טכנולוגיות אלחוטיות · 802.11 · רכיבים · אבטחת WLAN

שבוע 20 · 04/02–31/01 · **פלנר עדי**

15 רשתות `WiFi` בכיתה. איזו הכי חזקה? למה שתיים עם אותו שם? מה 5G ליד השם? ומה קורה אם מישהו מקים רשת בשם של בית הספר? 21 סעיפי סילבוס — וסולם אבטחה אחד שצריך לזכור. הולכים מהר, עם טבלאות.

1. למה אלחוט, ואיזה סוגים

סוג	טווח	טכנולוגיה	דוגמה
`WPAN`	מטרים	`Bluetooth` · `IrDA` · `RF` (`Zigbee`)	אוזניות, שלט
`WLAN`	עשרות מטרים	`WiFi 802.11`	הבית, בית הספר
`WMAN`	קילומטרים	`WiMAX`	עיר, ספקית
`WWAN`	ארצי/עולמי	`Cellular 4G/5G` · לוויין	הטלפון, `Starlink`

יתרונות: ניידות, פריסה בלי כבלים, קנה מידה (עוד לקוח = אפס כבלים). **מגבלות**: מדיה משותפת (`half-duplex` — כולם על אותו אוויר), טווח, הפרעות, אבטחה (כל אחד 'שומע').

2. תקנים, תדרים, ארגונים, אנטנות

```
2.4 GHz: long range, walls OK, only 3 non-overlapping channels: 1 · 6 · 11.  crowded (microwave, Bl
5 GHz:   shorter range, many channels, faster, less interference

ITU  = radio frequencies (who may use what)    IEEE = 802.11 (the standard)    Wi-Fi Alliance = cer

antennas:  omnidirectional (all directions, short)  ·  directional (one direction, far)  ·  MIMO (s
```

1/6/11 — שני `AP` סמוכים על ערוץ 6 מפריעים זה לזה. 5 `GHz` מהיר, 2.4 עובר קירות.

תקן	שנה	תדר	מהירות מרבית	שם שיווקי
802.11a	1999	5 GHz	54 Mbps	—
802.11b	1999	2.4 GHz	11 Mbps	—
802.11g	2003	2.4 GHz	54 Mbps	—
802.11n	2009	2.4 + 5	600 Mbps (MIMO)	Wi-Fi 4
802.11ac	2013	5 GHz	+1.3 Gbps	Wi-Fi 5
802.11ax	2019	2.4 + 5 (+6)	9.6 Gbps	Wi-Fi 6/6E

3. רכיבים — AP מול נתב ביתי (שאלת בחינה)

רכיב	מה	שכבה	איפה
כרטיס אלחוטי (NIC)	בלקוח — מחשב, טלפון	1–2	כל לקוח
נקודת גישה (AP)	גשר אלחוט ↔ קווי בלבד. מחובר למתג (trunk), מקבל VLAN . אין DHCP/NAT	2	ארגון
נתב ביתי אלחוטי	נתב + מתג 4 פורטים + AP + DHCP + NAT + firewall — בקופסה אחת	2–3+	בית
AP אוטונומי	מוגדר לבד — GUI משלו	—	בית, משרד קטן
AP מנוהל (lightweight)	WLC מגדיר את כולם דרך CAPWAP — SSID אחד, ערוצים מתואמים, roaming	—	ארגון, עשרות AP

טיפ · בחינה 2026 ש'8: AP = גשר בלבד. נתב ביתי = הכול בקופסה אחת.

4. איך זה עובד — מסגרת, `CSMA/CA`, התחברות

```
BSS = one AP + its clients (BSSID = the AP's MAC)      ESS = several APs, same SSID -> roaming

802.11 frame: up to 4 MAC addresses (receiver · transmitter · destination · source) — Ethernet has

CSMA/CA (collision AVOIDANCE) — you can't hear a collision while transmitting on air:
  listen -> random wait -> (RTS/CTS) -> send -> wait for ACK -> no ACK? resend
  vs CSMA/CD (Ethernet): send, DETECT collision, back off.   -> WiFi is half-duplex + ACK = slower

joining:  1 discover (passive: hear beacon / active: send probe)  ->  2 authenticate  ->  3 associa
SSID = the network name in the beacon.  hidden SSID? the probe reveals it anyway
```

`CA` = מונעים מראש כי אי אפשר לשמוע התנגשות באוויר. `probe` → `authenticate` → `associate`.

5. אבטחה — הסולם

```
WPA2/WPA3-Personal    = PSK — one password for everyone          (home)
WPA2/WPA3-Enterprise  = 802.1X + RADIUS — user + password each    (organization: revoke one user)

threats:  Rogue AP (someone plugged in their own)  ·  Evil Twin (same SSID, stronger, attacker in t
          DoS (jamming, deauth)  ·  MITM
defense:  WPA2/3-AES · Enterprise in orgs · HTTPS/VPN on any open network · WLC detects rogue APs
```

`SSID` מוסתר + סינון `MAC` = הסתרה, לא אבטחה. `WPA2-AES` לפחות. `Enterprise` בארגון.

שיטה	מה	מספיק?
הסתרת `SSID`	לא משדרים את השם ב-`beacon`	✗ נחשף ב-`probe`
סינון `MAC`	רק כתובות מהרשימה	✗ `MAC` מזייפים בפקודה
`Open` / `Shared key`	אימות 802.11 מקורי	✗ `Shared` = `WEP`
`WEP`	הצפנה `RC4`, מפתח קבוע	✗ שבור — דקות
`WPA`	`TKIP` — תיקון ל-`WEP`	✗ ישן
`WPA2`	`AES-CCMP`	✓ הסטנדרט
`WPA3`	`AES` + `SAE` (הגנה מניחוש `offline`)	✓ החדש

⚠ **שימו לב** · רשת פתוחה בקפה: כל מה שלא `HTTPS` — גלוי. `VPN`.

6. הגדרות `AP` — בסיסיות ומתקדמות

בסיסי	מתקדם
`SSID` (שם)	עוצמת שידור (טווח מול הפרעות)
ערוץ (1/6/11 או `auto`)	רוחב ערוץ (20/40/80 `MHz`)
אבטחה: `WPA2-AES` + סיסמה	סינון `MAC` · הסתרת `SSID`
`DHCP` (בנתב ביתי)	גיבוי / שחזור תצורה
סיסמת ניהול (לא ברירת המחדל!)	איפוס לברירת מחדל (`reset 10` שנ׳)
	עדכון קושחה (`firmware`) · `QoS` · `port forwarding`

טיפ · הדבר הראשון בכל `AP`: להחליף את סיסמת הניהול. `admin/admin` = הרשת של כולם.

דוגמה פתורה

השאלה

משרד בשתי קומות, 40 עובדים, מדפסות ואורחים. תכננו את ה-`WLAN` : תקן, תדרים, כמה `AP` , ערוצים, אבטחה, `SSID` .

הפתרון צעד אחר צעד

1. **תקן**: 802.11ax (`Wi-Fi 6`) — `dual band` . לקוחות ישנים ב-2.4, חדשים ב-5.
2. **כמה `AP`** : 3–2 לקומה (טווח 5 `GHz` ~15 מ' דרך קירות) → 4–6. `ESS` : אותו `SSID` בכולם — `roaming` .
3. **ערוצים**: 2.4 → 1/6/11 לסירוגין, `AP` סמוכים לא על אותו ערוץ. 5 `GHz` → `auto` (או תכנון ידני, 40 `MHz`).
4. `SSID` : שניים. `OFFICE` — `WPA2/3-Enterprise` (802.1X + `RADIUS` , כל עובד עם משתמש) על `VLAN 20.` `GUEST` — `WPA2-PSK` או `captive portal` , `VLAN 50` מבודד (רק אינטרנט).
5. `AP` : מנוהלים ב-`WLC` (או `controller` בענן) — `SSID` אחד מוגדר פעם אחת. `AP` על `trunk` (שני `VLANs`) עם `portfast` .
6. **מתקדם**: סיסמת ניהול חזקה, קושחה מעודכנת, עוצמת שידור בינונית (שלא יגיע לרחוב), הסתרת `SSID` — לא (לא עוזר).

תשובה · `ax` · `dual band` · `ESS` · 1/6/11 · `Enterprise` לעובדים + `Guest` מבודד · `WLC` .
הצדקה לכל בחירה — כמו בפרויקט.

תרגילים — פתרו לבד לפני שאתם בודקים בכיתה

1. `AP` מול נתב ביתי — משפט לכל אחד.
2. `WPAN` · `WLAN` · `WMAN` · `WWAN` — דוגמה לכל אחד.
3. למה 1/6/11?
4. 2.4 מול 5 `GHz` — יתרון של כל אחד?
5. `CSMA/CA` מול `CD` ?
6. `BSS` מול `ESS` ?
7. הסתרת `SSID` — אבטחה?
8. `WEP` · `WPA` · `WPA2` · `WPA3` — מי בסדר?

9. `Personal` מול `Enterprise`?

10. `TKIP` מול `AES`?

11. `Evil Twin`?

12. `ITU` · `IEEE` · `Wi-Fi Alliance`?

13. `omni` · `directional` · `MIMO`?

14. `AP` אוטונומי מול מנוהל?

דף עבודה — אלחוט — 21 סעיפים · סולם אבטחה · תכנון `WLAN`

שם: _____ תאריך: _____ חוליה: _____

המטרה: משפט לכל סעיף סילבוס, סולם האבטחה מהזיכרון, ותכנון `WLAN` אחד מנומק.

מהלך — סמנו כל שלב שהושלם

- ☐ סרקו `WiFi` בטלפון: 5 רשתות — שם · תדר · ערוץ · עוצמה · אבטחה. שתיים באותו ערוץ? שתיים באותו שם?
- ☐ טבלת 802.11 מהזיכרון: `a/b/g/n/ac/ax` — תדר ומהירות.
- ☐ סולם האבטחה מהזיכרון: 7 שלבים, ✓/✗ ליד כל אחד. `Personal` מול `Enterprise` . `TKIP` מול `AES` .
- ☐ 3 תרחישים: בית · משרד · קפה — תקן, תדר, `AP` /נתב, אבטחה, `SSID` , למה.
- ☐ 21 הסעיפים (`NET-5-01` ...21) — משפט לכל אחד מהחוברת.
- ☐ בחינה: 2026 ש'8 — ענו. + 'למה 1/6/11' + ' `CA` מול `CD` '.

רישום התוצאות

#	מה למלא	חישוב · הערות · ראיות (פלט פקודה)
1	סריקה: _____	_____
2	802.11: a _____ b _____ g _____ n _____ `ac` _____ `ax` _____	_____
3	סולם: _____ · `Personal` _____ · _____ `Enterprise` _____ `TKIP` _____ `AES` _____	_____
4	תרחישים: _____	_____
5	21 משפטים: ☐	_____ _____
6	בחינה: _____	_____

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: ☐

מפעיל/ת האלחוט · חתימה _____

כרטיס יציאה — 3 שאלות, 5 דקות, נמסר ביציאה

1. `AP` = ?

2. ערוצים ב-2.4?

3. מינימום אבטחה?

עוד לבדיקה עצמית — ענו בעל פה, בלי להסתכל אחורה

1. `SSID` מוסתר = אבטחה?

מילון מונחים

עברית	אנגלית	הסבר קצר
רשת אלחוטית מקומית	`WLAN · 802.11`	`WiFi`
נקודת גישה	`Access Point (AP)`	גשר בין אלחוט לרשת הקווית
בקר אלחוט	`WLC`	מנהל `AP` מרובים — `CAPWAP`
מזהה רשת	`SSID`	שם הרשת ב-`beacon`
קבוצת שירות	`BSS / ESS`	`AP` אחד / כמה `AP` באותו `SSID`
מניעת התנגשויות	`CSMA/CA`	המתנה + `ACK` — כי באוויר לא שומעים התנגשות
מפתח משותף	`PSK`	סיסמה אחת לכולם — `Personal`
אימות ארגוני	`802.1X / RADIUS`	משתמש וסיסמה לכל אחד — `Enterprise`
תאום מרושע	`Evil Twin`	`AP` מזויף באותו `SSID`
נקודת גישה סוררת	`Rogue AP`	`AP` שחובר לרשת בלי אישור

להעמקה

בספר הקורס

- **SRWE 12.2** — WLAN Components · עמוד 356
- **SRWE 12.3** — WLAN Operation · עמוד 362
- **SRWE 12.1.4** — Standards 802.11 · עמוד 353

קבצים שנעבוד איתם

- SRWE_Module_12.pptx
- SRWE_Module_13.pptx
- 06 - Wireless Security.docx
- 13.1.10 Packet Tracer - Configure a Wireless Network.pka
- 4.6.5 Packet Tracer - Connect a Wired and Wireless LAN.pka