Trunk · 802.1Q · DTP · native VLAN · pruning

שבוע 9 · 12/11–08/11 · **פלנר עדי**

`VLAN 10` בשני מתגים, מחשב בכל אחד, קישור רגיל ביניהם — ו- `ping` לא עובד. הקישור נמצא ב- `VLAN 1` בלבד. כדי ש- `VLAN` יחצה מתגים צריך קישור שנושא **כמה** `VLANs` יחד: `trunk` . ואיך המתג השני יודע לאיזה `VLAN` שייכת כל מסגרת? תג.

1. `Trunk` ותג 802.1Q

על קישור `trunk` כל מסגרת מקבלת **תג** של 4 בתים בתוך המסגרת, עם מספר ה- `VLAN` . המתג מוסיף את התג ביציאה ל- `trunk` ומסיר אותו בכניסה לפורט `access` — המחשבים לא רואים תג לעולם.

```
PC (VLAN 10) --access--> [SW1] ==trunk==> [SW2] --access--> PC (VLAN 10)
               no tag         tagged 10          no tag

802.1Q tag (4 bytes) inserted after the source MAC:
| DST MAC | SRC MAC | TPID 0x8100 | PRI(3) CFI(1) VLAN ID(12) | Type | DATA | FCS |
VLAN ID: 12 bits -> 4096 values -> 1..4094 usable
```

התג נכנס אחרי כתובת המקור. 12 סיביות ל- `VLAN ID` — 4094 `VLANs` אפשריים (0 ו-4095 שמורים).

	פורט `access`	פורט `trunk`
`VLANs`	אחד	כמה (`allowed`)
תג	אין	יש (חוץ מ- `native`)
מחובר ל	מחשב, שרת, טלפון	מתג, נתב

2. תצורת `trunk` — שלוש פקודות

```
SW1(config)# interface g0/1
SW1(config-if)# switchport mode trunk
SW1(config-if)# switchport trunk allowed vlan 10,20,30
SW1(config-if)# switchport trunk native vlan 99

SW1# show interfaces trunk
Port    Mode   Encapsulation  Status    Native vlan
Gi0/1   on     802.1q         trunking  99
Port    Vlans allowed on trunk
Gi0/1   10,20,30
```

`mode trunk` · `allowed vlan` · `native vlan. show interfaces` `trunk` מאמת את שלושתם — ואת שני הצדדים.

> ⚠ **שימו לב ·** `allowed vlan 10` ואז `allowed vlan 20` = נשאר רק 20! להוסיף: `allowed vlan add 20` . (בבחינה 2026: `.allowed vlan all`)

3. `Native VLAN` — המסגרות בלי תג

מסגרות של ה-`native VLAN` עוברות על ה-`trunk` **בלי תג**. ברירת המחדל: `.VLAN 1` חובה שיהיה זהה בשני הצדדים — אחרת מסגרת שיצאה בלי תג מ-`VLAN 1` בצד אחד נכנסת ל-`VLAN 99` בצד השני: דליפה בין `VLANs` , ופרצת אבטחה.

מצב	מה קורה
`native` זהה בשני הצדדים	תקין
`native 1` מול 99	`CDP` : ' `Native VLAN mismatch` ' · דליפה
נוהג טוב	`native` ייעודי (99), ריק, לא `VLAN 1`

4. `DTP` — מי מחליט שזה `trunk`

`DTP` מנהל 'משא ומתן' בין שני מתגים על מצב הפורט. ארבעה מצבים:

```
            auto        desirable    trunk
  auto      ACCESS      trunk        trunk
  desirable trunk       trunk        trunk
  trunk     trunk       trunk        trunk
```

`auto` + `auto` = `access`. שני מתגים 2960 בברירת מחדל לא יקימו `trunk` לבד. זו השאלה שנופלת.

מצב	מה הוא עושה
`dynamic auto`	מחכה שהצד השני יבקש (ברירת מחדל ב-2960)
`dynamic desirable`	מבקש להיות `trunk`
`trunk`	`trunk` קבוע (ושולח `DTP`)
`nonegotiate`	בלי `DTP` בכלל — מה שהוגדר ידנית

טיפ · למה מכבים `DTP` (`nonegotiate`)? כי תוקף שמתחזה למתג יכול 'לבקש' `trunk` ולקבל גישה לכל ה-`VLANs` — `VLAN hopping`. ערן ירחיב.

דוגמה פתורה

השאלה

`SW1 Gi0/1` ב-`dynamic auto`, `SW2 Gi0/1` ב-`dynamic auto. VLAN 10` בשניהם עם מחשב בכל אחד. `ping` נכשל. מה קורה, ומה התיקון המינימלי?

הפתרון צעד אחר צעד

1. `auto` + `auto` = `access`. הקישור ב-`VLAN 1` (`native/access`), לא `trunk`.
2. **מסגרות** `VLAN 10` לא עוברות — הפורט `access` ב-`VLAN 1`.
3. `show interfaces trunk` ריק — אין `trunk`.
4. **תיקון מינימלי**: בצד אחד `switchport mode dynamic desirable`, או בשני הצדדים `mode trunk` (מומלץ — צפוי ובטוח).
5. **אימות**: `show interfaces trunk` מראה `trunking` · `ping` ✓.

תשובה · `auto` מול `auto` לא מקים `trunk`. ידני (`mode trunk`) בשני הצדדים + `nonegotiate` — הדרך הבטוחה.

תרגילים — פתרו לבד לפני שאתם בודקים בכיתה

1. למה המחשב לא רואה את התג?
2. כמה סיביות ל-`VLAN ID`, וכמה `VLANs` שמישים?

3. `auto` + `auto` — `trunk`?

4. `auto` + `desirable`?

5. `native 1` בצד אחד, 99 בשני. מה קורה?

6. `allowed vlan 10` ואז `.allowed vlan 20` מה נשאר?

7. השלימו: `SW1` (`config-if`)# `switchport mode` _____ .
`switchport trunk allowed vlan` _____

8. למה `nonegotiate`?

דף עבודה — דף עבודה 9 — `trunk`, `native` ו-`DTP`

שם: _____ תאריך: _____ חוליה: _____

המטרה: להבין את התג, לזכור את שלוש הפקודות, ולנבא את טבלת `DTP`.

מהלך — סמנו כל שלב שהושלם

- ☐ ציירו מסגרת `Ethernet` עם תג 802.1Q: סמנו איפה התג ומה בתוכו.
- ☐ כתבו את 3 פקודות ה-`trunk` ל-`Gi0/1` עם `VLANs 10` ,20,30 ו-`.native 99`
- ☐ פתחו 3.5.5 `.Configure DTP` לכל צירוף בטבלה: נבאו (`access/trunk`), הגדירו, בדקו ב-`.show dtp interface` סמנו ✓/✗.
- ☐ בטופולוגיה של 3.4.5: הגדירו `trunk` בצד אחד בלבד. `show interfaces trunk` בשני הצדדים. מה רואים?
- ☐ שנו `native` ל-99 בצד אחד בלבד. מה `CDP` אומר? (`show cdp neighbors` / הודעת קונסול). תקנו.
- ☐ כתבו: מה ההבדל בין `allowed vlan` ל-`.allowed vlan add`

רישום התוצאות

#	מה למלא	חישוב · הערות · ראיות (פלט פקודה)
1	ציור המסגרת עם התג: _____	_____
2	3 הפקודות: _____	_____
3	`DTP` : `auto` + `auto` ניבוי _____ תוצאה _____ · `auto` + `desirable` _____ / _____ _____ · `auto` + `trunk` _____ / _____ · `desirable` + `nonegotiate` _____ / _____	_____
4	`trunk` בצד אחד: `show interfaces trunk` בצד השני: _____	_____
5	`native mismatch` — ההודעה: _____	_____
6	`allowed vs add:` _____	_____

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: ☐ בונה ☐ הגשר · חתימה _____

כרטיס יציאה — 3 שאלות, 5 דקות, נמסר ביציאה

1. תג 802.1Q — כמה בתים?

2. `auto` + `auto` =

3. `native VLAN` עובר עם תג?

עוד לבדיקה עצמית — ענו בעל פה, בלי להסתכל אחורה

1. שלוש הפקודות?

מילון מונחים

עברית	אנגלית	הסבר קצר
קישור גזע	`Trunk`	קישור שנושא כמה `VLANs` עם תגים
תג	`802.1Q Tag`	4 בתים במסגרת: `VLAN ID` ועדיפות
VLAN טבעי	`Native VLAN`	ה-`VLAN` שמסגרותיו עוברות בלי תג
פרוטוקול משא ומתן	`DTP`	מכריע `access/trunk` בין מתגים
ללא משא ומתן	`nonegotiate`	`DTP` כבוי — הגדרה ידנית בלבד
VLANs מותרים	`Allowed VLANs`	אילו `VLANs` עוברים על ה-`trunk`

להעמקה

בספר הקורס

- **SRWE 3.4** — VLAN Trunks · עמוד 83
- **SRWE 3.5.1** — Introduction to DTP · עמוד 88

קבצים שנעבוד איתם

- SRWE_Module_3.pptx
- 3.4.5 Packet Tracer - Configure Trunks.pka
- 3.5.5 Packet Tracer - Configure DTP.pka
- Lab 3.4.2 Configuring a Trunk Port to Connect Switches.pdf