Broadband Access Division

נתב
B-FOCuS Wireless 352+
B-FOCuS MultiPort 342+

מדריך מורחב
למנהלי רשת

כל הזכויות שמורות לאי.סי.איי טלקום בע"מ, 2005.©
כל הזכויות במידע המופיע בעלון זה שמורות וכפופות לדיני הגנת זכויות הקניין הרוחני המתאימים לרבות מכוח דיני זכויות יוצרים, פטנטים והסכמים פרטניים. אין להעתיק, לצלם, להפיץ או לשכתב עלון זה או את המידע המופיע בו בכל צורה ודרך ללא קבלת רשות אי.סי.איי מראש ובכתב. כמו כן אין לעשות שימוש בעלון זה או במידע המופיע בו שלא למטרה לשמה הוא סופק.
העיצוב והמפרטים הטכניים הינם נתוני היצרן, אי.סי.איי שומרת לעצמה את הזכות לשנותם ללא הודעה מוקדמת ומבלי שתחול עליה חבות כלשהי עקב כך.
מצגים בעלון זה הנוגעים לביצועי המוצר הינם למטרות אינפורמטיביות בלבד ולא ייחשבו, במפורש או במשתמע, כהתחייבות או אחריות היצרן. אחריות היצרן מוגבלת לאחריות המופיעה בהסכם המכירה הפרטני. מסמך זה עשוי להכיל טעיות ו/או השמטות; אי.סי.איי מסירה מעצמה כל אחריות עד לרמה המותרת בחוק או בהתאם להסכם המכר, לכל נזק או אובדן שייגרמו לאדם מחוסר מידע עדכני או אי דיוקים בהוראות ההפעלה שבעלון זה, כמו גם מהתקנה פגומה של הציוד. אי.סי.איי מעדכנת מעת לעת את המידע המופיע בעלון זה, לפיכך אם נתקלת בטעות אנא הודיע על כך לאי.סי.איי.
הערה: יש להתייחס לכל האמור בחוברת זו כבלשון זכר ונקבה כאחד.

תוכן העניינים

1 תצורת תוכנה מתקדמת 1
2 קביעת תצורה ל- LAN 2
2.1.1 חיבורים חדשים 2
2.1.2 שינויים בחיבורים קיימים (PPP Connection) 2
3 חלוקת כתובות IP אוטומטית (DHCP) 4
4 כתובת IP של הנתב 5
5 שירותי Firewall/NAT 6
6 תצורת ה- Modem 7
7 תצורה אלחוטית מתקדמת 8
8 אופציות מתקדמות 10
9 בטחון אלחוטי - Wireless Security 11
10 הכנס והפעל אוניברסלי - UPnP 15
11 SNMP 16
12 הפניית פורטים - Port Forwarding 17
13 תצורת DMZ 18
14 קביעת מסנני Access Control IP 19
15 לקוחות LAN - LAN Clients 20
16 סינון גשרים - Bridge Filters 21
17 ניתוב סטטי - Static Routing 22
18 ניתוב דינמי - Dynamic Routing 23
19 פקודות מערכת 24
19.1 רישום מרחוק 26

20 ניהול משתמשים 28
21 עדכון תוכנה 29
22 בדיקת Ping 30
23 בדיקת הנתב 31
24 סטטוס 32
25 איתור תקלות 33
25.1 הנתב אינו פועל 33
25.2 נורית ה- DSL Sync מהבהבת אך אינה דולקת קבוע ... 34
25.3 נורית ה- DSL Sync תמיד כבויה 34

1 תצורת תוכנה מתקדמת

לנתב שלך תכונות מתקדמות רבות. הנתב מסופק בתצורה האופטימלית לעבודה ברשת ביתית; במידה והנתב מותקן בבית ומיועד לגלישת אינטרנט על ידי מספר מחשבים ביתיים אין כל צורך בשינויי תצורה.

מדריך זה מיועד לאנשי רשת מקצועיים בלבד וכולל הסברים לגבי קביעת תצורות מורכבות כאשר קיים צורך בכך.

לאחר כל שינוי תצורה בנתב, יש לבצע פעולת שמירה (Save) כדלהלן:

➢ **לשמירת שינויים בתצורה:**

1. ממסך הבית, לחץ על **Tools** ובחר ב- **System Commands**.
2. לחץ על **Save All**.
3. כדי שהשינוי שבוצע יופעל, מומלץ לאתחל את הנתב על ידי לחיצה על **Tools / System Commands / Restart**.

2 קביעת תצורה ל- LAN

2.1.1 חיבורים חדשים

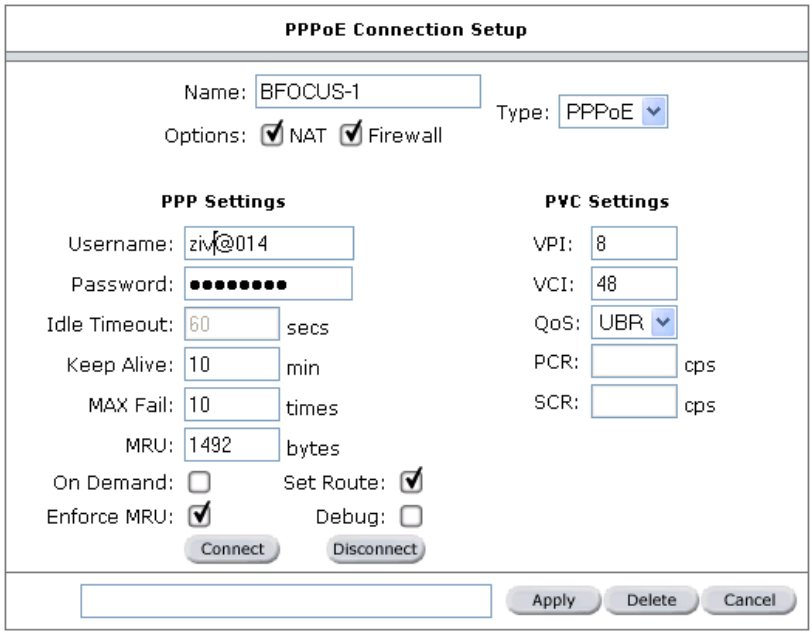
הנתב שלך יכול לתמוך בשמונה חיבורים וירטואליים, וזאת במידה וספק השרות שלך תומך בכך. החיבורים מופיעים כ- **Connection 1** עד **Connection 8**.

2.1.2 שינויים בחיבורים קיימים (PPP Connection)

➢ **לשינוי חיבור קיים:**

- ממסך הבית, לחץ על **Setup**. לחץ על החיבור (connection) שברצונך לעדכן. ערוך את השינויים הנדרשים ובצע פעולת שמירה.

האופציות המתקדמות אותן ניתן לקבוע עבור חיבורי PPPoA ו- PPPoE מוצגות בטבלה הבאה.



טבלה 1. אופציות לחיבור חדש

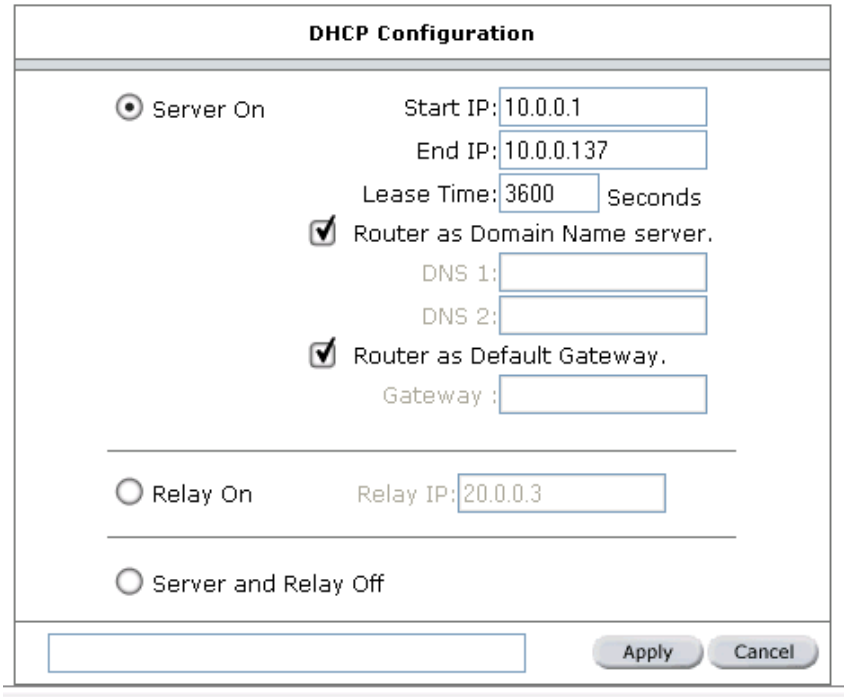
שם	תיאור	ברירת מחדל
Firewall	מאפשר להפעיל או לבטל את ה- Firewall. מומלץ מאוד לא לבטל את הגנת ה- Firewall.	פעיל
NAT	מאפשר תרגום כתובות IP, ומאפשר הגנה על הרשת הפנימית מפני חדירה למחשבי הרשת.	פעיל
On-Demand	מאפשר מצב הפעלה On-Demand. החיבור מתנתק אוטומטית אם לא קיימת פעילות במשך זמן ה- Idle Timeout הנקוב.	כבוי
Idle Timeout	אם אין פעילות במשך 'n' שניות, החיבור מתנתק. ערך זה משמש יחד עם פונקצית ה- On-Demand. על מנת לוודא שהחיבור פעיל באופן קבוע הכנס '0'.	60 שניות
Keep Alive	כאשר On-Demand אינו מאופשר, ערך זה קובע את זמן ההמתנה לניתוק, כשאין חיבור לספק השירות. על מנת לוודא חיבור מתמיד, הכנס '0'.	10 דקות
Set Route	הפוך חיבור זה לחיבור ברירת המחדל.	מופעל
MRU	יחידת קבלה מקסימלית (Maximum Receive Unit) של חיבור ה-DSL. ערך זה נקבע במשא ומתן, והוא מבקש מהספק לשלוח חבילות בעלות מקסימום של 'n ' בייטים. תחום הערכים הוא מ-128 ועד 1500 (קיימים ספקים שדורשים יותר).	1492
Enforce MRU	מאלץ את כל תנועת ה- TCP להתאים ל- MRU PPP על ידי שינוי ה- TCP Maximum Segment Size ל- MRU PPP.	PPPoE בלבד כבוי
Debug	מאפשר את פונקציות ה- Debug לחיבורי PPPoE ו- PPPoA.	כבוי

3 חלוקת כתובות IP אוטומטית (DHCP)

כברירת מחדל, פונקצית ה- DHCP Server (בצד ה- LAN) הינה מאופשרת. אם קיים ברשת שלך DHCP Server, עליך להפסיק את פעולתו של אחד מהשניים, אחרת הרשת לא תתפקד כראוי.

➢ אפשור או חסימת ה- DHCP Server:

1. ממסך הבית, לחץ על **Setup**. מ- LAN Setup, לחץ על **DHCP Configuration**. מופיע חלון ה- DHCP Configuration:

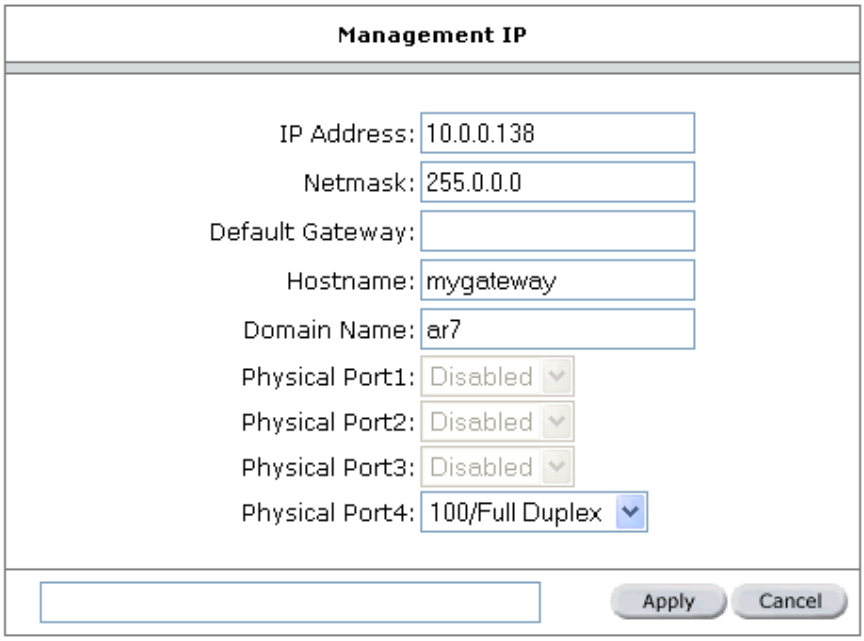


2. סמן **Server On**, על מנת לאפשר את ה- DHCP Server של הנתב. הכנס Start IP ו- End IP. הנתב יחלק כתובות IP למחשבים המקומיים, החל מ- Start IP וכלה ב- End IP.
3. סמן **Relay On**, על מנת לחסום את ה-DHCP Server של הנתב. במצב זה הנתב אחראי להפנות בקשות ותשובות בין לקוחות DHCP ל- DHCP Server של הרשת.
4. סמן **Server and Relay Off**, על מנת לקבוע תצורה באופן ידני.

4 כתובת IP של הנתב

➢ החלפת כתובת ה- IP של הנתב:

1. ממסך הבית, לחץ על **Setup**. מ- LAN Setup, לחץ על **IP Management**.
מופיע חלון ה- Management IP:



2. ערוך את השינויים הרצויים לך.

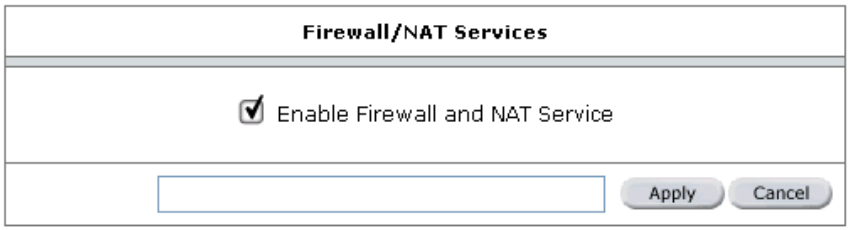
שם המארח (Hostname), יכול להיות כל שם שהו בעל תווים אלפאנומריים שאינו מכיל רווחים. ה- Domain Name משמש יחד עם שם המארח בכדי להגדיר את הנתב באופן בלעדי.
על מנת לגשת לדף האינטרנט של הנתב ניתן להקיש את כתובת ה- IP של הנתב, או את שם המארח יחד עם ה- Domain Name, בדוגמה זו: **myGateway.ar7**.

5 שירותי Firewall/NAT

ניתן לבטל את שירותי ה- Firewall/NAT עבור כל חיבורי הנתב.

➢ **ביטול שירותי Firewall/NAT:**

1. ממסך הבית, לחץ על **Setup**. מ- LAN Setup, לחץ על **Firewall/NAT Services**.
מופיע חלון ה- Firewall/NAT Services:

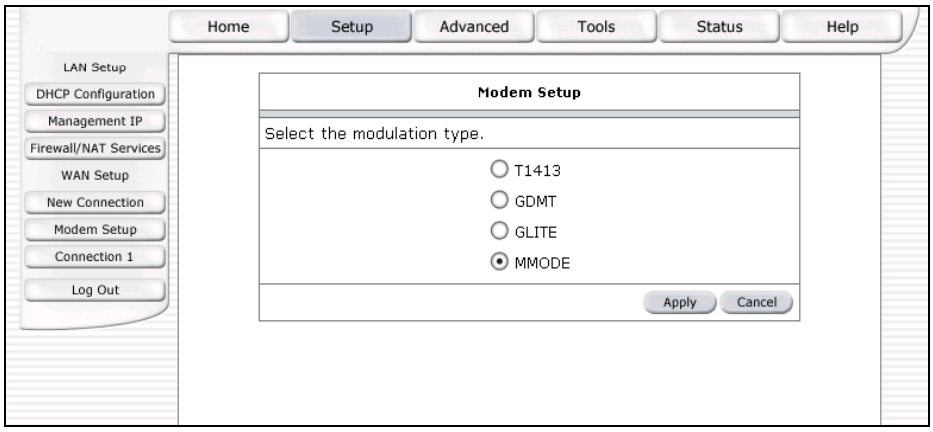


2. אם סימנת **Enable Firewall and NAT Services**, עליך לקבוע תצורה לשירותים אלו עבור כל חיבור בנפרד.
אם לא סימנת **Enable Firewall and NAT Services**, שירותים אלו חסומים באופן גלובלי.

6 תצורת ה- Modem

➢ קביעת תצורת ה- Modem:

- ממסך הבית, לחץ על **Setup**. מ- WAN Setup, לחץ על **Modem Setup**.
מופיע חלון ה- Modem Setup:

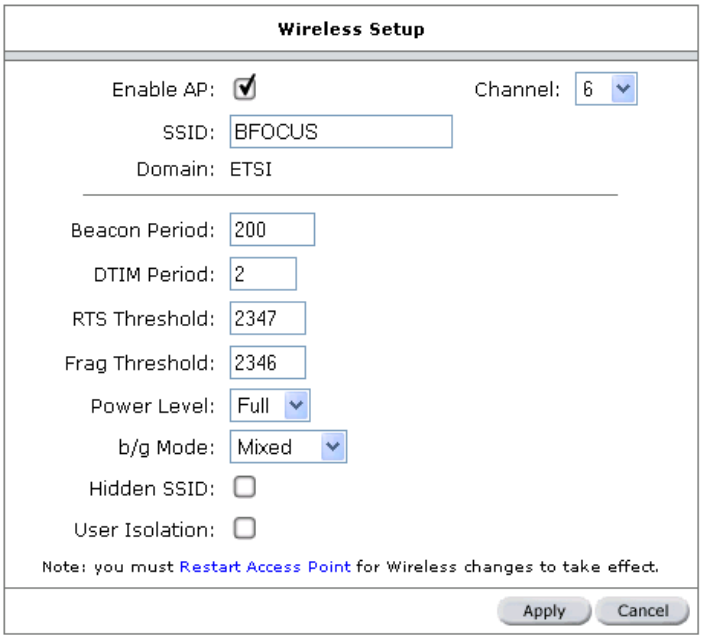


<u>שים לב:</u> אין לשנות את ברירת המחדל. שינוי ברירת המחדל יפגע בסנכרון המודם !

7 תצורה אלחוטית מתקדמת
(עבור דגם: B-FOCuS Wireless 352+)

➢ קביעת אפשרויות מתקדמות לחיבור האלחוטי:

1. ממסך הבית, לחץ על **Setup**. מ- LAN Setup, לחץ על **Wireless**. מופיע חלון ה- Wireless Setup.
2. לחץ על **Advanced**. חלון ה- Wireless Setup מתרחב וכעת ניתן לקבוע בו תצורה של פרמטרים נוספים המתייחסים לחיבור האלחוטי.

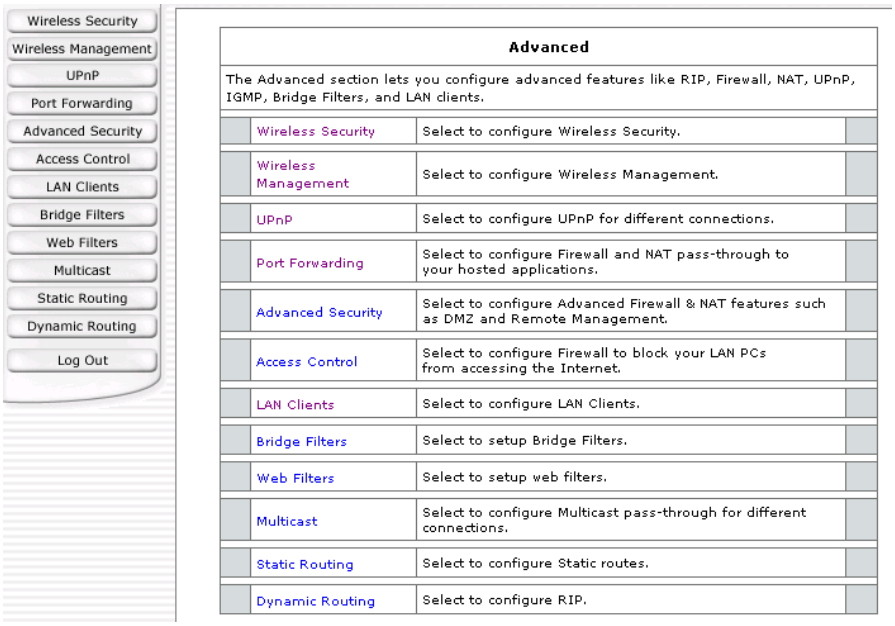


3. **Beacon Period** הוא פרק הזמן שבין נתוני Beacon המכילים נתוני בקרה. אין לשנות תצורה זאת.
4. **DTIM Period** הוא Delivery Traffic Indication Map. אין לשנות תצורה זאת.
5. **RTS Threshold** הוא Request to Send. אין לשנות תצורה זאת.
6. **Frag Threshold** נועד לשפר את התפוקה של החיבור האלחוטי. אין לשנות תצורה זאת.
7. **Power Level**: במידה וכל המחשבים ברשת האלחוטית נמצאים קרוב לנתב, ניתן להפחית את עוצמת האות האלחוטי על מנת למנוע מאנשים זרים קליטה ממרחק.
8. קבע את **b/g mode** בהתאם לסוגי הכרטיסים האלחוטיים המותקנים במחשבים. במידה ומותקנים במחשבי הרשת שלך כרטיסי wireless LAN משני התקנים, קבע **Mixed**.
9. סמן **Hidden SSID** בכדי למנוע שידור שם הרשת האלחוטית. דבר זה יקשה על זרים לזהות את הרשת שלך.

8 אופציות מתקדמות

➢ הצגת אופציות מתקדמות:

- ממסך הבית, לחץ על **Advanced**. מופיע מסך ה- Advanced:



9 בטחון אלחוטי - Wireless Security

(עבור דגם: B-FOCuS Wireless 352+)

הנתב שלך תומך בשלוש רמות של בטחון אלחוטי:

- **WEP** (Wired Equivalent Privacy) - השיטה הסטנדרטית עבור שימוש ביתי.
- **802.1x** - שיטה המיועדת עבור משתמשים עסקיים בעלי שרת Radius.
- **WPA** (Wi-Fi Protected Area) - השיטה החדשה עבור שימוש ביתי. שיטה זו מספקת בטחון אופטימלי ומומלצת עבור משתמשים ביתיים.

➢ לקביעת בטחון אלחוטי:

1. ממסך הבית, לחץ על **Advanced** ובחר ב- **Wireless Security**. מופיע חלון ה- Wireless Security.
2. בחר את רמת הביטחון האלחוטי (security level) הרצויה ולחץ **Apply**.

3. השלם את הפרטים הנדרשים, בהתאם לרמת הביטחון שבחרת:

i. אם בחרת ברמת בטחון **WEP**, מופיע החלון הבא:

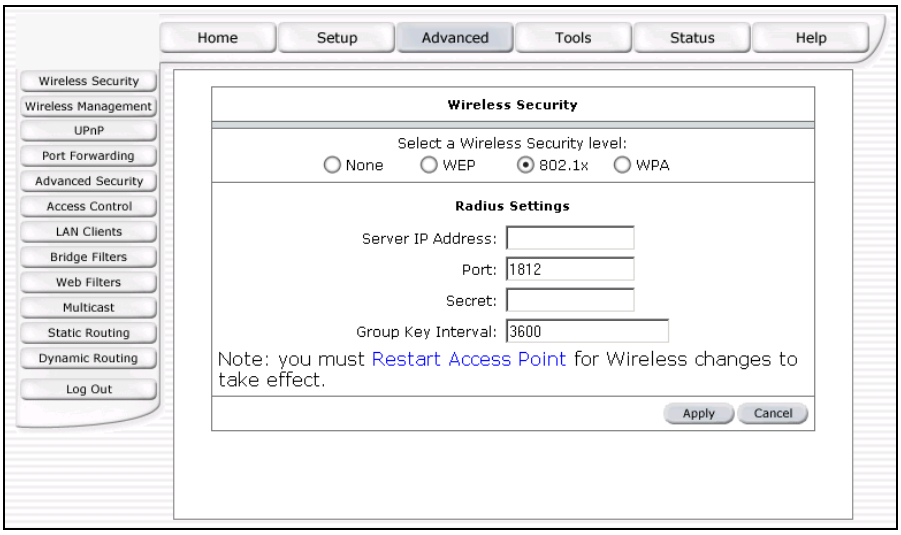
a. סמן **Enable WEP Wireless Security**.

b. קבע **Authentication Type**.

c. בחר **Cipher** (חוזק קידוד) וחבר שורת ספרות שתשמש כ- **Encryption Key** (מפתח קידוד). ניתן לחבר עד ארבעה מפתחות קידוד בדרך זאת. סמן אחד מהם במקום המיועד. עליך להכניס את אותה שורת ספרות גם בכרטיסי הרשת האלחוטיים של המחשבים שלך.

d. לחץ על **Restart Access Point**.

ii. אם בחרת ברמת בטחון **802.1x**, מופיע החלון הבא:



a. הקלד **Server IP Address** של שרת ה- Radius.

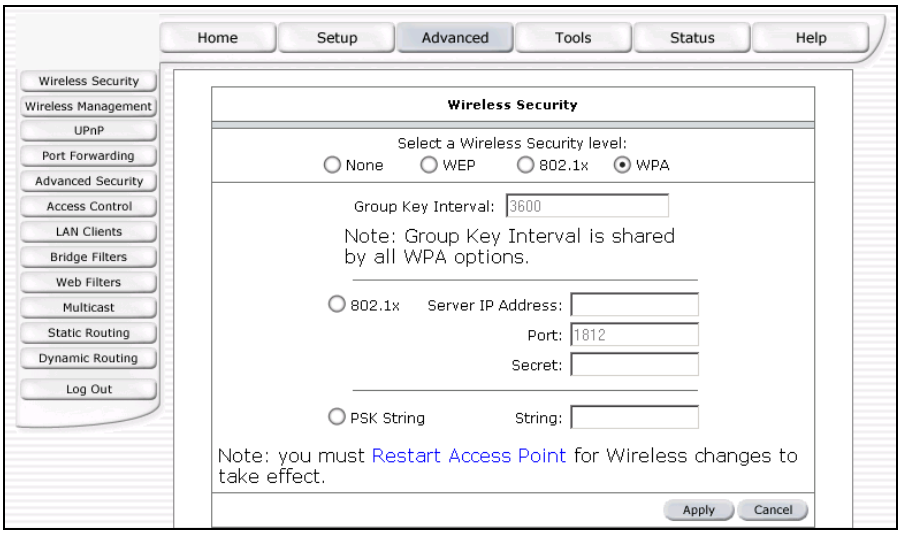
b. הקלד מספר **Port**.

c. בתיבת ה- **Secret**, חבר שורה של ספרות.
עליך להכניס את אותה שורת ספרות גם בכרטיסי הרשת האלחוטיים של המחשבים שלך.

d. בתיבת ה- **Group Key Interval**,קבע פרק זמן. בכל פעם שפרק זמן זה מסתיים, שרת ה- Radius שולח Secret חדש לכל הלקוחות האלחוטיים, דבר המקשה על אנשים בלתי מורשים להתחבר לרשת האלחוטית שלך.

e. לחץ על **Restart Access Point**.

iii. אם בחרת ברמת בטחון **WPA**, מופיע החלון הבא:



אם יש לך שרת Radius וכרטיסי הרשת האלחוטיים שלך תומכים ב- **WPA**, תוכל לבחור בשיטות הביטחון האלחוטי **802.1x** ו- **WPA** גם יחד.

a. סמן **802.1x** אם רצונך בכך וחבר שורת ספרות.
עליך להכניס את אותה שורת ספרות גם בכרטיסי הרשת האלחוטיים של המחשבים שלך.

b. סמן **PSK String** וחבר שורת ספרות.
עליך להכניס את אותה שורת ספרות גם בכרטיסי הרשת האלחוטיים של המחשבים שלך.
בזמן חיבור המתח, הנתב משתמש בשורה שחיברת זה עתה ולאחר מכן הוא מחבר שורת ספרות באופן אוטומטי, דבר המקשה על אנשים בלתי מורשים להתחבר לרשת האלחוטית שלך.

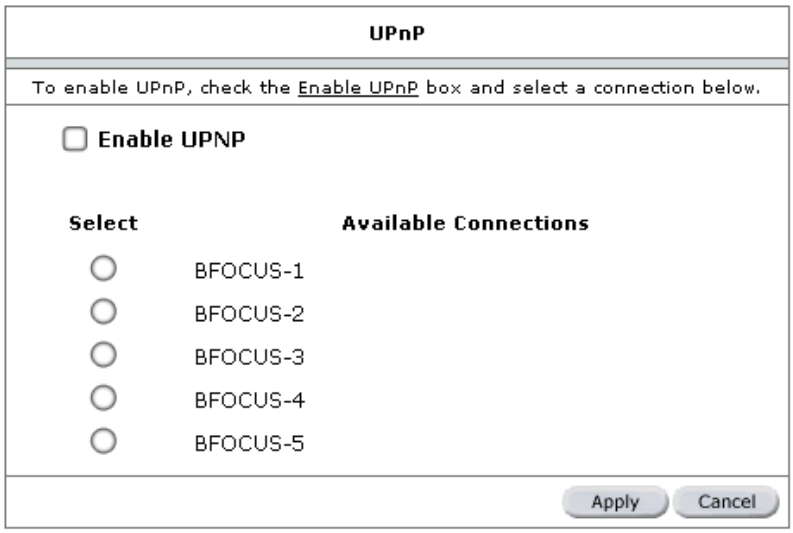
c. לחץ על **Restart Access Point**.

10 הכנס והפעל אוניברסלי - UPnP

הכנס והפעל אוניברסלי (UPnP) מאפשר לתנועות NAT ו- Firewall לעבור דרך הנתב עבור יישומים המשתמשים בפרוטוקול זה. אם יש לך מספר חיבורים, בחר בחיבור בו נכנסת התנועה.

➢ **הפעלת UPnP:**

1. ממסך הבית, לחץ על **Advanced** ובחר ב- **UPnP**.
מופיע חלון ה- UPnP:



2. סמן **Enable UPnP** ובחר את החיבור שינצל את ה- UPnP.

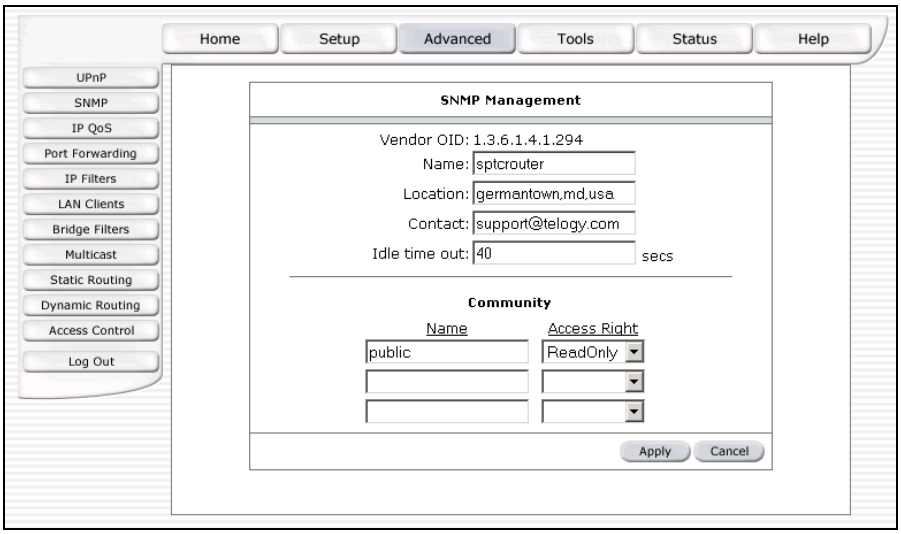
11 SNMP

(עבור דגם: B-FOCuS Wireless 352+)

אתה יכול לקבוע את אפיון ה- SNMP של הנתב שלך.

➢ קביעת אפיון SNMP:

- ממסך הבית, לחץ על **Advanced** ובחר ב- **SNMP.**
  מופיע חלון ה-SNMP:

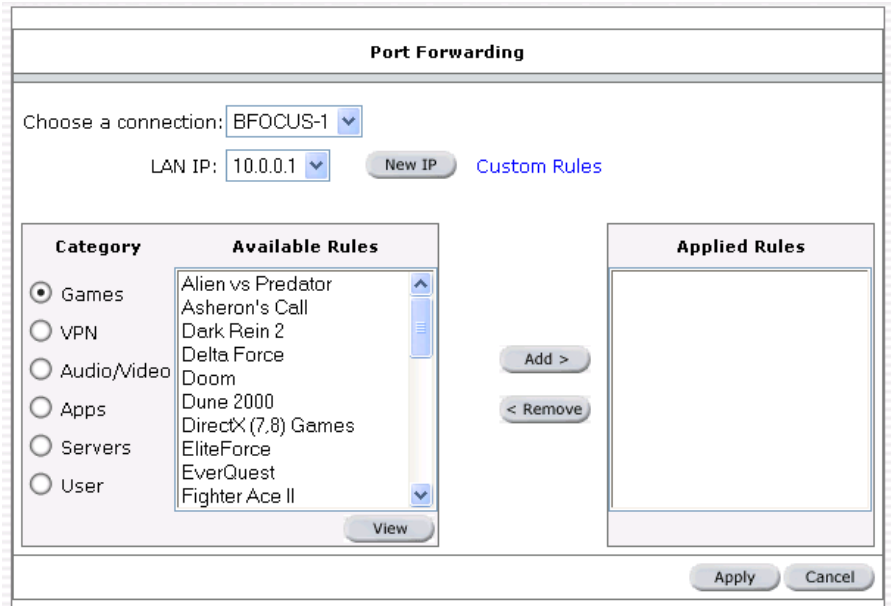


12 הפניית פורטים - Port Forwarding

הפניית פורטים מאפשרת לך לספק שירותים מקומיים, כדוגמת ה- Web Hosting. כאשר משתמשים שולחים בקשות לרשת שלך, הנתב שלך מפנה אותן למחשב המתאים. ניתן להשתמש בהפניית פורטים גם במצב חלוקת כתובות של DHCP, אך עליך לזכור שכתובת DHCP אינה קבועה. לכן במקרה של שרת Netmeeting לדוגמא, ראוי להקצות כתובת קבועה לשרת זה. זכור גם, שאם משתמש אינטרנט מבקש לגשת ליישום אינטרנטי, עליו להשתמש בכתובת ה- WAN. הפניית פורטים מתרגם את כתובת ה- WAN לכתובת LAN.

➢ קביעת תצורה של הפניית פורטים עבור יישום:

1. ממסך הבית, לחץ על **Advanced** ובחר ב- **Port Forwarding**. מופיע חלון ה- Port Forwarding:



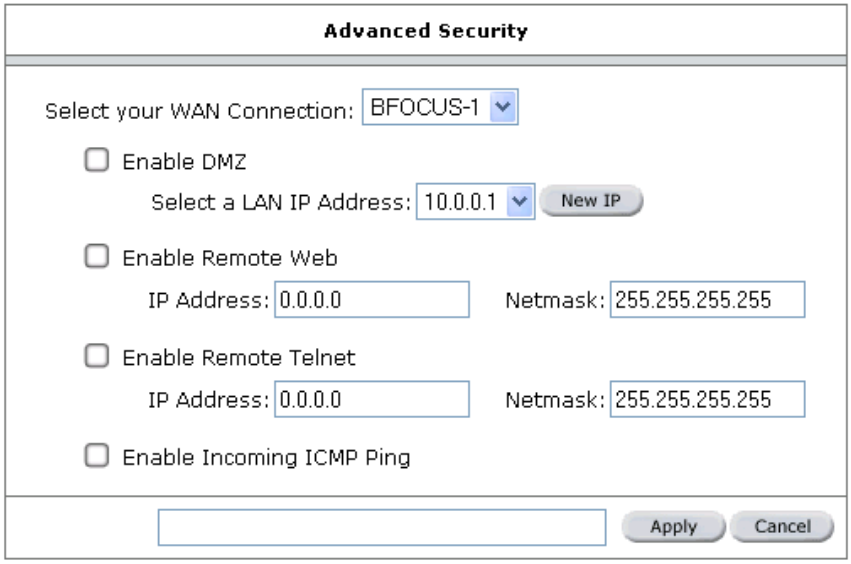
2. בחר WAN Connection ומחשב מארח.
3. הוסף את חוק ה- Firewall הרצוי.
4. אם רצונך לחבר חוק ייחודי, בחר ב- **User** ולחץ על **New**. קבע פורט, פרוטוקולים, ותיאור לחוק החדש.

13 תצורת DMZ

אם תקבע שמחשב אחד ברשת שלך יהיה "אזור מפורז" (Demilitarized Zone), כל תנועה שאינה מופנית למחשב מסוים ברשת, תנותב למחשב זה. התוצאה היא שמחשב ה- DMZ חשוף לרשת האינטרנט.

➢ **קביעת מצב DMZ למחשב ברשת המקומית:**

1. מחלון ה- Advanced Security:

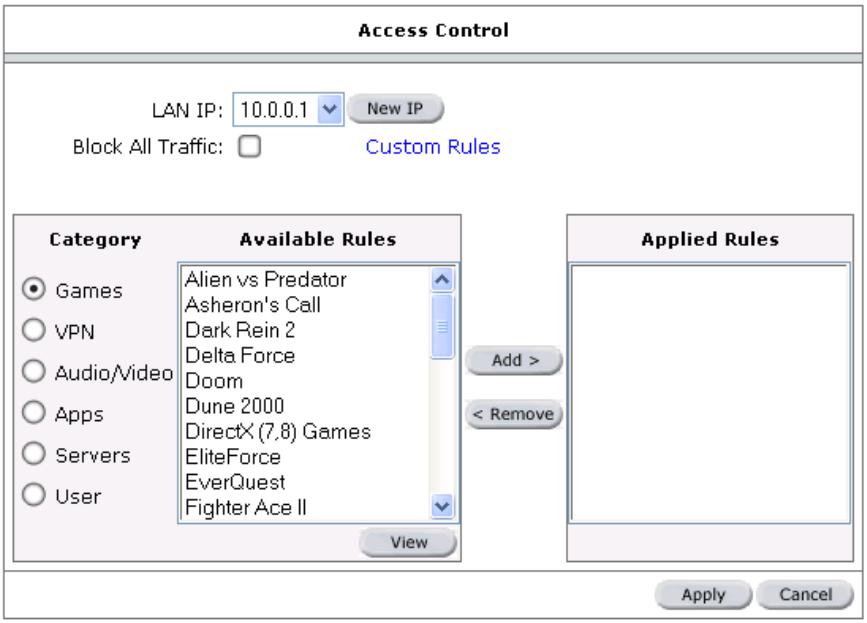


2. בחר את חיבור ה- WAN.
3. סמן **Enable DMZ**.
4. בחר בכתובת ה- IP של המחשב שברצונך להגדיר כ- DMZ.
5. לחץ על **Apply**.

14 קביעת מסנני Access Control IP

➢ **לקביעת מסנני Access Control IP:**

- ממסך הבית, לחץ על **Advanced** ובחר ב- **Access Control**.
  מופיע חלון ה- Access Control:

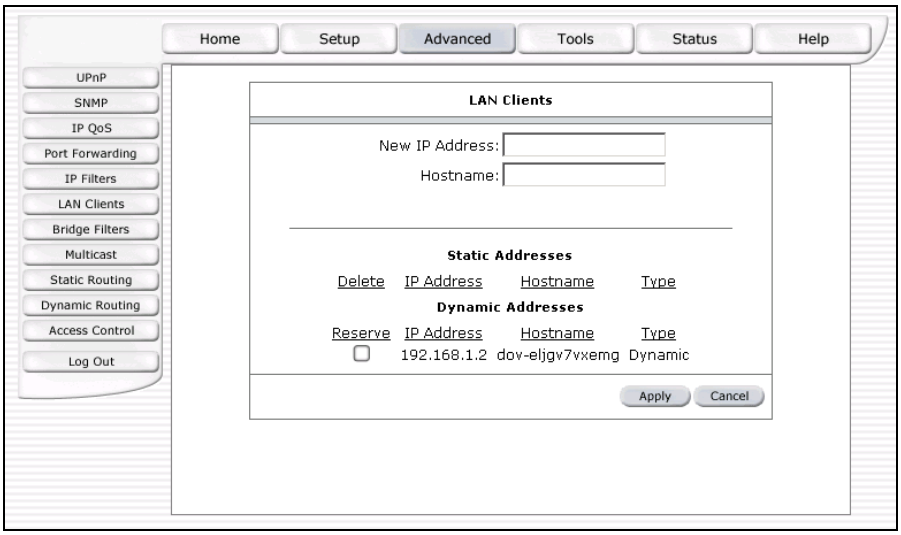


בכדי לאפשר לאפליקציה מסוימת גישה לרשת הביתית יש לבחור מהרשימה את האפליקציה הרצויה וללחוץ **Add / Apply**.
כמו כן ניתן גם ליצור חוק (**Rule**) חדש על ידי לחיצה על **Custom Rules** והכנסת הפרמטרים הדרושים.

15 לקוחות LAN - LAN Clients

➢ להוספת לקוח ל- LAN:

1. ממסך הבית, לחץ על **Advanced** ובחר ב- **LAN Clients**.
מופיע חלון ה- LAN Clients:



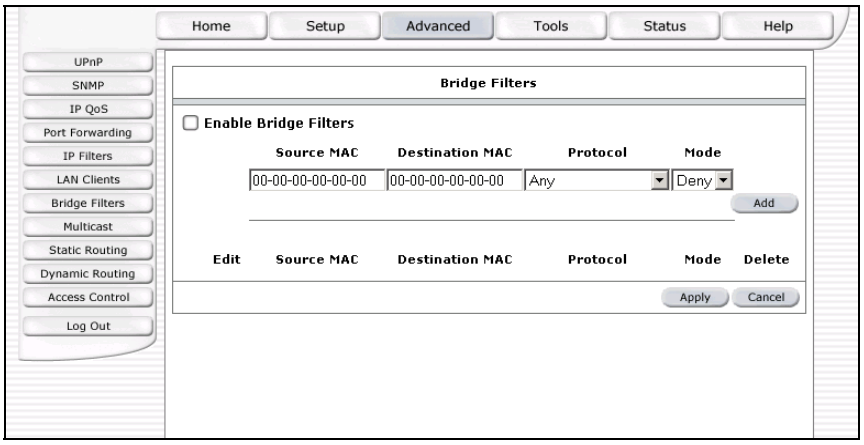
2. כל לקוחות ה- DHCP מוקצים באופן אוטומטי.
3. אם יש לך שרת בעל כתובת IP קבועה ב- LAN, ורצונך ששרת זה יהיה נגיש דרך ה- WAN, עליך להוסיף את כתובת ה- IP שלו. לאחר מכן תוכל להוסיף הפניית פורטים וחוקי גישה עבור כתובת ה- IP הזו.

16 סינון גשרים - Bridge Filters

בעזרת סינון גשרים ניתן לאפשר או לחסום גישת נתונים דרך הגשר. כל חבילה נבדקת עבור כתובת MAC המקור שלה, כתובת MAC היעד שלה, ו- Frame type.

➢ קביעת סינון גשרים:

1. ממסך הבית, לחץ על **Advanced** ובחר ב- **Bridge Filters**.
   מופיע חלון ה- Bridge Filters:



2. לחץ על **Enable Bridge Filters**.
3. הוסף, ערוך, או מחק חוקי סינון כרצונך.
4. על מנת להוסיף חוק סינון, מלא את השדות **Source MAC**, **Destination MAC**, **Protocol**, ו- **Mode**, ולחץ על **Add**.
5. לחץ על כפתור ה- **Edit** שליד חוק סינון קיים על מנת לערוך בו שינויים.
6. לחץ על כפתור ה- **Delete** שליד חוק סינון קיים על מנת למחוק אותו.
   ניתן למחוק חוקים אחדים בפעולה אחת.
7. לחץ על **Apply**.

קיימים שלושה חוקי סינון מוסתרים. חוקים אלו מוכנסים לנתב באופן אוטומטי על מנת לוודא שהמשתמש לא "נועל" אותם בחוץ. אלו החוקים:

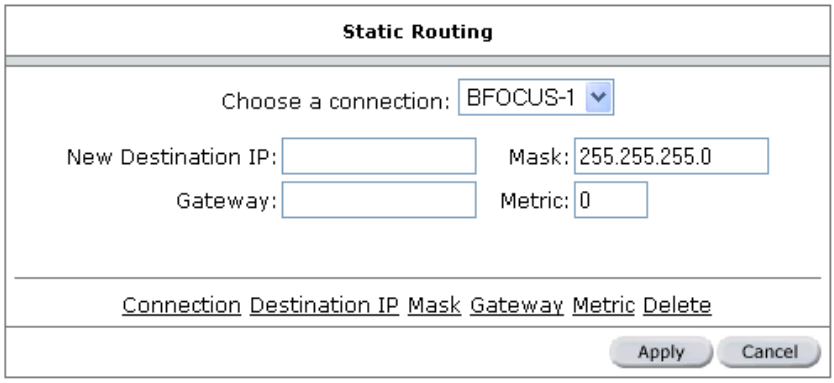
- כל נתוני ARP מורשים לעבור במערכת.
- כל נתוני Ipv4 אשר יש להם כתובת MAC יעד של הגשר מורשים לעבור במערכת.
- כל נתוני Ipv4 אשר יש להם כתובת MAC מקור של הגשר מורשים לעבור במערכת.

17 ניתוב סטטי - Static Routing

אם הנתב שלך מחובר ליותר מאשר רשת אחת, אתה יכול להקים נתיב סטטי ביניהם.

➢ **קביעת ניתוב סטטי:**

1. ממסך הבית, לחץ על **Advanced** ובחר ב- **Static Routing**.
   מופיע חלון ה- Static Routing:



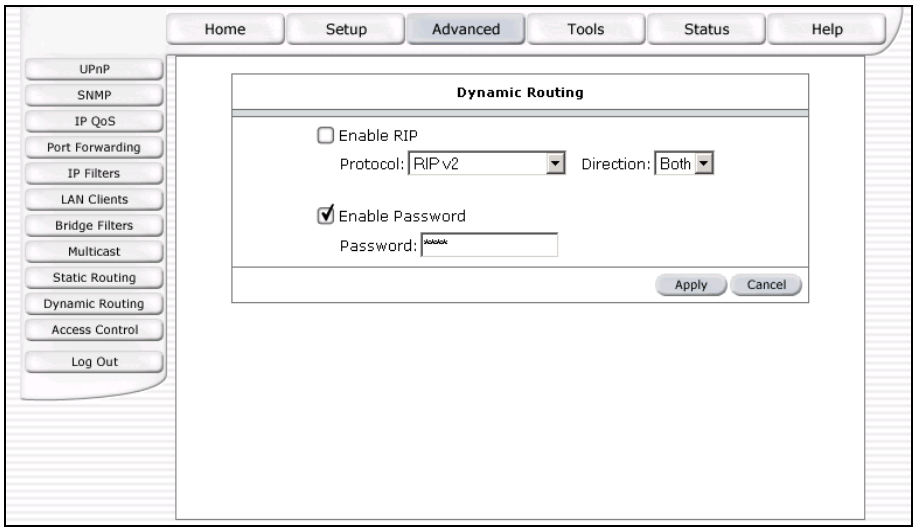
2. בחר בחיבור עבור ניתוב סטטי.
3. הכנס את ה- **New Destination IP**.
4. ב- **Gateway** הכנס נתב.
5. לחץ על **Apply**.

18 ניתוב דינמי - Dynamic Routing

ניתוב דינמי מאפשר לנתב להגיב באופן אוטומטי לשינויים פיזיים ברשת. הנתב משתמש בפרוטוקול ה- RIP בכדי לחשב את נתיב חבילות הנתונים, בהתבסס על כמות מינימלית של קפיצות בין תחנת המוצא לתחנת היעד. פרוטוקול ה- RIP משדר באופן תדיר לנתבים אחרים מידע עדכני על הנתיבים.

➢ **קביעת ניתוב דינמי:**

1. ממסך הבית, לחץ על **Advanced** ובחר ב- **Dynamic Routing**.
   מופיע חלון ה- Dynamic Routing:



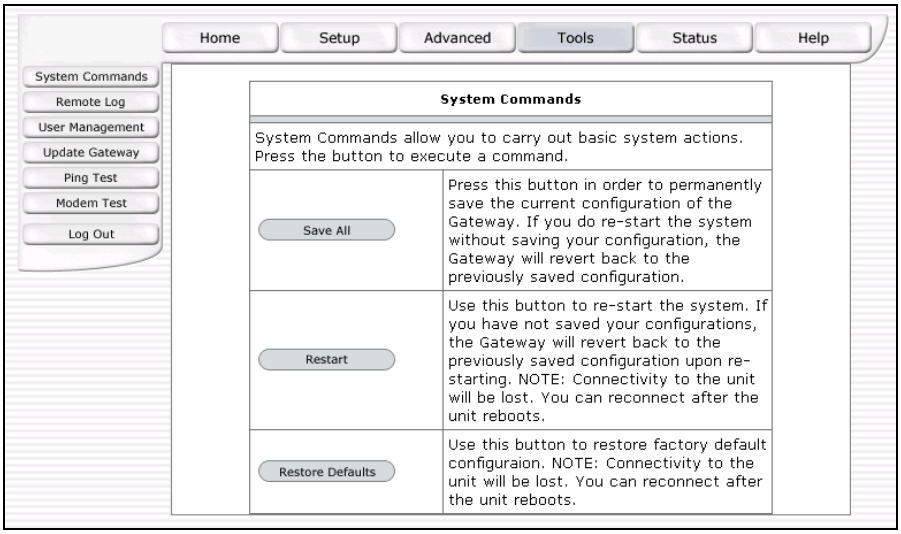
2. לחץ על **Enable RIP**.
3. בחר פרוטוקול עבור שידורי ה- RIP.
4. בחר כיוון לשידורי ה- RIP.
5. לחץ על **Apply**.

19 פקודות מערכת

אחרי כל שינוי שביצעת בתצורת הנתב שלך, עליך לשמור את התצורה החדשה.

➢ גישה לפקודות המערכת:

- ממסך הבית, לחץ על **Tools** ובחר ב- **System Commands.**
  מופיע חלון ה- System Commands:



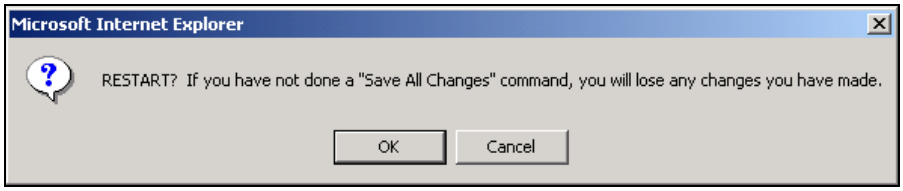
➢ שימור שינויי תצורה:

- **לחץ על Save All.**

פעולה זאת שומרת באופן קבוע את התצורה הנוכחית. אם תבצע אתחול למערכת בלי לבצע פעולת **Save All** לפני כן, הנתב ישמור על התצורה הקודמת.

➢ לאתחול הנתב:

1. לחץ על **Restart**. מופיע חלון אישור האתחול:

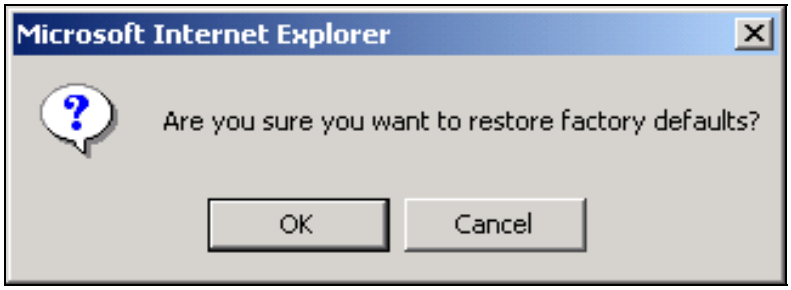


2. לחץ על **OK**.

פעולה זאת מפעילה מחדש את הנתב. אם לא שמרת את התצורה החדשה שלך, הנתב יחזור לתצורה הקודמת. אין תקשורת עם הנתב עד אחרי סיום פעולת האתחול. יש צורך לבצע פעולת Login מחדש.

➢ טעינת תצורת ברירת המחדל המפעלי:

1. לחץ על **Restore Defaults**. מופיע חלון שחזור ברירות המחדל המפעליות:



2. לחץ על **OK**.

פעולה זאת מחזירה את הנתב לתצורת ברירת המחדל בה יצא מהמפעל. הפעולה שימושית אם אבדה התקשורת עם הנתב מסיבה כלשהי. אין תקשורת עם הנתב עד אחרי סיום פעולת האתחול. יש צורך לבצע פעולת Login מחדש.

אם הנתב שלך תומך בחיבור אלחוטי, אפשר גם לאתחל את נקודת הגישה מחלון ה- System Commands.

➢ אתחול נקודת הגישה:

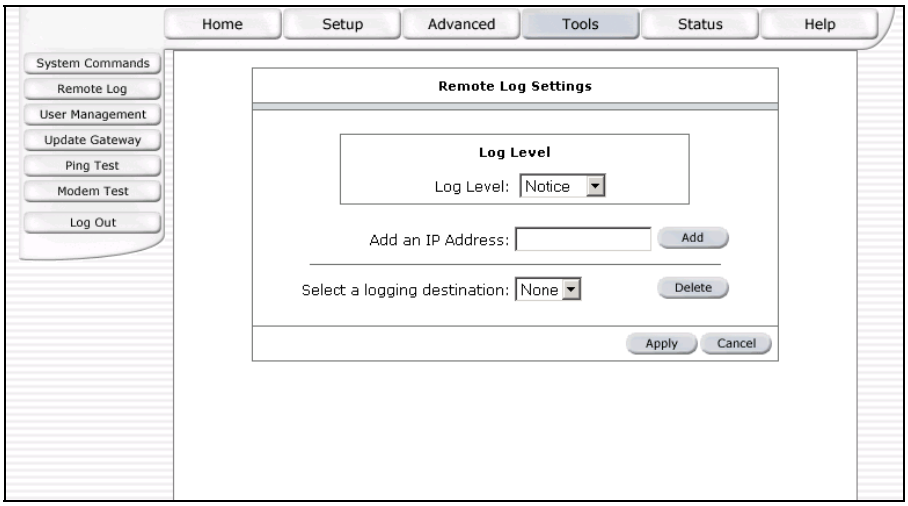
- לחץ על **Restart Access Point**.

19.1 רישום מרחוק

פונקצית הרישום מרחוק פעילה כאשר אפשרת את מצב העבודה **Debug** עבור חיבורי PPPoA ו- PPPoE. הרישום מרחוק יעזור לאתר בעיות התחברות.

➢ **לאפשר רישום מרחוק:**

1. ממסך הבית, לחץ על **Tools** ובחר ב- **Remote Log**.
   מופיע חלון ה- Remote Log Settings:



2. בחר ב- **Log Level** הרצוי. הודעות בעלות רמת חומרה שווה או גבוהה יותר יישלחו למחשב המרוחק. רמות החומרה של ההודעות מוצגות בטבלה הבאה.
3. הוסף כתובת IP עבור כל מחשב עבורו ברצונך לקבל מעקב.

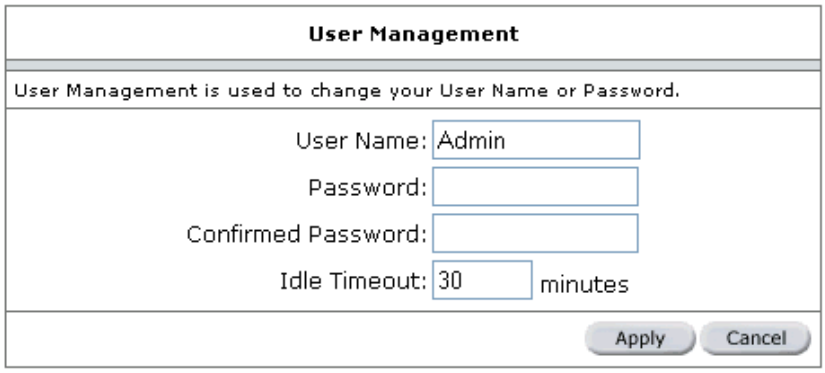
טבלה 2. רמות חומרה של הודעות שגיאה

רמת החומרה	תיאור
Panic	"בהלה" במערכת או כל מצב שגורם לנתב שלא לפעול.
Alert	מצבים שדורשים תיקון מיידי.
Critical	מצבים קריטיים.
Error	מצבי שגיאה שיש להם תוצאה פחות חמורה מאשר אלו ברמות Panic, Alert, או Critical.
Warning	מצבים שכדאי לעקוב אחריהם.
Notice	מצבים שאינם שגיאה אך אולי יצטרכו טיפול מיוחד.
Info	מאורעות או מצבים שאינם שגיאה אך הם בעלי עניין.
Debug	הודעות על איתור תקלות תוכנה. יש לציין רמה זאת רק אם התבקשת על ידי איש שירות מוסמך.

20 ניהול משתמשים

➢ **לשינוי שם משתמש וסיסמה של הנתב:**

1. ממסך הבית, לחץ על **Tools** ובחר ב- **User Management**.
מופיע חלון ה- User Management:

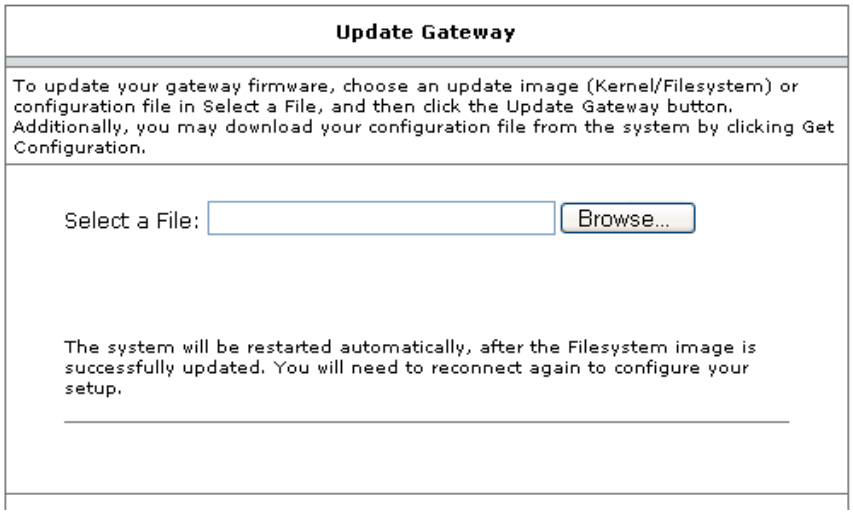


2. הכנס שם משתמש חדש.
3. הכנס סיסמה חדשה.
4. הכנס שוב את הסיסמה שבחרת לצורכי אשרור.
5. קבע מספר דקות לניתוק אוטומטי במקרה ואין פעילות.
6. אם שכחת את הסיסמה שבחרת, לחץ על לחצן האתחול (שנמצא על הפנל האחורי של הנתב) למשך עשר שניות. הנתב יחזור לתצורת ברירת המחדל שבה יצא מהמפעל, וכל תצורה אישית תאבד.

21 עדכון תוכנה

➢ לעדכון תוכנת הנתב:

1. ממסך הבית, לחץ על **Tools** ובחר ב- **Update Gateway**.
   מופיע חלון ה- Update Gateway:



2. לחץ על **Browse** ואתר את קובץ התוכנה המעודכן.
3. לחץ על **Update Gateway**. כאשר העדכון מסתיים, הנתב יבצע אתחול, ועליך לבצע התחברות מחדש.

אם העדכון אורך למעלה מחמש דקות, זהו סימן לכך שאירעה תקלה.

אל תכבה את הנתב במשך פעולת העדכון.

➢ שמירת תצורת הנתב:

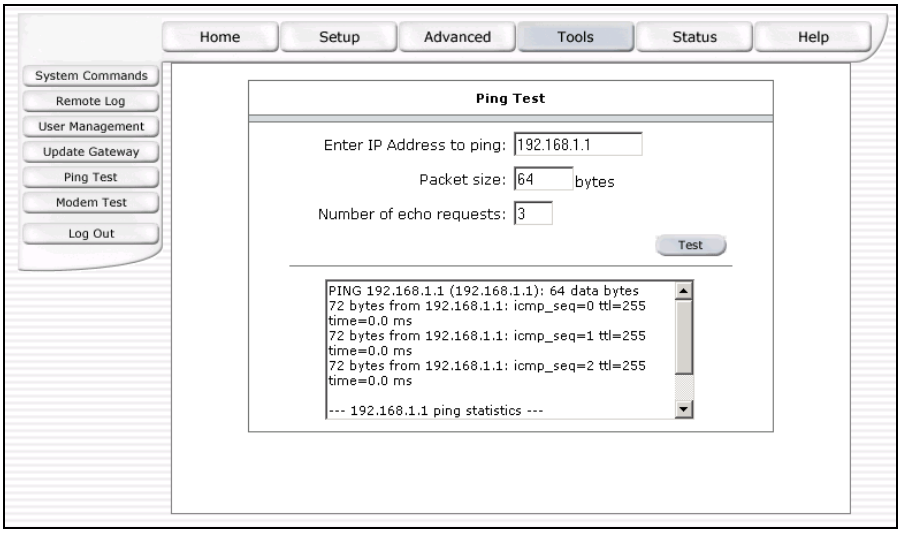
- לחץ על **Get Configuration**. הנתב ייצר קובץ המפרט את התצורה שלו לשמירה במחשב שלך למטרת Backup.

22 בדיקת Ping

לאחר שקבעת את התצורה של הנתב שלך, תוכל לבדוק את החיבור בעזרת בדיקת Ping.

➢ **לביצוע בדיקת Ping:**

1. ממסך הבית, לחץ על **Tools** ובחר ב- **Ping Test**.
מופיע חלון ה- Ping Test:



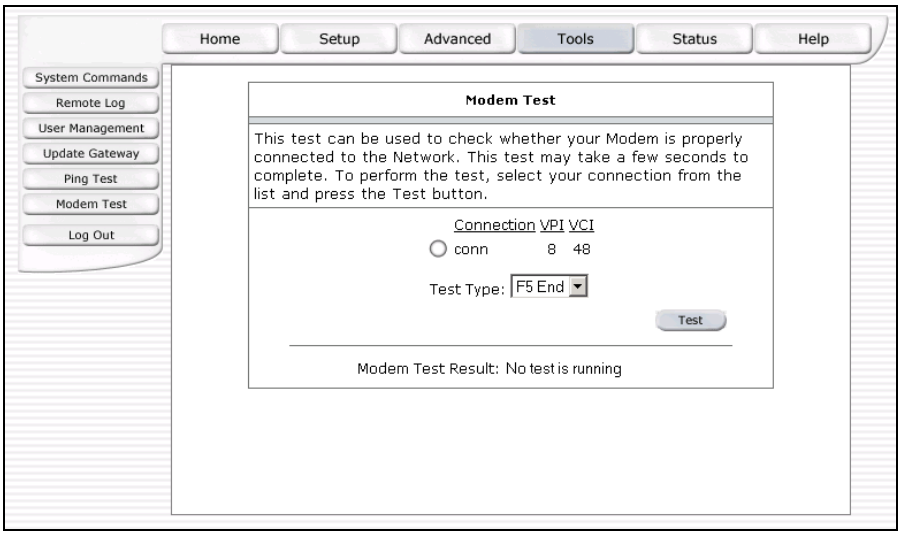
2. הכנס את כתובת היעד שאליו ברצונך לשלוח את ה- Ping.
אם המחשב שלך מחובר לנתב בתצורת ברירת המחדל של DHCP, אזי תוכל לבצע בדיקת Ping לכתובת הנתב.
אם ה- ISP שלך נתן את הכתובת של השרת שלו, נסה לבצע בדיקת Ping מולו.
3. לחץ על **Test**.
4. כברירת מחדל, כשתפתח את חלון ה- Ping Test, הנתב יבצע בדיקת Ping שלוש פעמים מול עצמו.

23 בדיקת הנתב

בדיקת הנתב בודקת את חיבור הרשת.

➢ **לבדיקת הנתב:**

1. ממסך הבית, לחץ על **Tools** ובחר ב- **Modem Test**.
מופיע חלון ה- Modem Test:



2. בחר בחיבור שלך מתוך הרשימה ולחץ על **Test**.

לפני ביצוע הבדיקה, בדוק שיש לך חיבור DSL תקין.

כדי שבדיקה זאת תצליח, ציוד חברת הטלפון צריך לתמוך בה. לא כל חברות הטלפון תומכות ב- F4 ו- F5.

24 סטטוס

כפתור הסטטוס מאפשר לך לעיין במצב הנוכחי של הנתב ובסטטיסטיקות של החיבורים והממשקים השונים.

➢ **דוחות מצב:**

- ממסך הבית, לחץ על **Status**. דוחות המצב והסטטיסטיקה הזמינים מופיעים בצד שמאל של חלון הסטטוס. הדוחות מוצגים בטבלה הבאה.

טבלה 3. דוחות מצב

סוג	תיאור
סטטיסטיקות רשת	סטטיסטיקות של ממשקים שוניםDSL/Ethernet.
מצב חיבורים	מצב של החיבורים השונים.
לקוחות DHCP	רשימת לקוחות DHCP.
מצב המודם	מצב וסטטיסטיקה של חיבור ה- DSL שלך.
פרטי המוצר	מידע על החומרה של הנתב שלך.
מערכת	עיון במידע השמור בזיכרון הנתב.

25 איתור תקלות

להלן רשימה של בעיות נפוצות בנתבים. עיין בפרק זה לפני שתפנה לתמיכה הטכנית, על מנת לנסות ולפתור את הבעיה באופן עצמאי.

25.1 הנתב אינו פועל

- בדוק שנורית ה- Power דולקת בצבע ירוק.
- בדוק שכבלי הרשת מחוברים היטב.
- בדוק שהנוריות LAN ו- Internet Link דולקות בצבע ירוק.
- בדוק שנורית ה- ADSL Sync דולקת בצבע ירוק.
- בצע בדיקת Ping מהמחשב לנתב:
  a. משולחן העבודה לחץ על **Start > Run**.
  b. בתיבת Open, רשום: **Ping 10.0.0.138**.
  c. תוצאה חיובית נראית כך:
  Reply from 10.0.0.138 bytes=32 time<10ms TTL=255.
- בצע בדיקת Ping מול ה- WAN.

אם בדיקת ה- Ping מול הנתב מצליחה, וקבעת תצורה נכונה לפרוטוקולים, גם בדיקת ה- Ping מול ה- WAN אמורה להצליח (ספקי שירות אמורים לספק כתובות IP של השרתים שלהם). אם אינך יכול לבצע בדיקת Ping מול ה- WAN, בדוק הכנסת פרוטוקולים נכונים וערכי VPI ו- VCI נכונים.

- בדוק ש-NAT מאופשר בחיבור שלך. אם לא כן, הנתב לא ינתב את הנתונים באופן תקין.
- יש לחסום סוכנים (Proxies) בדפדפן האינטרנט.
- אם בזמן ההתחברות לנתב אתה מקבל הודעת הפניה, וודא ש- JavaScript מאופשר.
- חסום את פעולת כרטיס הרשת שלך וחזור ואפשר את פעולתו.
- מחק את קבצי האינטרנט הזמניים, קבצי ההיסטוריה, וה- Cookies.
- וודא שב- Windows הגדרת את ה- LAN עבור Dynamic IP Addresses.
- וודא שאף יישום לא מנסה להקים קשר עם האינטרנט בשיטת Dial-up.

- אם ביצעת את כל הבדיקות והפעולות הרשומות מעלה ועדיין הנתב אינו פועל כראוי, לחץ על לחצן ה- **Reset** שנמצא על הפנל האחורי והחזק אותו למשך 10 שניות. הנתב יחזור לתצורת ברירת המחדל שבה יצא מהמפעל. חזור על כל הבדיקות והפעולות.

25.2 נורית ה- DSL Sync מהבהבת אך אינו דולקת קבוע

קו ה-DSL מנסה ליצור קשר, אך אינו מצליח להקים חיבור תקף. פנה לשרות לצורך המשך טיפול.

25.3 נורית ה- DSL Sync תמיד כבויה

וודא ששירות ה- DSL מסופק לביתך. בדרך כלל תקבל הודעה כלשהי על כך שהשירות מותקן בביתך. קו DSL מאופיין על ידי רעש בעל צליל גבוה וניתן להבחין בו אם תקשיב מקרוב. במידה ואינך שומע רעש זה, פנה לשרות לצורך המשך טיפול.

וודא שקו הטלפון מחובר היטב לשקע הטלפון ומשם לשקע ADSL של הנתב שלך. אם התקנת מפצל על קו הטלפון, ובטעות חיברת את קו הנתב לצד הטלפון של המפצל, נורית ה- DSL לא תדלוק.