המדריך לאיפוס סיסמה בנתב Cisco.

מטרת המסמך:
מסמך זה בא לפרט את התהליך אותו יש לבצע על מנת לאפס סיסמה אבודה בנתב.

כללי:
תחילה יש להבהיר כי לא מדובר בשחזור הסיסמה, אלא בשינוייה, מכיוון שסיסמאות מוצפנות לא ניתן לשחזר. התהליך מצריך התחברות מקומית לנתב לצורך ביצוע אתחול ואילוצו להיכנס למצב עבודה ROMMON.

מתי נבצע תהליך זה:
באם שכחנו את אחת מסיסמאות הנתב, קרי סיסמה למצב Privileged, סיסמה לכניסה לנתב מ-Console.

השלבים בתהליך:

שלב א'
תחילה יש לאתחל את הנתב ולאלצו להיכנס למצב עבודה ROMMON, על ידי לחיצה על ה- Brake sequence בתוכנת האמולציה אותה אנו מריצים. במרבית התוכנות ה- Brake sequence הנו צרוף המקשים: Ctrl+Brake או Ctrl+C.

טיפ – במידה ואינך יודע מהו ה- Brake sequence בתוכנת האמולציה בה הנך משתמש, ניתן להתחבר לנתב בקצב 1200bps, ובעת האתחול שלו להקיש כ- 10 שניות על מקש הרווח. לאחר מכן בעת ביצוע כניסה בקצב 9600bps הנתב יהיה במצב Rommon.
שווה להוסיף את הטיפ אם לא יודעים את הקצב של הממשק

```
System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)
Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.

Self decompressing the image :
##########
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

כאן הקשתי Ctrl Brake

שלב ב'
כעת עלינו לאלץ את הנתב לבצע טעינה מלאה, איך להתעלם מקובץ הקונפיגורציה השמור ב-NVRAM (שם מוגדרת הסיסמה שאיננו זוכרים).
נבצע זאת על-ידי שינוי ערך ה- Configuration-Register, על מנת להודיע לתוכנת ה- Bootstrap להתעלם מה- NVRAM בתהליך הטעינה. הערך אותו נזין יהיה 0x2142. והפקודה בה נשתמש במצב ROMMON תהיה – *confreg 0x2142*
לאחר שינוי ערך ה- Configuration-register נבצע אתחול לנתב.

```
Self decompressing the image :
##########
monitor: command "boot" aborted due to user interrupt
rommon 1 >
rommon 1 >
rommon 1 > confreg 0x2142
rommon 2 > reset
```

שינוי ערך ה- register

אתחול הנתב

הנתב יעלה כרגיל, אך בשלב חיפוש קובץ הקונפיגורציה הוא יתעלם מה- NVRAM ויעלה קובץ הגדרות בסיסי. הנתב יאפשר לנו להיכנס למצב Setup. אנו נדלג על מצב Setup ונעבוד ב- CLI כרגיל.

```
31360K bytes of ATA CompactFlash (Read/Write)
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M)
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: n

Press RETURN to get started!


Router>
```

הנתב יאפשר כניסה למצב Setup

<u>שלב ג:</u> כעת עלינו לשחזר את הגדרות הנתב (אילו שנשמרו לפני שביצענו איפוס לנתב). אמנם התעלמנו מקובץ ה- Start-up Config, אך הוא עדיין קיים ולא מחקנו אותו, תארו לכם נתב שיושב בחברת ISP שאתם צריכים לאפס לו סיסמא, ה- Down Time שלו צריך להיות מינימאלי ולכן מה שנעשה הוא שנעתיק את ה-Start-up Config . ל-- Running-config שמכיל עכשיו את ההגדרות הבסיסיות בשל השינוי שביצעו ל- Configuration register.
פעולת ההעתקה מתבצעת במצב Privileged, ומרגע שנכנס אליו, נוכל לבצע את כל ההגדרות שנרצה (כולל שינוי הסיסמאות). את ההעתקה נבצע באמצעות הפקודה – *copy startup-config running-config*

תחילה נציג את ההגדרות עמם הנתב עלה:

```
Router>ena
Router#sh run
Building configuration...

Current configuration : 357 bytes
!
version 12.4
no service password-encryption
!
hostname Router
!
!
```

```
!
!
!
ip ssh version 1
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
!
!
!
!
!
line con 0
line vty 0 4
 login
!
!
End
```

אנו רואים שאלו ההגדרות הבסיסיות, כפי שנקבע על ידי מערכת ההפעלה.
כעת נבצע העתקה של ההגדרות שנשמרו ב- NVRAM אל ה- RAM:

```
Router#copy startup-config running-config
Destination filename [running-config]?

405 bytes copied in 0.416 secs (973 bytes/sec)
jamus#
```

אנו רואים שה- Hostname של הנתב השתנה, מכאן ניתן להבין כי אכן היו הגדרות ב- NVRAM.
נציג את ההגדרות כעת

```
jamus#sh running-config
Building configuration...
```

```
Current configuration : 405 bytes
!
version 12.4
no service password-encryption
!
hostname jamus
!
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
!—output omitted—
```

מהשורה המודגשת ניתן לראות כי ישנה סיסמה בנתב. הסיסמה מוצפנת אך מכיוון שביצענו כניסה למצב Privileged טרם העתקת הקונפיגורציות יש לנו את כל ההרשאות הדרושות לשינויי קונפיגורציה ולכן נוכל להחליף את הסיסמה וכך לקבל גישה להגדרות הנתב.

שלב ד': כעת עלינו להחליף את הסיסמה. על ידי הפקודה *enable secret [new password]*

```
jamus#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
jamus(config)#en
jamus(config)#ena
jamus(config)#enable se
jamus(config)#enable secret cisco
```

שלב ה': שמירת הגדרות ושינוי ערך ה- Configuration register לערך ברירת המחדל:
את ערכו של ה- Configuration register נשנה באמצעות הפקודה *configuration-register 0x2102*
מתוך Global Configuration Mode

```
jamus(config)#config-register 0x2102
jamus(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
jamus#cop
jamus#copy run
jamus#copy running-config star
jamus#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
jamus#
```

הערך החדש ייכנס לתוקף בעת האתחול הבא. את ערכו של ה- Configuration register ניתן להציג באמצעות הפקודה *show version*

```
jamus#show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
```

Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"

-- *Output omitted* --

Cisco 1841 (revision 5.0) with 114688K/16384K bytes of memory.
Processor board ID FTX0947Z18E
M860 processor: part number 0, mask 49
2 FastEthernet/IEEE 802.3 interface(s)
191K bytes of NVRAM.
31360K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2142 (will be 0x2102 at next reload)