מעבדה: ARP, ICMP וכלי אבחון (על ARP)

שבוע 5 · 15/10–11/10 · **בנימין נאור**

בשבוע שעבר למדתם מה `ARP` עושה ומה `TTL` סופר. היום רואים את זה בפועל בשלוש פעילויות רשמיות של סיסקו: טבלת ה-`ARP` , `ping` ו-`traceroute` על מסלול של כמה נתבים, ותקלה שאתם מאבחנים לפי `Top-Down` — עם טבלת תיעוד. הציון על התיעוד, לא רק על התיקון.

1. איך עובדים עם פעילות `PT` רשמית

פעילויות סיסקו (`pka`.) פותחות חלון הנחיות באנגלית ומציגות אחוז השלמה (`Completion`) בפינה. הכללים:

כלל	למה
קוראים את ההנחיה עד הסוף לפני שלוחצים	חצי מהטעויות — דילוג על משפט
מעתיקים לדף העבודה שורה אחת מכל פלט	`Completion 100` % בלי הבנה = 0
צילום מסך של ה-`Completion` בסוף	זו ההוכחה שהוגש
`Check Results` מראה מה חסר	לא לנחש — לבדוק

טיפ · `Alt` +D פותח את חלון ה-`Activity` ב-`PT` אם סגרתם אותו בטעות.

2. חלק א — 9.2.9 טבלת ה-`ARP`

מה תראו: `arp` -a ריק, `ping` , ואז רשומה. ב-`Simulation` — הבקשה מתפצלת לכל היציאות והתשובה חוזרת בקו אחד. בנתב, `show ip arp` מציג רשומות לכל הרשתות שהוא מחובר אליהן.

```
PC> arp -a
No ARP Entries Found
PC> ping 172.16.31.3
...
PC> arp -a
  Internet Address      Physical Address      Type
  172.16.31.3           0001.4374.a9a3        dynamic

Router# show ip arp
Protocol  Address       Age (min)  Hardware Addr   Type   Interface
Internet  172.16.31.1   -          0001.9640.7e01  ARPA   GigabitEthernet0/0
Internet  172.16.31.2   4          00e0.f9d8.e3bc  ARPA   GigabitEthernet0/0
```

הרשומה עם `Age` '-' היא הנתב עצמו. השאר — תחנות שדיברו איתו בדקות האחרונות.

3. חלק ב — 13.2.7 `ping` ו- `traceroute`

המסלול עובר דרך כמה נתבים. לכל `ping` רושמים `TTL`, ומחשבים כמה נתבים היו בדרך. ואז `tracert` — וסופרים שורות. שני המספרים חייבים להתאים.

```
PC> ping 10.10.10.1
Reply from 10.10.10.1: bytes=32 time=1ms TTL=254   <- 255-254 = 1 router

PC> tracert 10.10.10.1
  1   0 ms   192.168.1.1
  2   1 ms   10.10.10.1      <- destination itself (not a router)

  routers on the path = lines - 1 = 1   OK
```

נתב סיסקו מתחיל `TTL` ב-255; `Windows` ב-128; `Linux` ב-64. השורה האחרונה ב- `tracert` היא היעד — לא נתב.

> ⚠ **שימו לב ·** כוכביות (* * *) בשורה = נתב שלא עונה ב- `ICMP`. אם היעד מגיע בסוף — אין תקלה.

4. חלק ג — 13.3.1 תקלה לפי `Top-Down`

תחנה לא מגיעה ליעד. לא מנחשים ולא מתקנים — קודם טבלה:

#	בדיקה	תוצאה	מסקנה	הצעד הבא
1	`ping` ‹יעד›	נכשל	יש בעיה	`ping` לשער
2	`ping` ‹שער›	...	...	...
3	`ipconfig`	...	...	...
4	...	...	...	...

טיפ · כל שורה שוללת שכבה. אם `ping` לשער עובד — הבעיה **לא** בתחנה ולא במתג. מסתכלים על הנתב והלאה.

דוגמה פתורה

השאלה

`tracert` ליעד מציג 5 שורות; השורה השלישית היא * * *. `ping` ליעד מציג `TTL` =124 (השולח: `Windows`). כמה נתבים במסלול, והאם יש תקלה?

הפתרון צעד אחר צעד

1. `tracert` : 5 שורות, האחרונה היא היעד ← 4 נתבים.
2. `TTL` : 128 − 124 = 4 נתבים. מתאים.
3. **הכוכביות**: הנתב השלישי לא שולח `Time Exceeded` (מסנן `ICMP`), אבל השורות 4 ו-5 מגיעות — כלומר הוא מעביר.
4. **מסקנה**: 4 נתבים, אין תקלה. הכוכביות הן מדיניות של הנתב.

תשובה · 4 נתבים, `ping` עובד, אין תקלה. שני המדדים (שורות ו- `TTL`) מאששים זה את זה.

תרגילים — פתרו לבד לפני שאתם בודקים בכיתה

1. `arp` -a בתחנה מציג רשומה אחת; `show ip arp` בנתב מציג שש. הסבירו.
2. `ping` ראשון בסימולציה: ' `Request timed out` ', ואז שלושה מצליחים. למה?
3. `ping` ל- `R2` עובד, ל- `R3` נכשל. איפה מחפשים?
4. `ping` מציג `TTL` =61 מתחנת `Linux` (64). `tracert` מציג 5 שורות. מתאים?
5. תיעדתם: `ping` לשער נכשל. מה **לא** בודקים עכשיו, ולמה?

6. למה חובה למלא את טבלת האבחון לפני התיקון?

דף עבודה — מעבדה 5 — `ARP` · `ping` · `traceroute` · אבחון

שם: _____ תאריך: _____ חוליה: _____

המטרה: שלוש פעילויות רשמיות + טבלת אבחון אחת מלאה.

מהלך — סמנו כל שלב שהושלם

- ☐ פתחו 9.2.9 `.Examine the ARP Table` בצעו את כל השלבים. העתיקו: `arp` -a לפני ואחרי · `show ip arp` מהנתב. צלמו `Completion` .
- ☐ פתחו 13.2.7 `.Use Ping and Traceroute` לכל יעד: `ping` → רשמו `TTL` . `tracert` → ספרו שורות. חשבו נתבים בשתי הדרכים.
- ☐ פתחו 13.3.1 `Use ICMP to Test` `.and Correct` **לפני כל תיקון** — מלאו את טבלת האבחון (4 שורות לפחות). רק אז תקנו ואמתו.
- ☐ כתבו ניתוח של מסלול חבילה אחת: `ARP` , `TTL` , מה קורה בכל נתב (6 שורות).

רישום התוצאות

#	מה למלא	חישוב · הערות · ראיות (פלט פקודה)
1	9.2.9 — `arp` -a לפני: _____ · אחרי: _____ _____ · `show ip arp:` _____ רשומות · `Completion` % _____	_____
2	13.2.7 — יעד 1: `TTL` _____ → נתבים _____ _____ · `tracert` שורות _____ · תואם? _____	_____
3	13.2.7 — יעד 2: `TTL` _____ → נתבים _____ _____ · `tracert` שורות _____ · תואם? _____	_____
4	13.3.1 — טבלת אבחון: בדיקה | תוצאה | מסקנה | הבא (4 שורות)	_____ _____
5	13.3.1 — התקלה הייתה: _____ · התיקון: _____ _____ · אימות: _____	_____
6	ניתוח מסלול (6 שורות): _____	_____

רפלקציה — שתי שורות

מה היה הכי קשה, ומה פתר את זה?

_____

מה הייתי עושה אחרת בפעם הבאה?

_____

אישור המורה: ☐ Completion במעבדה (150) ☐ התוצר (קובץ + תיעוד) (50) ☐ בונוס: ההרחבה (50) · **XP** _____ · תג: ☐ בלש/ית הרשת · חתימה _____

כרטיס יציאה — 3 שאלות, 5 דקות, נמסר ביציאה

1. `TTL` בתשובה 124, שולח `Windows` — כמה נתבים?

---

2. השורה האחרונה ב-`tracert` היא...

---

3. * * * ב-`tracert` עם יעד שמגיע =

עוד לבדיקה עצמית — ענו בעל פה, בלי להסתכל אחורה

1. מה ממלאים לפני שמתקנים?

מילון מונחים

עברית	אנגלית	הסבר קצר
פעילות PT	`PKA Activity`	קובץ עם הנחיות ובדיקה אוטומטית
השלמה	`Completion`	אחוז המשימות שבוצעו — ההוכחה להגשה
Time Exceeded	`ICMP type 11`	הודעה מנתב שה-`TTL` הגיע לאפס
פג הזמן	`Request timed out`	לא חזרה תשובה בזמן — לעיתים בגלל `ARP`
טבלת אבחון	`Troubleshooting Log`	בדיקה · תוצאה · מסקנה · הבא

להעמקה

בספר הקורס

- **ITN 13.2** — Ping and Traceroute Tests · עמוד 449
- **ITN 9.2** — ARP · עמוד 301

קבצים שנעבוד איתם

- 9.2.9 Packet Tracer - Examine the ARP Table.pka
- 9.2.9 Packet Tracer - Examine the ARP Table.docx
- 13.2.7 Packet Tracer - Use Ping and Traceroute to Test Network Connectivity.pka

- 13.3.1 Packet Tracer - Use ICMP to Test and Correct Network Connectivity.pka
- 3.7.10 Lab - Use Wireshark to View Network Traffic.docx
