי שניתן לראות מהגרף הבא, ⁶ הזינוק בכמות הכתובות מסוג IPv4 המוקצות ברמה העולמית בעשור הראשון של המאה ה-21 יצר מצב שבו כמות הכתובות שנותרה להקצאה היא מוגבלת ונמצאת לפני סיום.

איור 2.3: קצב חלוקת כתובות IPv4 ברמה העולמית



⁶ Internet Assigned Numbers Authority - IANA. רשות הקצאת הכתובות / מספרים העולמית. <http://www.iana.org>

⁷ http://www-public.tem-tsp.eu/~maignon/RIR_Stats (הנתונים מעודכנים לחודש פברואר 2018). פירוט הגרפים בחלוקה לאזורים השונים (RIR) מצוי בנספח ב'.

עוד מעניין לראות, שחלוקת ההקצאות של כתובות IPv4 אינה מאוזנת בין אזורי העולם השונים⁸:

טבלה 2.1: כמות כתובות IPv4 בחלוקה ל-RIR העולמיים

RIR	כמות כתובות בשימוש	אחוז ההקצאה מכלל הכתובות
AFRINIC	106,598,912	2.91%
APNIC	873,107,456	23.87%
ARIN	1,679,236,096	45.91%
LACNIC	187,069,184	5.11%
RIPE NCC	811,796,536	22.19%
סה"כ עולמי	3,657,808,184	100.00%

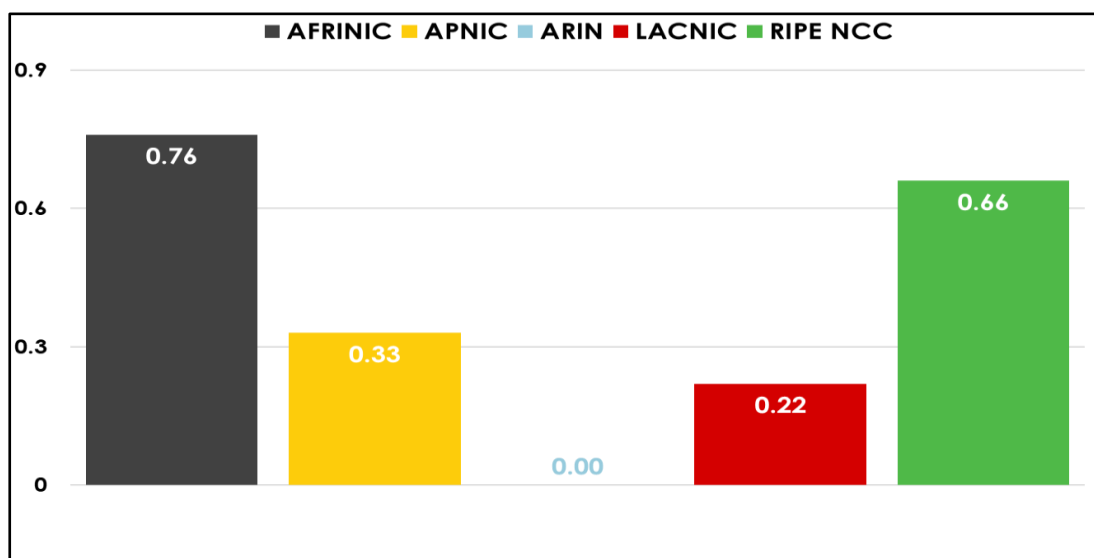
המשמעות העולה מנתונים אלה היא כי נכון לחודש פברואר 2018 הוקצו מעל 3.6 מיליארד⁹ כתובות, מתוך המשאב של כ-4 מיליארד כתובות אפשריות. כלומר, ניצול של כ-90% מהכתובות. יתר על כן, IANA הקצתה לכל הארגונים האזוריים (RIR) את יתרת כתובות IPv4 העולמית כבר בחודש מאי 2014 ולפיכך **לא נותרו כתובות פנויות לחלוקה ברמה העולמית**. מנתונים שנאספו על ידי NRO¹⁰ (ואשר מוצגים בגרף להלן) עולה כי המאגר הגדול ביותר של כתובות IPv4, שטרם הוקצו ברמה האזורית, נותרה בידי הארגון של מדינות אפריקה, לאחר מכן אירופה, אסיה ואוקיאניה, ודרום אמריקה. ארה"ב נותרה ללא יתרת כתובות להקצאה.

⁸ שם.

⁹ נכון ל-19 בפברואר 2018 מוקצות 3,657,808,184 כתובות מסוג IPv4.

¹⁰ Number Resource Organization – NRO. (www.nro.net). נכון לחודש דצמבר 2017.

איור 2.4: כמות הכתובות הפנויות להקצאה באזורי RIR העולמיים (במיליונים)

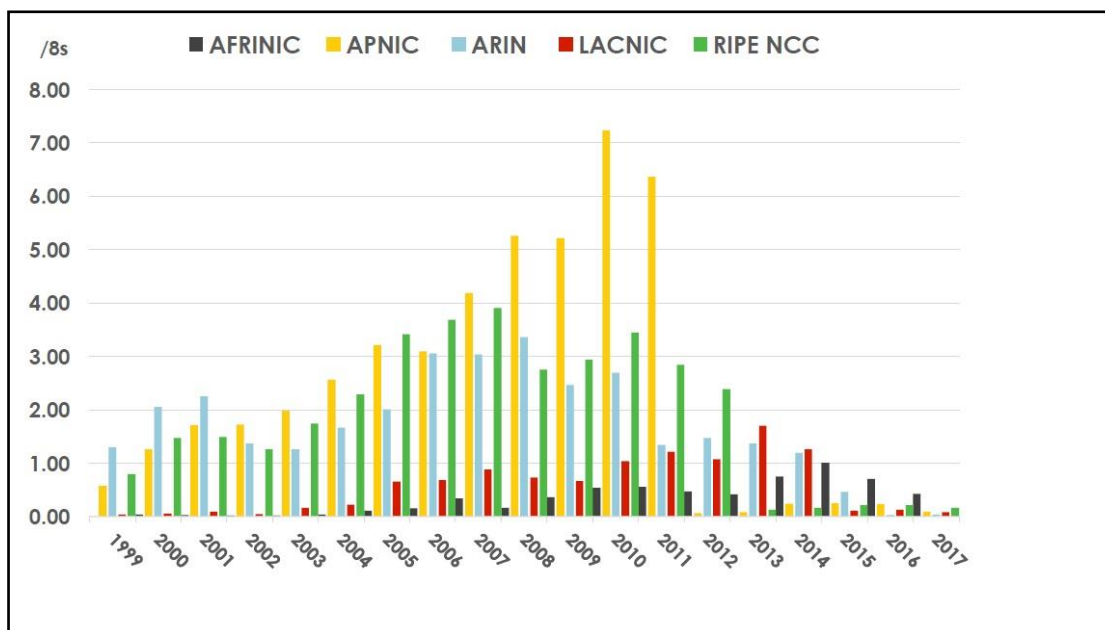


קצב הקצאת כתובות האינטרנט למדינות אסיה, בעשור הראשון של המאה ה-21 היה בעל הגידול הגבוה ביותר. בעשור השני של המאה ה-21 נצפה גידול בקצב הקצאת הכתובות למדינות אפריקה, אף כי עדיין בהיקפים נמוכים משמעותית מאזורים אחרים (ראו הגרף להלן)¹¹. זאת, באופן שמשקף, לכאורה, עלייה משמעותית בכמות השימושים באינטרנט במדינות המתפתחות. יש לציין, עם זאת, שהנתון של היקף הקצאת כתובות IPv4 על ידי ה-RIR אינו תואם בהכרח את היקף היישום של הכתובות בפועל. כלומר, אם מדינה כלשהיא קיבלה הקצאה גדולה של כתובות, אחוזי היישום שלה וההטמעה אינם בהכרח הגבוהים ביותר. באותו הקשר, לאחרונה החלו ה-RIR לבדוק את השימוש בפועל בכתובות, לאור תלונות על סחר בכתובות IPv4 והמחסור בהן.¹² גם בישראל התפתח שוק כתובות משני ועל כך יורחב בהמשך.

¹¹ מתוך נתוני מחקר של חברת NRO.

¹² כל גוף הנדרש להקצאת כתובות (ספק אינטרנט, חברה פרטית וכד') יכול לפנות ל-RIR האזורי, ולבקש שיקצה לו כתובות. באופן עקרוני, ניתן אף לקבל הקצאת כתובות גדולה יותר מצורכי הגוף המבקש.

איור 2.5: קצב הקצאת כתובות IPv4 לאזורים השונים



4) הרחבת יכולת השימוש בכתובות IPv4 באמצעות טכנולוגיית NAT

מאחר שהמחסור בכתובות IPv4 היה ידוע לקהילת האינטרנט מבעוד מועד, נעשו מספר מהלכים על מנת לטפל במשאב שבמחסור. לאורך השנים, הומצאו פתרונות שמטרתם להקטין ולצמצם את התלות בכתובות IP. הפתרון השכיח ביותר להתמודדות עם מחסור כתובות היא טכנולוגיית ה-NAT (Network Address Translation). טכנולוגיית ה-NAT מתמקמת בין הרשת הפנימית של ארגון והחיבור שלו לאינטרנט, ומקצה ברשת הפנים ארגונית לכל מחשב כתובת IP פנימית שאינה ייחודית¹³, אולם כאשר המחשב יוצא לאינטרנט, הוא מקבל כתובת IP חיצונית מתוך המאגר שהוקצה לארגון. בתהליך אופטימיזציה זה, ארגון יכול לאפשר גישה של כמות גדולה של ציוד קצה לאינטרנט, תוך שימוש במאגר מוגבל של כתובות IPv4¹⁴. באופן זה, נחסכות כתובות IP שמקושרות אל עולם האינטרנט. טכנולוגיית ה-NAT משמשת גם כ"גישור" בין פרוטוקול IPv4 לבין IPv6, כפי שיורחב בהמשך.

פתרונות נוספים שנועדו להתגבר על המחסור בכתובות IPv4 כוללים, בין היתר:

¹³ כלומר, יכולה להיות כתובת פנימית זהה בארגונים שונים, שכן ההבחנה בין הכתובות מתבצעת ברמת הארגונים, להם כתובות שונות.

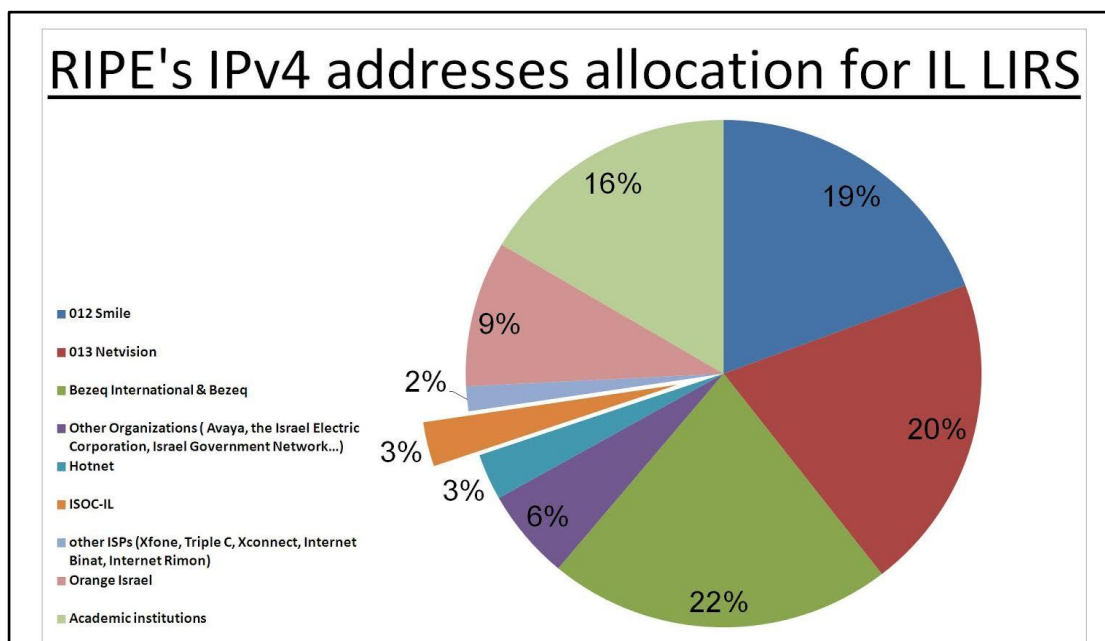
¹⁴ אך כמות ציודי הקצה שיוכלו לעשות שימוש באינטרנט בו זמנית תהא מוגבלת למאגר כתובות ה-IPv4 שהוקצו לארגון.

- רשת פרטית - מאפשרת שימוש בחיבורים רבים בתוך הרשת, ללא כתובת, אך כל יציאה לאינטרנט מחייבת לעשות שימוש בכתובת השער. שיטה זו נפוצה בחיבורים ביתיים.
- שרת מארח וירטואלי - מאפשר לעשות שימוש בכתובת השרת המארח.
- DHCP (Dynamic Host Configuration Protocol) - פרוטוקול תקשורת המשמש להקצאה של כתובות IP ייחודיות למחשבים ברשת מקומית (LAN).

5) תמונת מצב הקצאת כתובות IPv4 בישראל

הקצאת כתובות האינטרנט לארגונים במדינת ישראל נעשית כאמור על ידי RIPE NCC (הארגון האירופאי). נכון לחודש נובמבר 2015 הוקצו על ידי RIPE ל-LIR (הארגונים המורשים להחזיק בכתובות ולמוכרם) הישראליים כ- **91 אחוזים מכלל ההקצאה של כתובות מסוג IPv4 לישראל**. מרבית כתובות ה-IPv4 שמוקצות לישראל מחולקות לספקיות האינטרנט הוותיקות והגדולות בשוק הישראלי (בזק בינלאומי, נטוויז'ן ו-012 smile אוחזות בכ- 61% מכלל ההקצאות לישראל), כ- 16% מוקצים לישויות אקדמאיות דרך מרכז החישובים הבין-אוניברסיטאי (מחב"א), 6% מוקצים לחברות מסחריות ו-3% מוקצה לאיגוד האינטרנט הישראלי.

איור 2.6: הקצאת כתובות IPv4 ל-LIR הישראליים



כמו ברמה העולמית, גם מאגר כתובות IPv4 הישראליות הפנוי להקצאה מצוי לפני סיום. אמנם, יש לזכור כי לא ניתן לדעת מהו השימוש בפועל בכתובות המוקצות על ידי ה-LIR הישראליים השונים, אך לאיגוד האינטרנט הישראלי מגיעות מדי פעם פניות של גורמים חדשים בשוק בבקשה לרכוש או לקבל כתובות, ועל העדר היכולת לקבל הקצאות גדולות

של כתובות, שהן משאב קריטי לפעילותם. זאת, באופן שבולס את התפתחותם, כמו גם את התפתחותם של ספקי גישה לאינטרנט.

6) צמיחתו של שוק מסחר בכתובות IPv4

הנתונים שפורטו לעיל על אודות היקף כתובות ה-IPv4 הפנויות מלמדים כי כמות כתובות האינטרנט שטרם נוצלה תחת IPv4 הולכת ומצטמצמת. כמו בכל שוק בעולם בו קיים משאב במחסור, החל להתפתח מסחר משני בכתובות מסוג IPv4 על ידי מי שקיימת לו הקצאה של כתובות מסוג IPv4 שאינה נדרשת לו לצורך פעילותו הישירה, למי שנמצא בחוסר¹⁵.

כך, אף שהיסטורית, המסחר של כתובות אינטרנט IPv4 היה אסור על מי שהוקצו לו כתובות ומוגדר כ-LIR (כגון ספקיות האינטרנט או חברות שנרשמו ככאלה)¹⁶, הרי שעם הגידול בביקוש ובהעדר יכולת אמיתית של ה-RIR לוודא כי הכתובות אכן נדרשות ל-LIR לצורך פעילותו, הותר על ידי גופי ה-RIR ל-LIR לסחור משנית בכתובות שהוקצו להם, תחת השגחתם של ה-RIR. מגמה זו קיימת גם בישראל וכיום המחיר המקובל לכתובות IPv4 בישראל עומד על כ-10-12 דולרים לכתובת וככל שהזמן חולף מחיר זה עולה¹⁷.

אמנם, במובן הכלכלי הצר של השוק, הוא ככל הנראה יעיל ומתמחר את המוצר במחסור על פי ההיצע והביקוש שלו. ברם, מלבד השאלה היסודית האם נכון שיתקיים שוק ניהול כתובות אינטרנט, עלינו לתהות מה המשמעויות הנלוות לקיומו של השוק הזה למשק הישראלי?

א) במישור הטכנולוגי - העולם מתקדם בקצב מהיר לכיוון של היפר-קישוריות, בה כל מכשיר או מוצר יחובר לאינטרנט במתאר הידוע בשם IoT (Internet of Things), קישוריות בין משתמשים (Peer to Peer) וקישוריות רציפה (Always On). לכך יש להוסיף את ריבוי היישומונים (אפליקציות) והשימושויות שלהם בעתיד הקרוב, בעיקר בקישורים הרבים שבין מחשבים. יישומונים רבים "מדברים" ומסתנכרנים האחד עם השני, כך שהם דורשים חיבוריות קבועה (דוגמא לכך הינם שירותי רפואה, שירותי חירום ושירותי ייצור תעשייתיים). שימוש בטכניקות שונות של מיצוי מרחב הכתובות של IPv4, כגון NAT, מקשים מאוד על קישוריות זו, קל וחומר על הרחבתה בעתיד.

ב) במישור הכלכלי - קיומו של שוק משני למסחר בכתובות IPv4 הנשלט בידי מעט שחקנים מונע כניסתם של שחקנים חדשים, הנאלצים במקרה הטוב לשלם סכומי כסף גבוהים

¹⁵ חברות בולטות של מסחר בכתובות IPv4 הן addrex, I-accuro.

¹⁶ העברה של כתובות היתה מותרת ל-RIR בלבד. לכאורה, כל LIR שקיבל הקצאת כתובות ולא ניצל אותן, אמור להחזיר את ההקצאה ל-RIR.

¹⁷ עלית המחיר הנצפית מעידה כאלף עדים על היות מאגר הכתובות במחסור.

לרכישת כתובות IPv4 ובמקרה הפחות טוב, נמנעת מהם עצם האפשרות לרכוש כמות מספקת של כתובות לשימושם. כך גם נמנעת האפשרות לפתח שווקים חדשים לחלוטין. (ג) במישור הציבורי/אזרחי - ספקי שירותי תשתיות ההולכה (infrastructure, כגון בזק והוט בישראל) וספקיות הקישוריות לאינטרנט (ISP- Internet Service Provider), הן ברשתות הנייחות והן ברשתות הניידות, יתקשו לחבר לקוחות חדשים לשירותי הגישה לאינטרנט, כאשר כמות המשתמשים תעלה על כמות הכתובות הניתנות להקצאה. השלכות אלה מחמירות לא רק בצד הקישוריות עצמה, אלא הן יוצרות קשיים גם בצד ניהול הלקוחות, אבטחת המידע, וחווית השירות. כך, אף שלא מוכרים לנו נתונים רשמיים בעניין, סביר שגם העלות הכספית החלופית של הישארות בפרוטוקול IPv4 עלולה להיות גבוהה מאוד (וייתכן שאף גבוהה מעלות המעבר לרשת בפרוטוקול החדש פרוטוקול IPv6).

ג. פרוטוקול IPv6

1) יתרונותיו של פרוטוקול IPv6

באמצע שנות ה-90 של המאה הקודמת, לאחר פתיחת האינטרנט לפעילות מסחרית ותחילת התפתחות שירותי האינטרנט המודרניים, זוהתה "תקרת הזכוכית" של היכולת להקצות כתובות IPv4 וצוות המשימה ההנדסי לאינטרנט IETF (Internet Engineering Task Force) התחיל בתהליך חשיבה שמטרתו לפתור את בעיית המשאב המוגבל של כתובות IP ב-IPv4. הפתרון שנבחר היה גיבוש גרסה חדשה לפרוטוקול שכבת הרשת, וזו סומנה IPv6¹⁸.

ההבדל המהותי בין IPv4 ו-IPv6 נובע מהגדלת מרחב הכתובות המקשרות בין אמצעי המחשוב השונים על גבי רשת העברת נתונים. בעוד ש-IPv4 מכיל 32 סיביות, IPv6 מכיל 128 סיביות, ועל כן כמות הכתובות האפשריות ב-IPv6 היא 2^{128} כתובות. כמות כתובות זו, משמעותה מספר בן 39 ספרות והוא:

340,282,366,920,938,000,000,000,000,000,000,000,000,000 כתובות¹⁹ ייחודיות.²⁰ משום כך, נהוג לומר כי בפרוטוקול IPv6 ניתן להצמיד כתובות IP לכל גרגיר חול ביקום. העולה מכך הוא שיישום IPv6 מאפשר הקצאה מחודשת של כתובות למשך העתיד הנראה לעין

¹⁸ <https://www.ietf.org/rfc/rfc2460.txt>

¹⁹ $10^{38} \times 3.4$ כתובות.

²⁰ באופן פרקטי, השינוי בפרוטוקול יוביל גם לשינוי בתצורת הכתובות. כיום כתובות IPv4 נכתבות בתצורה הבאה: 179.84.135.204. אותה כתובת IP, בתצורתה החדשה תיכתב: ffff:b354:87cc:0:0:0:0:0. לדוגמא, כתובת ה- IPv4 של שרת ה-DNS של חברת Google היא 8.8.8.8, ואילו במעבר ל- IPv6, הכתובת הינה: ffff:808:808:0:0:0:0:0.

ומבטל את הצורך בפתרונות זמניים שהומצאו על מנת להתמודד עם מחסור הכתובות ב-IPv4 כגון NAT, DHCP וכו'.

מלבד הגדלת מרחב כתובות ה-IP, טופלו במסגרת הפרוטוקול החדש נושאים נוספים, אשר משמעותם המרכזית תבוא לידי ביטוי בעתיד בהיבטים של הוספת שירותים חדשניים, אופטימיזציה של השירות באינטרנט והתמודדות עם סוגיות של אבטחת מידע ופרטיות. להלן עיקר השיפורים הנוספים, שמציע פרוטוקול IPv6:

- א. הוספת סוג חדש של כתובת מסוג Anycast, המאפשרת לשלוח מידע אל מרחב כתובות, ולא רק לכתובת בודדת.
- ב. פישוט מבנה הכותרת של הפרוטוקול לעומת IPv4.
- ג. שיפור התמיכה בהרחבות (extensions) לפרוטוקול, כך שתתאפשר הוספת שירותים חדשים בעתיד ביתר קלות.
- ד. הכנסת יכולת של תיוג (labeling) של מנות מועברות, כך שניתן יהיה להגדיר שירותי איכות שירות לפי התיוג.
- ה. הוספת הרחבות ייעודיות לתמיכה במנגנוני הזדהות, אימות מידע ופרטיות במסגרת הפרוטוקול.

2) גישות למעבר טכנולוגיות מ-IPv4 ל-IPv6

מעבר מפרוטוקול IPv4 והכנסת IPv6 לשימוש מחייב יישומו של תהליך מורכב, בעל משמעויות טכנולוגיות, תפעוליות וכלכליות רחבות היקף, אשר דורש בחירה בין חלופות שונות. חלופות אלה, המשמשות כבסיס תכנוני רב-שנתי עבור כלל המדינות המבצעות מעבר לפרוטוקול החדש, הוגדרו על ידי קבוצת העבודה NGTrans²¹. אף אחת מחלופות אלה אינה פשוטה²²,

²¹ קבוצת עבודה שהוקמה על ידי IETF (The Internet Engineering Task Force). לשורה של מסמכים בסוגיה ראה: <https://datatracker.ietf.org/wg/6man/documents/>

²² כאשר עוברים משימוש בפרוטוקול אחד לפרוטוקול אחר עשויות להיווצר בעיית תאימות בין הפרוטוקולים השונים, כך שמידע שפרוטוקול אחד מכיל אינו מובן על ידי הפרוטוקול השני. המפרט הטכני של IPv6 מציג שינויים גדולים ומשמעותיים. לא רק שאורך הכתובת הוגדל ל-128 סיביות, אלא שגם מבנה הכותרות (header format) ואופן העיבוד של המידע שבכותרות עברו שינויים. על כן, המעבר מ-IPv4 ל-IPv6 אינו פשוט, ויש צורך לתקן מנגנונים שיאפשרו דו-קיום ומעבר חופשי בין שתי הגרסאות של פרוטוקולי התקשורת. זאת ועוד, מאחר שמיליארדי אנשים מחוברים כיום לאינטרנט, ומספר גדול אף יותר של מחשבים מארחים והתקנים משתמשים ב-IPv4, אין כלל אחיד שניתן להחיל על תהליך המעבר מ-IPv4 ל-IPv6.

מהירה לביצוע²³ או זולה. סעיף זה יציג את שלוש החלופות,²⁴ תוך הצגה תמציתית של היתרונות והחסרונות שלהן:

א) רשת כפולה (Dual Stack Network)

הרשת הכפולה (Dual Stack Network) הוא פתרון המממש את שני הפרוטוקולים גם יחד, על שרתים ונתבים כאחד. מימוש כזה מאפשר לרשתות לתמוך בשירותים וביישומים בשני הפרוטוקולים בתקופת המעבר, שבמהלכה יופיעו שירותי IPv6 ותגדל זמינותם של יישומים ל-IPv6. ההנחה היא שלאורך זמן ילכו ויתרבו הזמינות והשירותים של פרוטוקול IPv6 עד שפרוטוקול IPv4 ייזנח באופן טבעי. בנוסף, בשל המעבר הממושך וה"טבעי", סביר שיימצאו פתרונות ביניים שיקלו על המעבר בזמן הביניים.

חסרונה המרכזי של שיטת הרשת הכפולה הוא בכך שלכל מחשב ברשת הדו-שכבתית צריכה להיות כתובת IPv4. בכך, למעשה, בזמן הביניים - שיכול להיות ממושך מאוד - ימשיכו להתקיים הבעיות הנלוות לארכיטקטורת הכתובות IPv4 אשר פורטו קודם לכן. חסרון נוסף הוא הצורך בתחזוקת שתי מערכות מקבילות, כך שמידע שעובר בפרוטוקול IPv4 יגיע לציוד קצה שתומך ב-IPv4 ואילו מידע שעובר בפרוטוקול IPv6 יעבור לאותו ציוד קצה שתומך ב-IPv6.

ב) מנהור (Tunneling)

מנהור הוא פתרון ההופך את רשת ה-IPv4 למקשרת בין "ענני IP" - לדוגמה, אפשר לקשר בין רשתות IPv6 נפרדות דרך שירותי רגיל (native) באמצעות מנהרה - כך שמנות מידע (packets) של IPv6 עוברות "אריזה" (encapsulation) בכתב גבול-BR (Border Router) לפני העברתן ברשת IPv4, ואחר-כך הן עוברות "פתיחה" (decapsulation) בנקודת הגבול של רשת IPv6 המקבלת.²⁵ פרוטוקול ISATAP²⁶ (Intra-Site Automatic Tunnel Addressing Protocol) הוא שיטה נוספת המונעת צורך בהגדרת מנהור באופן ידני. שיטה זו גורמת לרשת ה-IPv6 לראות ברשת ה-IPv4 כשכבת חיבור (link Layer), ויוצרת מנהור אוטומטי בין רשתות ה-IPv6.

²³ מספר מחקרים צופים כי תקופת המעבר תימשך עד השנים 2030-2040.

²⁴ פירוט של שיטות טכנולוגיות קונקרטיות להמרה בין הפרוטוקולים ניתן למצוא בנספח ג'.

²⁵ שירותים מסוג "מתווך מנהרה" (TB – Tunnel Broker) מוצעים כדי לנהל אוטומטית בקשות מנהור המגיעות מן המשתמשים ולהקל על תהליך הבנייה. לאפיון השירותים ראו

<https://tools.ietf.org/html/rfc3053>.

²⁶ <https://tools.ietf.org/html/rfc5214>.

היתרון המשמעותי של שיטת המנהור הוא הפסקת הצורך להקצות כתובות IPv4 נוספות. בנוסף, המשך השימוש בארכיטקטורת IPv4 הופך, הלכה למעשה, ל"שקוף" למשתמשי הקצה, אשר מבחינתם עושים שימוש בארכיטקטורת IPv6. בשלבים מאוחרים יותר של המעבר מה-IPv4 ל-IPv6, ניתן יהיה לעשות שימוש במנהור גם כדי לקשר את רשתות IPv4 הנותרות באמצעות תשתית IPv6.

החסרונות המרכזיים של גישת המנהור, מעבר לעלויות האחזקה של שתי מערכות מקבילות (כמו בשיטת הרשת הכפולה), הוא הפוטנציאל לפגיעה בחוויית השירות והזמינות, כמו גם פגיעות רבה יותר לאימי אבטחה.

ג) המרה (Translation)

בעוד ששתי השיטות הקודמות מבוססות על הרעיון שנשמרת לטווח הביניים פעילות עצמאית של שתי הרשתות IPv4 ו-IPv6 (מקבילות בחלופת ה-dual stack ונפרדות בחלופת ה-tunneling), הטכניקה השלישית מבוססת על הניסיון ליצור באופן מיידי רשת אחת באמצעות שימוש במנגנון המרה בין כתובות הפרוטוקולים השונים.

ההמרה נחוצה כאשר מחשב המממש רק IPv6 צריך להתקשר עם מחשב IPv4. במקרה כזה, לכל הפחות, יש צורך להמיר את הכותרת החיצונית, אבל ברור שההמרה תהיה מורכבת יותר אם היישום המחשבי מטפל בכתובות IP בתוכו. למעשה, המרה כזו "יורשת" את מרבית הבעיות האופייניות לממירי הכתובות ברשת IPv4, דוגמת NAT. גישורים ברמת היישום (ALG's²⁷) נחוצים כדי להמיר כתובות IP הכלולות במידע, לחשב מחדש סכומי בדיקה (checksums) וכדומה.²⁸ בדומה לטכניקות המנהור, אפשר לממש את ההמרה בנתבי גבול (BR) ובמחשבים. מערך מורכב זה של טכניקות דו-קיום ומעבר מאפשר "ערבוב ושילוב" בדרכים רבות.

יתרונה הגדול של גישת ההמרה הוא הדרבון שיווצר לכלל השחקנים לעבור וליישם את הארכיטקטורה החדשה, כמו גם צמצום היכולת של שחקנים חזקים לפגוע או לשבש את המעבר. בנוסף, הגישה מצמצמת חלק ניכר מעלויות האחזקה של שתי מערכות במקביל. חסרונה הגדול של הגישה הוא בעלויות ההקמה הגבוהות. בנוסף, בשל בסיס המכניזם של הפרוטוקולים, ניהול הרשתות ומגבלות הזמן של מעבר המנות, המחייבים בניית המנה מחדש. כך, עשויות להיווצר בעיות בעת קצר או שיהוי בהעברת המידע, בהעברה בו זמנית של מנות והדרישה לשימוש ב-DNS (Domain Name System) ככלי למיפוי שמות המתחם (domain names) הקשורים לכתובות.

Application- Level Gateways - ALG's²⁷

²⁸ SIIT ו-PT NAT הן טכניקות ההמרה הרלבנטיות. תערובת של שיטת ההמרה והמודל הכפול, הידועה בכינוי DSTM הוגדרה כדי לענות למקרה של חוסר בכתובות IPv4.

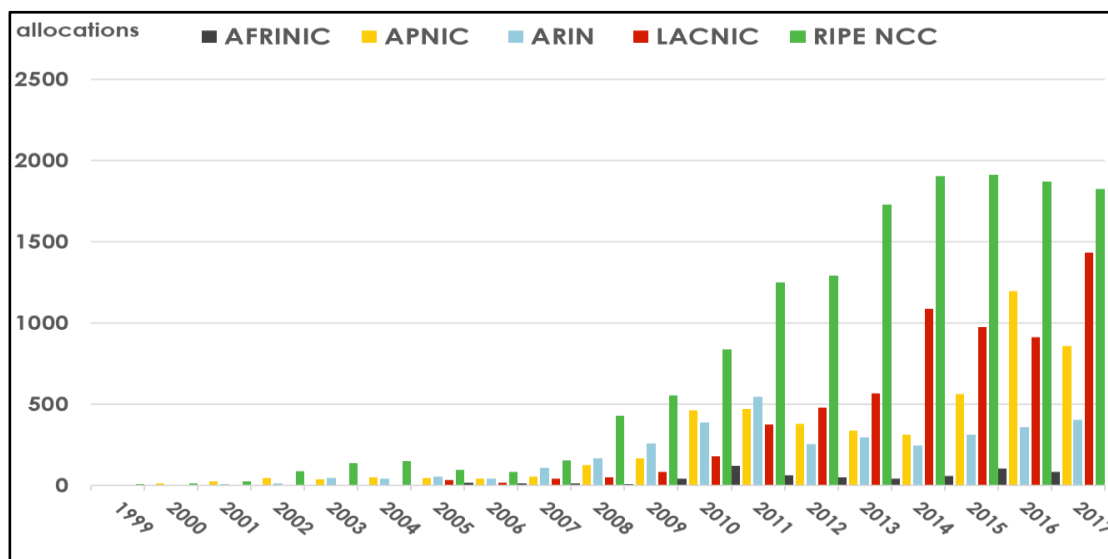
טבלה 2.2: היתרונות והחסרונות של חלופות מעבר ל-IPv6

שיטת ההמרה	יתרונות	חסרונות
הרשת הכפולה (Dual Stack) (Network)	<ul style="list-style-type: none"> חפיפה בין הרשתות, למניעת וצמצום הטעויות. 	<ul style="list-style-type: none"> מחייב השקעות גבוהות. דורש המשך שימוש נרחב בכתובות IPv4 שנמצאות במחסור.
מנהור (Tunneling)	<ul style="list-style-type: none"> לא מחייב שדרוג מלא של הרשת ל-IPv6. קל יחסית ליישום. 	<ul style="list-style-type: none"> אפשרות להשפעה על איכות המעבר. אפשרות שחלק מהיישומים לא יפעלו. יכול ליצור בעיות אבטחה.
המרה (Protocol Translation)	<ul style="list-style-type: none"> הפתרון היחיד שאינו מותיר את פרוטוקול IPv4. עידוד מעבר מהיר של כל השחקנים. 	<ul style="list-style-type: none"> עלות הקמה גבוהה יחסית. לא חף מבעיות טכנולוגיות ובעיות המרה. לא חף מבעיות אבטחה.

3. תמונת תהליכי מעבר ל-IPv6 בעולם

התמונה הכללית העולה מהמידע,²⁹ ובפרט אלו של ארגון ה-OECD, היא כי **המעבר ל-IPv6 נמצא עדיין בשלבים התחלתיים שלו**.³⁰ ישנן בעיות מובנות במבנה הכלכלי של המעבר, בו נדרשת חשיבה לטווח ארוך על ידי גופים שבדרך כלל נדרשים לחשוב לטווח הקצר ולמקסם את שורת הרווח. העדרו של גוף אחד, או קבוצה מוגדרת וקטנה של גופים, שהשפעה עליה תחולל את השינוי מקשה גם היא על התהליך. מצד שני, **המכנה המשותף לכל המדינות בהן תהליך האימוץ של פרוטוקול IPv6 מתקדם יחסית הוא מעורבותו של הממשל/רגולטור ביצירת תמריצים מעודדי מעבר והקמת פורומים או מנגנונים, בהם שותפים בעלי עניין מגוונים, לקידום התהליך.**

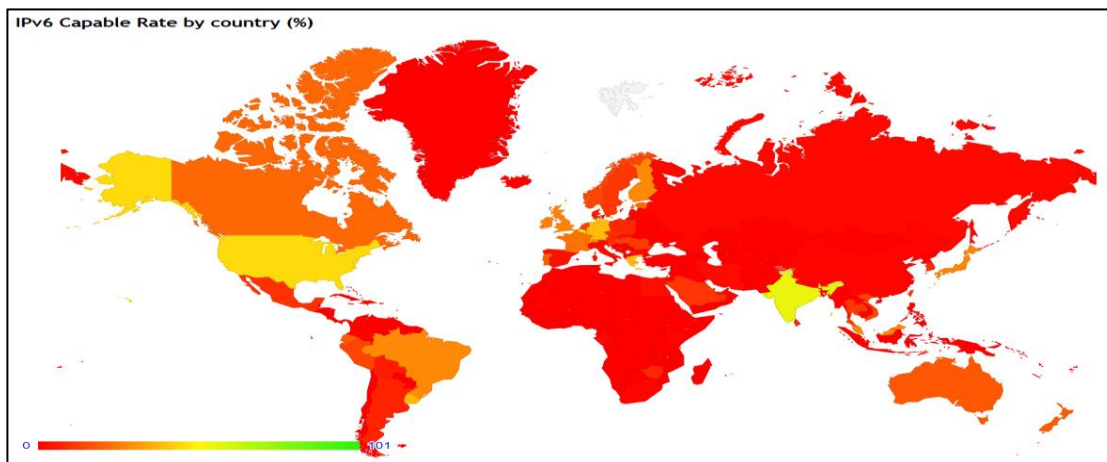
איור 3.1: העלייה בכמות הכתובות מסוג IPv6 המוקצות לאזורים השונים בעולם



²⁹ המידע בנושא מבוסס בעיקר על חברות גלובליות, שתנועת אינטרנט משמעותית עוברת ברשתם כגון Google, Akamai ועוד. נתונים אלה מצביעים רק על התנועה שעברה דרך חברות אלה ולכן התוצאות מוטות.

³⁰ הגרף מתוך [www.nro.net](https://stats.labs.apnic.net/ipv6). המפה מתוך <https://stats.labs.apnic.net/ipv6> (מאי 2018) והטבלה מתוך www-public.tem-tsp.eu/~maignon/RIR_Stats (ינואר 2018).

איור 3.2: מפת אחוז השימוש בפרוטוקול IPv6



טבלה 3.1: כמות כתובות IPv6 שהוקצתה לאזורים השונים

אחוז ההקצאה מכלל הכתובות	כמות כתובות בשימוש	RIR
3.93%	602,866,557	AFRINIC
23.03%	3,535,219,679	APNIC
19.34%	2,969,146,615	ARIN
5.01%	768,674,855	LACNIC
48.70%	7,477,791,887	RIPE NCC
100.00%	15,353,699,593	סה"כ עולמי

מהניסיון שנצבר בעולם עד עתה עולה כי נדרש זמן רב ליישום המעבר ל-IPv6, שנמדד במספר שנים רב. מעורבות התעשייה, ובעיקר חברות גדולות, מסייעת לזירוז התהליך, ומספקת פרנסה לגורמים רבים. הניסיון העולמי מלמד עוד כי המעבר ל-IPv6 הינו מהלך אסטרטגי ארוך טווח ברמת המדינה, המסייע לקידום ועידוד הכלכלה, החברה, הביטחון והתעשייה, כמו גם מאיץ את החיבור של המשק לכלכלה הגלובאלית.

א. גישות של המדינות המובילות במעבר ל-IPv6

בחלק זה נפרט את הגישות המרכזיות בהן נקטו מדינות המדורגות בשיעור חדירה גבוה יחסית של IPv6 (מעל 10%)³¹. ישראל, לשם השוואה מדורגת במקום ה-37 ושיעור החדירה בה מוערך ב-0.183%.

1) אירופה

האיחוד האירופי פעל רבות, מאז תחילת תהליך השקת IPv6 במטרה לאמץ ולקדם את מימושה של ארכיטקטורת IPv6 במרחב האירופי. האיחוד הקים והפעיל פרויקטים רבים, בהשקעה כספית גבוהה (מעל 100 מיליון אירו), שמטרתם הייתה להטמיע IPv6 במדינות החברות, בחברות האינטרנט ובעסקים. כך, לדוגמא, פעלו באיחוד האירופי הפרויקטים 6DISS³², 6NET³³, Go4IT, שמטרתם הייתה לשתף מידע וידע ולבחון חלופות ליישום והטמעה מהירה של פרוטוקול IPv6. בפרויקט האחרון שהוקם, GÉANT³⁴, שותף גם גורם ישראלי – מחב"א.

א) אנגליה

מאז ומעולם, הובילה אנגליה בקידום והתפתחות של טכנולוגיות ורגולציה בשוק התקשורת. רשות התקשורת האנגלית (Ofcom) מהווה לאורך שנים רבות סמן ימני ומודל בכל הנוגע לקידום תחרות, פיתוח טכנולוגי וקידום שוק התקשורת. גם בנושא של הטמעת IPv6 נטל הרגולטור הבריטי יוזמה ואימץ מדיניות של הטמעה והמרה לפרוטוקול החדש.

Ofcom הקימה פורום מקצועי בנושא המעבר ל-IPv6 - UK IPv6 Council³⁵, שמטרתו לקדם את הנושא וחברים בו נציגי התעשייה, הספקים, האקדמיה, חברות ייעוץ וגופים נוספים בעלי עניין. פורום זה הוקם ביולי 2014 והמפגשים העיתיים בו מקדמים את יישום המעבר בבריטניה. בין מובילי הפורום נמצאים ספקי התוכן העיקריים (מיקרוסופט, Facebook, BBC); חברות התקשורת (British Telecom, SKY)

³¹ ראה טבלה בנספח א'.

³² <https://www.6diss.org/>

³³ <https://www.6net.org/>

³⁴ http://www.geant.org/Projects/GEANT_Project_GN4-1/Documents/D3-1_Annual-Compendium.pdf

³⁵ <http://www.ipv6.org.uk>

והאקדמיה (מכון טכנולוגי למחקר). הנושאים שעולים בפורומים השונים נוגעים בקידום המעבר לפרוטוקול החדש; בעיות וסוגיות שנתקלים חברי הפורום בפועל; שיתוף ידע והטווית קשרים.

חברת British Telecom, שהינה מונופול בשוק התקשורת הנייח הודיעה בחודש אוקטובר 2016 ל-UK IPv6 council שכל התשתית שלה עברה ל-IPv6.³⁶ OFCOM מדווחת לציבור בכל שנה על סטטוס ההתקדמות של תהליך המעבר ל-IPv6³⁷, ולאחרונה פרסמה דו"ח מאמץ על סטטוס הקצאת כתובות IPv4 ו-IPv6 בבריטניה³⁸, ממנו עולה כי למרות גידול בהקצאת כתובות IPv6 על ידי LIRs בריטיים, השימוש ב-IPv6 עדיין נמוך מהרצוי. על פי נתוני APNIC, שיעור החדירה בבריטניה עומד על 27.5%.

ד) צרפת

הרגולטור התקשורתי הצרפתי ARCEP שם לעצמו מטרה לקדם את נושא ה-IPv6 באמצעות מסמך מדיניות שכלל, בין היתר, לוחות זמנים ליישום³⁹. בתחילת 2016 נשאלה ARCEP על ידי מזכירת המדינה הצרפתית לנושאים דיגיטליים, כיצד מתקדם יישום המעבר ל-IPv6 בצרפת. השאלה נשאלה מתוך הבנה כי הרגולטור הצרפתי אינו פועל דיו לקדם את הנושא ובכך ייפגעו תחומי הטכנולוגיה (בדגש על ה-IOT), התעשייה והכלכלה הצרפתיים והמשק לא יותאם לעידן החדש ולא תתאפשר הובלה צרפתית בזירה העולמית.

בשנה האחרונה נראית התקדמות משמעותית במעבר לפרוטוקול IPv6 ושיעור החדירה צמח מכ-5% ל-14%. ARCEP השיקה "לוח מחוונים" (Dashboard) שמסייע להבין היכן "צוואר הבקבוק" במעבר של מידע לפרוטוקול IPv6. המידע כולל, בין היתר, מידע על סטאטוס הספקים במעבר לפרוטוקול החדש⁴⁰. גופים נוספים בצרפת מעודדים את המעבר לפרוטוקול החדש באמצעות תקינה רלוונטית שמתאימה רק לפרוטוקול IPv6.

³⁶ <https://www.ispreview.co.uk/index.php/2016/11/bt-broadband-lines-now-support-ipv6-internet-addresses.html>

³⁷ https://www.ofcom.org.uk/_data/assets/pdf_file/0035/95876/CN-Report-2016.pdf

³⁸ https://www.ofcom.org.uk/_data/assets/pdf_file/0020/108128/ip-address-usage.pdf

³⁹ https://www.arcep.fr/uploads/tx_gspublication/rapport-gvt-transition-IPv6-sept2016.pdf

⁴⁰ <https://www.arcep.fr/index.php?id=13169>

ה) בלגיה

הנתונים המפורסמים על ידי APNIC 41 מצביעים כי המדינה בה אחוז התעבורה הגבוה ביותר ב-IPv6 הוא בלגיה – כ-56% (המדינה שלאחריה, הודו מעבירה כ- 51.8% מהתעבורה ב-IPv6 ולאחריה גרמניה - כ-43%).

ישנן כמה סיבות המסבירות נתון זה. הראשונה, נובעת כנראה מהגאוגרפיה של המדינה. בלגיה היא מדינה שטוחה יחסית, אוכלוסייה המונה כ- 11 מיליון תושבים הפרוסים על לא יותר מ- 250 ק"מ בין קצוות המדינה. המדינה מרושתת באופן טוב בתשתיות תקשורת. סיבה נוספת עשויה להיות תרבות של חשיבה ל"טווח ארוך". בנוסף, לבד מחברת התקשורת הגדולה (Proximus, בעבר Belgacom) ישנו מתחרה משמעותי אחד בעל תשתיות כבלים שנקלע למצוקת כתובות IPv4 ולכן המיר את הרשת ל-IPv6.

כמו כן, הוקם פורום לטובת המעבר ל-IPv6⁴² ששלושת ספקי הגישה הגדולים בחרו לשתף עמו פעולה לטובת קידום הנושא. בפורומים האלה, מתכנסים ספקי התשתיות, ספקי התוכן וכל בעלי העניין בשינוי. כל משתתף בפורום משתף את הקשיים, הבעיות, ההצלחות והכשלונות, ומשתף מידע עם אחרים בשינויים הנדרשים לצורך הצלחת המעבר לפרוטוקול החדש.⁴³

2) צפון אמריקה

א) ארה"ב

בארה"ב קמו ארגונים עצמאיים במטרה לקדם את המעבר ל-IPv6, כדוגמת: IPv6 North American Task Force, Forum, אולם עד להתערבות הממשלתית של משרד ההגנה האמריקאי, אימוץ הפרוטוקול לא התקדם. לאחר התערבותו של משרד ההגנה, בו נקבע גם מועד ליישום (2008), החלו הגופים השונים בצפון אמריקה להניע את גלגלי המעבר, בעיקר גופים שעבדו עם משרד ההגנה האמריקאי.

הממשל האמריקאי לא הזרים כסף לקידום הנושא, אלא הודיע כי הוא דורש שהספקים שלו והגופים שאיתם הוא עובד יעברו עד למועד האמור ל-IPv6. גופים רבים ראו בכך הזדמנות לקדם את המוצרים ושירותים שלהם עבור משרד ההגנה, בעילה של מעבר ל-IPv6.

⁴¹ <https://stats.labs.apnic.net/ipv6/>

⁴² <https://www.ipv6council.be/>

⁴³ דוגמא לסטאטוס וסוגיות שהועלו על ידי חברת Proximus – מפעיל ותיק, וחברת VOO – חברת הכבלים ראה: https://www.ipv6council.be/IMG/pdf/02A_PROXIMUS_IPv6_Program_status_20170419.pdf; https://www.ipv6council.be/IMG/pdf/02C_IPv6_at_Voo_2017-pptx.pdf

בשלב מסוים (2004) גם משרד האוצר האמריקאי דרש כי גופים יחלו לעבוד מולו בפרוטוקול החדש. לשם המעבר לפרוטוקול, השקיע סכומי כסף עבור גופי הממשל השונים ובכך התעשייה שמסביב לגופי הממשל נדרשו אף הם לעבור ל-IPv6 על מנת להמשיך ולספק שירותיהם לגופי הממשל.

תוצרי הלוואי של המהלכים הללו גרמו לכך שקמו גופים וארגונים רבים בארה"ב שהתמקצעו בשינוי וצברו ידע מקצועי רב בנושא. גופי תקשורת, כמו: קומקסט (Comcast) אף ניצלו את המעבר ל-IPv6 על מנת לשפר את הביצועים של הרשת שלהם ואת חווית השירות ללקוחות, כתוצאה מהגדלת כתובות ה-IP של לקוחותיהם, כלומר, השינוי פתר בעיה טכנולוגית שהיתה קיימת לחברה. גם חברת Verizon הקימה את רשת הדור הרביעי כרשת תומכת IPv6 באופן מוחלט.

(ו) קנדה

ממשלת קנדה גיבשה מסמך אסטרטגי להטמעת IPv6 בשירותי הממשל בשנת 2012⁴⁴, בו שמה לעצמה כיעד לאומי להנגיש את שירותיה המבוססים על רשת האינטרנט שיתמכו ב-IPv6. לצד זה, פעלה הממשלה הקנדית כל העת להמשיך לשמור על רמת שירות גבוהה מצד גורמי הממשל גם בפרוטוקול הקיים.

במקביל, ממשלת קנדה פעלה מול כל הגופים המעורבים בתהליך, החל משרדי הממשלה השונים, רשויות הממשל (בעיקר על ידי הכוונת המדיניות), דרך שיתוף ממשלות אחרות בעולם, ושיתוף התעשייה, תוך הקפדה על צמצום הסיכונים וצמצום עלויות. התוצרים של מהלך מבוקר זה גרמו לכך שהשווקים שכבר פעלו בפרוטוקול החדש מצאו "שפה משותפת" עם גופי הממשל הקנדיים וכך האיצו את ההתפתחות הטכנולוגית והכלכלית של המדינה; וחווית השירות של האזרחים משירותי הממשל התעצמה.

(3) אסיה

מדינות אסיה היו הראשונות לאמץ את פרוטוקול IPv6, בעיקר בסין, יפן, טאיוון, הונג קונג, דרום קוריאה ומלזיה. במדינות אלה, הממשל הוא זה שתמך במעבר ל-IPv6.

הסיבה העיקרית לאימוץ המוקדם של IPv6 נבע ממחסור בכתובות IPv4 שחוו מדינות אלה. מעבר לכך, ראו מדינות אסיה גם הזדמנות עסקית גדולה בכך שהן היו הראשונות להטמיע את

<https://www.canada.ca/en/treasury-board-secretariat/services/information->

[technology/ipv6-adoption-strategy.html](https://www.canada.ca/en/treasury-board-secretariat/services/information-technology/ipv6-adoption-strategy.html)

הפרוטוקול החדש ובכך ייצרו פלטפורמות מסחריות טכנולוגיות וימכרו אותן בהמשך לשאר מדינות העולם.

(א) הונג קונג

מחלף האינטרנט של הונג קונג הוסב לתמוך בפרוטוקול IPv6 החל משנת 2004. שנתיים מאוחר יותר, החל רשם שמות המתחם בהונג קונג לספק אפשרות לשייך כתובות IPv6 לשמות מתחם (domains). בהתאם לכך, מרבית ספקיות האינטרנט, חוות השרתים המסחריות וספקיות אירוח האתרים מספקות שירותים התומכים בפרוטוקול IPv6.

הממשל ההונג קונגי בוחן מעת לעת את השימוש בפרוטוקול מסוג IPv4 ואת המחסור הצפוי בפרוטוקול זה. במקביל, הוא תומך במעבר לפרוטוקול IPv6 ומבצע פעולות שיסקרו להלן:

- בשנת 2006, באמצעות השימוש ברשת הגישה הממשלתית, הוסבו שירותי הממשל בהונג קונג לתמוך בפרוטוקול IPv6. בחלוף 3 שנים, מעל 200 אתרי ממשל ומעל 60 רשויות ממשלתיות תמכו בפרוטוקול IPv6.
- כמו כן, כל האתרים הממשלתיים, שתומכים בשירותים לאזרח ולמסחר הועברו לפרוטוקול IPv6, ובכך ניתנו שירותים לציבור באמצעות פרוטוקול זה.
- הממשל ההונג קונגי היה שותף בכל הפורומים הבינ"ל (ICANN) והמקומיים (APEC) שדנו בנושאי המעבר לפרוטוקול IPv6 ותרם את תרומתו הרבה מניסיונו ליישום השינויים.
- הממשל ההונג קונגי סייע וליווה את ספקיות האינטרנט וחברות הפיתוח האינטרנטיות (שוק ה-ICT) בהונג קונג למעבר חלק לפרוטוקול IPv6, באמצעות הקמת פורומים מקצועיים.
- בנוסף, מימן הממשל ההונג קונגי את תוכנית "IPv6 in Action!"⁴⁵ שמטרתו היתה ליידיע את העסקים וציבור הצרכנים של האינטרנט על המעבר לפרוטוקול IPv6 ומשמעותיות על כל עסק / בית / ציוד תקשורת שנדרש לבצע המרה לפרוטוקול IPv6.

(ז) סין

הגידול בשימושי האינטרנט בסין היווה את הקרקע הפורייה לאימוץ המעבר ל-IPv6 על ידי גופי הממשל. המחסור בכתובות IPv4 היה ממשי מאד ולכן הממשל הסיני ניצל את ההזדמנות ומעבר להכרח המציאותי, עודד את התעשייה הסינית ללמוד ולייצר שירותים ומוצרים שתומכים בפרוטוקול IPv6 ובכך להפוך את סין למדינה המובילה בידע, בשירותים ובמוצרים שתומכים בפרוטוקול החדש. כך לדוגמא, הקים הממשל הסיני גוף בשם China Next Generation Internet בשנת 2003 שמטרתו היתה שכל השירותים שיינתנו במשחקי האולימפיאדה בבייג'ין בשנת 2008 יתמכו ב-IPv6, החל משירותי התקשורת וכלה במכונות השתייה ברחובות העיר.

ייחוד נוסף לסין הוא העובדה שכל ציודי התקשורת שתומכים ב-IPv6 והוטמעו במדינה הינם תוצרת סין. בכך, כאמור, יצרו הסינים יתרון תחרותי במכירה והפצת השירותים למדינות אחרות בעולם ושיעור ההתפתחות התעשייתית של שוק זה הינו הגבוה בעולם.

(ח) הודו

הכלכלה ההודית, בדומה לכלכלה הסינית צמחה ופרחה אודות להתקדמות הטכנולוגית שהתרחשה במדינה. הגידול הניכר בתעשייה זו, המחסור בכתובות IPv4 שהתרחש והתלות בשימושי אינטרנט, אילצו את הממשל ההודי, בהובלת משרד התקשורת ההודי, לקדם המעבר ל-IPv6.

אחת מחברות התקשורת הגדולות בעולם, TATA, אימצה והטמיעה את פרוטוקול IPv6 ברשתה וכך, בין היתר, היא ממשיכה בהצלחה רבה לגדול לצמח בשוק התקשורת העולמי.

(ט) יפן

הממשל היפני קבע מטרה של יישום והטמעה של פרוטוקול IPv6 במדינה. העובדה המעניינת בשוק היפני היא שהתעשייה אף הקדימה את הממשל. חברת התקשורת הגדולה ביפן, NTT, יישמה את השינוי כבר משנת 2001. רק כעשור לאחר מכן, ספקיות האינטרנט האחרות, כמו גם שאר התעשייה החלו לעבוד בפרוטוקול IPv6.

גם ביפן, בעזרת התמיכה הממשלתית, התעשייה היפנית למדה, פיתחה והטמיעה את הפרוטוקול החדש ורכשה לעצמה ידע וניסיון להובלת השינוי. חשוב לציין כי מהמידע עולה כי שיטות המעבר בין הפרוטוקול IPv4 ל-IPv6 הינן מגוונות, וגם שיטת מנהור וגם שיטת הרשת הכפולה הוטמעו ביפן.

(4) ארגונים בין-לאומיים

OECD (א)

הארגון הכלכלי למדינות המפותחות, ה-OECD, זיהה את החשיבות הכלכלית של מעבר ל-IPv6 במסמך ראשוני שהוכן לקראת ועידת השרים של המדינות החברות בארגון בבירת דרום קוריאה סיאול בשנת 2008.⁴⁶

בשנת 2014 פורסם על ידי הוועדה לכלכלה דיגיטלית של ה-OECD מסמך ניתוח של ההיבטים הכלכליים של המעבר ל-IPv6.⁴⁷ מדובר במסמך חשוב ביותר, אשר מנתח את החסמים הכלכליים המעכבים מעבר לשימוש ב-IPv6, והתייחסות אליו מפורטת בהמשך.⁴⁸

IETF (ב)

ארגון IETF - Internet Engineering Task Force פרסם אף הוא מסמך בשנת 2007 בו הוא זיהה את הבעייתיות של פרוטוקל IPv4 וקרא לפעול ליישום והמרת הרשתות לפרוטוקל החדש.⁴⁹

Internet Society (ג)

איגוד האינטרנט העולמי ISOC⁵⁰ קרא אף הוא לפעול לבצע את ההמרה של הפרוטוקול הישן לחדש. יתר על כן, יזם האיגוד תכנית Deploy360 Programme⁵¹ שנועדה לגשר במעבר בין הפרוטוקולים ולסייע לכל גוף שנדרש לכך. בנוסף, יזם האיגוד "יום עולמי של IPv6" בשנת 2011 ו-2012 במטרה להגביר את המודעות לשינוי הנדרש באינטרנט.

⁴⁶ Economic Considerations in the management of IPv4 and in ,DSTI/ICCP(2007)20/FINAL
Ministerial background report ,the deployment of IPv6

⁴⁷ The Economics of the Transition to Internet Protocol ,DSTI/ICCP/CISP(2014)3/FINAL
version 6 (IPv6)

⁴⁸ ראו פרק 5 להלן.

⁴⁹ <https://tools.ietf.org/html/draft-narten-ipv6-statement-00>

⁵⁰ <https://www.internetsociety.org/what-we-do/internet-technology-matters/ipv6>

⁵¹ <http://www.internetsociety.org/deploy360>

4. החסמים המונעים מעבר לשימוש ב-IPv6

בפרק זה ננסה למפות את החסמים המונעים מעבר לשימוש ב-IPv6.

א. רשת רב-צידיית רבת גורמים

על פי מסמך ניתוח כלכלת המעבר ל-IPv6 של ה-OECD התהליך הוא טיפוסי לפעפוע (דיפוזיה) של טכנולוגיה חדשה, ובמקרה זה הקמתה של פלטפורמת רשת חדשה, ולפיכך מהווה מקרה ייחודי של רשת רב-צידיית מרובת גורמים (multit-sided network). רשת רב-צידיית מתאפיינת בכך שככל שהיא גדלה נוצר "אפקט רשת" המגדיל באופן מעריכי את התועלת לכלל המשתתפים בה. מקובל לטעון כי כדי שרשת רב-צידיית תגדל, נדרש גורם מתווך הנמצא בין כל צידי הרשת, שפעילותו תצית את אפקט הרשת. בהקשר של IPv6, הרשת היא האינטרנט עצמה על כל מרכיבי שרשרת הפעולה והערך שלה (ספקי תשתית, גישה לאינטרנט, טכנולוגיה, תוכן וכד').

על פי הניתוח של ה-OECD, רק הטמעה של IPv6 בכל שרשרת הערך יאפשר את תהליך המעבר אליו וגזירת התועלת הכוללת מכך. לחלק מהמשתתפים בשרשרת הערך, כגון ספקי גישה לאינטרנט וספקי תשתית קל יחסית ליישם IPv6, והם יכולים לראות את הערך בכך אם השותפים האחרים לשרשרת ישתתפו ביישומם. לאחרים, כגון ספקי תוכן או גופים המבוססים על מערכות legacy, קשה לראות את התועלת המיידית ו-ROI חיובי באופן ברור. משתמשי הקצה (users) לרוב אינם נתקלים במשמעויות של מגבלת הכתובות של פרוטוקול IPv4 ואינם מבינים את משמעותה. הם גם אינם יודעים כי מגבלת הכתובות משפיעה על העלויות שהם משלמים עבור שירותי אינטרנט, כמו גם על נוחות השימוש בה. על כן, הדרישה אינה מגיעה, נכון להיום, ממשתמשי הקצה.

אף שהניתוח מעיד על כך שמעבר ל-IPv6 מקיים את המודל של רשת רב-צידיית, יש מאפיינים מיוחדים לתהליך זה. האחד הוא העובדה שהמודל של רשת כפולה (dual stack) משאיר לכל אורך התהליך במקביל את רשת ה-IPv4, ולכן התועלת הגלומה במעבר מלא לרשת IPv6 לא יבוא לידי ביטוי אלא עם המעבר המלא אליו והפסקת השימוש ב-IPv4. כשל זה הוא גורם מרכזי בהאטת המעבר ל-IPv6. בניגוד לרשתות רב-צידייות מוכרות אחרות⁵², כשל שני בא לידי ביטוי בטכנולוגיות להרחבת השימוש ב-IPv4, המקילות על מגבלת משאבי הכתובות של הפרוטוקול, כגון NAT ומקטינות את המוטיבציה של השחקנים השונים לעבור ל-IPv6.

⁵² לדוגמה, google מתווכת בין הרשת הדו-צידיית של שוק מאתרי המידע (משתמשים) ושוק המפרסמים (חברות) וממננת את הרשת מעמלות הפרסום שהיא גובה.

נראה כי לא ניתן להצביע על גורם יחיד, במגזר הפרטי או הממשלתי, אשר יש לו את המוטיבציה הכלכלית לקדם את המעבר ל-IPv6 ויכול לקחת על כתפיו את המהלך הזה. בחלקה, עובדה זו נובעת ממודל הפעולה הבסיסי המבוסס של האינטרנט. למרות זאת, לספקי הגישה הגדולים לאינטרנט (ISP) עשויה להיות השפעה על האצת התהליך, וכן גם לגורמי תיווך (intermediaries) כגון google, Facebook, yahoo ואחרים. על כן, **נדרשת פעולה מתואמת של כלל בעלי העניין הקשורים למימוש הפרוטוקול.**

ב. מרכיבי העלויות של מעבר ל-IPv6

כפי שנסקר בפרקים הקודמים, הפתרונות האפשריים למעבר ל-IPv6 הינם רבים ומגוונים. ארגון או גוף יכול לבחור פתרון אחד, בעוד גוף דומה או מקביל יבחר פתרון אחר. כל גוף או ארגון יכול גם לשלב מספר גישות של מעבר מ-IPv4 ל-IPv6, באותו גוף או ארגון. המשמעות הינה כי **אין פתרון מובנה ואחיד לביצוע השינוי וכל מימוש של IPv6 כרוך בעלות של רכש ציוד מתאים ו/או רכישת ידע והכשרת כ"א ו/או פגיעה בהכנסות כתוצאה מכשלים תפעוליים.**

המשמעות היא שלשחקנים הוותיקים והגדולים קיים יתרון תחרותי מובנה על פני השחקנים החדשים ו/או הקטנים. אף שקל יותר להטמיע IPv6 ברשת קטנה עם מספר קטן של משתמשים, הבעיה אינה רק ברשת ספק הגישה, אלא גם בשרתי המידע המאוחסנים. ספקיות גדולות נהנות מיתרון לגודל ומסוגלות לטפל בהיקף משתמשים גדול יותר ושירות התמיכה ללקוחות שניתן על ידן יהא, בדרך כלל, מקצועי יותר.

1) רשת כפולה

סקירות במדינות שונות בעולם מצביעות כי ספקיות הגישה לאינטרנט, כמו גם ספקיות התשתית, בחרו בשלב ראשון בגישת הרשת הכפולה כבסיס לתחילת השינוי. שיטה זו הוכיחה יותר מהימנות, יעילות והתאמה לשינויים משאר השיטות. אולם, ישנם גופים שהחליטו להוסיף עוד שיטת מעבר לצורך השלמת פערים שנתגלו בביצוע המעבר לפרוטוקול החדש.

החיסרון של שיטת הרשת הכפולה הוא בעיקר בנושא העלויות, כאשר האינטרס של אותם גופים לא תמיד עולה בקנה אחד עם התכנון הפיננסי שלהם (גופים אלה לרוב פועלים לפי שיקול כלכלי לטווח קצר) וחוסר היכולת לגבות פרמיה מהלקוחות עבור שירות שתומך ב-IPv6.

המשמעות של שיטת הרשת הכפולה היא למעשה להקים עוד רשת אינטרנט, במקביל לרשת הקיימת. חברות רבות, בעולם ואף בארץ, הקימו רשתות כפולות (לדוגמא: חברות הסלולר, בעת מעבר משיטת CDMA ל- GSM) אולם ברמות התעריפים הקיימות בשוק הישראלי ובהינתן מגבלות הגודל של השוק, הנטל הכלכלי של הקמת רשת נוספת עשויה להיות גבוהה מאד על כל חברה.

2) מנהור (Tunneling)

שיטת המנהור (Tunneling) דורשת עלויות נמוכות יותר מאשר הקמת רשת כפולה חדשה, ויישומו של השינוי מהיר יותר, אולם קיימות עלויות אחרות שמשפיעות על יישום שיטה זו.

העלויות של כל "מנהרה" (Tunnel) גבוהות יחסית בהיבט של שימוש במשאבים נוספים (תשתיות, מחשוב) ופוגע גם בביצועים, בחוויית הגלישה והשירות של האינטרנט. עלויות אלה נוספות לעלויות הניהול והמעקב אחר תקלות של שימוש בשיטה זו. בנוסף, בהיבט אבטחת המידע, קיים פוטנציאל רב של כשלים. מומחי אבטחה טוענים כי הבעיה העיקרית היא בזיהוי מקור ההתקפה בשיטה זו. ככל ששיטת ההמרה בין שני הפרוטוקולים מורכבת יותר, כך יכולת מעקב אחר בעיות אבטחה גדולה יותר.

3) הכשרות והסבות

העלויות של חברות התשתית וספקיות הגישה לאינטרנט אינן מסתיימות בהוצאות ישירות על ציוד או שיטת המרה שתוארה לעיל. עלויות נוספות הנובעות ממהלך זה הינן עלויות הכשרת טכנאים ואנשי מקצוע ייעודים לנושא ההטמעה; הכשרת צוות תמיכה עבור הלקוחות להטמעה ויישום אצל הלקוחות; ובניית תהליכי עבודה חדשים לנושא.

4) עסקים קטנים

גופים אחרים שנדרשים לבצע שינוי והתאמה הינם עסקים וארגונים המבוססים על מערכות מחשוב מתקדמות. אלו נדרשים לשינויים גם בתחום החומרה (שרתים, מחשבים אישיים ועוד) וגם בתחום התוכנה (מערכות הפעלה ותוכנות ייעודיות).

רוב חברות הציוד הגדולות מייצרות מזה מספר רב של שנים ציוד שתומך הן בפרוטוקול IPv4 כמו גם ב-IPv6. גם חברות התוכנה הגדולות החלו לפני שנים לא מעטות לתמוך בפרוטוקול IPv6 במקביל לשימוש ב-IPv4. אולם חברות קטנות, שלא החליפו ציוד או תוכנות בשנים האחרונות ומשתמשות, לדוגמה במערכת הפעלה Windows Vista, ידרשו לבצע שינוי והחלפת ציוד קצה ותוכנות לצורך ביצוע המעבר ל-IPv6. הדבר נכון גם לבתי תוכנה שמתחזקים עדיין תוכנות המבוססות על מערכות הפעלה ישנות.

לקוחות פרטיים שקיים ברשותם ציוד קצה (בעיקר מודם משולב עם נתב) התומך ב-IPv6, שקיבלו מספקיות הגישה לאינטרנט או מספקיות התשתית, לא ידרשו כנראה לבצע כל שינוי, בשל אפשרות התמיכה מרחוק שספקיות הגישה לאינטרנט מיישמות כבר היום (TR69). יחד עם זאת לקוחות שאין ברשותם ציוד קצה תומך ידרשו להחליף את הציוד במזה התומך בפרוטוקול החדש (סדר גודל של \$100-150 לקופסא).

יש להדגיש, כי בהיבט החומרה, לא רק שרתים ומחשבים אישיים נדרשים לתמוך בפרוטוקול החדש, אלא כלל הציוד הנלווה לרשת או לשירותים שכיום נמצאים אצל ארגונים וגופים. כך

לדוגמא: מצלמות אבטחה, בקרי כניסה ויציאה, מערכות שעון נוכחות, בקרים במערכות טכנולוגיות בתעשיות שונות (חקלאות, מים, רפתות ועוד) ומגוון רב של ציוד, ישן יחסית, שהחומרה שלו אינה תומכת ב-IPv6, נדרשים לבצע התאמות לתמוך בפרוטוקול החדש.

מכל מקום, גם תמיכה מלאה של ספקיות התוכנה אינו מונע תחלואים. ישנן לא מעט בעיות שחווים לקוחות בשימוש ב-IPv6 בארגונים שונים. חלק מהבעיות נובעות מנושאי אבטחה, חלוקת כתובות IP ועוד. כלומר, אף שבהיבט הישיר, המעבר שלהם הוא לכאורה בעלות אפס (שכן המערכות תומכות ב-IPv6), בפועל - עלויות ההתאמות, השינויים והתמיכה של אנשי מערכות המידע עשויות להיות גבוהות (כגון לצורך לימוד אנשי IT על השינוי ועלות העסקתם לצורך הטיפול בשינוי). במקביל חווית השירות והפגיעה בעסקים (זמינות, איבוד מידע ועוד) יכולים לפגוע הן כלכלית והן בתדמית של הארגון.

לאור המודעות הגוברת לחשיבות של הגנת סייבר, גם בנושא זה עולות סוגיות כלכליות רבות המשפיעות על ההערכות לשינוי, במיוחד בעסקים הקטנים.

ג. סיכונים טכנולוגיים

כאמור, עצם המעבר בין פרוטוקול IPv4 לבין IPv6 מייצר סיכונים ואינו נטול אתגרים, ללא קשר לשיטת המעבר. יישומים חדשניים מסוימים מחייבים IPv6 לצורך פריסה נרחבת; פריסת מנגנוני מעבר בהיקף נרחב עשויה להוביל גם לסוגיות של יכולת גידול (scalability), העלויות לפגוע קשות בביצועי IPv6 בהשוואה לפתרון מקומי ועוד. הסיכונים הטכנולוגיים אשר יכולים להיות מכשול מהותי בקידום השינוי ל-IPv6 ואותרו על ידינו הינם:

1) דו-קיום בין שתי הגרסאות

במקרים שבהם חייב להיות דו-קיום בין שתי הגרסאות, שמירת תהליך המעבר מ-IPv4 ל-IPv6 תחת שליטה היא חיונית, כדי למנוע פריסה של שתי תשתיות אינטרנט מקבילות. יישומי IPv6 ייהנו מן ההשקעות הכבדות שכבר בוצעו כדי לפרוס רשתות IPv4 קיימות.

יתכן שבארגון עדיין קיימים יישומים ישנים אשר מוטמעים בהם פרוטוקולים של IPv4, והמעבר לגרסה החדשה יותר, לא יהיו אפשריים. יישומים אלה יצטרכו, כנראה, להיכתב מחדש על מנת להמשיך לפעול ברשתות עם פרוטוקול IPv6.

2) המשכיות השירות

המעבר מ-IPv4 ל-IPv6 אינו רק שאלה של כתובות או ניתוב. שירותי IPv4 מתקדמים, הזמינים כיום או המצויים בפיתוח, כגון IP Security, IP Telephony, IP QoS, מחייבים המשך שירות רצוף בלי קשר לסוג תשתית ה-IP.

3) סיכומי אבטחת מידע

במעבר ל-IPv6 מסתתר גם איום הגנת סייבר. בניגוד לפרוטוקול IPv4, בו התפתחו הגנות שונות המתמודדות עם איומי סייבר שונים, בפרוטוקול IPv6, ובעיקר בשיטות המעבר בין הפרוטוקולים השונים, יש פוטנציאל לאיומי סייבר מהותיים שיכולים להשפיע על כל האינטרנט ולהוות סכנה גדולה לגלישה ושימוש ברשת, ואשר טרם התגלו, קל וחומר נמצא להם מענה.

ד. האם ניתן להמיר את כל כתובות האינטרנט ביום אחד?

קביעת יום מוסכם ("D-Day") למעבר מ-IPv4 ל-IPv6 בנוסח המודל של באג שנת 2000 (Y2K) אינה מעשית. מעבר ל-IPv6 יחייב הגדרה מחדש של תוכנית הקצאת כתובות (addressing plan) בהיקף כלל עולמי ב-IPv6, התקנת פרוטוקול IPv6 על כל נתב ומחשב ושינוי כל היישומים הקיימים כך שיפעלו על IPv6.

מעבר כזה יגרום להוצאות כבדות ושיבושים בלתי-סבירים בשירות וכן עלול ליצור נזקים חמורים ליישומים קריטיים מבזורים. גישה כזו תהיה גם חסרת-תכלית, שכן יישומים פעילים רבים אינם מחייבים מיידית את הכנסת השיפורים הגלומים ב-IPv6 או שלא תוכננו להפיק תועלת מן הפונקציונליות הנוספת שמאפשרת הגרסה החדשה.

במקרים מסוימים, בעיקר ברמת המאקרו המדינתית, מעבר ישיר ל-IPv6 יכול לזרז את תהליך המעבר. לדוגמה, אפשר לקדם את IPv6 באמצעות החלטה פוליטית להגדיל את מספר כתובות IP כדי לשמור על צמיחתה הכלכלית של מדינה כלשהי. דוגמה נוספת היא פריסה רחבה של ארכיטקטורת IP חדשה (כגון רשתות תקשורת ניידת או ביתית) לצורך אספקת יישומים ושירותים חדשניים.

ה. האם יש צורך בתקינה אחידה לשלב המעבר?

הניסיון בעולם מלמד שאין פתרון אחד אולטימטיבי שניתן לאמץ כתקינה או סטנדרט עולמי ואף לא סטנדרט מדינתי. המעבר ל-IPv6 צריך להיבחן פרטנית אצל כל ספק והוא יקבל את ההחלטה הנכונה עבורו. יתר על כן, הניסיון גם מלמד שאימוץ פתרונות שונים ברמת המדינה ואפילו ברמת החברה אינו מעכב את תהליך המעבר.

יחד עם זאת, הניסיון מלמד שברמת המדינה יש לקבוע תוכנית אב למעבר, לגבש אסטרטגיות למעבר (הכוללת את בחירת המנגנונים הנוחים ביותר להובלת התהליך, חיבור בעלי העניין המרכזיים - דוגמת ספקיות האינטרנט וחברות התשתיות - והחלטה אילו מהפתרונות ליישם וכיצד), לקבוע תמריצים לחברות וספקיות שיבצעו את המעבר, ולנטר את השינוי באופן הדוק.

5. תמריצים מוכחים למעבר ל-IPv6

הניסיון המצטבר בעולם מלמד שיש מספר צעדים ששימוש בחלקם, וביתר שאת, יכולים – במינוחים משתנים – מאפשר קידום אפקטיבי של המעבר מפרוטוקול IPv4 לפרוטוקול IPv6. להלן פירוט המהלכים:

א. רגולציה

מקובל כי לצורך קידום נושא ברמה הארצית או העולמית יש לבצע מהלכים רגולטוריים. מהלכים אלה יכולים לנבוע מכוח משפטי (אכיפת חוקים, תקנות, הוראות רשיון), כלכלי (תמריצים כלכליים) או חברתי (שינויים חברתיים). היתרון של רגולציה כופה הינו בכך שהיא קובעת את המועד והיקף השינוי באמצעות אבני דרך לביצוע השינוי. החסרון הוא ביכולת של השחקנים בשוק לנצל את כוחם כדי להשפיע על הרגולציה, והסיכון שההוראה הרגולטורית לא תהיה מדויקת מספיק או נכונה, ואז ייגרם נזק לשוק.

מספר מדינות בעולם פעלו בדרכים רגולטוריות שונות על מנת לקדם את המעבר לפרוטוקול IPv6. מהמידע שלמדנו לגבי שימוש במדיניות רגולטורית כופה במדינות שנסקרו עולה כי כל מדינה שנעשתה בה התערבות רגולטורית, המעבר לפרוטוקול IPv6 הצליח, במידה כזו או אחרת. לא מצאנו מדינה שבה היתה התערבות רגולטורית ולא חלה התקדמות במעבר לפרוטוקול החדש. כפי שסקרנו, כל מדינה בחרה בגישה שלה לביצוע השינוי, חלקן העבירו את שירותי הממשל לפרוטוקול החדש, חלקן התערבו במדיניות התעשייה ועודדו את התעשייה לבצע שינויים וחלקן ביצעו תיקוני חקיקה או תיקוני רשיון שחייבו מעבר של חברות תשתית תקשורת וספקי גישה לאינטרנט. בשורה התחתונה, כל התערבות של רגולציה סייעה לאותה מדינה להתקדם טכנולוגית לפרוטוקול החדש.

ב. תחרות

דרך נוספת ומועדפת על מרבית המדינות לביצוע שינוי ומעבר לפרוטוקול החדש הינה באמצעות יצירת כלים תחרותיים שיעודדו את השחקנים בשוק לבצע את השינוי. כלים תחרותיים כאלה מבוססים לרוב על תמריצים כלכליים (מענקים, סובסידיה או הקלות מס שונות), שבאמצעותם כל שותפי השינוי ו/או שחקנים חדשים יבצעו את המעבר והשינוי. תחרות תוכל להיווצר גם אם גורם מסוים בשוק ימתג את השימוש ב-IPv6 כתהליך חדשני וישקיע משאבי פרסום לצורך כך, ובדרך זו ימשוך אחריו את השוק.

ג. העצמת הפעילות של חברות גלובליות

הניסיון עם פעילותן של חברות גלובליות מלמד שהן עשויות להיות רגולטור משמעותי בביצוע שינויים רחבי היקף, לעיתים אף יותר מגופי המדינה. נראה כי אם חברות אלה יפעלו ביתר שאת לקדם את המעבר ולבצע שינוי מהיר, כל השוק יצטרך להתאים את עצמו למהלך.

כפי שנסקר לעיל, החברות הגלובליות הגדולות (Akamai, Google, Facebook, Yahoo, Limelight ועוד חברות קטנות יותר) ביצעו מספר "ימים מרוכזים" של מעבר לפרוטוקול IPv6 – IPv6 Day. ימים אלה הוגדרו כהצלחה גדולה ביצירת מודעות ועידוד, קידום והטמעה של הפרוטוקול החדש. לפיכך, יש להניח כי הן בשלות להובלת מהלך דומה בישראל.

ד. פגיעות לאיומי סייבר

אחת השיטות שבאמצעותן מתרחש שינוי באופן מהיר הוא הפחד מאיומים. בדומה להיערכות לבאג 2000 (Y2K), בו החשש הגדול היה שבסיסי מידע עצומים ימחקו או ישתבשו בשל המעבר למילניום החדש, נערכו כמעט כל החברות המשתמשות במחשוב לקרות השינוי במהירות רבה מאד. באופן יחסי השינוי בוצע תוך מספר מועט של שנים, כאשר השינויים העיקריים בוצעו בשנה האחרונה לפני שינוי המעבר למילניום החדש.

אירועי אבטחת סייבר, אשר יתבססו על חולשות הקשורות לשימוש ב-IPv4, עשויים להאיץ מעבר ל-IPv6, ככל שהוא יספק פתרון לאיום כזה.

ה. ROI (החזר השקעה)

כל חברה עסקית בוחנת את צעדיה ושיקוליה בהיבטים כלכליים, ועל כן גם שינוי של מעבר ל-IPv6 יבחן בכדאיות ההשקעה בו. האתגר המרכזי שעומד בפני המעבר לפרוטוקול החדש הוא משך הזמן הצפוי עד להחזר ההשקעה. לפיכך, ככל שהחברות יראו במעבר צעד אסטרטגי ואפשרות להחזיר את ההשקעה (גם אם בטווח הבינוני והרחוק) הרי שהן ייטו לבצע את השינוי. מאידך גיסא, ככל שחברה תיאלץ להוציא את כספה על ביצוע השינוי מבלי שתראה פוטנציאל משמעותי להחזר השקעתה, קיים חשש כי המהלך לא יבוצע כראוי וכנדרש וייתכן אף שייבלם.

6. מפת בעלי העניין הרלוונטיים להטמעת IPv6 בישראל

א. ממשלה

1) משרד התקשורת

מירב הנושאים הנוגעים לתחומי התקשורת בישראל נקבעים על ידי משרד התקשורת, הממונה על תחום התקשורת בממשלת ישראל. בשנים האחרונות היה מעורב משרד התקשורת באופן פעיל בשינוי טכנולוגיות שקרו בשוק, בעיקר בנושאים הנוגעים לתחומי התקשורת האלחוטיים, וזאת באמצעות הקצאת תדרי תקשורת. אך בנושא של שינוי פרוטוקולי האינטרנט התערב משרד התקשורת מספר פעמים מועט, כפי שיפורט להלן:

- ההתייחסות הראשונה של משרד התקשורת לנושא IPv6 נעשתה בהשתתפותו של מנכ"ל המשרד בדיון בוועדת מדע וטכנולוגיה בחודש מאי 2011 שהתבסס על נייר עמדה קודם של איגוד האינטרנט. במהלך הדיון נטען שאין שינוי סדרי עולם בנושא המעבר ל-IPv6 (ראו פירוט להלן, בסעיף ב1 – ועדת מדע וטכנולוגיה).
- בתחילת שנת 2014, הקים המשרד פורום הנדסי עם ספקיות התקשורת, וספקיות הגישה לאינטרנט. פורום זה התנהל בראשות סמנכ"ל הנדסה ורישוי של משרד התקשורת, מר חיים גירון.

- במהלך הדיון נסקרו הסיבות לצורך לעבור מפרוטוקול IPv4 ל-IPv6, ובסיכומו ציין סמנכ"ל הנדסה ורישוי כי: "על אף שלמשרד התקשורת יש סמכויות רגולטוריות לאכוף המעבר ל-IPv6, בשלב זה נבחן באורח וולונטרי ולא בכפיה, ונראה כי פורום הנדסי של המפעילים שיתכנס לפגישות עבודה ועדכון תקופתיות לאורך כל תהליך המעבר, היא המיטבית למעבר נכון ל-IPv6".
- עוד נקבע כי עד ליום 1/5/2014 (חודש מיום המפגש של הפורום) כל ספק אינטרנט בישראל (ISP או ספק תשתית) ימציא למשרד מסמך המתאר את רמת מוכנותו למעבר ל-IPv6, קשיים שהספק רואה ביישום, תובנות שיש לו מתהליך זה ולוח זמנים ליישום IPv6. בנוסף, נכתב כי המשרד ילמד את מוכנות הענף למעבר ל-IPv6 ויקיים כחודשיים לאחר מכן (יוני 2014) מפגש נוסף במהלכו ינסה לגבש יחד מתווה להתקדמות לעבר היעד, לרבות לוח זמנים.
- בפועל, חברת הוטנט וחברת טריפל C התייחסו לבקשת המשרד והעבירו את התייחסותם למוכנותם למעבר ל-IPv6. נראה כי נכון לאותו מועד, מעבר לצידו שהיה ברשות החברות, שנמצא כתומך ב-IPv6, לא נעשו כל פעולות נוספות מעבר לכך לקידום המעבר. נציין כי חיפוש מדויקדק בכל רישיונות הכללים של חברות

התקשורת וברישיונות המיוחדים למתן שירותי גישה לאינטרנט, לא מעלה כל אמירה, שימוש או מונח הנוגע ל-IPv6 (וגם לא ל-IPv4).

○ במהלך שנת 2017 עורר משרד התקשורת את העניין מחדש:

- ביום 20/4/2017 כינס סמנכ"ל טכנולוגיות עתידיות, מר חיים גירון, את כל ספקי התקשורת הרלוונטים לדין בנושא מעבר לפרוטוקול IPv6. בדיון זה ביקש המשרד להתעדכן ברמת המוכנות של כל ספק תקשורת ליישום פרוטוקול IPv6 (יפורט בהמשך).
- ביום 5/12/2017 נערכה פגישה שנייה במשרד התקשורת, בראשות סמנכ"ל טכנולוגיות עתידיות, מר חיים גירון. בסיכום המפגש הפיץ משרד התקשורת נייר עמדה והציג בו מספר יעדים, כאשר היעד העיקרי הינו עיגון התאריך 31/12/2018 ברשיון חברות התקשורת להטמעת פתרון לתמיכה מלאה בפרוטוקול IPv6. עוד צויין כי המשרד יבצע פעולות נוספות להטמעת הפרוטוקול החדש בהקדם (כגון: מדיניות אישור ציוד קצה, מדיניות הקצאת כתובות לאחר תאריך יעד וכו').

(2) מערך הסייבר הלאומי

עם התפתחות המרחב והאיומים הקיברנטיים, הנחה ראש ממשלת ישראל בנובמבר 2010 על הקמת צוות מיוחד, שיעסוק בגיבוש תוכנית לאומית להצבת ישראל בין חמש המדינות המובילות במרחב הקיברנטי. ב-7 באוגוסט 2011 אישרה ממשלת ישראל את הקמתו של המטה הקיברנטי הלאומי וקבעה כי המטה יוביל את פיתוח התחום הקיברנטי בארץ, יתאם בין הגורמים השונים העוסקים בתחום, ירחיב את ההגנה על תשתיות לאומיות מפני התקפות קיברנטיות ויעודד את קידום הנושא בתחום התעשייתי. כל זאת במטרה, להציב את מדינת ישראל בין חמש המדינות המובילות את התחום תוך מספר שנים מועט.

לאורך שנות פעילות מטה הסייבר הלאומי הוציא המטה מסמכי מדיניות וקולות קוראים רבים. בכל המסמכים שהוצאו, לא נמצאה התייחסות לנושא המעבר מפרוטוקול IPv4 ל-IPv6 כאיום או סיכון למרחב הסייבר הישראלי.

בפברואר 2015 החליטה הממשלה על הקמת רשות סייבר לאומית. בהודעה מטעם משרד ראש הממשלה נכתב כי הרשות "תקבל את האחריות ואת הסמכויות הנדרשות להגנת המרחב האזרחי מפני איומי סייבר ותהווה גוף אופרטיבי, שיפעל לצד מטה הסייבר הלאומי". הלכה למעשה מדובר בגוף ייעודי שמטרתו לחבר בין המרחב האזרחי לעולם הביטחוני ולהוביל את כלל פעילות ההגנה בסייבר בישראל "בהסתכלות ארוכת טווח של האיומים הגוברים והמתפתחים". בין הגדרות ההקמה של הרשות ישנם נושאים רבים ומגוונים ואולם, אין בנמצא כל איזכור או התייחסות לנושא המעבר בין פרוטוקול IPv4 לבין פרוטוקול IPv6.

לאחרונה הוחלט לאחד את מטה הסייבר הלאומי ורשות הגנת הסייבר לכדי גוף אחד בשם מערך הסייבר הלאומי. בשל היבטי אבטחת המידע והגנת הסייבר הקשורים במעבר מ-IPv4

ל-IPv6 מערך הסייבר הלאומי עשוי להוות אכסניה טובה עבור ייזום, פיקוח והסדרה של המעבר בגופים וארגונים אזרחיים ובטחוניים, ובפרט אלה הנמצאים תחת סמכות האסדרה הישירה שלו.

(3) רשות התקשוב הממשלתי

רשות התקשוב הממשלתי הוקמה בשנת 2012 כמטה התקשוב הממשלתי במשרד האוצר. מינואר 2015 פועלת הרשות תחת משרד ראש הממשלה. לאחרונה פרסמה רשות התקשוב הממשלתי תוכנית אסטרטגית אשר שמה לה למטרה לקדם ולפתח שירותים דיגיטליים במשרדי הממשלה וביחידות הסמך, במטרה לספק לאזרחים שירותי ממשלה נגישים יותר, חדשניים ועדכניים; כמו גם, להפחית את העלויות הישירות והעקיפות של מתן השירות ואת הצורך בפעולות פרונטליות של האזרח מול משרדי הממשלה; ולהבטיח שנושא ההגנה על הפרטיות ושיקולי אבטחת מידע יהיו חלק בלתי נפרד משלב התכנון והעיצוב של שירותים ממשלתיים חדשים.

המסמך המפורט של התכנית האסטרטגית כולל את החזון של הרשות החדשה, את הייעוד, ערכים, יעדים ואת הפעילות הבינלאומית של הרשות. התוכנית כוללת שורה רבה וארוכה של נושאים שהרשות אמורה לטפל בהם בשנים 2016-2018. בכל המסמך המפורט והמקיף על התוכנית האסטרטגית של הרשות, לא מציין את השינוי הנדרש למעבר לפרוטוקול IPv6.

(4) חשב כללי

אגף החשב הכללי שבמשרד האוצר הינו האחראי העיקרי על כל המכרזים הגדולים שגופי המדינה לוקחים בהם חלק, ובכלל זאת גם בנושא המחשוב והתקשורת. חיפוש באתר מנהל הרכש הממשלתי, באתר מרכ"ה, באתר משרד האוצר ודו"ח ממשל זמין לא מעלה את הערך IPv6. כלומר, כל מכרזי הממשלה שיצאו בשנים האחרונות לא התייחסו לעמידה של המציע או הזוכה במכרז התומך בפרוטוקול IPv6.⁵³ לחשב הכללי עשויה להיות השפעה רגלוטורית רבה, אם יכניס את המעבר ל-IPv6 כדרישה במכרזי הממשלה בתחום המחשוב והתקשורת.

⁵³ בבחינת הנושא עלו שתי התייחסויות אגביות שכללו את הערך IPv6:

במכרז מרכזי ממ-2008-07, אספקת מערכות תקשורת נתונים, אשר מטרתו "להסדיר אספקה של מערכות תקשורת נתונים למשרדי הממשלה", במסגרת "דוגמה למחירון יצרן", מופיעה ההתייחסות היחידה שאותה במכרזים ממשלתיים למילה IPv6 בדו"ח מספר 16.3.8 בתוך <http://mof.gov.il/takam>.

בבקשה לקבלת מידע 28-15 (RFI), "אספקה, הטמעה ותחזוקה של התקני איזון עומסים עבור משרד המשפטים" התבקשה, באופן אגבי, בשנת 2015, הדגמה כיצד תתקיים תמיכה עתידית ב-IPv6 (סעיף 2.2.10 לבקשה לקבלת הצעות, בקשה לקבלת מידע מס' 28-15 אספקה, הטמעה ותחזוקה של התקני איזון עומסים עבור משרד המשפטים, 09/08/2015).

5) משרד הבטחון

משרד הבטחון מוציא מכרזי רכש רבים ומגוונים, שאינם נמצאים בתכולת המכרזים של החשב הכללי. חיפוש במכרזים שהפיץ משרד הבטחון בשנה האחרונה, לא מעלה אף תנאי בהתקשרות עם ספק (בפרט ספקי תקשורת או ציוד תקשורת) של תמיכה בפרוטוקול IPv6. מעבר לכך, משרד הבטחון מנהל רשת תקשורת פרטית סגורה וזאת על מנת לשמור על בטחון המידע. לא ידוע האם משרד הבטחון, או כל ארגון וגוף בטחוני שמפריד רשתות בצורה פיזית, שוקל מעבר לפרוטוקול IPv6.

קיימים מומחים בתחום הטוענים כי אם שתי רשתות תקשורת מופרדות, ניתן להמשיך להשתמש בפרוטוקולים ישנים ברשת הפנימית והם יעבדו בצורה טובה. מערכות ביטחוניות הן מערכות שפועלות במשך שנים רבות, וייתכן שמערכות אלה ימשיכו לעבוד על IPv4, בעוד ששאר המערכות מסביבן תעבורנה ל-IPv6, אך עשויה להיווצר אי התאמה.

לשם השוואה, משרד ההגנה האמריקאי ותעשיות רבות, כגון תעשיית הרכב, המטוסים או האנרגיה, עוברות לתשתית IPv6. הסיבה העיקרית לכך נובעת מהבנתם שבעוד מספר שנים שימוש ב-IPv4 לא ייתמך ולכן הם מתכננים כבר היום למהלך.

6) משרד הכלכלה

משרד הכלכלה אמון על קידום הכלכלה הישראלית, ונמצא שהוא מקדם IPv6 באמצעות ייזום ותמיכה בקורסים מקצועיים שהוא מפרסם עבור אזרחים שמעוניינים לרכוש מקצוע הקשור לנושא הטכנולוגי.

מעבר לכך, לא נמצא שמשרד הכלכלה מעודד או מקדם את המעבר לפרוטוקול החדש.

7) רשות החדשנות

רשות החדשנות והמדען הראשי, שהינו חלק ממשד הכלכלה, חרט על דגלו לקדם את הצמיחה של ענף ההייטק הישראלי בשנים הקרובות.

בחודש יוני 2016 הגיש יו"ר הרשות לחדשנות דו"ח מקיף לראש הממשלה בו הוא הציג את המצב הקיים בישראל בנושא חדשנות וצמיחה בענף ההייטק. במקביל לניתוח שנתי מקיף על מצב התעשייה וניתוח המגמות העתידיות שישפיעו על ענפי ההיי-טק, התעשייה ומנועי הצמיחה של המשק ב-2016-2017, פרסם יו"ר הרשות לחדשנות שורת המלצות ושיפור לתחום.

המלצות אלה כללו שורה ארוכה של נושאים ואולם לא צויין כלל נושא המעבר ל-IPv6 כנושא מהותי או מרכזי בתהליך הצמיחה, וזאת בניגוד למדינות אחרות בעולם שראו במעבר לפרוטוקול החדש כאמצעי להגביר את החדשנות והתעשייה.

הדוגמא הבולטת לכשל בהעדר קידום IPv6 הוא תחום ה-IoT. תחום זה דורש הקצאת כתובות IP ייעודיות רבות וללא המעבר לפרוטוקול החדש, הפיתוח של נושא יישאר הרחק מאחור.

8) המיזם הלאומי "ישראל דיגיטלית"

החל משנת 2010 התקבלו מספר החלטות ממשלה בעניין פריסת רשת תקשורת כלל ארצית מתקדמת, שמטרתה לקדם צמיחה כלכלית, להגדיל את הרווחה החברתית ולצמצם פערים חברתיים באמצעות טכנולוגיות מידע ותקשורת (Information Communication Technology).

לצורך גיבוש ויישום מדיניות לאומית זו הקימה הממשלה את המיזם הלאומי "ישראל דיגיטלית". יעדיה העיקריים של ישראל דיגיטלית הוגדרו כפיתוח חדשנות ואספקת שירותים ציבוריים חדשניים, איכותיים ויעילים המותאמים למאה ה-21, לרבות שירותים מרחוק בתחומים כגון חינוך, בריאות ורווחה; הטמעת כלים טכנולוגיים בעסקים קטנים ובינוניים ועידוד מסחר מקוון; שיתוף מידע וידע ממשלתי ושימוש באמצעים מקוונים לשיפור ויעול השירות הניתן לאזרח וצמצום בירוקרטיה.

בחיפוש במסמכי המדיניות והיוזמות של "ישראל דיגיטלית" לא מוזכר כלל הצורך במעבר לפרוטוקול IPv6. יחד עם זאת, למיזם פוטנציאל השפעה גבוהה על המעבר ל-IPv6 בשירותי הממשלה. מעבר כזה יחייב ספקים שונים הפועלים באותה סביבה לעבור גם הם לפרוטוקול זה.

9) הרשות להגנת הפרטיות (לשעבר רמו"ט)

הרשות להגנת הפרטיות (לשעבר רמו"ט) היא רשות הגנת המידע האישי של ישראל. לא ידוע על פעילות כלשהיא של הרשות להגנת הפרטיות בסוגיות של מימוש פרוטוקולי האינטרנט IPv4 או IPv6. זאת, אף שמעבר לשימוש בפרוטוקול IPv6 מעלה סוגיות שונות הקשורות בפרטיות במידע, בשל האפשרות להקצות כתובת אינטרנט לכל אדם, ואף לסנסורים רבים הנמצאים בשירות האדם (במימוש של IOT).

לסיכום, לבד מפורום שנערך בחודשים אפריל 2014 ומספר פורומים נוספים שנערכו החל מאפריל 2017 במשרד התקשורת, לא נמצא גוף או גורם ממשלתי אשר עסק או עוסק באופן משמעותי בצורך המעבר של מדינת ישראל לפרוטוקול החדש, IPv6.

ב. כנסת

1) ועדת מדע וטכנולוגיה

בועדת המדע והטכנולוגיה של כנסת ישראל נערך בחודש מאי 2011, ביוזמת איגוד האינטרנט הישראלי, ועל בסיס מסמך מדיניות שנכתב על ידי האיגוד, דיון בנושא IPv6. הדיון התקיים בראשות יו"ר ועדת המדע והטכנולוגיה דאז, ח"כ מאיר שטרית ונכחו בו מנכ"ל משרד התקשורת דאז, מר עדן בר טל, נציגי איגוד האינטרנט הישראלי, נציגי ספקיות האינטרנט ונציגים של גופים וחברות הנוגעות לשינוי האמור. נייר העמדה שהגיש איגוד האינטרנט הישראלי התריע מפני מצוקת כתובות IPv4 והמליץ לקדם את המעבר לשימוש בפרוטוקול החדש IPv6. משרד התקשורת (מר עדן בר טל, מנכ"ל המשרד דאז), מנגד, טען:

- א. באופן טבעי משרד התקשורת רואה באינטרנט נושא חוץ-ממשלתי ולא פנים ממשלתי, והמשרד עוסק בו בזהירות.
- ב. הרגולציה של האינטרנט הינה נושא בעייתי, בשונה מנושאי תקשורת פנים מדינתיים כגון קישוריות בין ספקי תקשורת סלולרית וכד'.
- ג. לא ברור האם, נכון למועד קיום הדיון, אכן קיים מחסור כתובות בישראל, או האם יהיה מחסור כזה בנקודה רחוקה בזמן.
- ד. אין בעולם שינוי סדרי עולם בנושא IPv6, לא מחברות הענק ומגופי התשתית המרכזים והשינוי בעולם טרם קרה.
- ה. ייתכן שהפורום הנכון מבחינה ממשלתית לטפל בנושא הוא ה-CIO הממשלתי שהולך ומוקם במשרד האוצר. הנושא יידון מול האוצר.

בסיום ישיבת המדע והטכנולוגיה סיכם יו"ר הוועדה כי הוא מוטרד שישראל לא ערוכה למעבר ל-IPv6 וכי הוא ממליץ לממשלה להיכנס לעניין ולהקים יחידה, כוח משימה שיבדוק את הסוגיה וידחוף את המערכת למעבר מ-IPv4 ל-IPv6.⁵⁴

לסיכום דיון זה נילווח הד תקשורת בעיתונים היומיים בנוגע לישיבת הוועדה, אך מאז שנת 2011 ועד היום, לא עלה נושא זה כנושא מרכזי לדיון ציבורי בוועדה. בדיון שנערך בחודש פברואר 2018 בנושא IoT הביע מנכ"ל איגוד האינטרנט הישראלי כי מעבר ישראל ל-IPv6 היא סוגיה מרכזית להצלחת שימוש ב-IoT. בדיון מאוחר יותר באותו חודש בנושא ערים חכמות, מסר נציג משרד התקשורת על פעולת המשרד לחיוב ספקי הגישה לאינטרנט לישראל לתמוך ב-IPv6 עד תום שנת 2018.

2) ועדת הכלכלה

ועדת הכלכלה של הכנסת עוסקת דרך קבע בהסדרת שוק התקשורת בישראל. בתאריך 6 במרץ 2011, בסמוך לדיון שערכה ועדת מדע וטכנולוגיה בנייר העמדה של איגוד האינטרנט בנושא IPv6, נערך בוועדה דיון בנושא של "איחוד תשתיות אינטרנט"⁵⁵. הדיון עסק בשוק שירותי האינטרנט בישראל, פעילותן של חברות התשתית וספקי הגישה לאינטרנט, אך נושא IPv6 לא נדון בו כלל.

מעבר לכך, לא אותר באתר הוועדה דיון אחר אשר עסק בנושא, או בנושאים דומים לו.

ג. מגזר עסקי

המגזר העסקי בישראל מספק את עיקר שרשרת הערך של תקשורת האינטרנט, החל בספקי התשתית (בזק, הוט ו-unlimited), עבור לספקי הגישה לאינטרנט (ISP) וחברות הסלולר, ספקי ציוד הקצה, ספקי התוכן (כגון ynet, walla וכד'), מערכת שמות המתחם (Domain Name System - DNS), ספקי שירותי האירוח (hosting) וכמובן החברות הגלובליות דוגמת Google ו-Facebook.

נתוני הגלישה של לקוחות ישראליים באינטרנט הישראלי בפרוטוקול IPv6 עומדים על כ- 0.97% מכלל השימוש באינטרנט, בהתאם לנתוני הגלישה שנמדדים על ידי שרתי חברת Google; 1.2% על פי נתוני הגלישה הנמדדים על ידי שרתי חברת Akamai; 1.5% בשיאה

⁵⁴ פרוטוקול מס' 90, ישיבת ועדת המדע והטכנולוגיה, יום שני, י"ט באייר התשע"א (23 במאי 2011).
http://fs.knesset.gov.il/18/Committees/18_ptv_171070.doc

⁵⁵ פרוטוקול מס' 479 משיבת ועדת הכלכלה, ל' באדר א' התשע"א (6 במרץ 2011), שעה 10:00

(באפריל 2017) בהתאם לנתוני המדידה של חברת סיסקו⁵⁶. כלומר, נתוני הגלישה בפועל בפרוטוקול IPv6 הינם נמוכים מאד.

בחינת מספר האתרים של חברות וגופים שמחברים ותומכים בפרוטוקול החדש מראה אבחנה בין חברות הבינלאומיות כגון Google וצ'ק פוינט העובדות ב-IPv6, וכך גם מספר קטן של אתרי תוכן ישראליים קטנים כגון: סלונה, IAS, אתר הפורומים fxp, מגילות ים המלח, ישראלספורט, jewsnews, אטרף ועוד⁵⁷.

1) ספקי התשתית הפיזית

ספקי התשתית הפיזית, בכל טכנולוגיה קיימת, נדרשים להיות הראשונים לבצע את השינוי מפרוטוקול IPv4 לפרוטוקול IPv6. ללא המעבר שלהם, בין אם הן משתמשות בטכנולוגיית DSL או בטכנולוגיית Cable Modem/DOCSIS, לא יתאפשר לספק גישה לאינטרנט, ספקי שירות, או כל משתמש אחר, להשתמש ב-IPv6, אלא אם יעשו זאת ב"משק סגור" שלהם בלבד.

בשלב ראשון, ידרשו ספקי התשתית לאפשר את הגישה בשני הפרוטוקולים, על מנת לאפשר גישה לכל המשתמשים האחרים במקביל. מכאן, שספקי התשתית, ידרשו, כנראה, לפעול בשיטת הרשת הכפולה (Dual Stack). עם הזמן, ניתן יהיה לבטל את הרשת התומכת בפרוטוקול IPv4, אולם שלב ביניים זה צפוי להיות ארוך.

שוק התקשורת הישראלי עבר בשנים האחרונות מספר שינויים, כאשר המהותי ביותר והרלוונטי למעבר ל-IPv6 הוא רפורמת "השוק הסיטונאי". רפורמה זו, צברה, על פי דיווחים עיתונאיים, מעל 400 אלף לקוחות. עבור לקוחות אלה, יתכן ותידרש התאמה ייעודית לשינוי, לאור תצורת הרשת ושיטת העבודה הקיימת בין חברת בזק לספקיות הגישה לאינטרנט. כלומר, כאשר חברת בזק תיישם את המעבר ל-IPv6 ברשת ה-core שלה, היא תידרש לבצע את השינוי גם עבור "לקוחות השוק הסיטונאי".

א) חברת בזק

חיפוש אחר המונח IPv6 באתר האינטרנט של חברת בזק לא העלה אף מידע.

בשיחה עם מנהלי בזק עלה כי רשת ה-core של בזק תומכת בפרוטוקול IPv6 (רשת Layer 2). בפועל, לא נדרש כל שינוי ברשת הגישה מאחר והיא אדישה לסוג הפרוטוקול שעובר עליה. אולם, בזק פועלת לשדרג את המערכות התומכות שלה, כך שיתמכו גם בפרוטוקול IPv6.

⁵⁶ <http://6lab.cisco.com/stats/cible.php?country=IL&option=all>

⁵⁷ <https://www.vyncke.org/ipv6status/detailed.php?country=il>

הסיבה העיקרית לרצון במעבר לפרוטוקול החדש, לדברי מנהלי החברה, מלבד סוגיית אספקת שירות איכותי יותר ותמיכה עתידית בשירותים, היא אפשרות השליטה על המודמים של החברה. כיום בזק מספקת כמויות גדולות של מודמים ללקוחותיה. המודמים שמשווקים בתקופה האחרונה תומכים בפרוטוקול IPv6 אולם קיימים עדיין מודמים שאינם תומכים בו. על כן נדרש שינוי במערכות התומכות כך שישנו את הגרסה של המודמים הישנים לצורך תמיכה ב-IPv6.

בדיון שנערך במשרד התקשורת באפריל 2017 הציגו נציגי החברה כי התקיים מהלך בשלוש השנים האחרונות לתמוך בציודי הקצה (נתבים / מודמים) של החברה אצל לקוחות הקצה ומרבית הנתבים תומכים בפרוטוקול החדש. נותרו אחוזים לא גבוהים של נתבים שאינם תומכים בפרוטוקול החדש.

(ב) חברת הוט

חיפוש אחר המונח IPv6 באתר של חברת הוט מעלה קישור למודם משולב עם נתב מסוג HotBox של חברת הוט, אולם הקישור לדף זה לא נותן אף מידע הנוגע ל-IPv6. לא אותר מידע נוסף ממנו ניתן להבין האם התשתית תומכת ב-IPv6.

בדיון שנערך במשרד התקשורת באפריל 2017 הציגה החברה שהיא פועלת לשדרג את ציודי הקצה של הלקוחות (מודמים) ומרבית הנתבים תומכים בפרוטוקול החדש. נותרו אחוזים לא גבוהים של נתבים שאינם תומכים בפרוטוקול החדש. עוד ציינו כי מתקיימת עבודה מול ספקיות קטנות לשדרג ל-IPv6.

(ג) מיזם הסיבים האופטיים Unlimited

בשנים האחרונות, התחיל ניסיון לקדם תשתית תקשורת נוספת בשוק התקשורת הישראלי על זו של בזק והוט. תשתית זו, הידועה בשם המסחרי Unlimited, מבוססת על הסיבים האופטיים המשמשים את רשת חברת החשמל. נכון למועד זה, המיזם עדיין בשלבי ההתחלה שלו ונבחנת אפשרות לגבי ביצוע השקעות נוספות ומציאת בעלי עניין שיקדמו את המיזם.

בהיבט הטכנולוגי, רשת הסיבים האופטיים של המיזם תומכת בפרוטוקול IPv6. בדיון שנערך במשרד התקשורת באפריל 2017 הציגה החברה שספקיות שמחוברות למיזם פועלות בפרוטוקול החדש.

(2) ספקי הגישה לאינטרנט (ISP)

ספקי הגישה לאינטרנט (ISP) נמצאים בתווך שבין ספקי התשתית (DSL/DOCSIS) לבין לקוחות הקצה (בעלי ציוד קצה אישי או מחשב אישי מחד גיסא, וספקי השירותים, התוכן והמידע מאידך גיסא). על מנת שלקוח קצה יוכל לקיים חווית גלישה בפרוטוקול IPv6 על ספקי

הגישה לאינטרנט לוודא שכל "שרשרת הערך" של הגישה לאינטרנט אצלו תומכת בפרוטוקול. עליהם לוודא את הנושאים הבאים:

- א. שהציווד המותקן אצל הלקוח הקצה תומך ב-IPv6, בין אם מדובר במודם משולב עם נתב הגישה או במחשב האישי של הלקוח;
- ב. שהשירותים והאפליקציות שמסופקים ללקוחות תומכים אף הם בפרוטוקול IPv6;
- ג. שהציווד של הספקים עצמם (BRAS, הרשאות גישה, הקצאת כתובות IP ועוד) תומכים בפרוטוקול.

המענה הראשוני לכל תקלה של לקוח קצה יהיה, בדרך כלל, אצל ספק שירותי הגישה שיידרש לאבחן את המצב ולספק פתרון ללקוח על מנת שיוכל להמשיך ולקבל את השירות, אף אם "התקלה" אינה באחריות הישירה של ספק הגישה לאינטרנט. נדרשת מומחיות גבוהה של צוות התמיכה והשירות של ספקיות הגישה לאינטרנט, בעיקר בעידן של "השוק הסיטונאי" שחל על אלפי לקוחות אינטרנט.

העולה מכך הוא כי במעבר מדינתי ל-IPv6, ספקי הגישה לאינטרנט הם מהשחקנים החשובים ביותר, ויש לבצע את המהלך בשיתופם האקטיבי. יודגש, עם זאת, שמניסיון שקיים במדינות רבות בעולם, המעבר לתמיכה בפרוטוקול IPv6 קל יותר עבור ספקיות גישה קטנות, מאשר זו המתרחשת בספקיות הגדולות.

א) נטוויזן / סלקום

חיפוש אחר המונח IPv6 באתר של חברת נטוויזן לא העלה אף מידע. פנייה אל חברת סלקום לקבלת מידע על הערכות החברה למעבר לפרוטוקול לא נענתה.

בדיון שנערך במשרד התקשורת באפריל 2017 הציגה החברה שהיא פועלת בשיטת Dual Stuck; קיימים מספר לקוחות עסקיים שנמצאים בפיילוט בפרוטוקול החדש וקיימת עוד עבודה במערכות תומכות להמרתן לתמוך בפרוטוקול החדש.

ב) 012 / פרטנר

חיפוש אחר המונח IPv6 באתר של חברת 012 לא העלה אף מידע. פנייה אל חברת פרטנר לקבלת מידע על הערכות החברה למעבר לפרוטוקול לא נענתה.

בדיון שנערך במשרד התקשורת באפריל 2017 ביקשה החברה לא להציג את המידע אודות המעבר לפרוטוקול החדש בפומבי.

ג) בזק בינלאומי

חיפוש אחר המונח IPv6 באתר של חברת בזק בינלאומי מעלה מידע כללי על שירות IPv6 שניתן ללקוחות עסקיים, בעיקר בחוות שרתים של החברה ולפי הפרסום באתר, IPv6 יופעל גם ללקוחות הפרטיים החל משנת 2013.

בשיחה עם מנהלי בזק בינלאומי עולה כי החברה הקימה רשת IPv6 בשיטת 4to6 הניתנת כשירות בשלב ראשון רק עבור לקוחות עסקיים. בשלב זה, באם תהיה דרישה מצד הלקוחות הפרטיים, שירות זה יסופק גם להם.

בדיון שנערך במשרד התקשורת באפריל 2017 הציגה החברה שהיא פועלת בשיטת Dual Stuck ומתקיים פיילוט של לקוחות עסקיים בפרוטוקול החדש.

(ד) אקספון

חיפוש אחר המונח IPv6 באתר של חברת אקספון מעלה דף מידע על השירות אותו מספקת החברה. לצורך קבלת השירות נדרש להתקשר לנציגי החברה.

בשיחה עם סמנכ"ל הנדסה של אקספון עולה כי החברה הקימה רשת IPv6 ומספקת ללקוחותיה כתובות IPv6. אקספון פעלה בשיטת Dual Stack והקימה רשת אינטרנט מקבילה, כך שלקוחותיה מקבלים למעשה את שני סוגי הכתובות (IPv6 + IPv4). בפועל רוב התנועה עדיין עוברת דרך פרוטוקול IPv4. לקוחות שנמצאים במסגרת "השוק הסיטונאי" ומקבלים ציוד קצה מאקספון או שרוכשים מודם משולב עם נתב חדש, מקבלים הקצאה של IPv6.

לדברי סמנכ"ל הנדסה קיימת בעיה עם ספקי התוכן שאינם מקושרים בפרוטוקול החדש ולכן לקוחות לא יכולים לקבל שירות בפרוטוקול IPv6.

בדיון שנערך במשרד התקשורת באפריל 2017 הציגה החברה שהיא פועלת בשיטת Dual Stuck; חלק מהלקוחות הפרטיים כבר מקבלים שירות בפרוטוקול החדש.

(3) ספקי התשתית והגישה הסלולריים

באופן שונה משוק התקשורת הקווי, שוק התקשורת הסלולרי עובר שינויים משמעותיים בתדירות גבוהה של כ- 5 שנים לערך. המעבר בין דורות ברשתות הסלולריות מאפשר ביצוע שינויים והתאמות מהירים יותר, אך בשל תאימות לאחור משאיר את המערכות הישנות לפעול. במקרה של שינוי פרוטוקולים בין IPv4 ל-IPv6, השינוי משמעותי מאוד.

בהיסטוריה של שוק הסלולר, הדור השלישי (3G) שהושק בעולם בתחילת שנות האלפיים, אמור היה לתמוך בפרוטוקול IPv6 כבר מלכתחילה. אולם, הלחץ של התעשייה על כל היבטיה, איפשר לחברות להמשיך להשתמש בפרוטוקול IPv4 גם במימוש של 3G. רק בשנים האחרונות, החלו חברות סלולריות בעולם להטמיע ברשתות שלהן גם את IPv6.

הדור הרביעי (4G) שונה לגמרי. שירותיו (שיחות, הודעות, אינטרנט ווידאו) מבוססים על פרוטוקול האינטרנט בלבד (Pure IP). על מנת לתמוך בכמות המכשירים הגדולה נדרשות חברות הסלולר להטמיע מבעוד מועד את פרוטוקול IPv6 כסטנדרט ברשת שלהן. אולם, עדיין נדרשות המרות של IPv4, על מנת לספק שירותים ובכללם שירותי תוכן שאינם תומכים

בפרוטוקול החדש. לכן חברות הסלולר מטמיעות את שיטות ההמרה שפורטו לעיל כדי לאפשר את הגישה לתכנים ולשירותים עבור לקוחותיהם.

(א) סלקום

חיפוש אחר המונח IPv6 באתר של חברת סלקום לא העלה אף מידע.

(ב) פרטנר

חיפוש אחר המונח IPv6 באתר של חברת פרטנר לא העלה אף מידע.

(ג) פלאפון

חיפוש אחר המונח IPv6 באתר של חברת פלאפון לא העלה אף מידע.

בשיחה עם מנהלי חברת פלאפון עולה כי החברה נערכת להטמיע את הפרוטוקול ברשת הדור הרביעי שלה ולהציע את השירות, כברירת מחדל, ללקוחות החברה שגולשים בדור הרביעי.

(ד) הוט מובייל

חיפוש אחר המונח IPv6 באתר של חברת הוט מובייל לא העלה אף מידע.

בדיון שנערך במשרד התקשורת באפריל 2017 הציגה החברה שנושא ה- IT עדיין לא תומך בפרוטוקול החדש.

(ה) גולן טלקום

חיפוש אחר המונח IPv6 באתר של חברת גולן טלקום לא העלה אף מידע.

(4) ספקי ציוד תקשורת

יצרני ציוד התקשורת בעולם מפתחים את המוצרים שלהם תוך תמיכה ב-IPv6 מזה שנים. מרבית הספקים מייצרים היום עדיין ציוד התומך בשני הפרוטוקולים גם יחד. ישנם ספקים שהגדירו שברירת המחדל של הציוד או השירות שמייצרים או מספקים תהיה תמיכה בפרוטוקול IPv6.

בישראל, עיקר ציוד התקשורת לחיבור לאינטרנט מסופק על ידי ספקי התשתית. ככל הנראה קיימת בעיה בציוד קצה ישן שנמצא אצל שיעור לא קטן של לקוחות (לדוגמה, מודמים ישנים של חברת בזק והוט, מדפסות, מרכזיות פרטיות, טלפונים) אשר אינם תומכים בפרוטוקול החדש.

העולה מכך שיצרני ציוד הקצה, באופן יחסי, נמצאים בהליך השינוי ונרתמו לתמיכה ב-IPv6.

5) ספקי תוכן ישראליים

קיימים מספר ספקי תוכן עיקריים בישראל. להלן נפרט את הסטאטוס של ספקי התוכן בהיבט של מעבר לפרוטוקול IPv6.

א) Walla

חברת וואלה, מקבוצת בזק, פועלת כספקית תוכן מובילה בשוק התקשורת הישראלי. על פי דירוג similar web מדורג האתר במקום ה-7 בכמות התעבורה בישראל. מערכות החברה פועלות כיום בפרוטוקול IPv4. משיחה עם אנשי החברה עולה כי בכוונת החברה לעבור למערכות חדשות התומכות גם בפרוטוקול IPv6. לדברי החברה, החל משנת 2018 יוכלו משתמשי האתר לגלוש בפרוטוקול IPv6.

ב) YENT

חברת ynet, מקבוצת ידיעות אחרונות, פועלת כספקית תוכן מובילה בשוק התקשורת הישראלי. על פי דירוג similar web מדורג האתר במקום ה-5 בכמות התעבורה בישראל. פגישה שנערכה עם אנשי הטכנולוגיות של ynet עולה כי אין לחברה תוכניות להעביר את הפלטפורמה לפרוטוקול IPv6. לדבריהם, המעבר ישולב במסגרת תוכנית עבודה של השנים הקרובות.

ג) Mako

אתר שבבעלות חברת קשת, מאקו, פועל כאחד מספקי התוכן מובילים בשוק התקשורת הישראלי. על פי דירוג similar web מדורג האתר במקום ה-13 בכמות התעבורה בישראל. לא מצאנו תוכניות למעבר ל-IPv6.

6) חברות גלובליות

חברות רבות בעולם, בעיקר החברות הגלובליות, ששירותיהם או מוצריהם נמכרים בהרבה מדינות בעולם, נקטו בצעד אקטיבי, וללא תלות במדינה בהם הן פעולות והחלו להמיר את הרשתות שלהן, ובכלל זאת, את השירותים שלהן לפרוטוקול החדש IPv6.

להלן נסקור דוגמאות לשינויים שביצעו או מבצעות חברות בינ"ל.

א) חברת Amazon

חברת אמזון, המתמחה בשירותי מסחר אלקטרוני ואספקת שירותי מחשוב מתקדמים בענף, שידרגה את הרשת שלה עבור לקוחותיה שמשתמשים בשירותי האחסון, כך שתתמוך בפרוטוקול IPv6.

אמזון השתמשה בטכניקה של "הרשת הכפולה", ומציינת כי יש ביכולתה לזהות את הפרוטוקול בו הלקוח ניגש לצרוך את שירותי החברה, כך שבמידה והלקוח משתמש בפרוטוקול IPv6, הוא יקבל את השירותים ברשת זו.

ב) חברת Facebook

חברת Facebook החלה להמיר את כל שירותיה הפנימיים לרשת התומכת בפרוטוקול IPv6 כבר בשנת 2014. במקביל, פעלה החברה להטמיע את כל שירותיה בפרוטוקול החדש עד סוף שנת 2015, כך שהרשת שלה תוגדר כרשת Pure IPv6.

מחקר מעניין שביצעה החברה הוכיח כי לקוחות שגולשים בפרוטוקול החדש IPv6 חווים חווית גלישה מהירה יותר בכ- 20-40% מאשר שימוש בפרוטוקול הישן IPv4⁵⁸.

נתון מעניין נוסף שנטען על ידי Facebook, הוא שככל שמתרבים השימושים במכשירי סלולר וכניסתו של הדור הרביעי לשוק הסלולר, נדרשים כל ספקי התוכן להמיר את רשתם ל- IPv6, וזאת על מנת לספק שירותים לכלל כתובות ה- IP, לחוויית שירות טובה יותר ויכולות טכנולוגיות גבוהות יותר.

ג) חברת Google

חברת Google מטמיעה מזה מספר שנים IPv6. בשנת 2011, הובילה Google, ביחד עם חברות גלובליות אחרות כמו Akamai, Yahoo, Facebook ועוד אלפי חברות קטנות יותר את יום ה- IPv6. ביום זה עוררו החברות הגלובליות את המודעות למעבר ולשינוי הנדרש באינטרנט. שנה לאחר מכן התקיים שוב יום מרוכז ומיוחד לקידום הפרוטוקול החדש. יום זה הוכיח את חשיבותה ונחיצותה של התעשייה לקידום מיזמים עולמיים.

מהמידע שחברת Google מפרסמת, היא טוענת כי היא מתעדפת בתוצאות מנוע החיפוש שלה את הקישורים שעוברים בפרוטוקול IPv6 על פני IPv4. פניה לקבל באופן רשמי את עמדת Google לגבי נושא IPv6 בכלל, והתייחסותה לנושא זה בהקשר הישראלי, לא נענתה.

7) מגזר שלישי - איגוד האינטרנט הישראלי

גוף המגזר השלישי המשמעותי לסוגיות של מעבר ל-IPv6 הוא איגוד האינטרנט הישראלי, אשר מנהל שתיים מהתשתיות החשובות באינטרנט הישראלי: מרשם שמות המתחם של IL, ומחלף האינטרנט הישראלי IOU.

⁵⁸ <http://www.internetsociety.org/deploy360/blog/2015/04/facebook-news-feeds-load-20-40-faster-over-ipv6/>

א) מרשם שמות המרשם .IL

איגוד האינטרנט הישראלי מנהל את מרשם שמות המתחם (domain names) של ה-IL ccTLD (country code Top Level Domain) משחר כניסתו של האינטרנט המסחרי בתחילת שנות ה-90. המרשם תומך ממחצית שנת 2014 בשיוך כתובות IPv6 לשמות מתחם.

הממשק מול רשמי שמות המתחם תומך ב-IPv6 ומותאם לרישום כתובות ב-ב-IPv6 בסיומת .IL.

ב) מחלף האינטרנט הישראלי IX

מחלף האינטרנט הישראלי (IX) מופעל על ידי איגוד האינטרנט משנת 1996, ומחבר בין רוב ספקי הגישה לאינטרנט בישראל, כך שתעבורת אינטרנט פנים ישראלית תשאר בגבולות המדינה.

המחלף תומך באופן מלא בפרוטוקול IPv6 מתחילת שנת 2008.

ג) איגוד האינטרנט כ-LIR לכתובות IPv4

איגוד האינטרנט משמש כ-LIR ורשום כמחזיק כ-3% מכתובות ה-IPv4 שהוקצו לישראל. חלק מכתובות אלה משמשות לפעילות האיגוד, ובאחרות הוא משמש כרשם עבור חברות שנדרשו להקצאה כפולה של כתובות.

על פי החלטת ועדת ההיגוי לשירותי התשתית של האיגוד יתרה קטנה שנותרה משמשת כעתודה למצב בו יתקיים מחסור חריף בכתובות.

ד) אתר האינטרנט של איגוד האינטרנט www.isoc.org.il

אתר האינטרנט של איגוד האינטרנט תומך בפרוטוקול IPv6.

ד. סיכום – תמונת מצב שימוש ומעבר ל-IPv6 בישראל

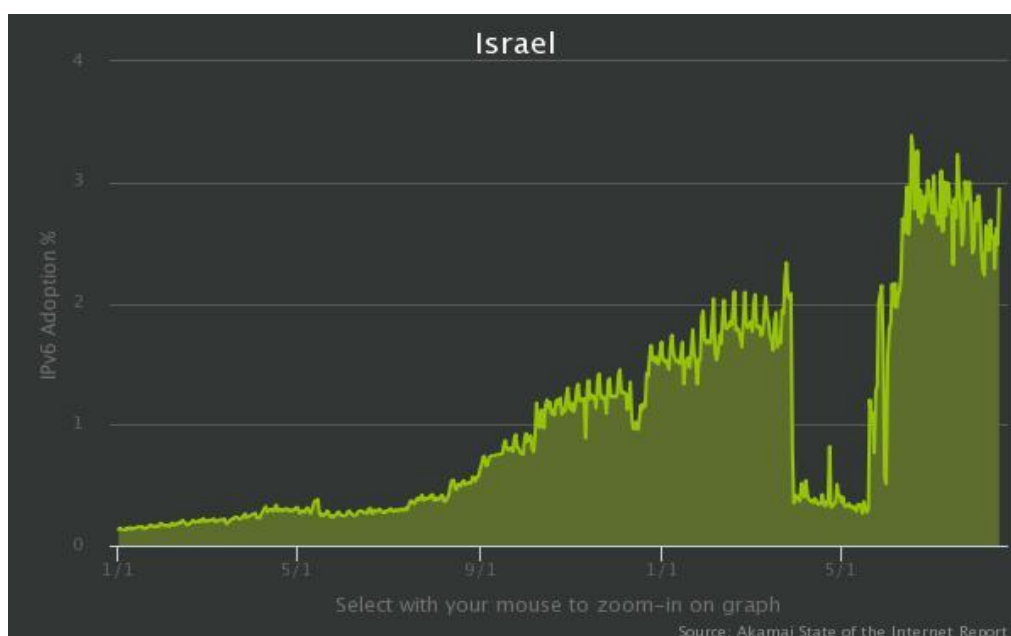
כפי שנסקר לעיל, בצד ספקי השירותים לא מתקיימת כל פעילות אקטיבית ויעילה לביצוע המעבר לפרוטוקול IPv6. רוב ספקיות שירותי הגישה לאינטרנט אינן ערוכות באופן מלא לספק את שירותי הגישה לאינטרנט בפרוטוקול החדש. המצב חמור יותר אצל ספקיות התוכן הישראליות, וזאת בניגוד להערכות של ספקיות התוכן הבינלאומיות (שנערכות ברמה העולמית לשינוי).

בקרב יצרניות הציוד קיימת הערכות מתאימה לשינוי בפרוטוקול, הנובע בעיקרו מההשפעה העולמית. מרבית ציוד הקצה החדש הקיים בשוק היום תומך בפרוטוקול החדש בעוד שעיקר הבעיה הינה בציוד קצה הישן שקשה יותר לבצע בו התאמות לפרוטוקול החדש.

על פי נתונים של חברת Akamai, התנועה שעוברת בפרוטוקול IPv6 בישראל עומדת על 2.9%, אשר ממקם אותה במקום ה-45 בעולם.⁵⁹ מדובר בירידה מהמקום ה-37 בו הייתה ישראל במחצית שנת 2017. על כל פנים, ישראל ממוקמת נמוך ביחס לרוב מדינות ה-OECD ולמדינות נוספות אליהן ישראל מעוניינת להיות משווה. מעבר לכך, נראה שנתונים אלה משקפים את התעבורה הישראלית בתווך של החברות הגלובאליות ולא דווקא את התעבורה בתשתיות הישראליות.

המגמה של היקף תנועת התעבורה לפרוטוקול IPv6 מצויה במגמת עלייה בעולם, באופן שמאיים להותיר את ישראל הרחק מאחור גם ביחס למדינות פחות מפותחות ממנה. להלן גרף מתוך אתר של חברת Google הנוגע למגמת תנועת IPv6 העוברת בשרתי Google.⁶⁰

איור 6.1: אחוז התעבורה בפרוטוקול IPv6 בישראל

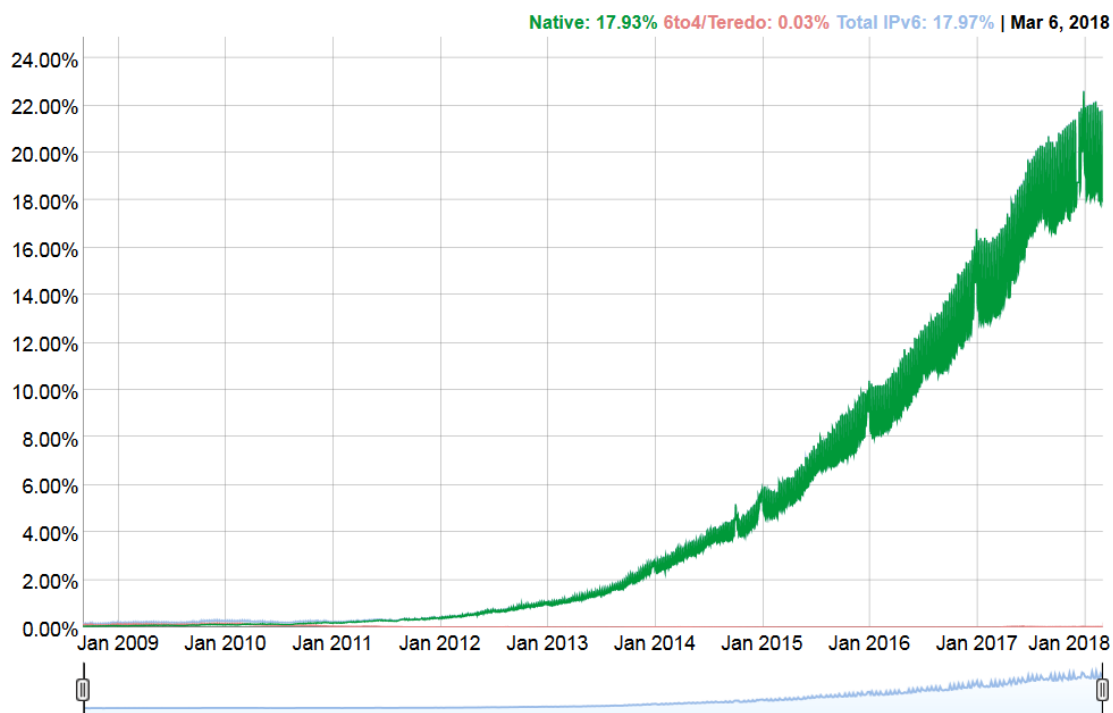


<https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/state-59-of-the-internet-ipv6-adoption-visualization.jsp#countries>

https://www-public.tem-tsp.eu/~maignon/RIR_Stats/RIR_Delegations/AFRINIC/IPv6-ByNb.html

<https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption&tab=ipv6-60adoption>

איור 6.2: אחוז התעבורה בפרוטוקול IPv6 בעולם



7. מדיניות מוצעת לקידום והטמעת IPv6 בישראל

א. הגדרת המעבר ל-IPv6 כיעד לאומי בתחום התקשורת בישראל

התמונה המפורטת המוצגת לעיל במסמך זה על אודות שימוש ב-IPv6 בישראל ואודות המוכנות התשתית לביצוע המעבר לשימוש בפרוטוקול זה היא עגומה. המדד ההשוואתי לקבוצת מדינות העולם שישראל מבקשת להיות שייכת אליהן ממחישה זאת בבירור. יתר על כן, ישראל - המתיימרת להיות אומה הדוגלת להוביל ולעמוד בחזית החדשנות והקידמה הטכנולוגית, כפי שהדבר בא לידי ביטוי במגוון החלטות ממשלה וברוח היוזמה הישראלית - אינה יכולה להרשות לעצמה להישאר מאחור ולא לאמץ ולקדם טכנולוגיה אשר, ללא ספק, תעמוד בבסיס האינטרנט, כפי שהעולם ישתמש בה בעשורים הקרובים.

גם בהיבט הכלכלי, עיכוב במעבר מפרוטוקול IPv4 לפרוטוקול IPv6 מעמיד את ישראל בנחיתות בהקשר של קישוריות לאינטרנט. באופן קונקרטי, עיכוב במעבר לפרוטוקול IPv6 עלול לפגוע ביכולת של מדינת ישראל להוביל את תחום ה-IoT. בנוסף, העיכוב במעבר עלול לגרום לתעשיות השונות, כמו גם לעוסקים בתחומים מדיניים וחברתיים, לאבד יתרונות תחרותיים שהאינטרנט מאפשר בשל אי התאמה לפרוטוקולי ה-IP שבשימוש, ולאליץ את אותם גופים לעבור לפעול במדינות המספקות תשתית מתקדמת. עוד יודגש כי הניסיון של מדינות, שנמצאות בשלבים מתקדמים יחסית של מעבר מלמד, שהוא עשוי לשמש מאיץ כלכלי לאומי.

איגוד האינטרנט הישראלי ממליץ שמדינת ישראל, באמצעות משרד התקשורת ו/או ועדת מדע וטכנולוגיה של כנסת ישראל תכריז על המעבר ל-IPv6 כיעד לאומי. במסגרת זאת, האיגוד ממליץ לקבוע תוכנית רב שנתית שתגדיר יעד ביניים של 40% מתעבורת האינטרנט ב-IPv6 עד שנת 2022 והשלמת המעבר (100%) תוך כעשור.

להחלטה זו תהא השפעה דרמטית על מוכנותו של המשק הישראלי לפיתוחים הטכנולוגיים המרכזיים באינטרנט.

ב. הקמת כוח משימה (Task Force) לאומי

איגוד האינטרנט הישראלי ממליץ להקים **כוח משימה (task force) מאוחד לקידום פרישת IPv6 בישראל**. האיגוד ממליץ שבראשות כוח המשימה יעמוד מנהל בכיר בשירות

המדינה העוסק בתחום (כגון מנכ"ל משרד התקשורת או ראש מערך הסייבר הלאומי), שכוח המשימה ימומן מתקציב המדינה, ותפקידו יהיה:

- א. להוציא לפועל את התוכנית הלאומית למעבר ל-IPv6;
- ב. לנטר ולמדוד את התקדמות התהליך על ידי כלל השחקנים במשק;
- ג. להוות מוקד ידע עבור המשק הישראלי בנושא.

איגוד האינטרנט הישראלי ממליץ שהחברים בכוח המשימה יכללו את הגורמים הבאים:

- א. משרד התקשורת
- ב. מטה הסייבר הלאומי
- ג. משרד הכלכלה
- ד. רשות הגנת הסייבר
- ה. הממונה על התקשוב הממשלתי
- ו. ישראל דיגיטלית
- ז. אגף תקשוב בצה"ל
- ח. רשות החדשנות
- ט. הרשות להגנת הפרטיות
- י. הלשכה המרכזית לסטטיסטיקה
- יא. רשות המסים בישראל
- יב. נציג של כל אחד מה-ISP בישראל⁶¹
- יג. נציג של כל אחד מספקי התקשורת הסלולרית הגדולים (פלאפון, סלקום, פרטנר וכד')
- יד. נציגות של ספקי תקשורת סלולרית קטנים
- טו. נציג מכל אחד מספקי התשתית (בזק, הוט ו- unlimited)
- טז. נציג של כל אחד מאתרי התוכן הראשיים (ynet, וואלה, מאקו וכד')
- יז. נציגים של אתרי תוכן קטנים
- יח. נציגים מחברות אינטגרציית ה-IT בישראל (IBM, מטריקס, HP, טלדור וכד')
- יט. מחב"א
- כ. איגוד האינטרנט הישראלי
- כא. התאחדות התעשיינים – איגוד תעשיות האלקטרוניקה והתוכנה

מומלץ שכח המשימה יהיה חייב בדיווח עיתי כל חצי שנה לוועדת מדע וטכנולוגיה של הכנסת על התקדמות התהליך, ושיפרסם על בסיס קבוע נתונים סטטיסטיים ודיווחי התקדמות של התהליך.

⁶¹ יש לוודא כי תהא נציגות מספקת של ISP's (ספקי הגישה לאינטרנט) קטנים

ג. אימוץ גישה המשלבת בין הסדרה עצמית לרגולציה רכה

הניתוח המפורט לעיל מראה שתהליך מעבר מלא והאפקטיבי לשימוש ב-IPv6 תלוי במידה רבה בשיתוף פעולה ואף בהובלה של השוק הפרטי ובעיקר של ספקי תשתית, ספקי שירותי גישה לאינטרנט וחברות גלובאליות. הניסיון מלמד שלא להעניק עשויה להיות השפעה דרמטית על הצלחת המהלך וההנחה היא שהמשק הישראלי יעקוב אחרי פעולתם, הרגולציה שיקבעו וההיצע המתפתח של השירותים שיגבשו. זאת ועוד, עיקר הידע בנושא ה-IPv6 נמצא בידיהם של ארגונים אלה וחלקם אף פרשו כבר מרכיבי IPv6 בפעילותם, והם יודעים היטב את מנגנוני העלות כמו גם את הקשיים הטכנולוגיים.

לצד זאת, הניסיון בעולם מלמד שרגולציה ומעורבות ממשלתית חיונית לשם עידוד המשק למעבר לשימוש ב-IPv6, וכי ללא תמיכה, תמרוץ ודחיפה ממשלתית, השוק האזרחי מתקשה לקדם את המהלך בקצב ראוי, אם בכלל.

לאור זאת, איגוד האינטרנט הישראלי ממליץ שהגישה הבסיסית לתהליך צריכה להיות הסדרה עצמית של השוק העסקי, ולשם כך יש לבנות מנגנון שישלב בין רגולציה (רזה), מעבר מהיר של רשויות הממשלה ל-IPv6 והתניית מכרזים ממשלתיים בביצוע מעבר דומה, ותמריצים כלכליים, שיעודדו את השחקנים השונים במגזר הפרטי להסדיר את המעבר באופן עצמי. בהקשר זה, ייתכן שתמריץ לביצוע אסדרה עצמית עשוי לעודד דווקא את ספקיות האינטרנט הקטנות, שמלאי כתובות ה-IPv4 שלהן במחסור, להרים את הכפפה ולייצר את השוק.

ד. מדיניות לאומית רב מימדית

סוגיית המעבר לפרוטוקול IPv6 הינה בעלת השלכות ומשמעויות מרחיקות לכת על תחומים רבים במשק הישראלי. חרף זאת, המסמך לעיל מראה שעד עתה משרדי הממשלה והגופים הלאומיים השונים לא מצאו לנכון לגבש מדיניות נושאית (כל אחד בתחומו) בעניין. משכך, קיימת יכולת מינימלית בלבד לפעול לצמצום הסיכונים והעלויות של המהלך, כמו גם למיצוי ההזדמנויות שבו.

איגוד האינטרנט הישראלי ממליץ שהמשרדים והגופים הבאים, לכל הפחות, **יגבשו מסמך מדיניות נושאי עד 31 דצמבר 2018**. עוד ממליץ האיגוד שמסמכי מדיניות אלה, יחד עם התוכנית האסטרטגית שתגובש במשרד התקשורת **ירוכזו למסמך אחד שישמש כמסמך אב לאומי לתהליך**. להלן המשרדים והגופים שאיגוד האינטרנט הישראלי ממליץ שיגבשו מסמך מדיניות:

(1) משרד התקשורת

משרד התקשורת, פנה לעסוק בשנת 2017 בלימוד סוגיית יישום IPv6 בישראל והחל בגיבוש צעדים מעשיים לחיוב ספקי הגישה לאינטרנט (ISP) ליישם את הפרוטוקול.

איגוד האינטרנט הישראלי ממליץ שהמשרד יקבע ויפרסם תוכנית אסטרטגית לאומית למעבר תשתית האינטרנט הישראלית לIPv6. בנוסף, האיגוד ממליץ שהמשרד יסיים במהירות לגבש מסמך מדיניות שיכלול את צעדי האסדרה והתמריצים לפרישת תשתית IPv6 באופן מלא בכל הגופים הכפופים למשטר האסדרה מכח חוק התקשורת (בזק ושידורים), ושחובה זו תוגדר היטב.

בנוסף, עמדת האיגוד היא כי על המשרד להיות שותף לכל התהליכים שיתקיימו אצל גורמים אחרים הקשורים לתהליך, גם אם אינם נמצאים תחת סמכות האסדרה הקונקרטית של המשרד.

(2) מערך הסייבר הלאומי

עמדת איגוד האינטרנט הישראלי היא **שעל מערך הסייבר הלאומי לבחון את הטמעת IPv6 באסטרטגיית הגנת הסייבר של מדינת ישראל**, והתועלות והסיכונים הכרוכים במעבר זה. מומלץ כי המטה יבחן את משמעותיות הגנת הסייבר העולות מהסתמכות של גופים מפוקחים על ידם על פרוטוקול IPv4 וכן את הסיכונים האפשריים ממעבר לשימוש ב-IPv6 על ידם.

בנוסף, עמדת האיגוד היא כי על המערך, כמי שאמון על הפיכת ישראל לאחת מחמשת המדינות המובילות בעולם בסייבר, לקדם סוגיות של הגנת סייבר בהקשר של IPv6 גם בתוכניות המחקר והפיתוח המדינתיות בנושאי הגנת סייבר, ובמערך יחסי החוץ של ישראל בסוגיות סייבר שהוא אמון על קידומן.

(3) הרשות לאבטחת מידע

עמדת איגוד האינטרנט הישראלי היא כי על הרשות לאבטחת מידע בשב"כ (רא"ם) לבחון את משמעותיות הגנת הסייבר העולות מהסתמכות של גופים מפוקחים על ידם על פרוטוקול IPv4 ולבחון את הסיכונים האפשריים ממעבר לשימוש ב-IPv6 על ידם.

4) הממונה על התקשוב הממשלתי

עמדת איגוד האינטרנט הישראלי היא כי על הממונה על התקשוב הממשלתי לפעול למעבר כל גופי הממשלה לתמיכה מלאה ב- IPv6 בהובלת מערך ממשל זמין⁶² המשמש כ-ISP הממשלתי.

בנוסף, מומלץ כי הממונה על התקשוב הממשלתי כגוף המטה הקובע את תוכן הליכי הרכש בתחום מערכות המידע בשירות המדינה, יקבע **דרישה רוחבית לכלל מכרזי התשתית לתקשורת מחשבים, ציוד, תוכנה, תמסורת ושירותים עבור שירות המדינה לתמיכה מלאה ב-IPv6.**

5) הרשות לחדשנות

עמדת איגוד האינטרנט הישראלי היא כי על הרשות לחדשנות לבחון את האפשרות **להגדיר את המעבר ל-IPv6 כמנוע צמיחה של המשק, וכאמצעי להגברת החדשנות והתעשייה** (בדגש על קידום תחום ה-IoT). כחלק מכך, על הרשות לקיים בקרה וניטור על מידת המעבר של המשק ל-IPv6 ועל מידת ההשפעה שלו על הצמיחה.

6) ישראל דיגיטלית

עמדת איגוד האינטרנט הישראלי היא כי על ישראל דיגיטלית **לשלב את המעבר ל-IPv6 במסגרת המיזם, ולהגדירו כבסיס לאספקת שירותים ציבוריים המותאמים למאה ה-21**, לרבות שירותים מרחוק; הטמעת כלים טכנולוגיים בעסקים קטנים ובינוניים ועידוד מסחר מקוון; שיתוף מידע וידע ממשלתי ושימוש באמצעים מקוונים לשיפור וייעול השירות הניתן לאזרח; עידוד תחרויות ומיזמים יעודיים; ועוד.

7) הרשות להגנת הפרטיות

עמדת איגוד האינטרנט הישראלי היא כי על הרשות להגנת הפרטיות **לגבש עמדתה לגבי הסוגיות הקשורות לפרטיות במידע העולות מתהליך הטמעת פרוטוקול IPv6 בשדרת האינטרנט הישראלי**, ותסנכרן עמדות אלה עם גיבוש המדיניות הממשלתית על ידי משרדי הממשלה השונים ותוודא כי זו תיושם על ידי כלל הגופים המפוקחים על ידה.

⁶² https://www.gov.il/he/departments/units/e_government

ה.איגוד האינטרנט הישראלי

איגוד האינטרנט הישראלי ישמש גורם מוביל בכח המשימה לקידום פרישת IPv6 בישראל, בשיתוף כלל הגורמים הרלבנטיים.

בנוסף, האיגוד יקים קהילת ידע (פיסית ווירטואלית⁶³) אשר תכלול את כלל הגופים בעלי העניין בתחום ותהווה מוקד ידע לכל תהליך ההמרה וגיבוש המדיניות בישראל. הפורום יספק מידע על שלבי היישום השונים, עצות של מומחים ו-use cases. על הפורום לשרת את צוות המשימה הלאומי ולאפשר שיתוף מידע בין גופים שונים, לתמיכה הדדית בתהליכים ובבעיות שעולות במהלך השינוי. במסגרת פורום זה, יערכו סדנאות ייעודיות עם גורמים מהארץ ומחו"ל בעלי ניסיון שיסייעו לביצוע ההטמעה; יבוצעו כנסים מקצועיים, ימי עיון ויפורסמו כתבות ומאמרים הנוגעים לקידום הנושא.

⁶³ על בסיס הפורום <http://www.ipv6forum-israel.com>, אשר בו נעשה שימוש בעבר.

נספח א' - טבלת מדינות מובילות בהקצאת IPv6⁶⁴

Rank	Country	Code	Number	Percentage
1	United States	US	2 934 191 106	19.592 %
2	China	CN	1 537 933 341	10.269 %
3	United Kingdom	GB	1 188 298 926	7.934 %
4	Germany	DE	1 160 577 470	7.749 %
5	France	FR	804 192 349	5.370 %
6	Japan	JP	637 411 497	4.256 %
7	Australia	AU	588 317 690	3.928 %
8	Italy	IT	506 331 154	3.381 %
9	Netherlands	NL	420 217 124	2.806 %
10	Russian Federation	RU	372 637 941	2.488 %
11	Korea, Republic of	KR	344 391 685	2.300 %
12	Argentina	AR	325 323 312	2.172 %
13	Brazil	BR	307 701 624	2.055 %
14	South Africa	ZA	306 380 921	2.046 %

⁶⁴ מתוך האתר www-public.tem-tsp.eu/~maignon/. הנתונים מעודכנים לחודש פברואר 2018.

15	European Union	EU	284 557 322	1.900 %
16	Poland	PL	280 953 012	1.876 %
17	Egypt	EG	269 090 818	1.797 %
18	Spain	ES	267 845 653	1.788 %
19	Switzerland	CH	165 609 609	1.106 %
20	Taiwan	TW	154 992 647	1.035 %
21	Sweden	SE	124 387 634	0.831 %
22	Iran	IR	118 161 414	0.789 %
23	Norway	NO	117 440 848	0.784 %
24	Czech Republic	CZ	115 474 531	0.771 %
25	Ukraine	UA	111 345 777	0.743 %
26	Turkey	TR	107 872 277	0.720 %
27	India	IN	97 976 699	0.654 %
28	Austria	AT	90 505 352	0.604 %
29	Denmark	DK	75 628 610	0.505 %
30	Belgium	BE	71 761 965	0.479 %
31	Romania	RO	64 159 808	0.428 %

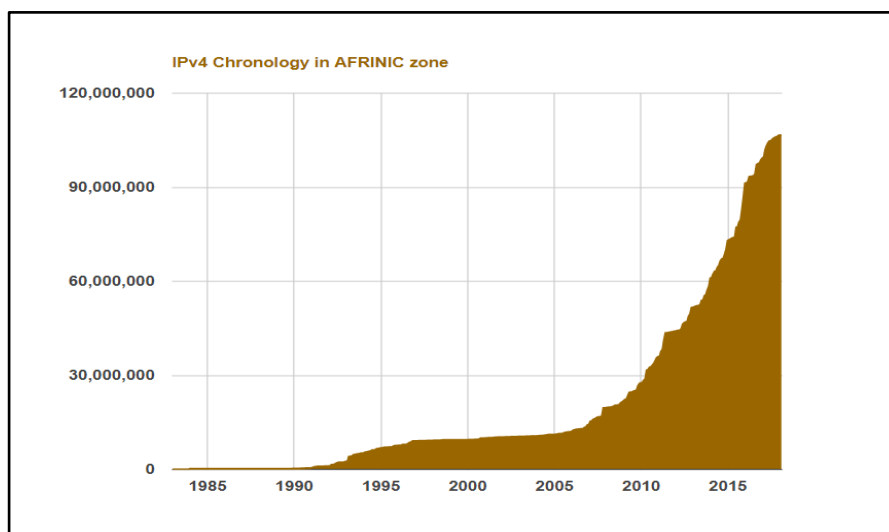
32	Finland	FI	56 098 860	0.375 %
33	Ireland	IE	54 067 209	0.361 %
34	Bulgaria	BG	48 693 283	0.325 %
35	Canada	CA	45 111 323	0.301 %
36	Slovakia	SK	27 656 209	0.185 %
37	Israel	IL	27 459 592	0.183 %
38	Mexico	MX	26 214 433	0.175 %
39	Lebanon	LB	25 427 971	0.170 %
40	Hong Kong	HK	24 707 225	0.165 %
41	Hungary	HU	24 182 791	0.161 %
42	Portugal	PT	22 937 604	0.153 %
43	Venezuela	VE	22 675 459	0.151 %
44	Iraq	IQ	22 478 848	0.150 %
45	Indonesia	ID	21 037 483	0.140 %
46	Saudi Arabia	SA	20 905 999	0.140 %
47	Slovenia	SI	19 398 720	0.130 %
48	Luxembourg	LU	19 267 594	0.129 %

49	Bangladesh	BD	19 071 027	0.127 %
50	Serbia	RS	18 153 479	0.121 %
51	Estonia	EE	17 891 337	0.119 %
52	Greece	GR	17 760 261	0.119 %
53	Jamaica	JM	17 039 361	0.114 %

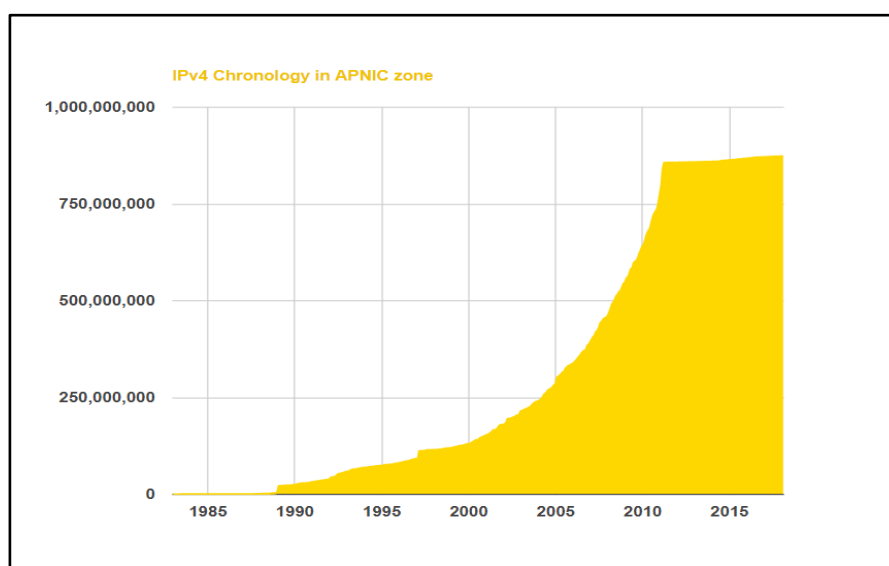
נספח ב' - הקצאת כתובות IPv4 בחלוקה לאזורים

(נכון לחודש פברואר 2018)⁶⁵

אחוז הקצאת IPv4 באזור אפריקה



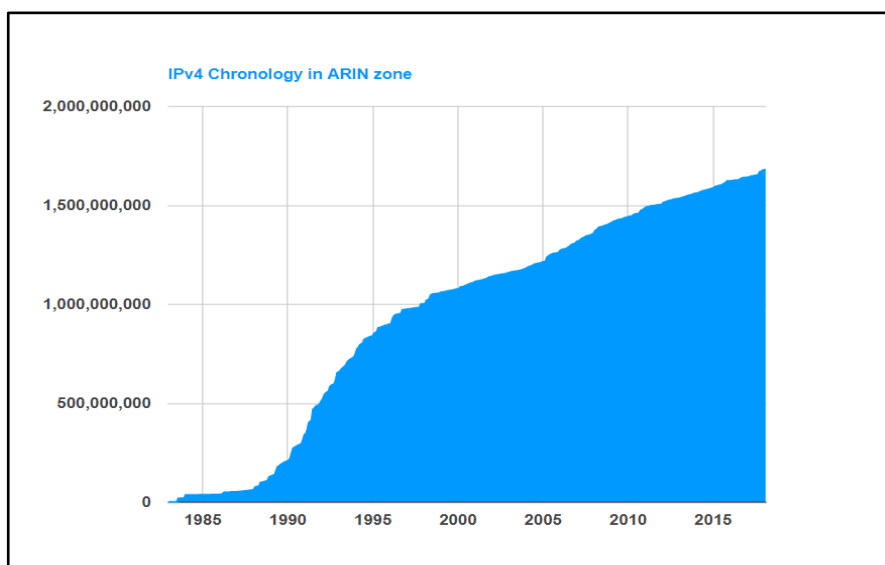
אחוז הקצאת IPv4 באזור אסיה ואוקיאניה



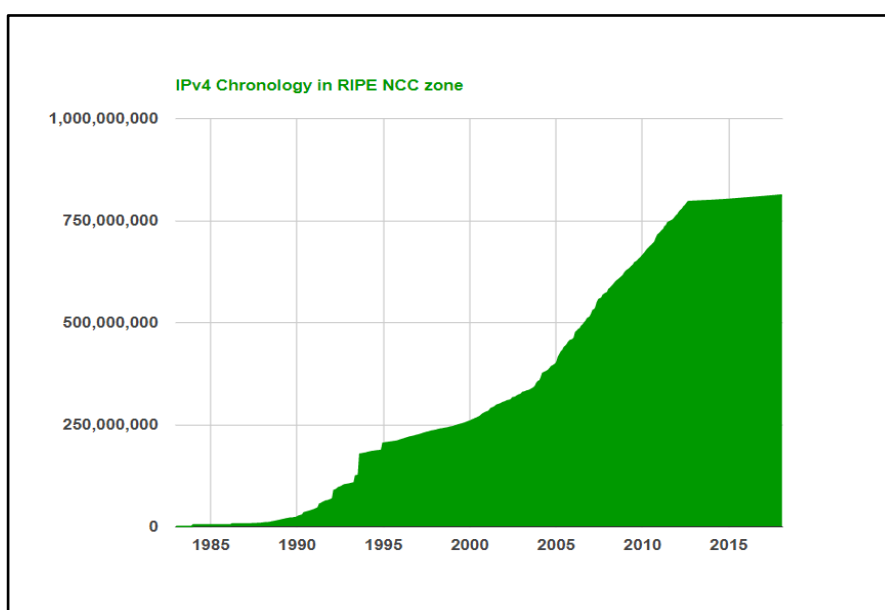
אחוז הקצאת IPv4 באזור באזור צפון אמריקה

⁶⁵ לקוח מתוך:

http://www-public.tem-tsp.eu/~maignon/RIR_Stats/RIR_Delegations/ByRIR/Stats-ByRIR.html



אחוז הקצאת IPv4 באזור באזור אירופה והמזה"ת



נספח ג' - שיטות טכנולוגיות עיקריות להמרה מפרוטוקול IPv4 לפרוטוקול IPv6

1) 6to4

בשיטת המרה 6to4, מקושרות רשתות התומכות בפרוטוקול IPv6 באמצעות נתבי ממסר מיוחדים (המכונים בשם זה - 6to4). נתבי הממסר מאפשרים למנות (Packets) של IPv4 להיות מומרות למנות של IPv6 וכך מנות של IPv4 ומנות של IPv6 יכולות להיות משונעות ליעדים התומכים בפרוטוקול IPv6. בנוסף, הנתבים "אורזים" מנות של IPv6 בתוך IPv4, ומאפשרות שינוע שלהם ליעדי רשתות IPv4.

2) IPv6 Rapid Deployment – 6rd

המגבלה בשיטת ה-6to4 היא שההמרה אינה תומכת בכתובות פרטיות. מגבלות השיטה משמעותיות, ולכן פותחה שיטת ⁶⁶IPv6 Rapid Deployment – 6RD. השיטה נתמכת רק בתוך רשת של ספק אינטרנט, לצורך המעבר מ-IPv4 ל-IPv6, ומאפשרת יתרון של שליטה וניהול עצמאי של הרשת ומעבר בין הגרסאות השונות.

3) TEREDO

פרוטוקול Teredo⁶⁷, אמור לגשר בין פרוטוקול IPv6 לבין גישה לכל סוג של פרוטוקול שהוא (לרבות כתובות פרטיות שתורגמו ב-NAT שאינן נתמכות ב-6to4) וכמובן שבכיוון ההפוך (מנות של פרוטוקולי IPv4 שנמצאים מאחורי NAT) שיתקשרו עם ציוד התומך בפרוטוקול IPv6. שיטה זו אמורה לגשר את תהליך המעבר ל-IPv6, עד לתמיכה "טבעית" (native) ב-IPv6, אך אינה חפה מקשיים.

4) DNS64-I NAT64

פתרונות נוספים שנמצאים בשימוש, בעיקר אצל מפעילים סלולריים, נקראים NAT64⁶⁸ ו-DNS64⁶⁹. פתרונות אלה דומים בעקרון לפתרון המרה אלגוריתמית של כתובות (NAT-PT⁷⁰) ואולם הם טובים יותר בעיקר למכשירי טלפון סלולריים הפועלים בגרסה IPv6 ואשר ניגשים לקבל מידע מאתרים הנמצאים בפרוטוקול IPv4.

⁶⁶ <https://tools.ietf.org/html/rfc5569>

⁶⁷ <https://tools.ietf.org/html/rfc4380>

⁶⁸ <http://tools.ietf.org/html/rfc6146>

⁶⁹ <http://tools.ietf.org/html/rfc6147>

⁷⁰ <https://tools.ietf.org/html/rfc2766> ו- <https://tools.ietf.org/html/rfc2765>

נספח ד' - מקורות מידע נוספים להרחבה

<http://www.iana.org/IANA> (א)
<https://www.ripe.net/> Ripe
<http://www.ipv6forum.com> IPv6 forum
<https://www.akamai.com/> Akamai
<https://www.google.com/intl/en/ipv6> Google
www.cu.ipv6tf.org/ Technical Brief IPv6 White Paper / 3COM University
<http://www.internetsociety.org/> IPv6 For All / Internet Society
<https://www.ovum.com/> -Ovum Research
<http://ipv6-test.com> - IPv6 Test
<http://www.oecd.org/sti/ieconomy/> OECD
www.isoc.org.il – איגוד האינטרנט הישראלי
<http://www.csd.uoc.gr> - 3COM University
<http://www.internetsociety.org> - Internet Society
www.public.temtp.eu- Regional Internet Registries Statistics
<http://www.worldipv6launch.org> - World IPv6 Launch
www.vyncke.org - IPv6 Deployment Status
<http://www.ispreview.co.uk> - ISP Review
tools.ietf.org - Internet Engineering Task Force (IETF)
<http://www.iotworldalliance.org> - IOT World Alliance
labs.apnic.net - Apnic
http://iot6.eu/ipv6_for_iot - IoT6.EU
<https://securityintelligence.com> - IBM Security IPv6