1 פרק

רקע

שימוש בנתב שמקבלים בחכירה מספק האינטרנט הוא פתרון נפוץ וקל. מכיוון שאני מעוניין להוציא מהרשת שלי יותר, ומכיוון שאני מכיר את הטכנולוגיה, החלטתי לקנות את הנתב בעצמי. שתי בעיות מרכזיות שעמדו בפני היו אלה:

- איזה מוצר תומך בטכנולוגיה בארץ.
- איזה הגדרות צריך בשביל שהמוצר יתחבר עם השירות הניתן באץ.

אחרי שחקרתי ולמדתי את הנושא, אני שמח להעלות כאן את מה שמצאתי ולשתף בידע שצברתי במהלך הדרך. קניתי נתב Cisco מדגם ISR 897VA שמשרת אותי כנתב מודם גישה למרשתת. הנתב מחליף את הנתבים שמקבלים בחכירה מבזק ובזק בינ"ל. בחרתי באפשרות הזו מכיוון שהיא מאפשרת הרבה יותר דברים מתקדמים על הנתב, ונותנת המון מידע של שליטה ובקרה על המכשיר והרשת. אפשר למצוא אותו במחירים של 700-1500₪ (דצמבר 2019) באתרים המוכרים ציוד יד שניה באינטרנט. אפשר גם לקנות את הדגם 887VA שהוא ישן יותר ולא כולל חיבורים של Gigabyte Ethernet אלא רק חיבורים של Fast Ethernet, וגם לא כולל ממשק SFP המאפשר שידרוג לסיב אופטי במידה והתשתיות בארץ יאפשרו FTTH (Fibers to the homes). הנתב המתקדם יותר הוא מסדרה של Cisco 1100, אך מכיוון שהוא דגם שעדיין משווק ע"י החברה המחיר שלו גבוה הרבה יותר ומתקרב לאזור של ה-4000₪. בנוסף לכל המכשירים בסדרות האלא קיימים דגמים שתומכים בתקשורת דור 4 סלולריות. אין לא דגם תומך ולכן איני יודע איך להגדיר את האפשרות הזו.

אתחיל בדבר שהכי הטריד אותי, מהי הטכנולוגיה שנתמכת בארץ. בגדול, שפונים לבזק ושואלים מקבלים תשובה שהטכנולוגיה היא VDSL, שבעיקרון זה נכון, אך לא מספק. צריך לדעת בדיוק באיזה טכנולוגיה להשתמש ע"מ שלא לטעות ולקנות נתב שאומנם תומך ב-VDSL אך אינו תומך בטכנולוגיה שקיימת בארץ.

לפי מה שה-Controller VDSL זיהה מדובר ב-G.993.2 (VDSL2) Profile 17a פרטים על הטכנולוגיה ניתן למצוא בקישור הזה. אם רוצים לקנות כל נתב מקצועי אפשר לראות במפרט שלו האם הוא תומך כמו שאפשר לראות בדוגמה שלי.

Standard	Feature Name	Broadcom		ST Micro
		6368	63268	20190P
G.993.1	VDSL	Every FW	Every FW	N
G.993.1	VDSL - Bit swapping	Every FW	Every FW	N
G.993.1	VDSL - Upstream Power Back Off (UPBO) (Reference PSD UPBO)	Every FW	Every FW	N
G.993.2	VDSL2	Every FW	Every FW	N
G.993.2	VDSL2 - Profile 8a/b/c/d, 12a/b, and 17a	Every FW	Every FW	N

ISR Model Part Number	Chipset Vendor	Chipset	V/A DSL Annex Support				Layer 2 Frame Mode	
			A	B	M	J	PTM	ATM
CISCO867	ST Micro	20190P	A					X
CISCO867VAE	Broadcom	6368	V/A				X	X
C867VAE-W	Broadcom	63268	V/A				X	X
CISCO887	ST Micro	20190P	A					X
CISCO887V	Broadcom	6368	V				X	X
CISCO887VA C887VA	Broadcom	6368	V/A				X	X
C897VA	Broadcom	6368	V/A				X	X

על מנת להגדיר נתב של Cisco צריך קודם להגדיר את ממשק הניהול דרך החיבור ה-Serial של הנתב. צריך למצוא מחשב שכולל את החיבור הזה, ויש פחות ופחות מחשבים שתומכים בחיבור הזה כיום, אפשר כמובן למצוא עדיין מתאמים שמתחברים ל-USB ומאפשרים להתחבר דרך החיבור ה-Serial של הנתב. ברוב המחשבים היום כבר לא קיימת תוכנה המאפשרת חיבור דרך הממשק serial ולכן צריך תוכנה שתעשה לנו את זה. אפשר להשתמש ב-SecureCRT המצויינת אך היקרה. פתרון חינמי אחר הוא Putty

שמאפשר לנו גם להתחבר לממשק ה-Serial. אחרי שמתחברים לנתב דרך החיבור ה-Serial אפשר להגדיר כתובת IP לשליטה הרבה יותר נוחה ופשוטה.

עם החיבור ה-Serial אנחנו נגדיר ראשית את ממשק הרשת הביתית.

```
Router#configure terminal <cr>

Router(config)#interface vlan <vlan-number> <cr>

Router(config-if)#ip address  <ip-address> <subnet-mask>

Router(config-if)#description ”<description>“

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

פקודה לכניסה למצב הגדרת תצורה	Router#configure terminal <cr>
הגדרת ממשק רשת וירטואלי דוגמה: Router(config)#interface vlan 1 <cr>	Router(config)#interface vlan <vlan-number> <cr>
הגדרת כתובת לממשק דוגמה: Router(config-if)#ip address 192.168.1.254 255.255.255.0	Router(config-if)#ip address <ip-address> <subnet-mask>
[אפשרי] נתינת תיאור לממשק דוגמה: Router(config-if)#description ”Home network“	[Optional] Router(config-if)#description ”<description>“
הפעלת הממשק	Router(config-if)#no shutdown

```
interface Vlan1

 description ”Home network“

 ip address  192.168.1.254 255.255.255.0
```

אחרי שהגדרנו את ממשק ה-IP אפשר להתחיל להגדיר את המשתמש שיגדיר את הנתב.

```
Router#configure terminal <cr>

Router(config)#username <username> secret <password>

Router(config)#enable secret <password>

Router(config)#service password-encryption

Router(config)#aaa new-model
```

פקודה לכניסה למצב הגדרת תצורה	Router#configure terminal <cr>

הגדרת שם משתמש וסיסמה חדשים דוגמה: `Router(config)#username admin secret P@ssword`	`Router(config)#username <username> secret <password>`
]אפשרי[הגדרת סיסמת enable לאבטחה של פעולות הדורשות הרשאות גבוהות יותר. `Router(config)#enable secret S3cret`	[Optional] `Router(config)#enable secret <password>`
[אפשרי] הגדרה של ערבול סיסמאות על מנת שלא יהיו גלויות בהצגת התצורה	[Optional] `Router(config)#service password-encryption`
הגדרה שבהעדר מצב שבו יש לנו מערכת לניהול משתמשים, המשתמשים יהיו אלה המוגדרים מקומית על הנתב	`Router(config)#aaa new-model`

```
service password-encryption

aaa new-model

username admin secret $1tOjWE$tvr08sTx1U3RTHRfWnp0n.

enable secret $1tOjWE$tvr08sTx1U3RTHRfWnp0n.
```

ולבסוף נגדיר צורת התחברות מאובטחת לנתב עצמו באמצעות פרוטוקול SSH.

```
Router#configure terminal <cr>

Router(config)#crypto key generate rsa

Router(config)#line vty <start line number> <end line number>

Router(config-line)#transport input telnet ssh

Router(config-line)#login authentication local_access

Router(config-line)#logging synchronous
```

פקודה לכניסה למצב הגדרת תצורה	`Router#configure terminal <cr>`
יצירת מפתח לשימוש הפרוטוקול	`Router(config)#crypto key generate rsa`
הגדרת line לגישה למכשיר, יש מספר התחלה ומספר סיום שאומרים כמה קוים יכולים להיות מחוברים בו-זמנית דוגמה: `Router(config)#line vty 0 4`	`Router(config)#line vty <start line number> <end line number>`
אישור גישה לקו באמצעות הפרוטוקולים SSH (מוצפן ומאובטח, ממולץ) ו-Telnet (לא מוצפן ולא מאובטח)	`Router(config-line)#transport input telnet ssh`

הגדרת ההזדהות לפי המשתמשים שמוגדרים מקומית	Router(config-line)#login authentication local_access
[אפשרי] הגדרת הודעות מתואמות עם הקו, כלומר פקודות חדשות לא יחתכו ע"י הודעות log	[Optional] Router(config-line)#logging synchronous

```
947054257-signed-self-crypto pki certificate chain TP

 signed 01-certificate self

  A0030201 91625C88 E092A3F5

…

  25DFF36C 7B6BE772 33C81721 24

      quit

line vty 0 4

 logging synchronous

 login authentication local_access

 transport input telnet ssh
```

לבסוף אחרי שסיימנו את כל ההגדרות ואנחנו מעוניינים לשמור אותם על הנתב שלא יעלמו לאחר הפעלה מחדש יש להקיש Ctrl-z על מנת לצאת ממצב הגדרות התצורה ולשמור את התצורה החדשה

```
Router(config)#<Ctrl-z>

Router
```

בשלב זה ניתן להתחבר כבר ישירות למכשיר על ידי הפרוטוקול SSH ואין כבר צורך בחיבור Serial. על מנת להתחבר למכשיר דרך SSH אפשר להשתמש בפקודה ssh <usarname>@<device ip>. דוגמה: ssh admin@192.168.1.254, לפי הדוגמאות שהגדרנו קודם, על מנת שנוכל להתחבר למכשיר ב-SSH אנחנו צריכים להיות איתו על אותה הרשת ולכן יש לחבר כבל Ethernet מכל ממשק פנוי מחיבורי ה-LANs הפנויים, ולהגדיר את ממשק המחשב להיות באותה רשת כמו המכשיר שלנו, לדוגמה 192.168.1.1/24.

אחרי שהגדרנו את הנתב בצורה שמאפשרת לנו להגדיר אותו בצורה פשוטה ונוחה, נעבור להגדרות של ממשק ה-VDSL מול בזק.

נגדיר את ממשק ה-Dialer.

```
Router#configure terminal <cr>

Router(config)#interface dialer <dialer-number> <cr>

Router(config-if)#mtu <max size> <cr>

Router(config-if)#ip address negotiated <cr>

Router(config-if)#ip virtual-reassembly in <cr>

Router(config-if)#encapsulation ppp <cr>
```

```
Router(config-if)#dialer pool <pool number> <cr>

Router(config-if)#dialer-group <group number>  <cr>

Router(config-if)#no cdp enable <cr>

Router(config-if)#ppp authentication chap pap callin <cr>

Router(config-if)#ppp chap hostname <username>@<service provider domain>
<cr>

Router(config-if)#ppp chap password <password> <cr>

Router(config-if)#ppp pap sent-username <username>@<service provider
domain> password <password> <cr>
```

פקודה לכניסה למצב הגדרת תצורה	`Router#configure terminal <cr>`
הגדרה של ממשק חייגן חדש דוגמה: `Router(config)#interface dialer1`	`Router(config)#interface dialer <dialer-number> <cr>`
הגדרת mtu, הגודל המירבי אותו ניתן להעביר אל הממשק, במידה ועובדים מול בזק מדובר על 1492 דוגמה: `Router(config-if)#mtu 1492`	`Router(config-if)#mtu <max size> <cr>`
ציון שהכתובת ה-IP של הממשק תתקבל על ידי משא ומתן באמצעות PPP/IPCP	`Router(config-if)#ip address negotiated`
מחבר מחדש חבילות שמגיעות לנתב	`Router(config-if)#ip virtual-reassembly in <cr>`
אפשור אריזה בתצורה של PPP	`Router(config-if)#encapsulation ppp <cr>`
פירוט מספר מאגר החייגן דוגמה: `Router(config-if)#dialer pool 1`	`Router(config-if)#dialer pool <pool number> <cr>`
שיוך הממשק לקבוצת חייגן דוגמה: `Router(config-if)#dialer-group 1`	`Router(config-if)#dialer-group <group number>  <cr>`
[אפשרי] הפסקת שליחת הודעות CDP (Cisco Discovery Protocol)	[Optional] `Router(config-if)#no cdp enable <cr>`
מאפשר את האימות עם הפרטים שמוגדרים מקומית ל-PPP המרוחק לפי הפרוטוקולים המפורטים	`Router(config-if)#ppp authentication chap pap callin <cr>`
הגדרת שם משתמש של פרטוקול CHAP. דוגמה לשם משתמש בבזק (014): `Router(config-if)#ppp chap hostname 123456788@014`	`Router(config-if)#ppp chap hostname <username>@<service provider domain> <cr>`
הגדרת סיסמה לפרוטקול CHAP. דוגמה: `Router(config-if)#ppp chap password 123456`	`Router(config-if)#ppp chap password <password> <cr>`

הגדרת שם משתמש וסיסמה לפרוטוקול PAP. דוגמה לשם משתמש בבזק (014): `Router(config-if)#ppp pap sent-username 123456788@014password 123456`	`Router(config-if)#ppp pap sent-username <username>@<service provider domain> password <password> <cr>`

אחרי שהגדרנו את ממשק החייגן יש להגדיר את ממשק ה-Ethernet שמחובר לחייגן

```
Router#configure terminal <cr>

Router(config)#interface dialer <dialer-number> <cr>
```

```
Router#configure terminal <cr>

Router(config)#interface eth0 <cr>

Router(config-if)#description <description> <cr>

Router(config-if)#pppoe enable group global <cr>

Router(config-if)#pppoe-client dial-pool-number <pool number> <cr>
```

פקודה לכניסה למצב הגדרת תצורה	`Router#configure terminal <cr>`
כניסה להגדרת ממשק הנתב שכבר קיים	`<Router(config)#interface eth0 <cr`
[אפשרי] נתינת תיאור לממשק דוגמה: `Router(config-if)#description "WAN interface"`	[Optional] `Router(config-if)#description <description> <cr>`
מקשר לפרופיל ה-PPPoE הגלובלי	`Router(config-if)#pppoe enable group global <cr>`
מקשר את המשתמש לממשק ה-Dialer דוגמה: `Router(config-if)#pppoe-client dial-pool-number 1`	`Router(config-if)#pppoe-client dial-pool-number <pool number> <cr>`

בשלב הזה כבר כמעט שסיימנו את הגדרת החיבור לאינטרנט. יש חיבור לאניטרנט אך כדי שתהיה גישה צריך להגדיר עוד כמה דברים מאוד פשוטים שקיים עליהם מידע רב באינטרנט.

ע"מ שהנתב ידע לגשת לאינטרנט דרך ממשק החייגן יש להגדיר את הניתוב ברירת המחדל החוצה

```
Router#configure terminal <cr>

Router(config)#ip route 0.0.0.0 0.0.0.0 Dialer1<cr>
```

פקודה לכניסה למצב הגדרת תצורה	`Router#configure terminal <cr>`
הגדרת ניתוב ברירת המחדל דרך ממשק Dialer1.	`Router(config)#ip route 0.0.0.0 0.0.0.0 Dialer1<cr>`

עכשיו כבר ניתן לבדוק בקלות שיש חיבור לאינטרנט, יש לבצע בדיקת Ping לכתובת ברשת

```
Router#ping 8.8.8.8 <cr>

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:

!!!!!
```

אם מעוניינים להשתמש בשמות מתחם ולא בכתובות IPv4 ניתן לעשות זאת אך נדרש קודם להגדיר DNS.

```
Router#configure terminal <cr>

Router(config)#ip name-server <DNS-IP> <cr>
```

Router#configure terminal <cr>	פקודה לכניסה למצב הגדרת תצורה
Router(config)#ip name-server <DNS-<IP> <cr	הגדרת כתובת DNS חדשה דוגמה: Router(config)#ip name-server 8.8.8.8

ואחרי שעשינו את זה ניתן לבדוק את הרשת אם שמות המתחם:

```
Router#ping ip google.com

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.217.18.46, timeout is 2 seconds:

!!!!!
```

רגע, האם זה אומר שהמחשבים שלנו יכולים לגשת עכשיו חופשי לרשת? עדיין לא, כעת יש לנו מכשיר אחד שקיבל את כתובת ה-IPv4 שהקצה לנו הספק. זה כמובן לא מספיק אם אנו מעוניינים לחבר יותר ממכשיר אחד. המכשיר שמחובר כעת הוא הנתב, הוא ישמש אותנו לגשת לרשת. כיצד אנו יכולים לקחת את הכתובת האחת שקיבלנו מהספק שלנו ולתת אותה לכל המכשירים בבית שצריכים גישה לרשת? בשביל זה אנחנו נשתמש בפרוטוקול חביב שנקרא NAT. מה שהפרוטוקול הזה עושה הוא למעשה לתרגם כתובות פנימיות שלנו בבית החוצה עם אותה כתובת אחת שקיבלנו מהספק. זו לא טכנולוגיה כל-כך נדירה, למעשה כל הנתבים שמקבלים מהספק משתמשים בה, אך שם לא נדרשת הגדרה מיוחד לכך, זה מגיע בתור ברירת המחדל.

לעניינו, כיצד נגדיר NAT? למעשה זה פשוט מאוד.

ראשית נגדיר את הכתובות הפנימיות, לכתובת הפנימית נשתמש ב-Interface Vlan 1 אותו הגדרנו מקודם עם הכתובת 192.168.1.254 חשוב מאוד לבחור בתחום של 192.168.x.x או בתחום 10.x.x.x משום שאלו כתובת לא מנותבות ברשת ה-Internet, והם לא יתנגשו אם כתובות של אתרים אחרים (דבר שימנע מכם לגשת לאתרים שמחזיקים באותה כותבת).

```
Router#configure terminal <cr>

Router(config)#access-list <rule-number> permit <subnet-address>
<<wildcard-mask> <cr

Router(config)#access-list <rule-number> remark <rule-description> <cr>
```

Router#configure terminal <cr>	פקודה לכניסה למצב הגדרת תצורה

הגדרת Access-List חדש (העדיפות היא בסדר עולה לפי המספר) עם כתובת IP ו-Mask שלה שהוא הפוך מ-Subnet-Mask רגיל ולפעמים נקרא Wildcard-Mask. דוגמה: `Router(config)#access-list 192 permit 192.168.1.0 0.0.0.255`	`Router(config)#access-list <rule-number> permit <subnet-address> <wildcard-mask> <cr>`
[אפשרי] נתינת תיאור ל-Access-List שיצרנו בעל אותו מספר כמו שהגדרנו מקודם. דוגמה: `Router(config)#access-list 192 remark NAT`	[Optional] `Router(config)#access-list <rule-number> remark <rule-description> <cr>`

בשלב הבא נגדיר את ה-NAT עצמו ונשייך אותו לממשקים

```
Router(config)#ip nat inside source list <access-list number> interface
<outside interface> overload <cr>

Router(config)#interface Dialer1 <cr>

Router(config-if)#ip nat outside <cr>

Router(config-if)#interface <inside interface>

Router(config-if)#ip nat inside
```

הגדרת פעולת ה-NAT וקישור בין הממשק החיצוני ל-Access List והכיוון (לרשת שב"עולם") שהגדרנו. דוגמה: `Router(config)#ip nat inside source list 192 interface Dialer1 overload`	`Router(config)#ip nat inside source list <access-list number> interface <outside interface> overload <cr>`
בחירת ממשק החייגן שקיבל את הכתובת שלנו מהספק	`Router(config)#interface Dialer1 <cr>`
סימון הממשק הזה כמשק שמתרגם את הכתובות כלפי חוץ	`Router(config-if)#ip nat outside <cr>`
בחירת הממשק הפנימי שלנו שמחובר לרשת בבית דוגמה: `Router(config-if)#interface Vlan1`	`Router(config-if)#interface <inside interface>`
סימון הממשק הזה כמשק שמתרגם את הכתובות כלפי פנים	`Router(config-if)#ip nat inside`

זהו יש לנו רשת מתפקדת, אפשר לחבר מכשירים לנתב ולגלוש באמצעותם ברשת, בהמשך אראה כיצד ניתן להגדיר שרת DHCP שיחלק כתובות בצורה אוטומטית. להגדיר חסימת Domains באמצעות ניתוב מחדש של DNS, הגדרת Firewall, הגדרת VPN, הגדרת NetFlow ועוד הרבה אפשרויות חביבות ביותר.