מעבדה: syslog, NTP ו-CDP (על ניהול רשת)

שבוע 21 · 11/02–07/02 · **בנימין נאור**

נתב אחד וכתובת. אין תרשים. מגלים את כל הרשת בלי לגעת בכבל, מסדרים לה זמן, יומן וגיבוי — היום הראשון של מנהל רשת. ובסוף: מוסרים את התיק של הרצועה.

1. שלב 1 — NTP (10.3.4)

```
R1# show clock
*0:03:12.771 UTC Mon Mar 1 1993              <- before
R1(config)# ntp server 209.165.200.225
R1(config)# clock timezone IST 2
R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
R1# show ntp associations
  address         ref clock       st   when   poll  reach  delay  offset  disp
*~209.165.200.225 127.127.1.1      1     3     64    377   0.00   0.00    0.12
R1# show clock
12:41:07.312 IST Tue Feb 9 2027              <- after
```

* = מסונכרן. `stratum` = מרחק מהשעון המדויק. לפני/אחרי — לתעד.

2. שלב 2 — `syslog` (8.1.2.5)

```
  PT server: Services -> SYSLOG -> On

R1(config)# logging 10.1.1.100
R1(config)# logging trap notifications           <- 0-5
R1(config)# service timestamps log datetime msec
R1(config)# interface Loopback0
R1(config-if)# ip address 10.255.255.1 255.255.255.255
R1(config)# logging source-interface Loopback0

R1(config)# interface g0/1
R1(config-if)# shutdown / no shutdown            <- generate a message

  on the server (SYSLOG tab):
  12:43:55  10.255.255.1  %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administrat
            ^ real time (NTP!)   ^ source = Loopback
R1# show logging
```

בלי `NTP` השורה הזו הייתה עם 1993. המקור = `Loopback` — גם אם ממשק פיזי נפל.

3. שלב 3 — `CDP` (10.1.5): למפות בלי להסתכל

```
  RULE: the topology window stays closed. CLI only. draw on paper.

Edge1# show cdp neighbors detail
Device ID: Switch1
  IP address: 192.168.1.2
  Platform: cisco 2960, Capabilities: Switch
  Interface: GigabitEthernet0/0, Port ID (outgoing port): GigabitEthernet0/1
Device ID: Router2
  IP address: 10.1.1.2 ...

Edge1# telnet 192.168.1.2                <- go to the neighbor (passwords in the instructions)
Switch1# show cdp neighbors detail       <- and again. and again.

  paper:  Edge1 Gi0/0 ---- Gi0/1 Switch1 (2960, 192.168.1.2)
          Edge1 Gi0/1 ---- Gi0/0 Router2 (...)
  at the end: open the topology. compare.
```

שוב. הציור על נייר. בסוף משווים. → `telnet` → `IP` → `show cdp neighbors detail`

4. שלב 4 — TFTP (10.6.10): גיבוי ששוחזר

```
R1# ping 10.1.1.100                                  <- FIRST. TFTP (UDP 69) fails silently
R1# show version                                     <- model · IOS · uptime · flash
R1# copy running-config tftp:
Address or name of remote host []? 10.1.1.100
Destination filename [R1-confg]? R1-backup.cfg
!!
1234 bytes copied

  now BREAK something:
R1(config)# hostname WRONG
R1(config)# no ip route 0.0.0.0 0.0.0.0

WRONG# copy tftp: running-config
Address or name of remote host []? 10.1.1.100
Source filename []? R1-backup.cfg
R1#                                                  <- hostname back, route back

  note: copy tftp: running-config MERGES. full restore = copy tftp: startup-config + reload
```

גיבוי ששוחזר פעם אחת = גיבוי. גיבוי שלא שוחזר = תקווה.

⚠ **שימו לב ·** `copy tftp: running-config` ממזג — פקודה שנוספה אחרי הגיבוי לא נמחקת. לשחזור מלא: `startup-config` + `reload` .

מסירת תיק העבודות — מה מגישים

```
<name>_<band>/
  README.md            <- the list: week · lab · file · completion / state
  w07_...pkt           <- every lab pkt of the band
  w08_broken_fixed.pkt + w08_report.docx     <- fault labs: fixed pkt + report
  ...
  w21_...pkt + w21_doc.docx

graded on: completeness (all weeks) · documentation (reports, README) · quality — not only C
```

תיקייה אחת, `README` אחד, כל השבועות. 30% מציון הרצועה. חסר — משלימים עד סוף השבוע.

דוגמה פתורה

השאלה

הפניתם `logging` לשרת, ההודעות מגיעות — עם '`Mar 1 1993`'. הוספתם `.ntp server` ההודעות הישנות עדיין 1993, החדשות נכונות. אבל ב-`show logging` הכול 1993. למה, ומה הסדר הנכון?

הפתרון צעד אחר צעד

1. **למה הישנות 1993**: `syslog` לא מתקן חותמות זמן שכבר נשלחו. הזמן נקבע ברגע ההודעה.
2. **למה ב-`show logging` הכול 1993**: ה-`buffer` המקומי הוקלט לפני הסנכרון. אחרי `NTP` — הודעות חדשות ב-`buffer` עם זמן נכון; הישנות נשארות.
3. **הסדר**: `ntp server` → `show ntp status` (`synchronized`) → `service timestamps` → `logging` ‹`ip`›. רק אז `shut/no shut` לבדיקה.
4. **ניקוי**: `clear logging` (`buffer`). בשרת — למחוק ידנית.
5. **תיעוד**: צילום ההודעה בשרת עם זמן נכון + `.show ntp status`

תשובה · `NTP` קודם, תמיד. הוכחה: שתי הודעות זו מתחת לזו — 1993 ו-2027.

תרגילים — פתרו לבד לפני שאתם בודקים בכיתה

1. * לפני כתובת ב-`show ntp associations` — מה?
2. `stratum 2` — מה?
3. `logging trap notifications` — רמות?
4. למה `logging source-interface Loopback0` ?
5. ב-10.1.5 — מה אסור?
6. `show cdp neighbors detail` — מה יש שאין ב-`show cdp neighbors` ?
7. לפני `copy` ... `tftp` : — מה?
8. `copy tftp: running-config` — מחליף או ממזג?
9. גיבוי שלא שוחזר = ?
10. מה בתיק?

דף עבודה — מעבדה 21 — `NTP` · `syslog` · `CDP` · `TFTP` · מסירת התיק

שם: _____ תאריך: _____ חוליה: _____

המטרה: 4 פעילויות ב-100%, מפה מ-`CDP` על נייר, גיבוי ששוחזר — והתיק מוגש.

מהלך — סמנו כל שלב שהושלם

- ☐ 10.3.4: `show clock` לפני _____. `ntp server` · `timezone`. `show ntp status`
  _____. `show clock` אחרי _____. `Completion`.
- ☐ 8.1.2.5: שרת `syslog On. logging` · `trap` · `timestamps` · `Loopback0` · `source-interface`.
  `shut/no shut` → ההודעה בשרת (העתיקו עם הזמן). `.show logging`
- ☐ 10.1.5: חלון סגור. `show cdp neighbors detail` → `telnet` → שוב. ציור על נייר: כל התקן · דגם · `IP` · ממשק↔ממשק. השוואה. `Completion`.
- ☐ 10.6.10: `ping TFTP` · `show version` (דגם _____ `IOS` _____) ·
  `:copy running-config tftp` · לשבור (`hostname` + `no ip route`) ·
  `copy tftp: running-config` · חזר? `Completion`.
- ☐ התיק: ‹שם›_ניתוב — 14 · 16 · 17 · 19 · 21 (+ תקלות). `README`. הגשה.

רישום התוצאות

#	מה למלא	חישוב · הערות · ראיות (פלט פקודה)
1	10.3.4: לפני _____ · `status` _____ · אחרי _____ · `Completion` _____ %	
2	8.1.2.5: ההודעה בשרת: _____	
3	10.1.5: מפה: _____ · `Completion` _____ %	
4	10.6.10: דגם _____ `IOS` _____ · שחזור _____ · `Completion` _____ %	
5	תיק: ☐ הוגש	

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) ☐ תיק העבודות של הרצועה (300)

· **XP** _____ · תג: ☐ מנהל/ת הרשת · חתימה _____

כרטיס יציאה — 3 שאלות, 5 דקות, נמסר ביציאה

1. הסדר?

2. `CDP` — הכלל?

3. לפני `TFTP` ?

עוד לבדיקה עצמית — ענו בעל פה, בלי להסתכל אחורה

1. `README` ?

מילון מונחים

עברית	אנגלית	הסבר קצר
שכבת זמן	`Stratum`	מרחק מהשעון המדויק — 1 = ישיר
מיזוג תצורה	`Merge`	`copy tftp: running-config` מוסיף, לא מחליף
מיפוי רשת	`Network Mapping`	גילוי הטופולוגיה מהפלט — `CDP/LLDP`
תיק עבודות	`Portfolio`	כל תוצרי הרצועה + `README` — 30%

להעמקה

בספר הקורס

- **ENSA 10.6.5** — Use TFTP to Back Up and Restore a Configuration · עמוד 428

- **ENSA 10.3.3** — Configure and Verify NTP · עמוד 402
- **SRWE 1.5.2** — Verify Interface Status · עמוד 30

קבצים שנעבוד איתם

- 10.3.4 Packet Tracer - Configure and Verify NTP.pka
- 10.3.4 Packet Tracer - Configure and Verify NTP.docx
- 8.1.2.5 Packet Tracer - Configuring Syslog and NTP.pka
- 10.1.5 Packet Tracer - Use CDP to Map a Network.pka
- 10.1.5 Packet Tracer - Use CDP to Map a Network.docx
- 10.6.10 Packet Tracer - Back Up Configuration Files.pka
- 10.6.10 Packet Tracer - Back Up Configuration Files.docx
- 10.8.1 Packet Tracer - Configure CDP, LLDP, and NTP.pka
- Syslog.docx
