ניהול רשת · CDP/LLDP · NTP · syslog · גיבוי תצורה

שבוע 20 · 04/02–31/01 · **בנימין נאור**

הקישור נפל. מתי? כמה פעמים? מי ידע? נתב שכותב הודעות רק לקונסול — עם תאריך 1993 — לא עונה על אף שאלה. היום: זמן נכון (`NTP`), יומן במקום אחד (`syslog`), מפה של הרשת (`CDP`), וגיבוי (`TFTP`). שלוש שאלות בחינה על שני מונחים.

1. `syslog` — לקרוא הודעה

```
*Mar  1 00:12:45.331: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
 ^timestamp            ^facility ^sev ^mnemonic    ^description

severity 0..7:
0 emergency   1 alert   2 critical   3 error   4 warning   5 notification   6 informational   7 deb
'Every Awesome Cisco Engineer Will Need Ice-cream Daily'

where messages go:  console (default) · buffer (show logging) · terminal (terminal monitor)  · SERVE
```

`facility-severity-mnemonic` . 0 הכי חמור, 7 הכי מפורט (`debug`). `logging trap` › `level` › = עד איזו רמה לשלוח לשרת.

2. `syslog` — לשרת (שאלת בחינה)

```
R1(config)# logging 10.1.1.100              <- send to syslog server (also: logging host 10.1.1.100
R1(config)# logging trap warnings           <- levels 0-4 only (default: informational = 0-6)
R1(config)# service timestamps log datetime msec
R1(config)# logging source-interface Loopback0
R1# show logging                            <- buffer + settings

R1# debug ip icmp                           <- level 7 messages, live. 10 seconds, then:
R1# no debug all
```

`logging` › `ip` › — בחינה 2023 ש'2ח ו-2026 ש'17. `debug` = רמה 7 בזמן אמת; לכבות מיד.

> ⚠ **שימו לב ·** `debug all` על נתב בייצור = הקונסול מוצף, הנתב נחנק. 10 שניות ו- `.no debug all`

3. NTP ו-Loopback — הזמן הנכון

```
R1# show clock
*00:14:02.115 UTC Mon Mar 1 1993                <- no NTP: every reboot starts in 1993

R1(config)# ntp server 10.1.1.100              <- client
R1(config)# clock timezone IST 2
R2(config)# ntp master 3                       <- R2 is the server (stratum 3)

R1# show ntp status
Clock is synchronized, stratum 4, reference is 10.1.1.100
R1# show ntp associations

R1(config)# interface Loopback0
R1(config-if)# ip address 10.255.255.1 255.255.255.255      <- never goes down
R1(config)# ntp source Loopback0
R1(config)# logging source-interface Loopback0
```

לוג בלי זמן = סיפור בלי תאריך. `stratum` = מרחק מהשעון האטומי. `Loopback` = הכתובת הקבועה של הנתב — מקור ל-`NTP`, `syslog`, `SNMP`.

4. CDP ו-LLDP — מפה בלי תרשים (שאלת בחינה)

```
R1# show cdp neighbors
Device ID   Local Intrfce   Holdtme   Capability   Platform   Port ID
S1          Gig 0/1         158       S I          2960       Gig 0/1
R2          Gig 0/0         142       R            C4331      Gig 0/0
R1# show cdp neighbors detail            <- + IP address, IOS version

R1(config)# interface g0/0/0
R1(config-if)# no cdp enable              <- toward the ISP: don't advertise model + IOS to strangers
R1(config)# no cdp run                    <- globally off

R1(config)# lldp run                      <- the open standard (802.1AB) — works with non-Cisco
R1# show lldp neighbors
```

`CDP` = `Cisco` בלבד, דלוק כברירת מחדל. `LLDP` = תקן. שניהם: מי מחובר לאיזה פורט, דגם, כתובת. בחינה 2023 ש'ד1.

5. גיבוי, שחזור, IOS

```
R1# show version                          <- model, IOS version, uptime, flash size, config-register
R1# show flash                            <- the IOS image file

! backup to TFTP (UDP 69 — ping the server first!)
R1# copy running-config tftp:
Address or name of remote host []? 10.1.1.100
Destination filename [r1-confg]? R1-backup.cfg
! restore
R1# copy tftp: running-config

! simplest backup: show run -> copy/paste to a text file (Tera Term / PuTTY log)

! IOS
R1# copy flash: tftp:                     <- backup the image
R1# copy tftp: flash:                     <- new image
R1(config)# boot system flash:‹image›     <- which one to boot
```

גיבוי לפני כל שינוי. TFTP שקט כשנכשל — ping קודם. הכי פשוט: show run לטקסט.

6. SNMP ו- MIB — מה מנהל הרשת רואה

```
  manager (PRTG / Zabbix)  <---- GET / SET ---->  agent (router, switch)
                           <---- trap ----------   'interface down!'
  ports: 161 (get/set)  162 (trap)

  MIB = a tree of everything the device knows.  OID = an address in the tree
  1.3.6.1.2.1.2.2.1.10.1  = ifInOctets on interface 1  (bytes in)

  v1/v2c: community string ('public' = read, 'private' = write) — in clear text
  v3: user + authentication + encryption

R1(config)# snmp-server community NetMon RO       <- read-only
R1(config)# snmp-server host 10.1.1.100 version 2c NetMon
R1(config)# snmp-server enable traps
```

GET = המנהל שואל. trap = ההתקן מודיע. MIB עץ, OID כתובת. מה רואים: גרף רוחב פס לכל פורט, CPU, up/down.

טיפ · `community` ' `public` ' בייצור = כל אחד קורא את הרשת. `v3` , או לפחות `string` חזק + `ACL` .

דוגמה פתורה

השאלה

נתב `R1` : הקישור לספקית נפל שלוש פעמים אתמול בלילה. אף אחד לא ראה. מה מגדירים כדי שבפעם הבאה: (א) ההודעה תישמר (ב) עם זמן נכון (ג) מישהו יקבל התראה?

הפתרון צעד אחר צעד

1. **(ב) קודם** — זמן: `ntp server 10.1.1.100` · `clock timezone IST 2` · `service timestamps log datetime msec` . `show clock` → אמיתי.
2. **(א)** — לשרת: `logging 10.1.1.100` · `logging trap notifications` (`LINK-3` % ו-`LINEPROTO-5` % בפנים). `logging source-interface Loopback0` — שההודעה תצא גם אם ממשק פיזי נפל.
3. **(ג)** — התראה: `snmp-server host 10.1.1.100 version 2c` `NetMon` · `snmp-server enable traps` → `trap linkDown` לשרת הניטור, שמוציא מייל/ `SMS` .
4. **אימות**: `shutdown/no shutdown` על ממשק → ההודעה בשרת ה- `syslog` עם זמן · `trap` בשרת ה- `SNMP` .
5. **ומה בבוקר**: `show logging` ב- `R1` + היומן בשרת → 'נפל ב-02:14, 02:31, 03:05' — ואפשר להתקשר לספקית עם נתונים.

תשובה · `NTP` → `syslog` → `SNMP trap.` שלוש פקודות ליבה: `ntp server` · `logging` › `ip` · `snmp-server host` .

תרגילים — פתרו לבד לפני שאתם בודקים בכיתה

1. הפקודה שמפנה יומנים לשרת 10.1.1.100?
2. % `LINEPROTO-5-UPDOWN` — `facility` ? `severity` ? מה זה אומר?
3. `logging trap warnings` — אילו רמות נשלחות?
4. `show clock` מראה 1993. מה חסר?
5. `stratum 1` מול `stratum 4` ?

6. למה `Loopback` כמקור?

7. הפקודה שמגלה שכנים סיסקו עם `IP` ו- `IOS` ?

8. למה `no cdp enable` על הממשק לספקית?

9. `:copy running-config tftp` נכשל בשקט. הבדיקה?

10. `GET` מול `trap` ?

דף עבודה — ניהול רשת — `syslog` · `NTP` · `CDP` · `TFTP` · `SNMP`

שם: _____ תאריך: _____ חוליה: _____

המטרה: 10 פקודות עם משפט, 3 שאלות בחינה, ותרחיש אחד מתוכנן.

מהלך — סמנו כל שלב שהושלם

- ☐ פענחו 4 הודעות `syslog` : %SYS-5-CONFIG_I · %LINK-3-UPDOWN · %OSPF-5-ADJCHG · %LOGIN_FAILED-4-SEC_LOGIN — `facility` , `severity` , מה קרה.
- ☐ המשפט של הרמות — כתבו 0–7 מהזיכרון.
- ☐ תרחיש: נתב שנופל בלילה — 3 קבוצות פקודות (זמן · יומן · התראה). סדר!
- ☐ `show cdp neighbors` (מהחוברת): ציירו את הטופולוגיה מהפלט בלבד.
- ☐ 10 פקודות — משפט לכל אחת (רשימה בשיעורי הבית).
- ☐ בחינה: 2023 ד1 · 2023 ח2 · 2026 17 — ענו.

רישום התוצאות

#	מה למלא	חישוב · הערות · ראיות (פלט פקודה)
1	4 הודעות: _____	_____
2	0 _____ 1 _____ 2 _____ 3 _____ 4 _____ 5 _____ 6 _____ 7 _____	_____
3	תרחיש: זמן _____ · יומן _____ · התראה _____	_____
4	טופולוגיה מ- `CDP` : _____	_____
5	10 פקודות: _____	_____
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: ☐

מנהל/ת הרשת · חתימה _____

כרטיס יציאה — 3 שאלות, 5 דקות, נמסר ביציאה

1. `logging` › `ip` › עושה...

_____

2. 0 או 7 — מה חמור?

_____

3. `NTP` לפני או אחרי `syslog` ?

_____

עוד לבדיקה עצמית — ענו בעל פה, בלי להסתכל אחורה

1. `CDP` — של מי?

מילון מונחים

עברית	אנגלית	הסבר קצר
יומן מערכת	`Syslog`	הודעות ההתקן — קונסול, `buffer`, שרת (`UDP 514`)
רמת חומרה	`Severity`	0 `emergency` ... 7 `debugging`
פרוטוקול זמן	`NTP`	סנכרון שעון — `UDP 123`, `stratum`
ממשק לולאה	`Loopback`	ממשק לוגי שלא נופל — כתובת קבועה
גילוי שכנים	`CDP / LLDP`	מי מחובר לאיזה פורט — `Cisco` / תקן
העברת קבצים פשוטה	`TFTP`	גיבוי/שחזור תצורה ו-`IOS` — `UDP 69`
ניהול רשת	`SNMP`	`GET/SET/trap` — 161/162 — `MIB/OID`
מסד מידע ניהולי	`MIB`	עץ הנתונים של ההתקן — `OID` = כתובת בעץ

להעמקה

בספר הקורס

- **ENSA 10.3** — NTP · עמוד 400
- **ENSA 10.2.1** — LLDP Overview · עמוד 396
- **ENSA 10.1.1** — CDP Overview · עמוד 390

קבצים שנעבוד איתם

- ENSA_Module_10.pptx
- Syslog.docx
- 8.1.2.5 Packet Tracer - Configuring Syslog and NTP.pka
- 10.1.5 Packet Tracer - Use CDP to Map a Network.pka
- 10.6.10 Packet Tracer - Back Up Configuration Files.pka
- 10.4.10 Lab - Research Network Monitoring Software - ILM.docx