

תקשוב ג' פרק 1 – תקציר

הגדרות בסיסיות למתג

מעובד וערוך מתוך חומרי הלימוד של האקדמיה של סיקו.

תוכנת מערכת הפעלה Cisco IOS

מערכת הפעלה אשר מספקת פונקציונאליות, הרחבה ואבטחה למוצרי חברת סיקו. באמצעות ממשק פקודה CLI.

ישנם מספר דרכים כדי להתחבר לממשק הפקודה:

1. **קונסול** – מחשב בעל תוכנת טרמינל המחובר מיציאת RS-232 ע"י כבל מיוחד (כבל קונסול בד"כ בצבע תכלת).

להגדרה ראשונית של מתג/ראוטר חייבים להשתמש בכבל קונסול!

בהתחברות ע"י המחשב יש להגדיר פרמטרי התקשורת: 9600,8,n,1,n

2. חיבור מרחוק Telnet או SSH

חיבור Telnet מצריך רשת עובדת והגדרת ממשק אחד לפחות לעבוד כ- Telnet ומוגדרת לו כתובת IP לצורך התחברות ברשת.

התקשורת החיבור זה היא **גלויה** וניתן לנטר את המידע העובר בקלות יחסית.

מסיבות אבטחה, מערכת ההפעלה דורשת לפחות **סיסמת זיהוי** משתמש כאשר עובדים מרחוק.

חיבור SSH – Secure Shell

דומה לחיבור Telnet אך **מאובטח יותר באמצעות הצפנת המידע** העובר בין המתג/ראוטר למחשב.

עדיף להשתמש ב- SSH מאשר ב- Telnet.

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

3. AUX

חיבור דרך קווי טלפון באמצעות חייגן ומודם, אך ניתן לעבוד גם מקומי כאשר לא ניתן לעבוד באמצעות קונסול.

קבצי הגדרת תצורה - Configuration

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

running-config

כאשר אנו מבצעים שינויי תצורה, הם מבוצעים מיד, ב-RAM יש לבצע שמירה של שינויי התצורה ב- **startup-config** כדי שישמרו גם לאחר כיבוי הציוד.

הפקודה לשמירת ההגדרות היא:

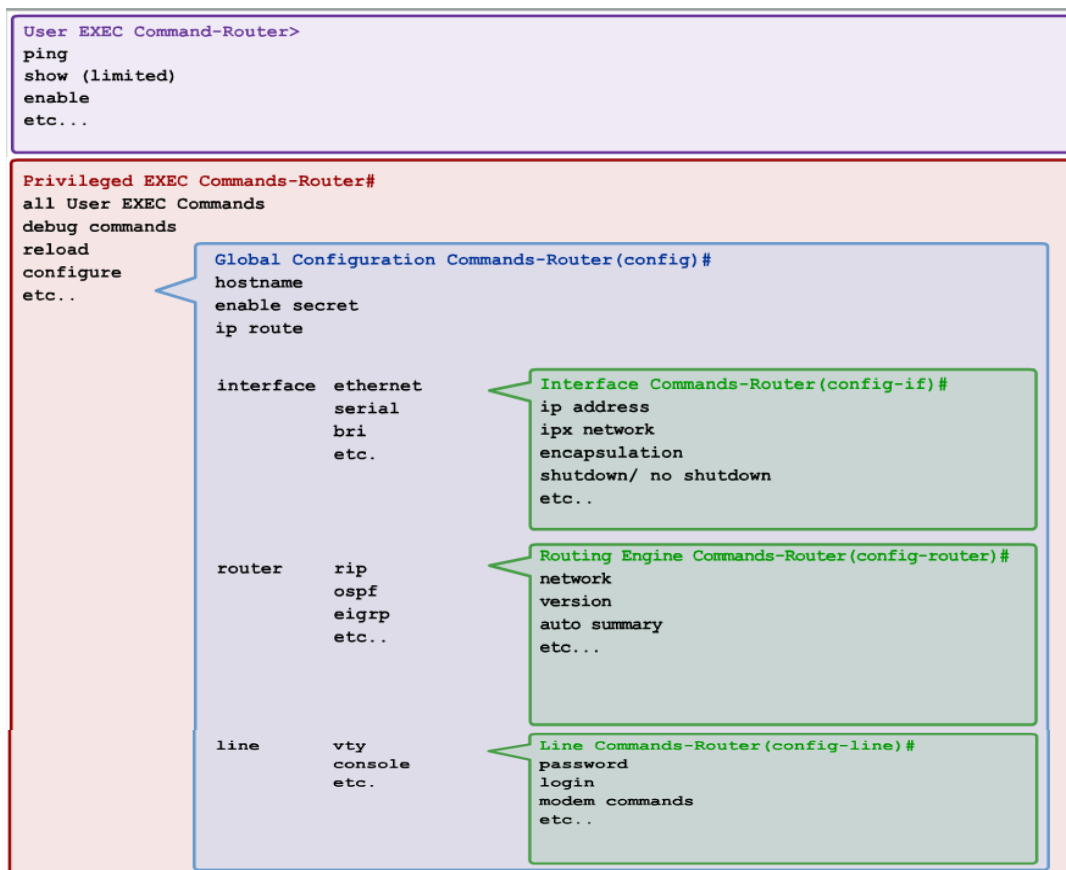
```
Switch#copy running-config startup-config
```

משיקולי אבטחה מערכת ההפעלה עובדת בשכבות.

השכבות מסודרות בצורה היררכית.

לכל שכבה אוסף פקודות משלה.

כל שורה מתחילה בשם ההתקן ולאחריו זיהוי השכבה.



שכבת משתמש (User)

- מאפשרת גישת משתמש למספר פקודות בסיסיות של ניטור (monitoring) להראות מצב.
- שכבה זו עולה עם הכניסה למתג או ע"י פקודת: **Switch> disable**
כדי לחזור משכבת Privilege
- סימון השכבה: > (Switch>)

שכבת זכויות (Privilege)

- מאפשרת גישה לכל הפקודות כגון קביעת תצורה וניהול.
- בתוכה תת-שכבות.
- שכבה זו ניתנת להגנה ע"י סיסמה.
- סימון השכבה: # (Switch#)
- כניסה לשכבה ע"י הפקודה: **Switch> enable**

תת-שכבה: תצורה כללית (Global configuration)

- מאפשרת גישה לפקודות כגון hostname, מאפשרת הגדרת ממשקים, הגדרת התחברות למתג ע"י קונסול או VTY וכו'
- סימון השכבה: # (config)#
Switch (config)#
- כניסה לשכבה ע"י הפקודה: **Switch#configure terminal**

עזרה

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

1. ? לאחר סימון השכבה תתן את כל רשימת הפקודות הקיימות לאותה 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 אות אחת או מס' אותיות תציג את הפקודות המתחילות באותיות אלו. למשל:

Switch>sh?

Show

3. ? לאחר רווח יתן את רשימת האפשרויות או נתונים שאפשר או שחייבים להכניס. 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 למתג

Switch(config)#**hostname <HILIK>**

ממצב זכויות:

HILIK (config) #

יצירת בנר

בנר משמש כהודעת פתיחה ברגע הכניסה למתג. ניתן לנצל את הבנר כדי: להעביר הודעות למפעיל, לשים הודעת אבטחה כגון "הכניסה למתג למורשים בלבד", לוגו של החברה וכו'

הבנר צריך להתחיל ולהסתיים ב**אותו התו (@ בדוגמה להלן)** אסור שתו זה יופיע בתוך הטקסט.

ממצב זכויות:

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

הגדרת ממשקים

שלבים להגדרת ממשק אתרנט.

1. כניסה למצב זכויות: Switch>**enable**
2. כניסה לתצורת קונפיגורציה: Switch#**configure terminal**
3. כניסה להגדרת ממשק או ממשקים. Switch(config)#**interface FastEthernet 0/0**
4. הפעלת הממשק: Switch(config-if)#**no shutdown**
5. כדי לכבות ממשק משתמשים בפקודה: Switch(config-if)#**shutdown**

הגדרת מספר ממשקים במקביל:

Switch#**configure terminal**

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

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

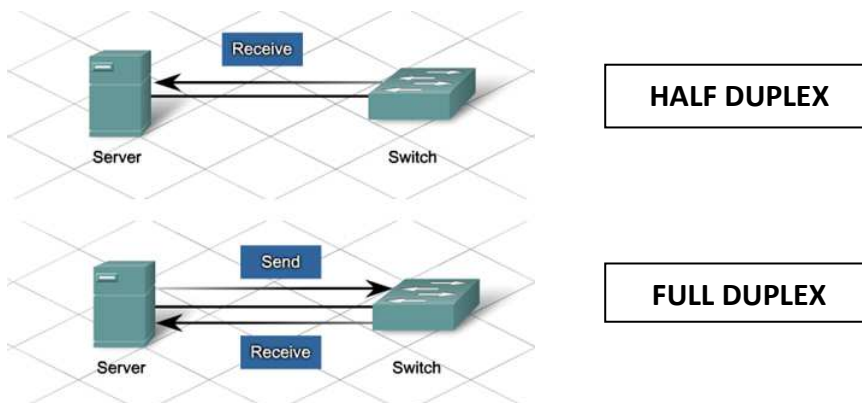
הגדרת מהירות וצורת תקשורת מול ממשק אחר

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

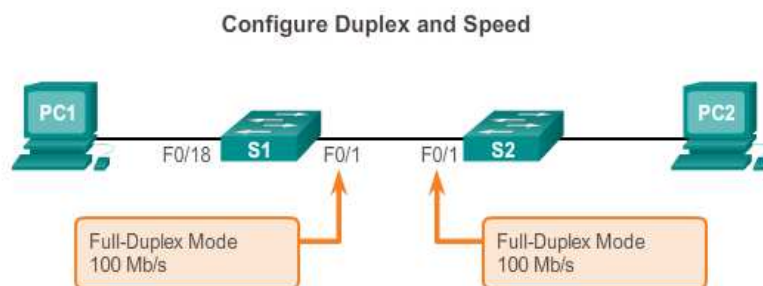
למהירות: 10/100 Mbps ידנית או להגדיר מצב אוטומטי (AUTO) שבו מהירות הממשק נקבעת ע"י דו-שיח בין שני הממשקים.

בנוסף ניתן להגדיר את צורת התקשורת בין שני הממשקים:

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



הגדרה ידנית משמשת כדי למנוע בעיות הגדרה בין יצרנים 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

בדיקת התצורה.

פקודת: Switch#**show running-config**

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

פקודת: Switch#**show startup-config**

תראה לנו את קובץ ההגדרות של המתג / נתב **השמורות בזיכרון** הלא מחיק NVRAM.

הגדרות שאנו מבצעים בנתב / מתג נשמרות בזיכרון RAM בקובץ: running-config אשר עלול להמחק בכיבוי המכשיר, לכן עלינו לשמור את ההגדרות בזיכרון **לא מחיק** (NVRAM) בקובץ: startup-config ונמנע את איבוד ההגדרות.

שמירת ההגדרות באמצעות הפקודה:

Switch#**copy running-config startup-config**

הפקודה הבאה אינה בתוכנית הלימודים: Switch# **Write Memory**

אבטחת המתג / נתב

סיסמאות הן ההגנה הראשונה להתחברות לא מורשית לאביזרי הרשת.

- סיסמת קונסול – מגבילה את הגישה דרך חיבור הקונסול.
- סיסמת Enable – מגבילה את הגישה למצב "זכויות" (Privileged Exec)
- סיסמת Enable מוצפנת – סיסמה כנ"ל רק מוצפנת.
- סיסמת VTY – מגבילה את הגישה באמצעות חיבור מרחוק (Telnet)

מומלץ להשתמש בסיסמאות שונות לכל רמת גישה.

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

למשל:

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

סיסמת קונסול.

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

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

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

סיסמת Enable ומוצפנת.

כדאי להשתמש בסיסמת Enable מוצפנת ולא בסיסמת Enable הרגילה, כשאפשר, משום שההצפנה מספקת אבטחה טובה יותר.

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

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

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

סימט VTY.

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

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

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

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

הסתרת הסימטאות המוצגות.

את הסימטאות ניתן לראות בקבצי הקונפיגורציה ע"י הפקודות:

show startup-config או **show running-config**

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

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

הגדרת ממשק VLAN למתג.

ממשקי המתג מוגדרים כברירת מחדל, לכן אין צורך להגדיר אותם.

מתג, בשונה מנתב, אינו צריך הגדרה של כתובת IP לממשקים שלו, משום שהממשקים שלו באותה הרשת.

ניתן להתחבר למתג מרחוק (גם דרך האינטרנט) ע"מ לנהל אותו, לשם כך יש צורך להגדיר:

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

כמו הגדרת כל מארח ברשת

מגדירים כתובת IP למתג ע"י ממשק וירטואלי: (VLAN) Virtual LAN interface

בד"כ מגדירים לצורך זה את: **VLAN 1**

כמו ממשק פיזי גם ממשק 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 למתג מרחוק:

בכדי להכנס למתג דרך הרשת, לאחר שהוגדר VLAN

יש להכנס ל- Command Prompt

ולהקיש: **pc>telnet < IP add >**

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

שימוש ב- בנר כדי למנוע גישה לציוד רשת:

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

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

@

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

```
Switch>
```

אבטחת ממשקים

• **ממשקים אשר אינם בשימוש – יש לכבות:** Switch(config-if)#**shutdown**

• **אבטחת ממשקים עפ"י כתובת MAC סטטית**

Switch(config) # interface fastEthernet 0/ <מס' יציאה>	הגדרת ממשק <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 לעבודה מול מחשב מסויים בעל כתובת MAC מסויימת.
---	---

• **אבטחת ממשקים דינאמית באמצעות שימוש "בדביק" - Sticky**

שימוש בדביק " (sticky) מאפשר "הדבקת כתובות MAC אשר מחוברות כרגע.

Switch(config) # interface fastEthernet 0/ <מס' יציאה>	הגדרת ממשק <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 < מס' >	קביעת מקסימום מתחברים לפורט

Switch(config-if)# switchport port-security mac-address sticky	"הדבקת" כתובות ה- MAC
---	-----------------------

