

תקשוב ג' פרק 1 – תקציר

הגדרות בסיסיות למוגדר

מעובד וערוך מtower חומרה הלימוד של האקדמיה של סיסקו.

תוכנת מערכת הפעלה Cisco IOS

מערכת הפעלה אשר מספקת פונקציונליות, הרחבת וابتחה למוצרי חברת סיסקו.
באמצעות ממשק פקודה CLI.

ישנם מספר דרכים כדי להתחבר למשק הפקודה:

1. **קונסול** – מחשב בעל תוכנת טרמינל המחבר מיציאת RS-232 ע"י כבל מיוחד
(כבל קונסול BD-9 בצע תכלת).

להגדירה ראשונית של מטג/ראוטר חיבים להשתמש בכבל קונסול!

בהתחברות ע"י המחשב יש להגדיר פרמטרי התקשרות: ח,א,8,0,9600

2. חיבור מרוחק Telnet או SSH

חיבור Telnet מציר רשות עובדת והגדרת ממשק אחד לפחות לעבוד כ- Telnet
ומוגדרת לו כתובת IP לצורך התabbrות ברשות.

התקשרות החיבור זה היא **גלוייה** וניתן לנטר את המידע העובר בקצב יחסית.

מסיבות אבטחה, מערכת הפעלה דורשת לפחות סיסמת **זיהוי** משתמש כאשר
עובדים מרוחק.

חיבור SSH – Secure Shell

דומה לחיבור Telnet אך **מאובטח יותר** באמצעות הצפנה המידע העובר בין
המטג/ראוטר למחשב.

עדיף להשתמש ב- SSH מאשר ב- Telnet.

לעבודה ב- SSH יש להתקן ולהגדיר את המחשב בתוכנת SSH.

AUX .3

חיבור דרך קו טלפון באמצעות חיגון ומודם, אך ניתן לעבוד גם מקומי כאשר לא ניתן
לעבוד באמצעות קונסול.

קבצי הגדרת תצורה - Configuration

startup-config קובץ תצורת העבודה של הנטב/ראוטר מאוחסן בזיכרון לא מחיק, ונקרא: בעת הדלקת הנטב/ראוטר הקובץ נטען לתוך ה- RAM ומשם הוא רץ ונקראCut:

running-config

כאשר אנו מבצעים שינוי תצורה, הם מבוצעים מיד, ב- RAM יש לבצע שמיירה של שינוי התצורה ב- startup-config כדי שישמרו גם לאחר כיבוי הציגו.

הפקודה לשמירת ההגדרות היא:

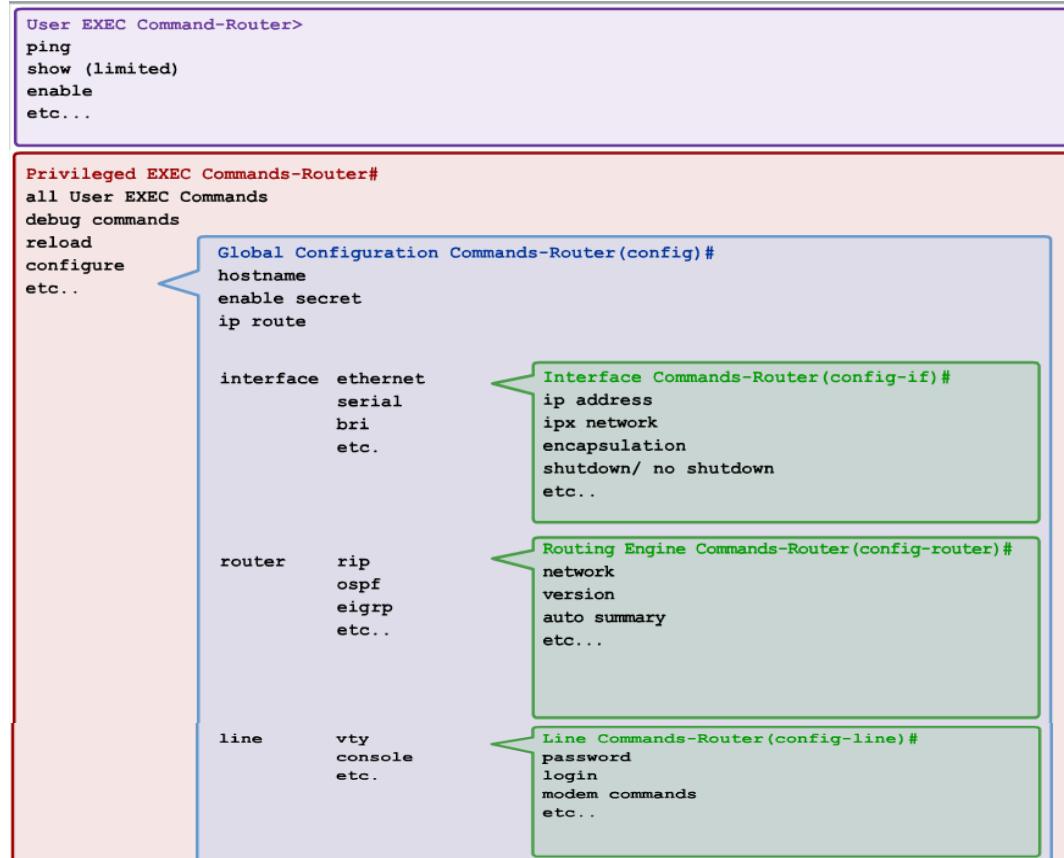
Switch#copy running-config startup-config

משיקולי אבטחה מערכת הפעלה עובדת בשכבות.

השכבות מסודרות בצורה היררכית.

לכל שכבה אוסף פקודות מיוחדת.

כל שורה מתחילה בשם התקן ולאחריו זיהוי השכבה.



שכבה משתמש (User)

- מאפשרת גישה משתמש למספר פקודות בסיסיות של ניטור (monitoring) להראות מצב.

Switch> disable

- שכבה זו עולה עם הכניסה למצב או ע"י פקודה:

Privilege

- סימון השכבה: >

שכבה זכויות (Privilege)

- מאפשרת גישה לכל הפקודות כגון קביעת תצורה וניהול.
- בתוכה תת-שכבות.
- שכבה זו ניתנת להגנה ע"י סיסמה.
- סימון השכבה: #

Switch> enable

- כניסה לשכבה ע"י הפקודה:

תת-שכבה: תצורה כללית (Global configuration)

- מאפשרת גישה לפקודות כגון hostname, הגדרת הגדרת ממשקים, הגדרת התחברות למצב ע"י קונסול או VTY וכן'

Switch (config)#

- סימון השכבה: #(config) #

Switch#configure terminal

- כניסה לשכבה ע"י הפקודה:

עזרה

מערכת הפעלה מספקת עזרה באמצעות **?** ללא **<Enter>** סוג העזרה תלוי במיקום ה- **?**

1. **?** לאחר סימון השכבה תתן את כל רשימת הפקודות הקיימות אותה השכבה למשל:

Switch>?

Exec commands:

```
<1-99> Session number to resume  
connect Open a terminal connection  
disable Turn off privileged commands  
disconnect Disconnect an existing network connection  
enable Turn on privileged commands  
exit Exit from the EXEC
```

2. **?** לאחר אחת או מס' אותיות תציג את הפקודות המתחילה באותיות אלו. למשל:

Switch>sh?

Show

3. **?** לאחר רווח יתן את רשימת האפשרויות או נתוני שאפשר או صحיבים להכנס. למשל:

Switch#clock set ?

hh:mm:ss Current Time

Switch#clock set 12:10:10 ?

<1-31> Day of the month

פקודה לא מלאה תגרום להודעה הבאה:

Switch#clock set 12:10:10 1 september

% Incomplete command.

יצירת שם למ tangent

Switch(config)#hostname <HILIK>

ממצב זכויות:

HILIK (config) #

יצירת בナー

בナー משמש כהודעת פתיחה ברגע הכניסה למ tangent. ניתן לנצל את הבナー כדי להעביר הודעות למפעיל, לשים הודעת אבטחה כגון "הכניסה למ tangent למורשים בלבד", לוגו של החברה וכו' הבナー צריך להתחיל ולהסתיים **באותנו התו** (@ בדוגמה להלן) אסור שתו זה יופיע בתוך הטקסט.

ממצב זכויות:

Switch(config)#banner motd @ !!! HILIK's SWITCH !!! @

הגדרת ממשיים

שלבים להגדרת ממשן אינטרנט.

Switch>**enable**

1. כניסה למצב זכויות:

Switch#**configure terminal**

2. כניסה לתצורת קונפיגורציה:

Switch(config)#**interface FastEthernet 0/0** 3. כניסה להגדרת ממשן או ממשיים:

Switch(config-if)#**no shutdown**

4. הפעלת המשן:

Switch(config-if)#**shutdown**

5. כדי לנכבות ממשן משתמשים בפקודה:

הגדרת מספר ממשיים במקביל:

Switch#**configure terminal**

Switch(config)#**interface range FastEthernet 0/1-4**

Switch(config-if-range)#**no shutdown**

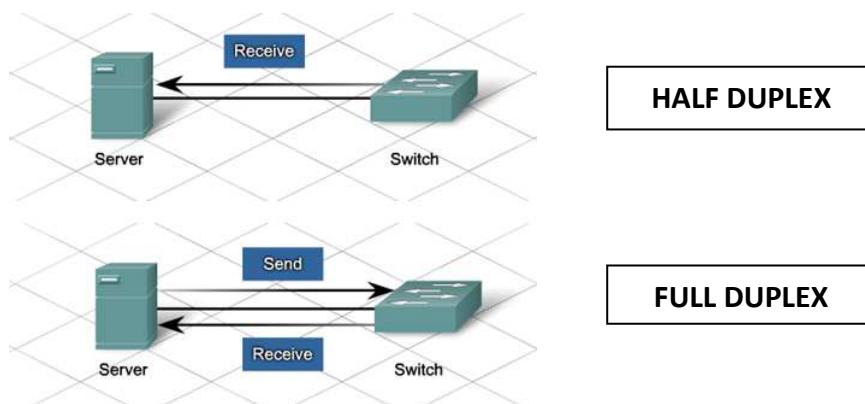
הגדרת מהירות וצורת תקשורת מול ממשך אחר

ניתן להגדיר את מהירות העבודה של הממשך באמצעות הפקודה: **speed**

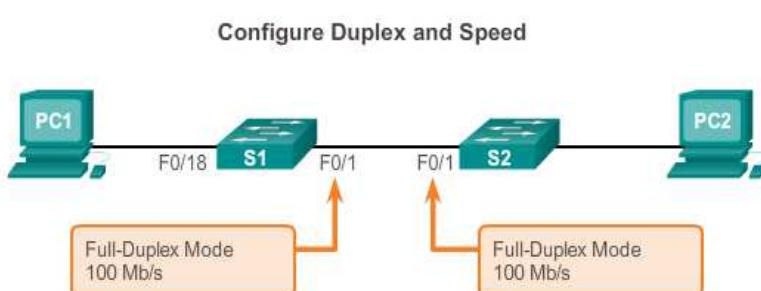
למהירות: **speed 10/100 Mbps** ידנית או להגדיר מצב אוטומטי (**AUTO**) שבו מהירות הממשך נקבעת ע"י דו-שיח בין שני הממשכים.

בנוסף ניתן להגדיר את צורת התקשרות בין שני הממשכים:

- **Half-duplex** – קליטת נתונים ושידורם **לסירוגין** (כמו במכשיר קשר)
- **Full-duplex** - קליטה ושידור הנתונים מתבצעים **בו-זמנית**. (כמו בשיחת טלפון).
- **AUTO** - צורת התקשרות נקבעת אוטומטית ע"י דו-שיח בין הממשכים.



הגדרה ידנית משמשת כדי למנוע בעיות הגדרה בין יצירנים שונים של ציוד.



Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode.	S1(config)# interface FastEthernet 0/1
Configure the interface duplex.	S1(config-if)# duplex full
Configure the interface speed.	S1(config-if)# speed 100
Return to the privileged EXEC mode.	S1(config-if)# end
Save the running config to the startup config.	S1# copy running-config startup-config

בדיקות התצורה.

Switch#show running-config

פקודת:

תראה לנו את קובץ ההגדרות של המtag / נתב שרצות כרגע בזיכרון RAM.

Switch#show startup-config

פקודת:

תראה לנו את קובץ ההגדרות של המtag / נתב **השמורות בזיכרון ללא מחיק NVRAM**.

הגדרות שאנו מבצעים בנתב / מtag נשמרות בזיכרון RAM בקובץ: running-config אשר עלול להמחק בכיבוי המכשיר, אך עליינו לשמר את ההגדרות בזיכרון **לא מחיק** (NVRAM) בקובץ: startup-config ומנעו את איבוד ההגדרות.

שמירת ההגדרות באמצעות הפקודה:

Switch#copy running-config startup-config

Switch# Write Memory

הפקודה הבאה אינה בתוכנית הלימודים:

אבטחת המתג / נתב

סיסמאות הן ההגנה הראשונה להתחברות לא מורשית לאביזרי הרשת.

- סיסמת קוונטול – מגבילה את הגישה דרך חיבור קוונטול.
- סיסמת Enable – מגבילה את הגישה למצב "זכיות" (Privileged Exec) (Enable)
- סיסמת Enable מוצפנת – סיסמה כנ"ל רק מוצפנת.
- סיסמת YVT – מגבילה את הגישה באמצעות חיבור מרוחק (Telnet)

מומלץ להשתמש בסיסמאות שונות לכל רמת גישה.

כדי להשתמש ב- "סיסמאות חזקות", אשר לא ניתן לנחש אותן.

למשל:

- אורך סיסמה מעל 8 תווים.
- שילוב של אותיות גדולות קטנות ומספרים.
- לא להשתמש באותה סיסמה לכל האביזרים.
- לא להשתמש במילים נפוצות כגון: admin, Password, Admin

סיסמת קוונטול.

```
Switch(config)#line console 0
```

```
Switch(config-line)#password <password>
```

```
Switch(config-line)#login
```

סיסמת Enable מוצפנת.

כדי להשתמש בסיסמת Enable מוצפנת ולא בסיסמת Enable הרגילה,-CSA, משומש שההצפנה מספקת אבטחה טובה יותר.

```
Switch(config)#enable password <password>
```

```
Switch(config)#enable secret password
```

לא ניתן להתחבר מרוחק (Telnet) במידה ולא הוגדרה סיסמת Enable !!!

סיסמת VTY.

כברירת מחדל, ציוד סיסקו תומך ב-5 קווי גישה מרוחק הממוספרים 4-0. יש להגדיר סיסמה לכל הקווים הללו. (ניתן להגדיר את אותה הסיסמה)

```
Switch(config)#line vty 0 4
```

```
Switch(config-line)#password <password>
```

```
Switch(config-line)#login
```

הסתרת הסיסמות המוצגות.

את הסיסמות ניתן לראות בקבצי הקונפיגורציה ע"י הפקודות:

show startup-config או show running-config

אפשרות זו יכולה להיות בעיה אבטחתית ולכן ניתן להסתיר את הסיסמות באמצעות הפקודה:

```
Switch(config)#service password-encryption
```

הגדרת ממוקם VLAN למstag.

ממשקי המtag מוגדרים כברירת מחדל, אך אין צורך להגדיר אותם. מtag, בשונה מנתב, אינו צריך הגדרה של כתובת IP לממשקים שלו, משום שהממשקים שלו באוטה הרשת.

ניתן להתחבר למtag מרוחק (גם דרך האינטרנט) ע"מ לניהל אותו, לשם כך יש צורך להגדיר:

- כתובת IP למstag,
- subnet mask
- שער ברירת מחדל (במידה ורוצים לפנות למtag מרשת חיצונית)

כמו הגדרת כל מארח ברשת

מגדירים כתובת IP למtag ע"י ממוקם וירטואלי: **(VLAN)** Virtual LAN interface

בד"כ מגדירים לצורך זה את: **1 VLAN**

כמו ממוקם פיזי גם ממוקם וירטואלי זה צריך לאפשר.

```
Switch(config)#interface vlan 1
```

```
Switch(config-if)#ip address <192.168.1.2> <255.255.255.0>
```

```
Switch(config-if)#no shutdown
```

```
Switch(config-if)#exit
```

הגדרת שער ברירת מחדל – להתחברות מרשת חיצונית:

```
Switch(config-if)#ip default-gateway <192.168.1.1>
```

```
Switch(config-if)#exit
```

התחברות למtag מרוחק:

בכדי להכנס למtag דרך הרשת, לאחר שהוגדר VLAN

יש להכנס ל- Command Prompt

ולהקש: pc>**telnet <IP add >**

הערה: ניתן להכנס למtag בערוץ זה רק לאחר שהוגדרה סיסמת Enable

שימוש ב- בקר כדי למנוע גישה לציר רשות:

```
Switch(config)#banner motd @
```

!!! This is a secure system. Authorized Access ONLY !!!

```
@
```

```
!!! This is a secure system. Authorized Access ONLY !!!  
Switch>
```

אבטחת מושקים

```
Switch(config-if)#shutdown
```

- מושקים אשר אינם בשימוש – יש לכבות:

- אבטחת מושקים עפ"י כתובת MAC סטטית

```
Switch(config) #interface fastEthernet 0/ < מס' יציאה >
```

הגדרת מושק < מס' > בנתב

```
Switch(config-if)#switchport mode access
```

מתן גישה לפורט

```
Switch(config-if)#switchport port-security
```

הפעלת אבטחה

```
Switch(config-if)#switchport port-security mac-address < 00e0.a32e.2134 >
```

הגדרת הפורט לעובדה מול מחשב
מוסים בעל כתובת MAC מסוימת.

- אבטחת מושקים דינמית באמצעות שימוש "בדביך" - Sticky

שימוש בדביך (sticky) מאפשר "הדקמת כתובות MAC אשר מחוברות כרגע.

```
Switch(config) #interface fastEthernet 0/ < מס' יציאה >
```

הגדרת מושק < מס' >
בנתב

```
Switch(config-if)#switchport mode access
```

מתן גישה לפורט

```
Switch(config-if)#switchport port-security
```

הפעלת אבטחה

```
Switch(config-if)#switchport port-security maximum < 'on' >
```

קביעת מקסימום
מחברים לפורט

```
Switch(config-if)#switchport port-security mac-address sticky
```

"הדקמת" כתובות ה- MAC

