NAT · סטטי, דינמי ו-PAT

שבוע 18 · 21/01–17/01 · **בנימין נאור**

למחשב שלכם יש כתובת 192.168.x — ולעולם יש 212.x. מישהו מחליף באמצע. זה `NAT` : הסיבה ש- `IPv4` עדיין חי, והסיבה שאי אפשר להריץ שרת בבית בלי להיכנס לנתב. היום: למה, ארבעה מונחים, שלושה סוגים, ופקודה אחת ששוכחים תמיד.

1. למה — מיצוי `IPv4` וכתובות פרטיות

4.3 מיליארד כתובות `IPv4` . 8 מיליארד אנשים, 30 מיליארד התקנים. הפתרון הזמני שנשאר לתמיד: **כתובות פרטיות** (`RFC 1918`) בפנים, כתובת ציבורית אחת בחוץ, ונתב שמתרגם.

בלוק	טווח	כמה
10.0.0.0/8	10.0.0.0 – 10.255.255.255	16.7M
172.16.0.0/12	172.16.0.0 – 172.31.255.255	1M
192.168.0.0/16	192.168.0.0 – 192.168.255.255	65K

טיפ · כתובת פרטית לא מנותבת באינטרנט. חבילה עם מקור 192.168.1.5 שיוצאת בלי תרגום — נזרקת בספקית.

2. ארבעת המונחים — ציור אחד

```
inside                    R1 (NAT)                   outside
PC 192.168.10.10 -------[ g0/0/1 | g0/0/0 ]------- Server 198.51.100.7
                          translation table
inside LOCAL      inside GLOBAL     | outside GLOBAL   outside LOCAL
192.168.10.10     209.165.200.5     | 198.51.100.7     198.51.100.7
(PC as seen       (PC as seen       | (server as seen  (server as seen
 from inside)      from outside)    |  from outside)    from inside)
```

`local` = כפי שרואים **מבפנים**. `global` = כפי שרואים **מבחוץ**. `inside/outside` = של מי הכתובת.

`outside local` = `outside global` כמעט תמיד (אין תרגום בצד החיצוני).

3. שלושת הסוגים

סוג	מה	מתי	כמה כתובות ציבוריות
סטטי	1:1 קבוע	שרת שצריך להיות נגיש מבחוץ	אחת לכל שרת
דינמי	`pool` + `ACL`, ראשון-בא-ראשון	כשיש כמה כתובות ציבוריות	כמספר המשתמשים בו-זמנית
`PAT` (`overload`)	כתובת אחת, פורט המקור מבדיל	הבית, המשרד, הכול	אחת

`PAT` הוא מה שיש לכולם. 30 מחשבים יוצאים דרך 209.165.200.5 — כל חיבור מקבל פורט מקור אחר (49152, 49153...), והנתב זוכר: 'פורט 49153 → 192.168.10.12'. עד ~64K חיבורים על כתובת אחת.

> ⚠ **שימו לב ·** `NAT` דינמי עם `pool` של 5 ו-20 משתמשים — השישי מחכה. לכן בפועל תמיד `PAT`.

4. תצורה — והפקודה ששוכחים

```
! interfaces — ALWAYS. this is the one everyone forgets
R1(config)# interface g0/0/1
R1(config-if)# ip nat inside
R1(config)# interface g0/0/0
R1(config-if)# ip nat outside

! static — server
R1(config)# ip nat inside source static 192.168.10.10 209.165.200.5

! dynamic — pool + ACL (the ACL says WHO gets translated)
R1(config)# ip nat pool POOL 209.165.200.10 209.165.200.20 netmask 255.255.255.224
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# ip nat inside source list 1 pool POOL

! PAT — one address, overload
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)# ip nat inside source list 1 interface g0/0/0 overload

R1# show ip nat translations
Pro  Inside global        Inside local         Outside local        Outside global
tcp  209.165.200.5:49153  192.168.10.12:49153  198.51.100.7:80      198.51.100.7:80
R1# show ip nat statistics      <- 'Interfaces: inside g0/0/1, outside g0/0/0' — if empty, THAT is th
R1# clear ip nat translation *
```

ה-`ACL` ב-`NAT` = 'מי מתורגם'. `permit` בלבד. `show ip nat statistics` → `Interfaces` — הבדיקה הראשונה כשכלום לא עובד.

5. מה `NAT` שובר

`NAT` יוצר רשומה רק כשחיבור **יוצא מבפנים**. חיבור יזום מבחוץ — אין רשומה, הנתב זורק. לכן: שרת בבית לא נגיש, משחקים צריכים '`port forwarding`', ו-`IPsec/FTP-active` סובלים. הפתרון: `NAT` סטטי לשרת, או `:port forwarding` `ip nat inside source static tcp 192.168.10.10 80` 209.165.200.5:80`.

טיפ · `NAT` מסתיר — לא מגן. אבטחה = `ACL/firewall`. ' `NAT` ' הוא `firewall` ' זו טעות נפוצה.

דוגמה פתורה

השאלה

משרד: 40 מחשבים ב-192.168.20.0/24, שרת `WEB` ב-192.168.20.100, כתובות ציבוריות 203.0.113.2–203.0.113.6 (/29), `G0/0/0` = .2. דרישות: כולם גולשים, השרת נגיש מבחוץ ב-.3. תכננו וכתבו.

הפתרון צעד אחר צעד

1. **גלישה ל-40** — `PAT` על `G0/0/0` (.2). לא דינמי: 5 כתובות ל-40 = תורים.
2. **שרת נגיש** — `NAT` סטטי: 192.168.20.100 ↔ 203.0.113.3.
3. **ממשקים**: `G0/0/1 inside` , `G0/0/0 outside`.
4. `ACL` : `access-list 1 permit 192.168.20.0` 0.0.0.255 — כולם, כולל השרת (הסטטי גובר עליו ליציאה).
5. `PAT` : `ip nat inside source list 1 interface g0/0/0 overload` .
6. **סטטי**: `ip nat inside source static 192.168.20.100 203.0.113.3`.
7. **אימות**: מ-`PC` → דפדפן החוצה → `:show ip nat translations` `:tcp 203.0.113.2` `port` › ... · מבחוץ → `http://203.0.113.3` → `:show ip nat translations` 203.0.113.3 ↔ 192.168.20.100.

תשובה · `PAT` לכולם + סטטי לשרת — השילוב הסטנדרטי. ושתי שורות `ip nat inside/outside` לפני הכול.

תרגילים — פתרו לבד לפני שאתם בודקים בכיתה

1. `PC 10.1.1.5` → 8.8.8.8, מתורגם ל-198.51.100.9. `inside local` ? `inside global` ? `outside global` ?
2. כתובת ציבורית אחת, 25 מחשבים. איזה `NAT` ?
3. 3 שרתים שצריכים להיות נגישים מבחוץ. איזה `NAT` וכמה כתובות?
4. הכול מוגדר, `show ip nat translations` ריק. הבדיקה הראשונה?
5. `access-list 1 deny 192.168.10.0` 0.0.0.255 ב-`NAT` — מה קורה ל-192.168.10.x?
6. 192.168.10.12:49153 ↔ 209.165.200.5:49153 — מה מזהה את החיבור בחזרה?
7. למה שרת בבית לא נגיש מבחוץ?

8. `NAT` = אבטחה?

דף עבודה — `NAT` — ארבעה מונחים · שלושה סוגים · פקודה אחת ששוכחים

שם: _____ תאריך: _____ חוליה: _____

המטרה: לתכנן `NAT` לתרחיש ולכתוב את התצורה המלאה על הנייר.

מהלך — סמנו כל שלב שהושלם

- ☐ `ipconfig` במחשב שלכם + `whatismyip` — שתי הכתובות. מי מהן `inside local` ומי `inside global`?
- ☐ תרחיש: `PC 172.16.5.20` → שרת 93.184.216.34, מתורגם ל-85.250.1.9. מלאו 4 מונחים.
- ☐ 3 דרישות → 3 סוגים: (א) שרת מייל נגיש מבחוץ (ב) 200 עובדים, כתובת אחת (ג) 10 עובדים, 10 כתובות ציבוריות.
- ☐ כתבו תצורת `PAT` מלאה לרשת 192.168.1.0/24 דרך `G0/0/0` — כולל ממשקים. ספרו שורות.
- ☐ מה יראה `show ip nat translations` אחרי ש-3 מחשבים גלשו? ציירו 3 שורות.
- ☐ 6.2.7 בבית: ענו על שאלות דף ההנחיות.

רישום התוצאות

#	מה למלא	חישוב · הערות · ראיות (פלט פקודה)
1	`inside local` _____ · `inside global` _____	_____
2	4 מונחים: _____ · _____ · _____ · _____	_____
3	(א) _____ (ב) _____ (ג) _____	_____
4	תצורת `PAT` : _____ שורות: _____	_____
5	`translations` : _____	_____

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: ☐ שער לעולם · חתימה _____

כרטיס יציאה — 3 שאלות, 5 דקות, נמסר ביציאה

1. `local` / `global`?

---

2. מה בבית?

---

3. הפקודה ששוכחים?

עוד לבדיקה עצמית — ענו בעל פה, בלי להסתכל אחורה

1. `NAT` שובר...

מילון מונחים

עברית	אנגלית	הסבר קצר
תרגום כתובות	`NAT`	החלפת כתובת מקור/יעד בנתב לפי טבלת תרגום
כתובת פנימית מקומית	`Inside Local`	הכתובת הפרטית של המחשב
כתובת פנימית גלובלית	`Inside Global`	הכתובת הציבורית שהעולם רואה
העמסה	`Overload / PAT`	כתובת אחת לכולם — הפורט מבדיל
מאגר	`Pool`	טווח כתובות ציבוריות ל-`NAT` דינמי

להעמקה

בספר הקורס

- **ENSA 6.5.3** — Analyze Dynamic NAT—Inside to Outside · עמוד 247

- **ENSA 6.6.3** — Configure PAT to Use an Address Pool · עמוד 253
- **ENSA 6.2.2** — Dynamic NAT · עמוד 232

קבצים שנעבוד איתם

- ENSA_Module_6.pptx
- 6.2.7 Packet Tracer - Investigate NAT Operation.pka
- 6.2.7 Packet Tracer - Investigate NAT Operation.docx
- NAT and PAT - תיאוריה.docx
- Cisco - NAT.docx
- nat.pkt
- 6.4.5 Packet Tracer - Configure Static NAT.pka
