פרוטוקול הDNS

מסמך זה ניתן להפצה באופן חופשי, כל עוד הוא נשאר ללא כל שינוי ותוספות.
כל נזק, ישיר או עקיף, שיגרם בעקבות מסמך זה הוא באחריות הקורא בלבד.
כל הזכויות שמורות ל**ניר אדר**.

Nir Adar
Email: underwar@hotmail.com
Home Page: http://underwar.cjb.net

במסמך זה נסביר מעט על הדרך בה עובד פרוטוקול הDNS (Domain Name Server).
נסקור דוגמא שבה נראה את פעולתו של הפרוטוקול.
ידע קודם נדרש: מושגים בסיסיים בתחום האינטרנט.

נתחיל בדוגמא, שבעזרתה נסביר כיצד פרוטוקול זה עובד:
מחשב לקוח (Client) שבדוגמא שלנו הוא יהיה bla.bibi.com רוצה את כתובת הIP של שרת בשם www.heike.com .

השלבים של פעולה זו:
הלקוח (bla.bibi.com) שולח בקשה לכתובת (request of resolution) של השרת www.heike.com. כדי למצוא את הכתות, bla.bibi.com משתמש בdns.bibi.com עבור DNS.

זה נראה ככה:

111.1.2.123 = bla.bibi.com
111.1.2.222 = dns.bibi.com

הצורה בה נשלחת ההודעה:

ערוץ:כתובת שרת DNS--->ערוץ:כתובת שולח

דוגמא:

111.1.2.123:2999 ---> 111.1.2.222:53

הפקודה בC שעושה את הפעולה של בקשת הכתובה היא gethostbyname():
לדוגמא:

gethostbyname("www.heike.com");

ממשיך בדוגמא שלנו:

[bla.bibi.com] [dns.bibi.com]
111.1.2.123:2999 ---> [?www.heike.com] ---> 111.1.2.222:53

הערה: הערוץ (Port) של DNS הוא תמיד 53.

נמשיך הלאה:

[dns.bibi.com] [ns.internic.net]
111.1.2.222:53 ---> [?www.heike.com] ---> 198.41.0.4:53

dns.bibi.com שואל את ns.internic.net מהו שרת הDNS היכול לתת לו את הכתובת של www.heike.com.

[ns.internic.net] [dns.bibi.com]
198.41.0.4:53 ---> [ns for.com is 144.44.44.4] ---> 111.1.2.222:53

ns.internic.net מודיע ל-dns.bibi.com שהשרת המספק את הכתובות של האתרים המסתיימים ב-com. הוא for.com והכתובת שלו היא 144.44.44.4.

[dns.bibi.com] [ns.for.com]
111.1.2.222:53 ---> [?www.heike.com] ---> 144.44.44.4:53

התשובה המתקבלת מ-ns.for.com היא:

[ns.for.com] [dns.bibi.com]
144.44.44.4:53 ---> [ns heike.com is 31.33.7.4] ---> 111.1.2.222:53

כעת יש לנו את הIP של שרת DNS שבו יש רישום של heike.com.
אנו פונים עכשיו אל השרת הזה:

[dns.bibi.com] [ns.heike.com]
111.1.2.222:53 ---> [?www.heike.com] ---> 31.33.7.4:53

וממנו אנו מקבלים את התשובה:

[ns.heike.com] [dns.bibi.com]
31.33.7.4:53 ---> [www.heike.com == 31.33.7.44] ---> 111.1.2.222:53

ואז dns.bibi.com שולח את התשובה לbla.bibi.com:

[dns.bibi.com] [bla.bibi.com]
111.1.2.222:53 ---> [www.heike.com == 31.33.7.44] ---> 111.1.2.123:2999

מבנה חבילה (packet) של הודעת DNS:

דגלים	ID
מספר התשובות	מספר השאלות
לא מעניין	*לא מעניין*
שאלה	
תשובה	
לא מעניין	

הקטעים הלא מעניינים זה קטעים שלא רלוונטיים עבור הנקודה אותה אני רוצה להראות.
הקטע של הדגלים מציין האם מגיעה עכשיו תשובה או שאלה, דיווחים על הצלחה וכישלון ועוד.

המבנה של השאלה:

שם השאלה	
סוג בקשה	סוג שאלה

שם השאלה הוא דבר כזה:
אם השרת המבוקש הוא www.heike.com
השאלה תהיה:

[3|w|w|w|5|h|e|I|k|e|3|c|o|m|0]

או במקרה שרוצים את השם של כתובת (לדוגמא 44.33.88.123):

[2|4|4|2|3|3|2|8|8|3|1|2|3|0]

סוג השאלה וסוג הבקשה מקבלים את אותו הערך. אלו קובעים האם מקבלים את הכתובת משם או את השם מכתובת.

EOF

כל הזכויות שמורות לניר אדר – 2002
Email: underwar@hotmail.com