העמקה · ACL, NAT ושירותי רשת

שבוע 24 · 04/03–28/02 · **לופו משה**

שתי שאלות `ACL` מורחב בשתי בחינות — השלישית תהיה בשלכם. עשר שאלות שירותים — הפרק ה'זול' בבחינה, משפט לכל אחת. ו- `NAT` בטבלה. התוצר: דף תרגול פתור וחתום — 12 תרגילים.

1. `ACL` — מדרישה מילולית לתצורה

```
step 1  'source only?'  -> STANDARD (1-99)   -> close to DESTINATION, out
        'protocol/port?' -> EXTENDED (100-199) -> close to SOURCE, in
step 2  one line per rule, specific before general
step 3  permit ip any any   (unless the requirement is 'block everything else')
step 4  interface + ip access-group <n> in|out
step 5  verify: show access-lists (counters) · show ip interface <if> (direction)

ports:  ftp 21 · ssh 22 · telnet 23 · smtp 25 · dns 53 (udp) · dhcp 67/68 (udp) · http 80 · pop3 11
wildcard: /24 0.0.0.255 · /25 0.0.0.127 · /26 0.0.0.63 · /27 0.0.0.31 · /28 0.0.0.15 · /30 0.0.0.3
```

חמישה צעדים. הצעד שנופל: 3 (`permit ip any any`) ו-4 (הכיוון).

2. ארבעה תרגילי `ACL` — פתורים

דרישה	סוג · מיקום	התצורה
רשת 192.168.10.0/24 לא לשרתים ב-192.168.30.0/24, השאר כן	סטנדרטי · מול 30., `out`	`access-list 10 deny 192.168.10.0` 0.0.0.255 · `access-list 10 permit any` · `int g0/2` · `ip access-group 10 out`
מהמחלקה 10.1.20.0/24: לחסום `Telnet`, לאפשר `SSH` והשאר	מורחב · מול המחלקה, `in`	`access-list 101 deny tcp` 10.1.20.0 0.0.0.255 · `any eq 23` · `permit tcp 10.1.20.0 0.0.0.255` · `any eq 22` · `permit ip any any`
רק `HTTPS` לשרת 10.0.1.5 מכולם, השאר לשרת חסום	מורחב · מול השרת, `out`	`access-list 102 permit tcp` `any host 10.0.1.5 eq` 443 · (`deny` מובלע) — ⚠ חוסם גם `ping/DNS` לשרת
`DNS` ו-`DHCP` כן, `WEB` לא, מ-192.168.20.0/24 (2023 ה3)	מורחב · `in`	`permit udp` … `eq 53` · `permit udp` … `eq 67` · `deny tcp` … `eq 80` · `permit ip any any`

⚠ **שימו לב** · `ACL` עם `deny` בלבד = הכול חסום. `ACL` עם `permit ip any any` ראשון = ה-`deny` לא נבדק.

3. `NAT` — טבלה + תצורת `PAT`

```
access-list 1 permit 10.0.0.0 0.255.255.255
ip nat inside source list 1 interface g0/0/0 overload
interface g0/0/1 -> ip nat inside
interface g0/0/0 -> ip nat outside
show ip nat translations · show ip nat statistics (Interfaces!)
```

5 שורות. הרביעית והחמישית — אלה ששוכחים.

שיטה	מתי	מה רואים ב-`translations`	מה שובר
סטטי	שרת נגיש מבחוץ	שורה קבועה (---), עובד מבחוץ	—
דינמי	`pool` של ציבוריות	`inside global` שונה לכל מחשב	`pool` מלא → `misses`
`PAT`	הבית, המשרד, הכול	`inside global` זהה, פורטים שונים	חיבור יזום מבחוץ

4. שירותים וניהול — 10 שאלות, 10 משפטים

#	השאלה	המשפט
1 2023ה	`TCP` ב-`L3` ? `IMAP` שולח? `UDP` אמין?	לא (`L4`) · לא (מקבל, 143) · לא
1 2023ז	`displaydns` / `ipconfig`	מציג את מטמון ה-`DNS` של המחשב
2 2023ד · 3ד	נתב מקבל כתובת מהספקית	`ip address dhcp` → ‹ `WAN` › `interface`
6 2026	`Discover` בלי `Offer`	שרת כבוי · `VLAN` אחר בלי `helper` · `pool` ריק
7 2026	אימות מרכזי + רישום פקודות	`TACACS` + (`AAA`)
14 2026	שער ל-`PC` מ-`DHCP pool`	`default-router` = כתובת תת-הממשק · `trunk allowed vlan`
1 2023ד	גילוי שכני `Cisco`	`show cdp neighbors detail` — `CDP`
2 2023ח · 17 2026	יומנים לשרת	`logging` ‹ `ip` › / `logging host` ‹ `ip` ›
(סילבוס)	זמן	`ntp server` ‹ `ip` › · `show ntp status`

טיפ · הפרק הזה: 10 שאלות = 25% מהבחינה. משפט לכל אחת. אין תירוץ.

דוגמה פתורה

השאלה

דרישה: 'מהמחלקה 172.16.5.0/24 — לאפשר `HTTPS` ו- `DNS` לשרת 10.0.0.10, לחסום את כל השאר לשרת, ולאפשר הכול לכל מקום אחר.' כתבו, מקמו, אמתו.

הפתרון צעד אחר צעד

1. **צעד 1**: פורטים → מורחב → קרוב למקור (ממשק המחלקה), `in` .
2. **צעד 2**: `permit tcp 172.16.5.0 0.0.0.255` `host 10.0.0.10 eq 443` ·
   `permit udp 172.16.5.0 0.0.0.255` `host 10.0.0.10 eq 53` ·
   `deny ip 172.16.5.0 0.0.0.255` `host 10.0.0.10`.
3. **צעד 3**: `permit ip any any` — 'הכול לכל מקום אחר'.
4. **צעד 4**: `interface g0/0/1` (מול המחלקה) → `ip access-group 110 in`.
5. **צעד 5**: מ- `PC` במחלקה: `HTTPS` לשרת ✓ · `nslookup` לשרת ✓ · `ping` לשרת ✗ · `HTTP` לאתר חיצוני ✓. `show access-lists` → מונים על 4 השורות.
6. **סדר**: הספציפי (`permit 443` , 53) לפני הכללי (`deny ip` ... `host`). הפוך — הכול לשרת חסום.

תשובה • 3 שורות ספציפיות → `deny` לשרת → `permit ip any any` → `in` על המחלקה. הסדר קובע.

תרגילים — פתרו לבד לפני שאתם בודקים בכיתה

1. 'מקור בלבד' → סוג? מיקום?
2. 'פורט' → סוג? מיקום?
3. `DNS` — `tcp` או `udp` ? פורט?
4. `host 10.0.1.5` = `wildcard` ?
5. `ACL` עם `deny` בלבד?
6. 50 מחשבים, כתובת אחת — `NAT` ?
7. `translations` ריק, הכול מוגדר — הבדיקה?
8. `Discover` בלי `Offer` — 3?
9. נתב לקוח `DHCP` — פקודה?

10. `TACACS` + — מה?

11. `logging` ‹ `ip` › — מה?

12. `SMTP` / `POP3` / `IMAP` — פורטים?

דף עבודה — דף תרגול 24 — `ACL` · `NAT` · שירותים — 12 תרגילים

שם: _____ תאריך: _____ חוליה: _____

המטרה: 12 תרגילים פתורים בפורמט הבחינה, נבדקים בזוגות, חתומים.

מהלך — סמנו כל שלב שהושלם

- ☐ `ACL` ×4: (1) רשת X לא לשרתים (2) `Telnet` ✗ `SSH` ✓ (3) רק `HTTPS` לשרת (4) `DNS` + `DHCP` ✓ `WEB` ✗ — סוג · מיקום · כיוון · שורות.
- ☐ `NAT` ×2: (5) שרת נגיש מבחוץ + 50 מחשבים — שיטות + תצורה (6) 'הכול מוגדר, `translations` ריק' — אבחון.
- ☐ `DHCP` ×3: (7) `DORA` — 4 שלבים ומי `broadcast` (8) נתב לקוח — פקודה (9) `pool` + `default-router` → שער ל- `PC` .
- ☐ ניהול ×3: (10) `logging` (11) `CDP` (12) `NTP` — פקודה + משפט.
- ☐ החלפה עם זוג · בדיקה · תיקון · חתימת המורה.

רישום התוצאות

#	מה למלא	חישוב · הערות · ראיות (פלט פקודה)
1	`ACL 1`–4: _____	_____
2	`NAT 5`–6: _____	_____
3	`DHCP 7`–9: _____	_____
4	ניהול 10–12: _____	_____
5	נבדק ע"י: _____ · חתימה: _____	_____

רפלקציה — שתי שורות

מה היה הכי קשה, ומה פתר את זה?

_____

מה הייתי עושה אחרת בפעם הבאה?

אישור המורה: ☐ דף המיקוד / דף התרגול (50) ☐ סבב שעון ב-(50) Moodle · **XP** _____ · חתימה _____

כרטיס יציאה — 3 שאלות, 5 דקות, נמסר ביציאה

1. השורה האחרונה ב- `ACL` ?

---

2. מורחב — `in` או `out` ?

---

3. `PAT` — 5 שורות, איזו נשכחת?

עוד לבדיקה עצמית — ענו בעל פה, בלי להסתכל אחורה

1. `ip address dhcp` — איפה?

מילון מונחים

עברית	אנגלית	הסבר קצר
חמשת הצעדים	`ACL in 5 Steps`	סוג → שורות → `permit any` → שיוך → אימות
ספציפי לפני כללי	`Specific Before General`	הסדר ב- `ACL` — השורה הראשונה שמתאימה מנצחת
העמסה	`Overload`	`PAT` — כתובת אחת, פורט מבדיל
דף תרגול	`Practice Sheet`	12 תרגילים פתורים וחתומים — התוצר

להעמקה

קבצים שנעבוד איתם

- 773501-press-Bchina-Dugma-2023.pdf
- tikshuv-ccna.pdf בחינת השלמה תשפג (2023) - הצעת פתרון אתר מגמת תקשוב_

- ENSA_Module_5.pptx
- ENSA_Module_4.pptx
- ENSA_Module_6.pptx
- SRWE_Module_7.pptx
- ENSA_Module_10.pptx
- 5.5.1 Packet Tracer - IPv4 ACL Implementation Challenge.pka

---