רשימות גישה · ACL סטנדרטי ומורחב · wildcard

שבוע 15 · 31/12–27/12 · **לופו משה**

'הסטודנטים לא ייגשו לשרת הציונים, אבל כן לאתר.' לנתב אין דעה — אלא אם נותנים לו רשימה: מי מותר, מי אסור, ובאיזה סדר. ארבע שאלות בחינה יושבות כאן, וכולן על אותם שני דברים: `wildcard` ו-`permit` בסוף.

1. איך `ACL` עובדת

```
packet arrives -> check rule 1 -> match? apply (permit/deny), STOP
               -> no match? rule 2 -> ...
               -> no rule matched?  ->  IMPLICIT DENY ANY  (the invisible last line)

access-list 10 deny 20.20.20.0 0.0.0.255      <- alone: blocks EVERYTHING
access-list 10 permit any                      <- now: blocks only 20.20.20.0/24
```

מלמעלה למטה, ההתאמה הראשונה מכריעה, ובסוף `deny any` שלא רואים. רשימה בלי `permit` = הכול חסום.

סוג	מספרים	מסננת לפי	איפה לשים
סטנדרטית	1–99 (1300–1999)	מקור בלבד	קרוב ליעד
מורחבת	100–199 (2000–2699)	מקור · יעד · פרוטוקול · פורט	קרוב למקור
בשם	`ip access-list standard/extended NAME`	כנ"ל	כנ"ל

⚠ **שימו לב ·** `access-list 10 deny 20.20.20.0` 0.0.0.255 — זו התשובה הנכונה בבחינה 2023 ש'ד4 ('`ACL` סטנדרטית לחסימת רשת'). המסיחים: 110 (מורחבת), `icmp` (מורחבת), מסכה במקום `wildcard`.

2. `Wildcard` — שוב

```
wildcard = 255.255.255.255 - mask
/24  ->  0.0.0.255      /26 -> 0.0.0.63      /30 -> 0.0.0.3
host 10.1.1.5  =  10.1.1.5 0.0.0.0
any            =  0.0.0.0 255.255.255.255
```

0 = חייב להתאים, 1 = לא משנה. `host` ו-`any` — קיצורים.

3. סטנדרטית · מורחבת · בשם — ושיוך

```
! standard: block LAN2 from reaching LAN3, keep everything else — place near the DESTINATION
R1(config)# ip access-list standard BLOCK_LAN2
R1(config-std-nacl)# deny 192.168.2.0 0.0.0.255
R1(config-std-nacl)# permit any
R1(config)# interface g0/2                      <- the interface toward LAN3
R1(config-if)# ip access-group BLOCK_LAN2 out

! extended: allow DNS and DHCP, block WEB, from the VLAN10 users — near the SOURCE
R1(config)# access-list 101 permit udp any any eq 53
R1(config)# access-list 101 permit udp any any eq 67
R1(config)# access-list 101 deny tcp any any eq 80
R1(config)# access-list 101 permit ip any any
R1(config)# interface g0/0/1
R1(config-if)# ip access-group 101 in

! extended: block Telnet, allow SSH, from 10.3.3.0/24 (exam 2026 q20)
R1(config)# access-list 102 deny tcp 10.3.3.0 0.0.0.255 any eq 23
R1(config)# access-list 102 permit tcp 10.3.3.0 0.0.0.255 any eq ssh
R1(config)# access-list 102 permit ip any any

R1# show access-lists     <- match counters
```

`deny` לפני `permit` כשרוצים חריג. `in` = נכנס לנתב דרך הממשק, `out` = יוצא. סופר `show access-lists` התאמות — האימות.

טיפ · שאלות 2023 ש'3ה ו-ש'7ה ו-2026 ש'20 — כולן בדיוק הדפוס הזה: `deny` ספציפי, `permit` רחב, שיוך לממשק בכיוון הנכון.

דוגמה פתורה

השאלה

`R1` עם שלוש רשתות: 192.168.1.0 (`G0/1`), 192.168.2.0 (`G0/2`), 192.168.3.0 `Restricted` (`G0/3`). לחסום תעבורה מ-2.0. ל-3.0. בלי לחסום גישה לרשתות אחרות. כתבו ושייכו.

הפתרון צעד אחר צעד

1. **סוג**: מסננים לפי מקור בלבד → סטנדרטית. → קרוב ליעד.
2. **הרשימה**: `ip access-list standard` BLOCK_LAN2 · `deny 192.168.2.0 0.0.0.255` · `.permit any`
3. **איפה**: על `G0/3` (מול 3.0.), `out` — רק מה שיוצא לרשת המוגבלת נבדק.
4. **למה לא על** `G0/2 in` : זה היה חוסם את 2.0. גם מ-1.0. ומהאינטרנט.
5. **אימות**: `ping` מ-2.0. ל-3.0. ✗ · ל-1.0. ✓ · `show access-lists` — מונה `deny` עולה.

תשובה · `deny` + `permit any` + `out` על הממשק מול היעד. (בחינה 2023 ש'7ה — המסיח הנכון: `deny 192.168.2.0` · `permit any` · `access-group` BLOCK_LAN2 `out`)

תרגילים — פתרו לבד לפני שאתם בודקים בכיתה

1. `access-list 10 deny 20.20.20.0` 0.0.0.255 — ורק זה. מה עובר?
2. `permit tcp any any` `eq 443` — חוקית? מה עושה?
3. לחסום `Telnet` , לאפשר `SSH` מ-10.3.3.0/24 — שלוש שורות?
4. `wildcard` ל-/26? למארח?
5. סטנדרטית — קרוב למקור או ליעד? למה?
6. `ACL 101: permit udp` `any any eq 53` · `permit udp any any` `eq 67` · `deny tcp any any` `.permit ip any any` · `eq 80` מה עובר ומה לא?
7. איזו פקודה מציגה כמה חבילות תאמו לכל שורה?
8. `deny tcp 10.0.0.0 0.0.0.255` `host 10.0.1.5 eq 80` — מה נחסם?

דף עבודה — דף עבודה 15 — `ACL` : כתיבה, מיקום, `wildcard`

שם: _____ תאריך: _____ חוליה: _____

המטרה: חמש רשימות מהזיכרון, כל אחת עם שיוך נכון.

מהלך — סמנו כל שלב שהושלם

- ☐ רשימה 1 (סטנדרטית, מספר): לחסום 172.16.5.0/24, לאפשר השאר. איפה? באיזה כיוון?
- ☐ רשימה 2 (סטנדרטית, בשם): תרחיש הבחינה 2023 ש'7ה.
- ☐ רשימה 3 (מורחבת): לאפשר `DNS` ו- `DHCP` , לחסום `WEB` , לאפשר השאר (2023 ש'3ה).
- ☐ רשימה 4 (מורחבת): לחסום `Telnet` , לאפשר `SSH` , מ-10.3.3.0/24 (2026 ש'20).
- ☐ רשימה 5: רק `HTTPS` לשרת 10.0.1.5 מכולם; השאר חסום.
- ☐ `wildcard` : /24 · /25 · /27 · /30 · `host` · `any` .
- ☐ לכל רשימה: הממשק והכיוון + משפט 'למה שם'.

רישום התוצאות

#	מה למלא	חישוב · הערות · ראיות (פלט פקודה)
1	1: _____ · ממשק/כיוון _____	_____
2	2: _____ · _____	_____
3	3: _____ · _____	_____
4	4: _____ · _____	_____
5	5: _____ · _____	_____
6	`wildcards` : _____ _____ _____ _____	_____

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: ☐

שומר/ת הסף · חתימה _____

כרטיס יציאה — 3 שאלות, 5 דקות, נמסר ביציאה

1. מה בסוף כל `ACL` שלא רואים?

---

2. סטנדרטית — מספרים ומסננת לפי?

---

3. `wildcard` ל-/24?

עוד לבדיקה עצמית — ענו בעל פה, בלי להסתכל אחורה

1. סטנדרטית שמים...

מילון מונחים

עברית	אנגלית	הסבר קצר
רשימת גישה	`ACL`	כללי `permit/deny` מלמעלה למטה
דחייה מובלעת	`Implicit Deny`	`deny any` בסוף — לא נראה
סטנדרטית	`Standard ACL`	1–99 · לפי מקור · קרוב ליעד
מורחבת	`Extended ACL`	100–199 · מקור/יעד/פרוטוקול/פורט · קרוב למקור
שיוך	`ip access-group`	מחבר `ACL` למשק · `in/out`
מונה התאמות	`show access-lists`	כמה חבילות תאמו לכל שורה

להעמקה

בספר הקורס

- **ENSA 4.2.1** — Wildcard Mask Overview · עמוד 168
- **ENSA 4.1.1** — What Is an ACL?· עמוד 164
- **ENSA 5.4.3** — Protocols and Ports · עמוד 206

קבצים שנעבוד איתם

- ENSA_Module_4.pptx

- ENSA_Module_5.pptx
- Access Control Lists.docx
- 4.1.4 Packet Tracer - ACL Demonstration.pka
- 5.1.8 Packet Tracer - Configure Numbered Standard IPv4 ACLs.pka

---