TTL · ICMP · ARP · כלי אבחון ושיטת עבודה

שבוע 4 · 08/10–04/10 · **בנימין נאור**

למחשב יש את כתובת ה-`IP` של היעד — ועדיין הוא לא יכול לשלוח: המסגרת צריכה כתובת `MAC`. הפרוטוקול שמתרגם `IP` ל-`MAC` נקרא `ARP`. אחריו נכיר את `ICMP` — הפרוטוקול שמאחורי `ping` — ואת ארבעת הכלים שכל מנהל רשת מריץ לפני שהוא נוגע בכבל.

1. `ARP` — מ-`IP` ל-`MAC`

החבילה נושאת `IP`; המסגרת שעוטפת אותה נושאת `MAC`. כדי לבנות את המסגרת התחנה חייבת לדעת את ה-`MAC` של **הקפיצה הבאה**. אם היא לא יודעת — היא שואלת את כל הרשת:

```
PC-A (192.168.1.10) wants to reach 192.168.1.20

  ARP REQUEST  (broadcast, dst MAC = FF:FF:FF:FF:FF:FF)
     "Who has 192.168.1.20?  Tell 192.168.1.10"
     --> every host on the LAN receives it

  ARP REPLY    (unicast, dst MAC = PC-A)
     "192.168.1.20 is at 00:1B:44:11:3A:B7"
     --> only PC-A receives it

  PC-A ARP table:  192.168.1.20  ->  00:1B:44:11:3A:B7  (dynamic)
```

הבקשה מוצפת לכולם כי אף אחד לא יודע מי היעד; התשובה חוזרת ישירות כי השואל כבר ידוע מהבקשה.

מצב	למי שולחים `ARP`	למה
היעד באותה רשת	ליעד עצמו	המסגרת מגיעה אליו ישירות
היעד ברשת אחרת	לשער ברירת המחדל	הנתב הוא הקפיצה הבאה; ה-`IP` של היעד נשאר בחבילה

⚠ **שימו לב** · `ARP` הוא **מקומי** תמיד. מעבר לנתב אף אחד לא יודע את ה-`MAC` של התחנה שלכם — ולא צריך. זה ההבדל בין שכבה 2 לשכבה 3.

2. טבלת `ARP` — בתחנה ובנתב

התשובה נשמרת בטבלה לזמן קצוב (דקות), כדי לא לשאול שוב על כל חבילה. הפקודות:

איפה	פקודה	מה רואים
`Windows`	`arp` -a	`IP` ↔ `MAC` · `dynamic/static`
נתב סיסקו	`show ip arp`	`IP` · `Age` · `MAC` · `Interface`
ניקוי בתחנה	`arp` -d	מוחק — ה-`ping` הבא ישלח `ARP` מחדש

טיפ · ב-`Packet Tracer: Desktop` → `Command Prompt` → `arp` -a. אם הטבלה ריקה — פשוט לא הייתה תעבורה לאחרונה.

3. `ICMP` — `ping` ו-`TTL`

`ICMP` הוא 'שירות ההודעות' של `IP`: 'הגעתי', 'לא הגעתי', 'פג הזמן'. `ping` שולח `ICMP Echo Request` ומחכה ל-`Echo Reply`. הוא מודד שני דברים: **זמן** (`ms`) ו**אובדן** (כמה לא חזרו).

`TTL` (**`Time To Live`**) הוא שדה בכותרת ה-`IP` — לא במסגרת! — שמתחיל בערך כמו 64 או 128, וכל נתב מוריד ממנו 1. כשהוא מגיע ל-0 הנתב זורק את החבילה ושולח `ICMP Time Exceeded`. כך חבילה אבודה לא מסתובבת לנצח.

```
ping 8.8.8.8
Reply from 8.8.8.8: bytes=32 time=14ms TTL=117

  TTL started at 128 (Windows)  ->  128 - 117 = 11 routers on the way

tracert 8.8.8.8
  1    1 ms   192.168.1.1        <- TTL=1 : first router answers
  2    9 ms   10.0.0.1           <- TTL=2
  3   12 ms   *  *  *            <- router that filters ICMP
  ...
 11   14 ms   8.8.8.8
```

`traceroute` מנצל את `TTL`: שולח עם `TTL`=1, 2, 3... וכל נתב שמגיע לאפס 'מתוודה' ב-`Time Exceeded`. כוכביות = נתב שלא עונה, לא בהכרח תקלה.

היגד	נכון?
`TTL` מוגדר במסגרת `Ethernet`	לא — בכותרת `IP`
`TTL` קטן ב-1 בכל נתב	כן
`TTL` נקבע על ידי שרת `DNS`	לא — על ידי מערכת ההפעלה השולחת
`TTL` גבוה = החבילה מגיעה מהר יותר	לא — זה מונה, לא מהירות

⚠ **שימו לב ·** ארבעת ההיגדים האלה הופיעו בבחינת 2026 (שאלה 4). לדעת אותם.

4. ארבעת הכלים

כלי	מה מראה	מתי
`ipconfig` / `all`	`IP` · מסכה · שער · `DNS` · `MAC`	תמיד ראשון — מה בכלל מוגדר
`ping` ‹יעד›	הגעה · זמן · `TTL`	האם הוא שם
`tracert` ‹יעד›	כל נתב במסלול	איפה זה נעצר
`arp` -a	`IP` ↔ `MAC` ברשת המקומית	האם השכן/השער נמצא
`ipconfig` / `displaydns`	מטמון ה-`DNS` של התחנה	שם לא נפתר? (בחינה 2023)
`nslookup` ‹שם›	איזה `IP` יש לשם	בעיית `DNS` או בעיית רשת

5. שיטת עבודה: `Top-Down` · `Bottom-Up` · `Divide and Conquer`

כשמשהו 'לא עובד', לא מנחשים — הולכים לפי שכבות, וכל בדיקה שוללת שכבה.

```
TOP-DOWN example: "the internet doesn't work"
  1. open another site / nslookup   -> works?  problem is the site (L7)
  2. ping 8.8.8.8                   -> works?  problem is DNS
  3. ping default gateway           -> works?  problem is beyond the router
  4. ipconfig  (address? mask? gw?) -> wrong?  fix config (L3)
  5. link light / cable             ->         physical (L1)
```

בבחינה (2023 ש'1ג) ביקשו לסדר בדיקות לפי `Top-Down`: דפדפן → שרת → כבל. הכיוון הוא מהיישום כלפי מטה.

שיטה	כיוון	מתי מתאימה
`Top-Down`	7 → 1: דפדפן, `DNS` , `ping` לשער, `ipconfig` , כבל	המשתמש 'לא גולש' והכול נראה מחובר
`Bottom-Up`	1 → 7: כבל, נורית, `ipconfig` , `ping` ...	ריח של כבל/פורט/חומרה
`Divide and Conquer`	מתחילים ב-3 (`ping`) ומשם למעלה או למטה	כשלא ברור — `ping` לשער חוצה את הבעיה לשניים

דוגמה פתורה

השאלה

`PC-A` (192.168.1.10/24, שער 1.) שולח `ping` ל-10.0.0.5. תארו את ה- `ARP` וה- `ICMP` צעד-צעד, ומה יהיה בטבלת ה- `ARP` של `PC-A` בסוף.

הפתרון צעד אחר צעד

1. `AND` : 10.0.0.5 אינו ב-192.168.1.0/24 → היעד רחוק → שולחים לשער 192.168.1.1.
2. `ARP` : `PC-A` בודק בטבלה את 192.168.1.1. אין → `ARP request` (`broadcast`) '`Who has 192.168.1.1` ?'. הנתב עונה ב- `unicast` עם ה- `MAC` שלו.
3. **מסגרת**: יעד `MAC` = הנתב · חבילה: יעד `IP` = 10.0.0.5 · `ICMP Echo Request` · `TTL`=128.
4. **הנתב** מוריד `TTL` ל-127, מחליף את המסגרת (`MAC` חדשים למקטע הבא) ומעביר. וכן הלאה בכל נתב.
5. **התשובה** חוזרת באותה דרך. `PC-A` מציג `time` ו- `TTL` .
6. **טבלת** `ARP` **של** `PC-A` : רשומה אחת בלבד — 192.168.1.1 ↔ `MAC` של הנתב. ה- `MAC` של 10.0.0.5 לא מופיע ולא יופיע לעולם.

תשובה · `ARP` תמיד לקפיצה הבאה; `ICMP` מקצה לקצה; `TTL` יורד ב-1 בכל נתב. שלוש שכבות, שלוש כתובות, שלושה כלים.

תרגילים — פתרו לבד לפני שאתם בודקים בכיתה

1. למה תחנה צריכה `ARP` אם היא כבר יודעת את ה- `IP` של היעד?
2. `ARP request` נשלח ב- `broadcast` . למה ה- `reply` נשלח ב- `unicast` ?

3. היעד ברשת אחרת. איזה `MAC` יופיע כיעד במסגרת?

4. `ping` מציג `TTL`=57. אם השולח הוא `Linux` (`TTL` התחלתי 64), כמה נתבים בדרך?

5. `tracert` מראה * * * בשורה 3 אבל מגיע ליעד בשורה 9. יש תקלה?

6. 'האינטרנט לא עובד'. כתבו שלוש בדיקות בסדר `Top-Down`.

7. נכון או לא: `TTL` הוא הזמן בשניות שחבילה יכולה לחיות.

8. איזו פקודה מציגה את מטמון ה-`DNS` של התחנה?

דף עבודה — מעבדה 4 (הכנה) — ארבעה כלים על המחשב שלכם

שם: _____ תאריך: _____ חוליה: _____

המטרה: להריץ את הכלים על רשת אמיתית ולקרוא את הפלט. המעבדה המלאה ב-`PT` — בשבוע הבא.

מהלך — סמנו כל שלב שהושלם

- ☐ פתחו `Command Prompt` (`Windows`: `cmd`).
- ☐ `ipconfig` / `all` — רשמו: `IP` · מסכה · שער · `DNS` · `MAC` (`Physical Address`).
- ☐ `ping` ‹השער› — רשמו זמן ו-`TTL`. `ping 8.8.8.8` — רשמו `TTL`. חשבו כמה נתבים.
- ☐ `tracert 8.8.8.8` — ספרו שורות. סמנו שורות עם * * *.
- ☐ `arp` -a — רשמו את הרשומה של השער. השוו ל-`MAC` שקיבלתם? (הוא של הנתב, לא שלכם.)
- ☐ `ipconfig` / `displaydns` — האם יש שם אתר שביקרתם בו?
- ☐ כתבו ב-4 שורות: מה כל כלי גילה לכם על הרשת שלכם.

רישום התוצאות

#	מה למלא	חישוב · הערות · ראיות (פלט פקודה)
1	`IP` _____ · מסכה _____ · שער _____ · `DNS` _____ · `MAC` _____	_____
2	`ping` שער: זמן _____ `TTL` _____ · `ping 8.8.8.8: TTL` _____ → נתבים _____	_____
3	`tracert` : מספר שורות _____ · שורות עם * _____	_____
4	`arp` -a: השער ↔ `MAC` _____	_____
5	ההסבר (4 שורות): _____	_____

רפלקציה — שתי שורות

מה היה הכי קשה, ומה פתר את זה?

מה הייתי עושה אחרת בפעם הבאה?

אישור המורה: ☐ שאלון היחידה ב-Moodle (100) ☐ שיעורי הבית (30) · **XP** _____ · תג: ☐

בלש/ית הרשת · חתימה _____

כרטיס יציאה — 3 שאלות, 5 דקות, נמסר ביציאה

1. `ARP request` נשלח ב-?

2. היעד רחוק — למי `ARP` ?

3. `TTL` יורד ב-1 איפה?

עוד לבדיקה עצמית — ענו בעל פה, בלי להסתכל אחורה

1. `Top-Down` מתחיל באיזו שכבה?

מילון מונחים

עברית	אנגלית	הסבר קצר
פרוטוקול פתרון כתובות	`ARP`	מתרגם `IP` ל-`MAC` ברשת המקומית
בקשת ARP	`ARP Request`	`broadcast` : מי מחזיק את ה-`IP` הזה
תשובת ARP	`ARP Reply`	`unicast` : אני, וזה ה-`MAC` שלי
פרוטוקול הודעות בקרה	`ICMP`	הודעות של `IP` : `echo` , `unreachable` , `time exceeded`
זמן חיים	`TTL`	מונה קפיצות בכותרת `IP` ; יורד ב-1 בכל נתב
מעקב מסלול	`traceroute / tracert`	מציג את הנתבים בדרך ליעד
מלמעלה למטה	`Top-Down`	אבחון משכבה 7 לשכבה 1

להעמקה

בספר הקורס

- **ITN 9.2.8** — ARP Issues—ARP Broadcasts and ARP Spoofing · עמוד 307
- **ITN 13.1** — ICMP Messages · עמוד 444
- **ITN 13.2.2** — Ping the Loopback · עמוד 450

קבצים שנעבוד איתם

- ITN_Module_9.pptx
- ITN_Module_13.pptx
- ENSA_Module_12.pptx
- 9.2.9 Packet Tracer - Examine the ARP Table.pka
- 3.7.10 Lab - Use Wireshark to View Network Traffic.docx