

6. פרוטוקול האינטרנט (IP)

הפרוטוקול הזה אחראי לנתב חבילות נתונים ברחבי האינטרנט, בדומה לאופן שבו דואר אחראי לנתב מכתבים ברשת הדואר.

כמו בדואר, נתונים באינטרנט צריכים להיות מסומנים עם כתובת מקור וכתובת יעד, הנקראות כתובת IP. כתובת ה-IP היא רצף של בייטים שמזהה באופן ייחודי כל מחשב באינטרנט.

6.1 מונחים

- **Host** - שם נוסף ל"מחשב".

6.2 שתי גרסאות נפוצות

ישנן שתי גרסאות נפוצות של IP: גרסה 4 וגרסה 6.

גרסת IP 4 נקראת "IPv4" או פשוט "IP".

גרסת IP 6 בדרך כלל מצוינת באופן מפורש כ-"IPv6".

אתה יכול להבחין בהבדל בין השתיים על ידי הצצה בכתובת IP:

דוגמת כתובת IP גרסה 4: 192.168.1.3

דוגמת כתובת IP גרסה 6: fe80::c2b6:f9ff:fe7e:4b4

ההבדל העיקרי הוא מספר הבייטים שמרכיבים את מרחב הכתובת. IPv4 משתמש ב-4 בייטים לכל כתובת, ו-IPv6 משתמש ב-16 בייטים.

6.3 תתי-רשתות

כל כתובת IP מחולקת לשני חלקים.

הביטים הראשונים בכתובת ה-IP מזהים רשתות נפרדות.

הביטים האחרונים בכתובת ה-IP מזהים מחשבים (hosts) בתוך אותה רשת.

הרשתות הנפרדות נקראות תתי-רשתות, ומספר המחשבים שהן יכולות לתמוך בהם תלוי בכמה ביטים הוקצו כדי לזהות מחשבים בתת-הרשת הזו.

לדוגמה לא-אינטרנטית, נניח שיש לנו "כתובת" בת 8 ביטים, ונגיד שה-6 ביטים הראשונים הם מספר הרשת וה-2 ביטים האחרונים הם מספר המחשב.

כתובת כזו:

00010111

מחולקת לשני חלקים (כיוון שאמרנו שה-6 ביטים הראשונים הם מספר הרשת):

רשת מחשב

כך שזו רשת 5 (101 בבינארי), מחשב 3 (11 בבינארי).

חלק הרשת תמיד מגיע לפני חלק המחשב.

שימו לב שאם יש רק שני ביטים ל"מחשב", אז יכולים להיות רק 4 מחשבים ברשת, ממוספרים 0, 1, 2 ו-3 (או 00, 01, 10 ו-11 בבינארי).

וב-IP, למעשה יהיו רק שני מחשבים, כיוון שכתובות שבהן כל הביטים אפס או כל הביטים אחדים הן שמורות.

הפרקים הבאים יסתכלו על דוגמאות ספציפיות של תתי-רשתות עבור IPv4 ו-IPv6. החלק החשוב עכשיו הוא שכל כתובת מחולקת לחלק רשת וחלק מחשב, עם חלק הרשת קודם.

6.4 פרוטוקולים נוספים בשכבת IP

ישנם כמה פרוטוקולים קשורים שפועלים יחד עם IP ובאותה שכבת רשת.

- **ICMP:** פרוטוקול הודעות שליטה באינטרנט, מנגנון לתקשורת בין צמתים של IP כדי לשוחח על מידע בקרה של IP.
- **IPSec:** אבטחת פרוטוקול אינטרנט, הצפנה ואימות. נפוץ בשימוש עם VPN (רשתות פרטיות וירטואליות).

משתמשים בדרך כלל בקשר עם ICMP כאשר משתמשים בכלי ping. זה משתמש בהודעות "echo request" ו-"echo response" של ICMP.

כלי traceroute משתמש בהודעות "time exceeded" של ICMP כדי לברר כיצד החבילות מנותבות.

6.5 רשתות פרטיות

ישנן רשתות פרטיות שמוסותרות מאחורי נתבים שאין להן כתובת IP ייחודית ברחבי העולם במכונות שלהן. (אך יש להן כתובות ייחודיות בתוך הרשת המקומית עצמה).

זה מתאפשר בעזרת מנגנון שנקרא NAT (תרגום כתובת רשת). אבל זה סיפור לעתיד.

בינתיים, נניח שכל הכתובות שלנו ייחודיות ברחבי העולם.

6.6 כתובת IP סטטית מול דינמית, ו-DHCP

אם יש לך לקוחות שפונים לאתר שלך, או אם יש לך שרת שאתה רוצה להתחבר אליו דרך SSH באופן תדיר, תצטרך כתובת IP סטטית. זה אומר שתקבל כתובת IP ייחודית ברחבי העולם והיא לא תשתנה.

זה כמו שיהיה לך מספר בית שלא משתנה. אם אתה רוצה שיבואו אליך הביתה פעמים רבות, זה חייב להיות המצב.

אבל מכיוון שיש מספר מוגבל של כתובות IPv4, כתובות IP סטטיות עולות יותר כסף. לרוב ספקי אינטרנט יש בלוק של כתובות IP על תת-רשת שהם מקצים באופן דינמי על פי דרישה.

זה אומר שכאשר אתה מאתחל את מודם ה-broadband שלך, ייתכן שתקבל כתובת IP ציבורית שונה כשחוזר לפעולה. (אלא אם כן שילמת על כתובת IP סטטית).

באמת, כשאתה מחבר את הלפטופ שלך ל-WiFi, אתה בדרך כלל מקבל כתובת IP דינמית. המחשב שלך מתחבר לרשת המקומית ומפיץ חבילה שאומרת "היי, אני כאן! משהו יכול לומר לי מה כתובת ה-IP שלי? בבקשה, עם סוכר מעל?"

וזה בסדר כי אנשים בדרך כלל לא מנסים להתחבר לשרתים בלפטופ שלך. לרוב הלפטופ הוא שמתחבר לשרתים אחרים.

איך זה עובד? על אחד השרתים ברשת המקומית יש תוכנה שמאזינה לבקשות כאלה, העומדות בתקן DHCP (פרוטוקול קונפיגורציית מארח דינמית). שרת ה-DHCP עוקב אחרי איזה כתובת IP על תת-רשת כבר הוקצתה לשימוש, ואיזה פנויה. הוא מקצה כתובת פנויה ושולח חזרה תגובת DHCP עם כתובת ה-IP החדשה שלך, יחד עם מידע נוסף על הרשת המקומית שהמחשב שלך זקוק לה (כמו מסכת תת-רשת, וכו').

אם יש לך WiFi בבית, סביר להניח שכבר יש לך שרת DHCP. רוב הנתבים שמגיעים מספקי אינטרנט מגיעים עם DHCP מוגדר כברירת מחדל, כך שהלפטופ שלך מקבל את כתובת ה-IP שלו ברשת המקומית.

6.7 חישוב

כמה פעמים יותר כתובות IPv6 יש בהשוואה לכתובות IPv4?

יישומים בדרך כלל גם מבצעים הצפנה בעצמם (למשל, SSH או דפדפנים עם HTTPS). השער את היתרונות או החסרונות של שימוש ב-IPSec בשכבת האינטרנט במקום לבצע הצפנה בשכבת היישום.

אם תת-רשת הקצתה 5 ביטים לזיהוי מחשבים, כמה מחשבים היא יכולה לתמוך בהם? אל תשכח שכתובות עם כל הביטים אפס או כל הביטים אחדים לשם המחשב הן שמורות.

מהו היתרון בכתובת IP סטטית? איך זה קשור ל-DNS?