**מה חשוב לשנן למבחן**

1. לשנן את היתרנות של התקנים ניידים ואת החסרונות
2. לשנן את כל החיבורים הנפוצים של המחשב dvi vga usb וכו'
3. סוגי מדפסות שיטות עבודה אבחון בעיות
4. טופולוגיות פיזיות ולוגיות נפוצות ?
5. מהו ציוד רשת ולמה משמש כל רכיב תזכרו לעיין במונחי בסיס ?
6. הסדר של מודל שבעת השכבות ישר והפוך מאוד חשוב!
7. מהו מודל TCP\IP איך השכבות שלו חופפות את מודל שבעת השכבות ?
8. מהו כתובת פיזית ומהו כתובת לוגית?
9. להבין מה תפקידם של טבלאות אותיות וסימנים ללמוד את הטבלאות הנפוצות Unicode ACSSI ובאיזה שכבה הם פועלים?

11. להכיר את מבנה כתובות ip להבין איך הכתובת נהפכת לכתובת בינארית ?

1. למה משתמש subnet mask ואיך משתמשים בפעולת NDA?
2. איזה כתובת Ip מותרות לשימוש ברשתות פרטיות ואיזה לא?
3. איך משתמשים ב Subnetting ומה החישוב שאנו עושים בכדי לדעת כמה כתובות יש לנו?
4. למה משמש כתובות IP מיוחדות ?
5. לדעת לקרוא את טווחי כתובות Ip זה חשוב בכדי להבין את ההסברים אם איזה כתובות אפשר להשתמש בכל סוג של רשת.
6. להבין היטב את שלשת הclass הקיימים בכתובות IP ולדעת מה subnet mask ברירת מחדל.
7. מהו פורט? איזה סוגי פורטים יש ללמוד היטב את הפורטים הנפוצים?
8. מה תפקיד שרת DHCP באיזה פורט הוא משתמש ובאיזה פרוטוקול משתמש להעברת נתונים ?
9. מהו תהליך העבודה מול שרת DHCPואיך נקרא הכתובת של המחשב מתי שאין

?DHCP שרת

21. מה תפקיד שרת DNS באיזה פורט הוא משתמש ובאיזה פרוטוקול העברת נתונים

?

1. מהו ISP ? באיזה טופולוגיות הם תומכות ) -ADSL כבלים(
2. להתמקד היטב בפרוטוקול NAT מה היתרונות והחסרונות של השיטה ומה תפקידו העיקרי?
3. חשוב להבין ולהפנים את תהליכי העבודה מול השרתים וסדר הפעולות המדויק לנסות לתאר תהליכים מציאותיים ומכורים בכדי להבין.
4. ללמוד על בעיות עיקריות בנושא הרישות ופתרונות כולל בדיקות פיזיות )לדוגמא ניתוק ציוד קצה( או ע"י פקודות שלמדנו.

.25

**כללים ליצירת תקשורת ברשת בנויה פיזית )זאת אומרת יש לנו לדוגמא רשת מסוג**

**)STAR**

* 1. מקור ערוץ יעד
  2. פרוטוקולים מתאימים לדוגמא להורדת קבצים משתמשים בשרות FTP שבמודל

TCP

* 1. שימוש בפורט ספציפי תואם השרות לדוגמא http שימוש בפורט 8080

לכל תנאי ביצירת תקשורת יש הרחבה כמו שלמדנו בכתה ונפרט

* + 1. **מקור ערוץ ויעד מקור – source**

בשפה המקצועית המקור הוא מכשיר קצה המוכנה Host וכן היעד כאשר המחשב המספק את השירותיים נקרא שרת Server צריך לזכור שלא בכל רשת מחשבים יש שרת יעודי אלא יש רשתות בדרך כלל ברשתות קטנות עד 11 מחשבים המחשבים משמשים גם כשרתים וגם כלקוחות רשתות כאלו מכונות Peer To Peer **ערוץ – Media**

הערוץ – הוא "הכביש" בו אנו מעבירים את המידע צריך לזכור כאשר אנו משתמשים בערוץ ספציפי ממילא גם הפרוטוקולים )החוקים( משתנים לדוגמא ברשת מחשבים שמחוברים ע"י hub אנו נשתמש בפרוטוקול אטרנט Ethernet שנמצא כזכור בשכבה השניה )והראשונה( במודל שבעת השכבות כאשר בהמשך נפרט יותר לעומק את שיטת העבודה של פרוטוקול Ethernet וכאשר נרצה להשתמש ברשתות גלובליות )זאת אומרת לגלוש לאתרים וכו'( נשתמש בפרוטוקול

Internet Protocol

* + 1. **Protocol - פרוטוקול**

פרוטוקול הוא שיטה ידועה בה אנו משתמשים בכדי לבצע פעולות העברת מידע הפרוטוקול בדרך כלל מבצע פעולות ספציפיות ואינו מתייחס לכלל התהליך כך שפרוטוקול יהיה בדרך כלל תואם שכבה אחת מתוך שבעת השכבות.

שים לב!

חשוב מאוד להבין את ההבדל בטרמינולוגיה )זאת אומרת בשפה בה אנו משתמשים(

צריך עוד לזכור שהפרוטוקולים בהם אנו משתמשים הם חופפים למודל שבעת השכבות אבל בעצם פועלים במודל TCP\IP תראה במונחי בסיס את ההשוואה.

ישנם שני סוגי פרוטוקולים כאשר סוג האחד הוא פרוטוקול כללי והסוג השני הוא פרוטוקול ספציפי בהמשך החוברת תמצאו מדריכים קצרים תשתמשו בהם בכדי להעמיק את ההבנה.

**הדגשה חשובה! לא להתבלבל כאשר מובא הסבר ובתוכו שם של פרוטוקל**

**אנו צריכים לצאת מנקודת מוצא שינם כללים מדויקים שאנחנו לא מכירים אבל עדיין זה לא אומר שאנחנו לא מבינים את כל הנושא לדוגמא אנחנו יודעים שהגלישה באינטרנט מחייבת כללים מדויקים ואפי שאנחנו לא יודעים אותם אנחנו עדיין יודעים איך להשתמש באתרים ובתוכנות תחשבו על זה, זה יעזור לכם!**

**3. פורטים**

בכדי שהשרת או המחשב ידע איזה שרות עליו להפעיל היה צורך בסימון מיוחד לכל סוג של שרות למדנו בשיעור שבתקשורת כיום אנו משתמשים בכדי לזהות תהליך מחשב למחשב בפורט + כתובת IP למושג זה נקרא סוקט socket

ניתן להסביר את המונח פורט באמצעות האנלוגיה הבאה: נניח שכתובת [IP](http://he.wikipedia.org/wiki/IP) היא כתובת של בניין מגורים. אם [מכתב](http://he.wikipedia.org/wiki/%D7%9E%D7%9B%D7%AA%D7%91) נשלח לכתובת מסוימת ללא מספר [דירה](http://he.wikipedia.org/wiki/%D7%93%D7%99%D7%A8%D7%94), לא ניתן לדעת למי הוא שייך. לכן על שולח המכתב לציין פרט לכתובת )IP( את מספר הדירה )Port(.

**שם לב!**

לא כל הפרוטוקולים [בשכבת התעבורה של מודל TCP/IP](http://he.wikipedia.org/wiki/%D7%A9%D7%9B%D7%91%D7%AA_%D7%94%D7%AA%D7%A2%D7%91%D7%95%D7%A8%D7%94_%D7%A9%D7%9C_%D7%9E%D7%95%D7%93%D7%9C_TCP/IP) משתמשים בפורטים.

**רישום פורטים**

פורטים מוכרים הם פורטים המשמשים פרוטוקולים מוגדרים כסטנדרט. הצורך בפורטים מוכרים קיים כדי לקבוע סטנדרטים בהתחברות לשרתים המספקים שירותים מסוימים. לדוגמה: על מנת שה[דפדפן](http://he.wikipedia.org/wiki/%D7%93%D7%A4%D7%93%D7%A4%D7%9F) יפנה [לאתר אינטרנט](http://he.wikipedia.org/wiki/%D7%90%D7%AA%D7%A8_%D7%90%D7%99%D7%A0%D7%98%D7%A8%D7%A0%D7%98) ב[-HTTP](http://he.wikipedia.org/wiki/HTTP), הדפדפן צריך לפנות לפורט פתוח על השרת שיקבל את הפניות אליו ויטפל בהן, והפורט הזה הוא הפורט המוכר לתעבורת HTTP - פורט 81.

הארגון האחראי על תיאום ורישום הפורטים המוכרים הוא IANA )קיצור של

:המחלק את מרחב הפורטים לשלושה )Internet Assigned Numbers Authority

Well Known Ports ,פורטים מוכרים - 1123 - 1

Registered Ports ,פורטים רשומים - 49151 - 1124

Dynamic or Private Ports ,פורטים פרטיים או דינמים - 65535 - 49152

**דוגמאות לפורטים רשומים**

1. - פרוטוקול העברת קבצים [)FTP](http://he.wikipedia.org/wiki/FTP)(.
2. - פרוטוקול [SSH.](http://he.wikipedia.org/wiki/Secure_Shell)
3. - פרוטוקול [Telnet.](http://he.wikipedia.org/wiki/Telnet)

25 - [דואר](http://he.wikipedia.org/wiki/%D7%93%D7%95%D7%90%D7%A8_%D7%90%D7%9C%D7%A7%D7%98%D7%A8%D7%95%D7%A0%D7%99) יוצא [)SMTP](http://he.wikipedia.org/wiki/SMTP)(.

53 - פרוטוקול [DNS](http://he.wikipedia.org/wiki/DNS)

68,67 - פרוטוקול הקצאת כתובות דינמית [)DHCP](http://he.wikipedia.org/wiki/DHCP)(.

81 - פרוטוקול העברת דפי [אינטרנט](http://he.wikipedia.org/wiki/%D7%90%D7%99%D7%A0%D7%98%D7%A8%D7%A0%D7%98) [HTTP.](http://he.wikipedia.org/wiki/HTTP)

111 - [דואר](http://he.wikipedia.org/wiki/%D7%93%D7%95%D7%90%D7%A8_%D7%90%D7%9C%D7%A7%D7%98%D7%A8%D7%95%D7%A0%D7%99) נכנס [)POP3](http://he.wikipedia.org/wiki/POP3)(.

161,162 - פרוטוקול [SNMP.](http://he.wikipedia.org/wiki/SNMP)

443 - פרוטוקול [HTTPs](http://en.wikipedia.org/wiki/HTTP_Secure) להעברת דפי אינטרנט מאובטחים.

1433 - פרוטוקול גישה לשרתי [SQL.](http://he.wikipedia.org/wiki/SQL)

שימוש ב-URL

כתובות [URL](http://he.wikipedia.org/wiki/URL) מתאימות כברירת המחדל את מספר הפורט בתחילית לפי רשימת הפורטים המוכרים.

http מפנה לפורט 81, https לפורט 443 וכן הלאה. כדי להגדיר פורט השונה מברירת המחדל, יש לציין אותו עם נקודתיים לאחר [שם התחום](http://he.wikipedia.org/wiki/%D7%A9%D7%9D_%D7%AA%D7%97%D7%95%D7%9D). למשל:

8111 בפורט HTTP מפנה לשרת http://www.example.com:8000/blah .וכך הדפדפן לא יפנה לפורט ברירת המחדל ,www.example.com בכתובת

# OSI מול מודל TCP\IP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TCP/IP | דוגמאות והערות |  | OSI | דוגמאות והערות |
| Application | HTTP, POP3, SMTP | 7 | Application | קישור בין התוכנה לרכיב התקשורת |
| 6 | Presentation | הגדרה של פורמטים: bin, |
|  |  |  |  | ascii,jpg |
| 5 | Session | בקרה של שיחות:התחלה,ניהול וסיום |
| Transport | TCP, UDP – **segment** | 4  3 | Transport | flow control ,בקרת שגיאה |
| Internet | IP, ICMP, ARP,DHCP–  **Packets** | Network | Logical address, routing and forwarding, path determination |
| Network access | Ethernet, Frame Relay, ADSL, PPP, **Frames** | 2 | Data link | מגדיר את הפורמט של ההדר  Frame Check ,והטריילר  **HDLC** ,)FCS( Sequence |
| 1 | Physical | **hub,**  :מחברים , כבלים **repeater** |

\* יש שטוענים כי שכבת Network access בנויה גם היא משתי שכבות כמו שכבה 2+1 במודל OSI

לפניכם מדריכים קצרים להסבר על הפרוטוקולים הנפוצים אנא התמקדו בהם ובאם יהיה לכם זמן הרחיבו את ידיעותיכם ע"י שתגלגלו את הפרוטוקלים.

**פרוטוקולים שחובה לדעת הם כדלקמן:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SSL  [Ethernet](http://he.wikipedia.org/wiki/Ethernet)  [10BASE-T](http://he.wikipedia.org/wiki/10BASE-T)  [802.11 WiFi](http://he.wikipedia.org/wiki/IEEE_802.11)  [Token ring](http://he.wikipedia.org/wiki/Token_ring) | FTP  DNS  DHCP  POP3 IMAP | IPV4 IPV6  HTTP  DHCP SMTP |  | Ethernet  Internet  [Telnet](http://he.wikipedia.org/wiki/Telnet)  UDP  TCP |

# Ethernet

? Ethernet אז מה זה

באופן כללי זוהי טכנולוגיה לתקשורת נתונים בשתי השכבות הראשונות של מודל OSI או TCP/IP .

בעבר הוצעו טכנולוגיות רבות על מנת לאפשר שידור מסודר של נתונים ברמה הפיסית. על מנת לאפשר שידור ללא התנגשויות וללא בלבול יש להתגבר על מספר קשיים. רוב השיטות לא הצליחו להתגבר על חלק מהמכשולים, או שסבלו מחוסר יעילות בשידור.

Ethernet הפכה להיות הטכנולוגיה הבלעדית למימוש התקשורת בשכבה הפיסית. זה קרה בשל העובדה שטכנולוגיה זו הצליחה להתגבר על כל המכשולים שניצבו בפני הטכנולוגיות המתחרות.

אז מהם היתרונות של הטכנולוגיה הנ"ל?

יתרון ראשון הוא בכך שטכנולוגיית ה-Ethernet מאפשרת לכל אחד מהמשתתפים ברשת לשדר במקביל, וללא התרעה מוקדמת לתווך המשותפת. זה מתאפשר בזכות טיפול יעיל בהתנגשויות.

הדבר מתבצע באופן הבא. כל אחד מהמשתתפים בודק אם התווך פנוי. הדבר מתבצע באמצעות מדידת מתח חשמלי בתווך. משתתף ששלח מנת נתונים ממשיך להאזין על הקו. במידה והוא חש שישנם נתונים נוספים שנשלחים במקביל, הוא שולח הודעת התנגשות וכל המשתתפים מפסיקים לשדר. כל אחד מגריל זמן המתנה שלאחריו ינסה לשדר.

יתרון נוסף הוא שימוש בזוגות שזורים. שימוש בפתרון זה מאפשרים לשפר את מאפייני האותות.

במילים אחרות האותות מועברים בקצב גדול יותר ולמרחקים גדולים יותר. עבור קצבים גבוהים במיוחד )מעל 111Mbps ( ישנו שימוש בסיב אופטי בעל תכונות טובות יותר מאשר זוגות שזורים.

יתרון חשוב נוסף הוא האפשרות להגדיל את קצב השידור בכפולות של 11 תוך שמירה על אותה מסגרת. הכוונה כאן היא בעצם שמירה על אותו פורמט של מנת נתונים. היתרון כאן הוא בכך שרכיבים בעלי קצב שידור שונה יכולים לתקשר ביניהם. יותר מזה ניתן לשדרג רכיב מסוים ברשת מבלי לשדרג את שאר הרכיבים.

## מבנה חבילת Ethernet

[חבילה](http://he.wikipedia.org/wiki/%D7%97%D7%91%D7%99%D7%9C%D7%AA_%D7%9E%D7%99%D7%93%D7%A2) בפרוטוקול Ethernet מורכבת מחמישה חלקים: מבוא, פתיח, תוכן, סוגר וגובל. אורכה של חבילה נע בין 84 ל- 1542 [בתים](http://he.wikipedia.org/wiki/%D7%91%D7%99%D7%AA_(%D7%9E%D7%97%D7%A9%D7%91))  בהתאם לגודל שדה התוכן.

)לזכור אנחנו מדברים על בתים ולא ביטים(

### מבוא

המבוא )Preamble( מורכב מסדרה של 7 [בתים](http://he.wikipedia.org/wiki/%D7%91%D7%99%D7%AA_(%D7%9E%D7%97%D7%A9%D7%91)) המכילים את הרצף 11111111 ואחריהם בית המכיל את הרצף 1111111**1** המסמן את סוף המבוא. מטרת המבוא היא לסנכרן את תחילת השידור באופן פיזי.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | בית |
| סיום מבוא |  |  |  | מבוא |  |  |  | תוכן |

### פתיח

הפתיח הבסיסי מורכב מ- 14 [בתים](http://he.wikipedia.org/wiki/%D7%91%D7%99%D7%AA_(%D7%9E%D7%97%D7%A9%D7%91)) לפי הפירוט הבא:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 14 | 13 | 12 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | בית |
| EtherType | |  |  | כתובת מקור | |  |  |  |  | כתובת יעד | |  |  | תוכן |

* כתובת יעד )שישה [בתים](http://he.wikipedia.org/wiki/%D7%91%D7%99%D7%AA_(%D7%9E%D7%97%D7%A9%D7%91))( - כתובת ה- MAC של רכיב היעד.
* כתובת מקור )שישה [בתים](http://he.wikipedia.org/wiki/%D7%91%D7%99%D7%AA_(%D7%9E%D7%97%D7%A9%D7%91))( - כתובת ה- MAC של רכיב המקור.

[EtherTyp e](http://en.wikipedia.org/wiki/EtherType) )שני [בתים](http://he.wikipedia.org/wiki/%D7%91%D7%99%D7%AA_(%D7%9E%D7%97%D7%A9%D7%91))( - שדה המציין את סוג הפרוטוקול של המידע אותו ההודעה מעבירה כתוכן )לדוגמא, עבור תוכן בפרוטוקול [IPv4](http://he.wikipedia.org/wiki/IPv4) יהיה ערך 1x0800 בעוד לתוכן בפרוטוקול [ARP](http://he.wikipedia.org/wiki/Address_Resolution_Protocol) יהיה ערך 1x0806(.

**הערה**: במידה והרשת עושה שימוש בפרוטוקול [רשת מקומית וירטואלית](http://he.wikipedia.org/wiki/%D7%A8%D7%A9%D7%AA_%D7%9E%D7%A7%D7%95%D7%9E%D7%99%D7%AA_%D7%95%D7%99%D7%A8%D7%98%D7%95%D7%90%D7%9C%D7%99%D7%AA) )812.1Q(, [המתג](http://he.wikipedia.org/wiki/%D7%9E%D7%AA%D7%92_(%D7%A8%D7%A9%D7%AA%D7%95%D7%AA_%D7%9E%D7%97%D7%A9%D7%91%D7%99%D7%9D)) אליו מחובר המחשב מוסיף לפתיח שדה "תווית [VLAN](http://he.wikipedia.org/wiki/%D7%A8%D7%A9%D7%AA_%D7%9E%D7%A7%D7%95%D7%9E%D7%99%D7%AA_%D7%95%D7%99%D7%A8%D7%98%D7%95%D7%90%D7%9C%D7%99%D7%AA)" בן ארבעה [בתים](http://he.wikipedia.org/wiki/%D7%91%D7%99%D7%AA_(%D7%9E%D7%97%D7%A9%D7%91)). שדה זה נושא את מזהה הרשת הוירטואלית לה שייך המחשב.

**תוכן**

שדה התוכן בחבילת Ethernet מכיל בין 46 ל- 1511 [בתים.](http://he.wikipedia.org/wiki/%D7%91%D7%99%D7%AA_(%D7%9E%D7%97%D7%A9%D7%91))

### סוגר

הסוגר של חבילת Ethernet מכיל שדה בן ארבעה [בתים](http://he.wikipedia.org/wiki/%D7%91%D7%99%D7%AA_(%D7%9E%D7%97%D7%A9%D7%91)) המורכב מסיכום ביקורת [)checksum(](http://he.wikipedia.org/wiki/Checksum), מספר האימות של הפתיח והתוכן.

### גובל

הגובל )[Interframe gap](http://en.wikipedia.org/wiki/Interframe_gap) ( הנו סדרה של 12 [בתים](http://he.wikipedia.org/wiki/%D7%91%D7%99%D7%AA_(%D7%9E%D7%97%D7%A9%D7%91)) המשודרים בסוף החבילה ומשמשים להפרדה לקראת תחילת השידור הבא.

## שכבת הקו

שכבת הקו בטכנולוגית Ethernet מתחלקת לשתי תת-שכבות:

1. )LLC ( Logical Link Control-שכבת ה
2. .)MAC ( Media Access Control-שכבת ה

### )LLC ( Logical Link Control-שכבת ה

לתת-שכבה זו שני תפקידים מרכזיים:

1. מהווה קישור בין [שכבת הערוץ](http://he.wikipedia.org/wiki/%D7%A9%D7%9B%D7%91%D7%AA_%D7%94%D7%A7%D7%95_%D7%A9%D7%9C_%D7%9E%D7%95%D7%93%D7%9C_%D7%94-OSI) [לשכבת הרשת](http://he.wikipedia.org/wiki/%D7%A9%D7%9B%D7%91%D7%AA_%D7%94%D7%A8%D7%A9%D7%AA_%D7%A9%D7%9C_%D7%9E%D7%95%D7%93%D7%9C_%D7%94-TCP/IP). בזכות שכבה זו אנו יכולים לציין במסגרת

)Frame( את הפרוטוקול ששימש [חבילת מידע](http://he.wikipedia.org/wiki/%D7%97%D7%91%D7%99%D7%9C%D7%AA_%D7%9E%D7%99%D7%93%D7%A2) זו [בשכבת הרשת](http://he.wikipedia.org/wiki/%D7%A9%D7%9B%D7%91%D7%AA_%D7%94%D7%A8%D7%A9%D7%AA_%D7%A9%D7%9C_%D7%9E%D7%95%D7%93%D7%9C_%D7%94-TCP/IP) [)](http://he.wikipedia.org/wiki/IP)[IPX,](http://he.wikipedia.org/wiki/IPX)[IP](http://he.wikipedia.org/wiki/IP)וכיוצא בזה(.

1. לעטוף את [חבילות המידע](http://he.wikipedia.org/wiki/%D7%97%D7%91%D7%99%D7%9C%D7%AA_%D7%9E%D7%99%D7%93%D7%A2) המגיעות [משכבת הרשת](http://he.wikipedia.org/wiki/%D7%A9%D7%9B%D7%91%D7%AA_%D7%94%D7%A8%D7%A9%D7%AA_%D7%A9%D7%9C_%D7%9E%D7%95%D7%93%D7%9C_%D7%94-TCP/IP) ב-Frame. יש לשים לב כי תת-שכבה זו אינה אחראית על ה-Frame עצמו, אלא על ההכנסה של המידע לתוך ה-Frame.

**)MAC ( Media Access Control-שכבת ה**

גם לתת-שכבה זו מספר תפקידים. העיקריים ביניהם הם:

# גישה לתווך

ניתן לדמות את המצב ברשת ה-Ethernet לדיון רב-משתתפים ללא מנחה. על מנת שהדיון יהיה פורה, יש לקבוע מראש כללי-דיון שימנעו ככל הניתן מצב שבו שני משתתפים ידברו בו זמנית. באופן אנלוגי, מכיוון שרשת ה-Ethernet היא [רשת מבוזרת](http://he.wikipedia.org/w/index.php?title=%D7%A8%D7%A9%D7%AA_%D7%9E%D7%91%D7%95%D7%96%D7%A8%D7%AA&action=edit&redlink=1) שבה מדיית התקשורת [)השכבה הפיזית](http://he.wikipedia.org/wiki/%D7%94%D7%A9%D7%9B%D7%91%D7%94_%D7%94%D7%A4%D7%99%D7%96%D7%99%D7%AA_%D7%A9%D7%9C_%D7%9E%D7%95%D7%93%D7%9C_%D7%94-OSI)( משותפת לכל הרכיבים ברשת, יש צורך למנוע שידור בו זמני של שתי תחנות לאותו [מתחם התנגשות.](http://he.wikipedia.org/wiki/%D7%9E%D7%AA%D7%97%D7%9D_%D7%94%D7%AA%D7%A0%D7%92%D7%A9%D7%95%D7%AA)

תת-שכבת ה-MAC מסדירה את תיזמון הגישה למדיית התקשורת של רשת ה-Ethernet כך שבכל רגע נתון רק תחנה אחת תשדר על מדיית התקשורת. האופן שבו היא עושה זאת מבוסס על [אלגוריתם](http://he.wikipedia.org/wiki/%D7%90%D7%9C%D7%92%D7%95%D7%A8%D7%99%D7%AA%D7%9D) [**CSMA/CD**](http://he.wikipedia.org/wiki/CSMA/CD) שבו תחנה משדרת מסגרת )frame( ברגע שהיא חשה שמדיום התקשורת פנוי. במהלך שידור המסגרת, התחנה מאזינה לקווי התקשורת על מנת לוודא שהאות שהתקבל הוא אכן האות שנשלח. במידה והתחנה מזהה הפרעה היא תפסיק את שליחת המסגרת ותשלח אות התנגשות )jam signal( אשר יגרום לכל התחנות ברשת להפסיק מיד את השידור. לאחר פרק זמן אקראי, חוזרת התחנה לשדר את המסגרת. אם נוצרת התנגשות נוספת, נשלח שוב אות התנגשות וכל אחת מהתחנות מכפילה את זמן ההמתנה שהגרילה על מנת להקטין את הסיכוי להתנגשות נוספת.

Ethernet הוא פרוטוקול המבטיח רק [מאמץ מיטבי](http://he.wikipedia.org/wiki/%D7%9E%D7%90%D7%9E%D7%A5_%D7%9E%D7%99%D7%98%D7%91%D7%99). אם חלו 16 התנגשויות או תקלות בהעברת חבילה מסוימת, ה-Ethernet יסיים את ניסיונות השליחה של החבילה הזאת. כמו כן, ה-Ethernet ידווח לשכבת התקשורת שמעליו על כישלון בשליחת החבילה. מרגע זה, השכבה הגבוהה יותר אחראית על הטיפול בבעיה. השכבה שיכולה ומבקשת שידור חוזר במקרה של שגיאות הינה כל שכבה שמשתתפת בתהליך התקשורת, מהשכבה השלישית ועד השכבה השביעית )במודל OSI(.

# השכבה הפיזית

**Autonegotiation Autonegotiation** הוא מנגנון ב-Ethernet לניהול משא ומתן בין התקנים שונים ברשת מקומית [)נתב](http://he.wikipedia.org/wiki/%D7%A0%D7%AA%D7%91) [למחשב](http://he.wikipedia.org/wiki/%D7%9E%D7%97%D7%A9%D7%91), למשל(, כך שהם יבחרו במאפייני שידור מידע, כמו קצב השידור ביניהם וכיווניות השידור )Half-duplex או Full-duplex(, שקיימים אצל שניהם. השאיפה במנגנון היא להשיג את קצב העבודה המרבי, בהתאם ליכולת שני הצדדים.

# משחזרים ורכזות

תופעות של דעיכת אותות ובעיות תזמון מגבילות את אורכם המקסימלי של מקטעי Ethernet, כתלות במדיית התקשורת. לדוגמה, לכבלים הקואקסיאליים 11BASE5 יש הגבלת אורך מקסימלי של 511 מטר. על מנת להגדיל את טווח הרשת נעשה שימוש [במשחזר](http://he.wikipedia.org/wiki/Repeater) )Repeater(, המגביר ומנקה את האות, מוסיף Preamble ומעביר אותו הלאה. ניתן להשתמש במשחזרים על מנת לחבר עד חמישה מקטעי אתרנט, כאשר לשלושה מתוכם מחוברים התקנים. הוספה של יותר מחמישה משחזרים תגרום לבעיה כיוון שכל משחזר בנוסף לפעולת ההגברה מוסיף עוד ביטים של PREAMBLE ולכן תיגרם חריגה ממסגרת ה ETHERNET.

עם המעבר לשימוש [בזוגות שזורים](http://he.wikipedia.org/wiki/%D7%96%D7%95%D7%92_%D7%A9%D7%96%D7%95%D7%A8) היה צורך בהתקן שיאפשר תקשורת של מספר התקנים על מדיה משותפת, לשם כך נוצרו משחזרים רב ערוציים הידועים בשמם [רכזות](http://he.wikipedia.org/wiki/%D7%A8%D7%9B%D7%96%D7%AA) )hubs(. כיום נפוץ יתר השימוש [במתגים](http://he.wikipedia.org/wiki/%D7%9E%D7%AA%D7%92_(%D7%A8%D7%A9%D7%AA%D7%95%D7%AA_%D7%9E%D7%97%D7%A9%D7%91%D7%99%D7%9D)) המשמשים כרכזות חכמות.

[**DHCP**](http://www.adir.me/introduction-to-dhcp/)

**DHCP )בעברית: פרוטוקול הגדרת מארחים דינמי(:**

DHCP, או בשמו המלא Dynamic Host Configuration Protocol, הוא פרוטוקול תקשורת המשמש להקצאה דינמית של כתובות IP למחשבים ברשת מקומית )LAN(.

מנהל הרשת מגדיר לשרת ה- DHCP תחום כתובות וכל מחשב ברשת מוגדר לבקש את כתובת ה- IP שלו מהשרת ברגע שהוא מתחבר לרשת.

הכתובת מוקצית למחשב לזמן מוגבל, בסופו אם המחשב לא יבקש לחדש את הכתובת שניתנה לו הכתובת תחזור למאגר כתובות ה- IP הזמינות והשרת ייתן אותה למחשב הבא שירצה להתחבר לרשת.

**למה צריך DHCP:**

בואו נתחיל בזה שלא חייב להשתמש ב- DHCP, ניתן להגדיר רשת גם בלעדיו, היא תעבוד והכל יהיה בסדר.

אז למה כן להשתמש ב- DHCP? בואו נדמיין מצב מסויים, רשת מסויימת, הרשת בסניף הקרוב של חברת הפלאפון שלכם.

נגיד שבאותו סניף יש 21 מחשבים, חלקם לשימוש אנשי המכירות, חלקם לשימוש אנשי התמיכה, חלקם בכלל בתוך המעבדה, אבל בסופו של דבר כולם שייכים לאותה רשת.

לכם, בתור מנהלי הרשת, יש 2 אופציות:

**האופציה הראשונה:** לעבור בין כל המחשבים, 21 מחשבים אמרנו, להגדיר להם כתובת IP, שרתי Subnet mask ,DNS, שער ברירת מחדל וכו'.

להגדיר בכולם את אותם הפרטים )פרט לכתובת ה- IP( – הרי אמרנו שהם שייכים לאותה רשת.

**האופציה השנייה:** להגדיר את כל הפרטים הללו במקום אחד, בשרת ה- DHCP.

כל מחשב שירצה לקבל את הפרטים הללו, שהם חיוניים עבור התקשורת שלו ברשת, יפנה לשרת הזה ויבקש ממנו אותם.

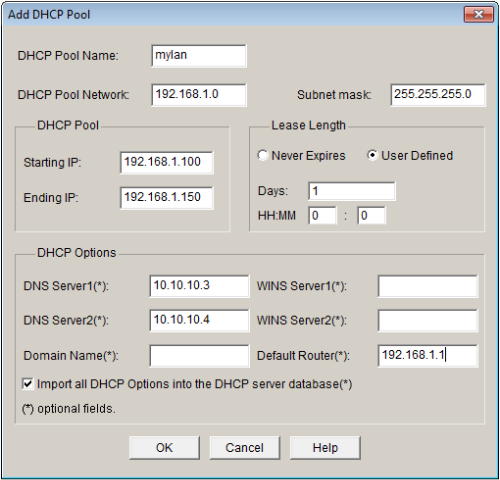
מה יותר פשוט? מה יותר נוח? במה תבחרו? אני מניח שברוב המקרים באופציה השנייה –

.DHCP בשרת

**איך מגדירים שרת DHCP:**

חשוב לדעת שגם ראוטרים וגם מחשבים יכולים לתפקד כשרתי DHCP, כל עוד הם תומכים בכך )ברמת התוכנה(.

לצורך המאמר אשתמש בתמונה המדגימה הגדרת שרת DHCP בראוטר של סיסקו.



**הסבר קצר על כל הגדרה:**

DHCP Pool Name – השם של המאגר )לא קריטי(.

.כתובת הרשת – DHCP Pool Network

Subnet mask – ה- subnet mask של הרשת. Starting IP – כתובת ה- IP הראשונה בטווח הכתובות שהשרת יחלק.

Ending IP – כתובת ה- IP האחרונה בטווח הכתובות שהשרת יחלק.

Lease Length – זמן ההשאלה, כמה זמן כתובת שהוקצתה עבור מחשב מסויים צריכה להישמר עבורו.

DHCP Options – כל הפרטים שכבר הזכרנו )שרתי DNS, שרתי WINS, שער ברירת מחדל

וכו'(.

קיימת עוד הגדרה שלא רואים במסך הזה, והיא הקצאת כתובות IP מסויימות עבור מחשבים ספציפיים.

בואו נחזור לסניף של חברת הפלאפון שלכם, בין כל המחשבים שם, סביר להניח שיש להם מחשב אחד שמוגדר כשרת?

שרת שעליו שמור כל המידע והמחשבים האחרים שואבים אותו ממנו, שרת שדרכו מתקשרים עם סניפים אחרים של אותה חברה וכד',

לשרת הזה – צריך שתהיה כתובת IP קבועה, רצוי לפחות שתהיה כתובת IP קבועה, הרי איך שאר המחשבים יוכלו לתקשר ספציפית איתו כאשר כתובות ה- IP מחולקות באופן דינמי ע"י שרת ה- DHCP ולא מוגדרות באופן קבוע במחשב עצמו.

בדיוק בשביל מקרים כאלו ניתן להגדיר שכתובות מסויימות יהיו שמורות עבור מחשבים מסויימים )על פי כתובת ה- MAC שלהם( ורק אותם מחשבים יוכלו לקבל אותן משרת ה- DHCP, ככה אומנם השרת מקבל את כתובת ה- IP שלו משרת ה- DHCP, אבל הוא מקבל את אותה הכתובת ורק הוא רשאי לקבל אותה, הכתובת שלו קבועה ואם נרצה לפנות אליו נדע לאיזה כתובת לפנות.

**איך זה עובד:**

למען האמת, זה די פשוט – תוך 4 פעולות, 2 מצד המחשב ו- 2 מצד השרת, התהליך מושלם.

תוך 4 פעולות, שמתחילות אוטומטית ברגע שהמחשב מזהה שהוא מחובר לרשת אך לא קיימים אצלו שום פרטים מעבר לזה, הוא מקבל את כל מה שהוא צריך.

**הפעולה הראשונה** – אותה מבצע **המחשב** – היא DHCP Discovery.

המחשב שולח בקשה ברשת, בקשה שמגיעה לכל מי שמחובר לרשת,

ובשפה פשוטה, הוא שואל: "שלום, אני חדש פה, האם יש פה איזה שרת DHCP שמוכן בבקשה לטפל בי?".

**הפעולה השנייה** – אותה מבצע **השרת** – היא DHCP Lease Offer.

שרת ה- DHCP מקבל את ההודעה ששלח המחשב, שומר בצד כתובת IP עבורו )עדיין לא מקצה לו אותה(,

ועונה לו: "שלום לך, אני שרת DHCP, אני יכול להקצות עבורך את הכתובת 1.2.3.4 ולספק לך את שאר הפרטים שאתה צריך, מעוניין?".

**הפעולה השלישית** – אותה מבצע **המחשב** – היא DHCP Request.

המחשב מקבל את ההודעה שהחזיר לו השרת, הוא ממש שמח שהוא מצא שרת DHCP,

ועונה לו: "כן, אשמח לקבל את הכתובת הזאת ואת שאר הפרטים, תוכל בבקשה לתת לי אותם?".

**הפעולה הרביעית** – אותה מבצע **השרת** – היא DHCP Lease Acknowledgement.

השרת מקבל את ההודעה שהחזיר לו המחשב, הוא מסיר את הכתובת ששמר מרשימת הכתובת הפנויות, מקצה אותה עבור המחשב,

ועונה לו: "כמובן, הנה הכתובת ושאר הפרטים שביקשת, אני מקווה שתהנה ברשת ושיהיה לך יום טוב".

בסיום התהליך הזה, מקבל המחשב את הפרטים שהוא ביקש והוא שייך לרשת באופן רשמי.

**הסבר קצת יותר קליל על מזה DHCP.?**

ראשית, עלינו להבין מהו MAC address. לכל רכיב רשת, ישנו כתובת MAC. כתובת זו היא כתובת שצרובה **פיזית** בכרטיס הרשת והינה **ייחודית** )בעולם(. לכל יצרן של כרטיסי רשת יש טווח של כתובות ייחודיות שרק הוא יכול לחלק. חשוב לא לבלבל בין כתובת IP לכתובת MAC – מדובר בשני מושגים שונים. ניתן לומר שכתובת ה-MAC היא הכתובת האמיתית של המחשב בעוד שכתובת ה-IP היא כתובת וירטואלית שמשתמשים בה באינטרנט או בכל רשת שמיישמת TCP/IP )כולל הרשת הביתית שלנו(. מה הכוונה כתובת "אמיתית"? אם נקליד בדוס )start, run, cmd( את הפקודה ipconfig /all נוכל לצפות בכתובת ה-MAC שלנו. לדוגמה:



ב-DHCP ישנו שרת וקליינט: ישנו מי שמחלק את הכתובות )DHCP server( ואת מי שמבקש אותם )DHCP Client(. כאשר כרטיס הרשת שלנו נמצא ב[-Optain IP automatically](http://www.timewarnercable.com/MediaLibrary/4/55/Content%20Management/In%20the%20Community/UTSAimages/utsa-support-IP.gif),

כשהמחשב עולה, הוא "צועק" בכל הרשת שהוא צריך כתובת IP. הכתובת שהמחשב מזדהה

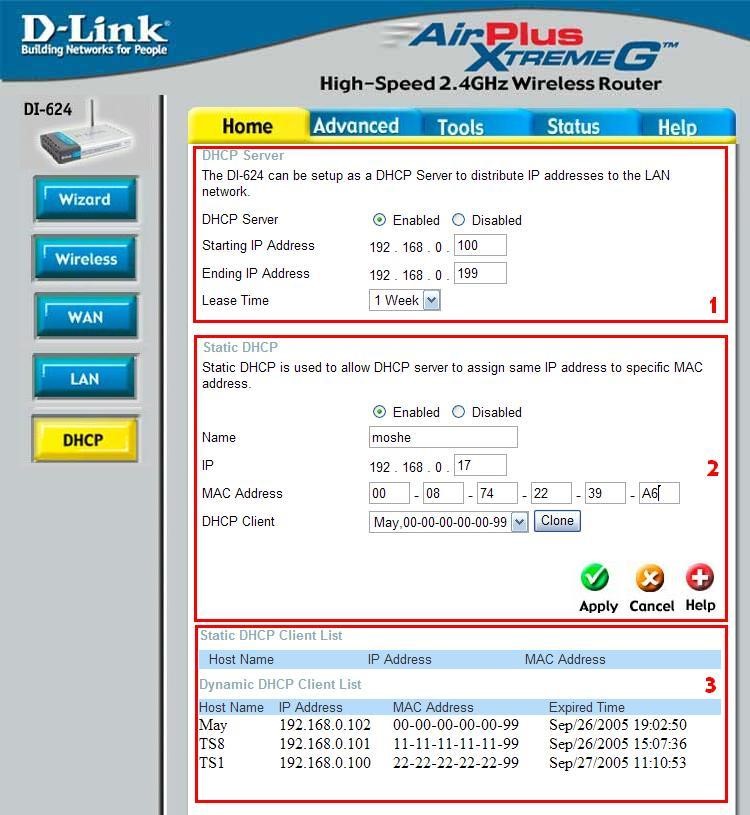
.MAC address-איתה היא ה

"אני 46-39-22-74-18-11 ואני רוצה כתובת IP"

אם יש שרת DHCP ברשת, הוא מחזיר למחשב שלנו תשובה שמכילה בתוכה את כתובת ה-IP שהשרת חילק למחשב, כתובות של שרתי DNS ועוד… שרת ה-DHCP מחלק למחשב שלנו כתובת לתקופה מסוימת. תקופה זו נקראת Lease Time. כאשר זמן זה נגמר, המחשב שלנו מבקש משרת ה-DHCP כתובת שוב. אם המחשב שלנו לא ביקש, שרת ה-DHCP יכול לתת למחשב אחר את הכתובת הישנה שלנו.

לפעמים, יש לנו צורך לשריין כתובת ברשת הפנימית שלנו )לא כתובת חוקית( עבור מחשב מסוים. אנחנו מעוניינים שמחשב מסוים ברשת תמיד יקבל את אותה כתובת ה-IP )למשל כשעושים port forwarding(. ניתן לעשות זאת בקלות.

ניקח לדוגמה נתב D-link



במסגרת שמספרה **1** ניתן לראות ששרת ה-DHCP מופעל. טווח הכתובות ששרת ה-DHCP יחלק לרשת הוא 192.168.1.111 עד 199.192.168.1 )הנתב יוכל לחלק ל-111 מחשבים כתובות IP(. ה-Lease Time הוא שבוע.

במסגרת שמספרה **2** ניתן לראות כיצד ניתן לשריין כתובת IP בשרת ה-DHCP. במקרה זה שיריינתי כך שהמחשב של משה, עם ה-MAC address שלו, תמיד יקבל את הכתובת 192.168.1.17 לזמן בלתי מוגבל.

במסגרת שמספרה **3** ניתן לראות את הדוחות. ניתן לראות את השמות של המחשבים ברשת, כתובת ה-MAC שלהם, ואיזה כתובת IP הקצה להם הנתב.

**יתרונות וחסרונות בעבודה עם שרת DHCP:**

**היתרון** העיקרי בשימוש בשרת DHCP הוא תפעול קל וגמיש יותר של הרשת.

ברגע שכל הפרטים מוגדרים ונשלטים ממקום אחד שמספק אותם לשאר המחשבים, הרבה יותר קל להגדיר ולשנות אותם במידת הצורך.

דוגמה נוספת היא שבמקרה ומחשב קורס ושמים במקומו מחשב אחר, לא צריך להתחיל לחפש מה הייתה כתובת ה- IP של המחשב הקודם ולהגדיר אותה במחשב החדש, פשוט מחברים אותו לרשת והוא שואב את הפרטים משרת ה- DHCP.

**החסרון** העיקרי בשימוש בשרת DHCP, בדומה ליתרון, הוא גם כן העובדה שכל הפרטים מוגדרים ונשלטים ממקום אחד.

אם השרת קורס או נתקל בבעיה כלשהי, כל הרשת בבעיה.

אם השרת מותקף, מתבצע ניסיון לזייף זהות של שרת DHCP או לחילופין לזייף זהות של מחשב מסויים, ניתן לגרום נזק רב לרשת.

**כתובות ip**

[**Subnetting & Basic IP Addressing**](http://www.adir.me/basic-ip-addressing-subnetting/)

נלמד לעבוד עם בינארי, אסביר מהי כתובת IP )תוך התייחסות ל- IPv4 בלבד(, מהי Subnet Mask ומהו Default Gateway, אסקור את ההבדלים בין כתובות פרטיות לכתובות ציבוריות ואסביר בקצרה כיצד מגדירים רשת.

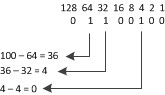
המאמר מיועד לקהל יעד בעל הבנה מינימלית-בסיסית במחשבים וברשתות תקשורת.

**עבודה עם בינארי:**

כדי להבין את המדריך, נצטרך לדעת לעבוד עם ערכים בינארים ולהמיר ערך דצימלי לערך בינארי ולהיפך.

נעבוד עם 8 סיביות בצורה הבאה )כל מספר מייצג ביט(: 1 2 4 8 16 32 64 128 נתחיל מהערך הגדול )128( לקטן )1(, עבור כל סיבית שהערך שלה נכנס במספר שברצוננו להמיר נסמן 1 ונפחית את הערך שלה מהמספר הנתון, במידה וערך הסיבית גדול מהמספר הנתון נסמן 1 ונמשיך הלאה לסיבית הבאה עד שנגיע ל- 1, אם הגענו ל- 1 לפני הסוף נסמן 1 בכל הסיביות שנשארו.

לדוגמה – נמיר את המספר 111 לבינארי.



מכאן הבנו שהערך הבינארי של 111 הוא 11111111, תרגלו בעצמכם המרה של כמה מספרים מבסיס אחד לשני, חשוב להבין את זה כדי להמשיך הלאה.

בהמרה עם 8 ביטים בצורה הזאת, ניתן להמיר מספרים בין 1 )11111111( ל- 255

.)11111111(

## :)IP בעברית: כתובת( IP Address

כתובת IP הינה מזהה ייחודי הניתן למכשירים )מחשבים, נתבים וכד'( ברשת IP על מנת שיוכלו לתקשר ביניהם. הכתובת מורכבת מ- 32 סיביות המחולקים ל- 4 חלקים של 8 סיביות כל אחד )נקראים גם octets( המופרדים ביניהם בנקודה ).(. נהוג להמיר את הכתובת לערך דצימלי, כך שכל אחד מארבעת חלקי הכתובת מכיל מספר בטווח 255-1.

כתובת IP לדוגמה: 743.125.231.8 )בבינארי:

.)11111111.11111111.11111111.11111111

בנוסף, ניתן לחלק את כתובות ה- IP ל- 5 מחלקות/ רשתות, A-E, אנו נתייחס לרשתות A-C בלבד היות והן הרשתות שבהן נעשה השימוש העיקרי כיום.

את המחלקה/ הרשת של כתובת ה- IP ניתן לזהות על פי ה- **octet** )החלק( הראשון בכתובת:

**רשת A** מכילה את הכתובות שבהן ה- octet הראשון הינו בטווח 127-1.

**רשת B** מכילה את הכתובות שבהן ה- octet הראשון הינו בטווח 191-128.

**רשת C** מכילה את הכתובות שבהן ה- octet הראשון הינו בטווח 223-192.

**Subnet Mask )בעברית: מסכת רשת משנה(:**

subnet mask הינה הגדרה בעלת מבנה זהה לזה של כתובת IP הבאה במטרה להגדיר איזה חלק מהכתובת מסמל את הרשת ואיזה חלק מסמל את המכשיר )לדוג': מחשב(.

בעזרת subnet masks ניתן לחלק כל אחת מן הרשתות המוזכרות לעיל לתת-רשתות וכך בעצם ניתן ליצור מספר רשתות גדול יותר בצורה משמעותית לעומת כמות הרשתות שיכולנו ליצור בשימוש ברשתות הקיימות במחלקות A-C בלבד.

כשמגדירים subnet mask חובה לשמור על רצף של 1 )המשמש לציון הרשת( ולאחר מכן רצף של 1 )המשמש לציון הרכיבים(, רצוי לכתוב את ה- subnet mask בבינארי לפני שהופכים אותו לדצימלי בכדי לוודא את תקינות ההגדרה.

כאשר לא נגדיר subnet mask, יעשה שימוש בהגדרת ברירת המחדל שהוגדרה עבור הרשת )A-C( של הכתובת בה השתמשנו -

**ברשת A** ברירת המחדל היא 255.1.1.1 \ 11111111.11111111.11111111.11111111, הרשת מוגדרת ע"י ה- octet הראשון בכתובת )8 bits(, הרכיבים ע"י שלושת האחרים )24

.)bits

**ברשת B** ברירת המחדל היא 255.255.1.1 \

,11111111.11111111.11111111.11111111

הרשת מוגדרת ע"י שני ה- octets הראשונים בכתובת )16 bits(, הרכיבים ע"י שני האחרים )16

.)bits

**ברשת C** ברירת המחדל היא 255.255.255.1 \

,11111111.11111111.11111111.11111111

הרשת מוגדרת ע"י שלושת ה- octets הראשונים בכתובת )24 bits(, הרכיבים ע"י האחרון )8

.)bits

**דוגמאות:**

11111111.11111111.11111111.11111111 \ 255.255.255.224 – **תקין subnet mask**

)קיים רצף תקין של 1 ו- 1(.

\ 255.255.255.153 – **לא תקין subnet mask**

11111111111111.11111111.11111111.11 )לא קיים רצף תקין של 1 ו- 1(.

**Default Gateway )בעברית: שער ברירת מחדל(:**

default gateway הינו כינוי לרכיב ברשת שתפקידו לאפשר ולנתב תקשורת בין הרשת הפנימית לרשתות אחרות, לרוב נשתמש בראוטר )שזה תפקידו העיקרי( בתור שער ברירת מחדל.

כשנגדיר רשת ונרצה להגדיר שרת ברירת מחדל, נפנה אליו באמצעות כתובת ה- IP שלו.

**כתובות ציבוריות וכתובות פרטיות:**

כתובות ציבוריות הינן כתובות IP המסופקות לנו ע"י ספק שירותי האינטרנט )ISP( שלנו, בכתובות אלו אפשר להשתמש גם בתוך הרשת המקומית וגם מחוץ אליה.

אחד החסרונות בשימוש בכתובות ציבוריות בתוך הרשת הפנימית הוא שאנו צריכים לרכוש אותן מהספק שלנו וזה עולה כסף, חסרון נוסף הוא שאם לכל רכיב ברשת שלנו תהיה כתובת ציבורית, גדל הסיכוי שיהיו יכולים לגשת לרכיבים ושירותים שלא היינו רוצים לאפשר אליהם גישה מחוץ לרשת המקומית.

מעבר לכך, כתובות ה- IP הציבוריות היו נגמרות מזמן אם לכל רכיב, בכל רשת פנימית, בכל העולם, הייתה כתובת ציבורית.

כתובות פרטיות הינן כתובות IP שאנו יכולים להשתמש בהן כרצוננו, ללא שום רכישה או התערבות של הספק שלנו. בניגוד לכתובות ציבוריות, לכתובות פרטיות אי אפשר לגשת מחוץ לרשת הפנימית, לא צריך לרכוש אותן מאף אחד והן לא מוגבלות לשימוש בודד )היות ומחוץ לרשת שלכם אי אפשר בכלל לדעת באיזה כתובות פרטיות אתם משתמשים(.

ישנם מספר טווחים שהוקצו לטובת כתובות פרטיות -

11.255.255.255 – 11.1.1.1

172.31.255.255 – 172.16.1.1

192.168.255.255 – 192.168.1.1

**:Subnetting**

אחרי שלמדנו והבנו כמה מושגים בסיסיים, הגיע החלק המעשי – איך מגדירים subnet masks.

ניתן להגדיר subnet masks על פי שני עקרונות: כמות הרשתות הרצויה או כמות הרכיבים הרצויה בכל רשת.

ב- 2 ההדגמות נשתמש בכתובת הרשת הבאה: 192.168.1.1

נתחיל עם הגדרה על פי **כמות רשתות רצויה**:

**שלב ראשון -** הגדרת כמות הרשתות הרצויה, המרת המספר לבינארי ומציאת כמות הביטים הדרושה לייצוג אותו מספר, לצורך הדגמה נצטרך 5 רשתות.

לאחר שנמיר את המספר 5 לבינארי נקבל 11111111, כמו שניתן לראות השתמשנו ב- 3 ביטים )11111111( כדי להגדיר את כמות הרשתות.

**שלב שני -** הצבת כמות הביטים הנחוצה ב- subnet mask ותחימת הטווחים ברשת.

כפי שניתן לראות אנו משתמשים בכתובת IP מרשת C )ה- octet הראשון הינו 192(, אנו יודעים שה- subnet mask ברירת המחדל של רשת זו הינה 255.255.255.1, או

11111.11111111.1111111111111111.111 בייצוג בינארי.

הסברנו שאנו משתמשים ב- 1 להגדרת הרשת וב- 1 להגדרת הרכיבים, לכן נגדיר 3 ביטים )כמות הביטים הדרושה לייצוג כמות הרשתות הרצויה( עבור הרשת ו- 5 ביטים עבור הרכיבים ונקבל: 11111111.11111111.11111111.11111111.

נמיר את ה- subnet mask שהתקבל לערכים דצימלים ונקבל: 255.255.255.224.

כדי לתחום את הטווחים ברשת נבצע את הפעולה הבאה -

מצאנו שצריך 3 ביטים כדי להגדיר 5 רשתות והצבנו אותם בצורה הבאה: 11111111, נבחר את ערכו של הביט הנמוך ביותר בו אנו משתמשים, במקרה הזה זה יהיה הביט השלישי משמאל )הראשון משמאל הוא 128, השני הוא 64, השלישי הוא 32 וכך הלאה(, הערך הנמוך ביותר הינו 32 וזה ישמש אותנו לתחימת הרשת בצורה הבאה:

192.168.1.31 – 192.168.1.1

192.168.1.63 – 192.168.1.32

192.168.1.95 – 192.168.1.64

192.168.1.127 – 192.168.1.96

192.168.1.159 – 192.168.1.128

עכשיו נעבור להגדרה על פי **כמות הרכיבים הרצויה בכל רשת**:

**שלב ראשון -** הגדרת כמות הרכיבים המירבית בכל רשת, המרת המספר לבינארי ומציאת כמות הביטים הדרושה לייצוג אותו מספר, לצורך הדגמה נצטרך 31 רכיבים בכל רשת.

לאחר שנמיר את המספר 31 לבינארי נקבל 11111111, כמו שניתן לראות השתמשנו ב- 5 ביטים )11111111( כדי להגדיר את כמות הרכיבים.

**שלב שני -** הצבת כמות הביטים הנחוצה ב- subnet mask, מציאת כמות הרכיבים המירבית בכל רשת ותחימת הטווחים ברשת.

כפי שניתן לראות אנו משתמשים בכתובת IP מרשת C )ה- octet הראשון הינו 192(, אנו יודעים שה- subnet mask ברירת המחדל של רשת זו הינה 255.255.255.1, או

11111111.11111111.11111111.11111111 בייצוג בינארי.

הסברנו שאנו משתמשים ב- 1 להגדרת הרכיבים וב- 1 להגדרת הרשת לכן נגדיר 5 ביטים )כמות הביטים הדרושה לייצוג כמות הרכיבים הרצויה( עבור הרכיבים ו- 3 ביטים עבור הרשת ונקבל: 11111111.11111111.11111111.11111111.

נמיר את ה- subnet mask שהתקבל לערכים דצימלים ונקבל: 255.255.255.224.

כדי לתחום את הטווחים ברשת נבצע את הפעולה הבאה -

מצאנו שצריך 5 ביטים כדי להגדיר 31 רכיבים בכל רשת והצבנו אותם בצורה הבאה:

11111111,

נבחר את ערכו של הביט הנמוך ביותר בו אנו משתמשים, במקרה הזה זה יהיה הביט השלישי משמאל )הראשון משמאל הוא 128, השני הוא 64, השלישי הוא 32 וכך הלאה(, הערך הנמוך ביותר הינו 32 וזה ישמש אותנו לתחימת הרשת בצורה הבאה:

192.168.1.31 – 192.168.1.1

192.168.1.63 – 192.168.1.32

192.168.1.95 – 192.168.1.64

192.168.1.127 – 192.168.1.96

192.168.1.159 – 192.168.1.128

**יש לשים לב** שאי אפשר לשייך את הכתובת הראשונה והכתובת האחרונה בכל טווח לרכיבים ברשת, הכתובות הללו שמורות ולא ניתן להשתמש בהן,

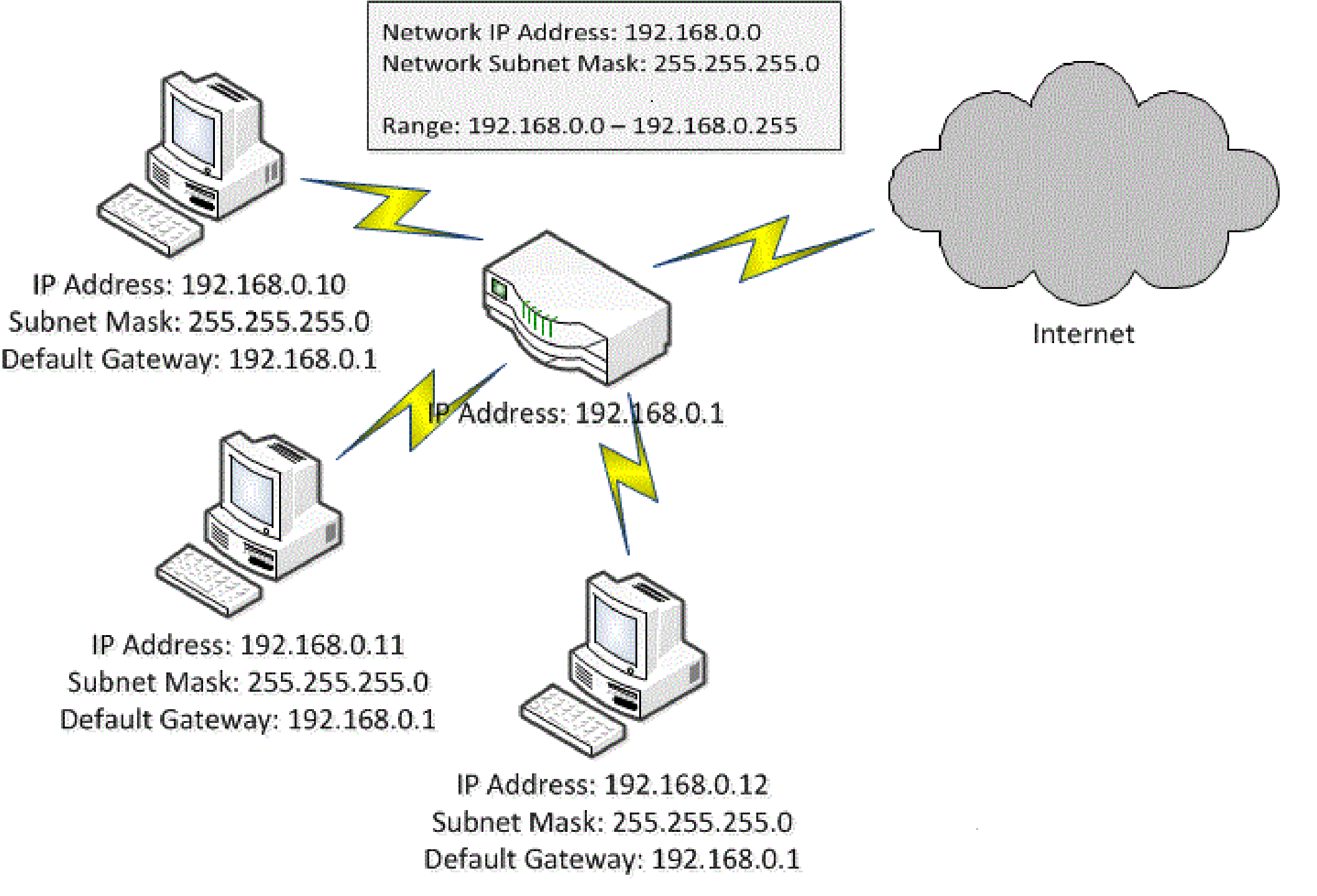
הכתובת הראשונה מציינת את כתובת הרשת והכתובת האחרונה הינה כתובת המשמשת ל- broadcast )לא ניכנס לזה כרגע(.

**חשוב לדעת!**

לכל רכיב ברשת IP חובה להגדיר IP address כדי שנוכל לתקשר איתו, לכל רשת IP חובה שתהיה subnet mask כדי לתחום את טווח הכתובות שלה,

הגדרת default gateway אינה בגדר חובה והיא דרושה רק במידה ורוצים לתקשר אל מחוץ לרשת המקומית.

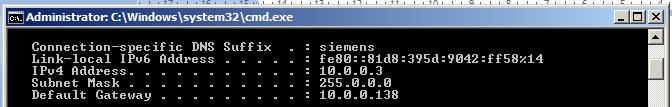
**הגדרת רשת לדוגמה:**



## :routers נתבים

בכדי לחבר בין שני רשתות אנו משתמשים בנתבים שמחברים בין הרשתות בדרך כלל בין רשת פנימית לרשת העולמית דרך isp הגדרות של הנתב הם חשובות וקריטיות לכל מנהל רשת כיום רוב הנתבים הביתיים יש להם ממשק גרפי זאת אומרת את הפקודות לא צריך להקליד ולשלוח לנתב אלא אנו נכנסים לנתב באמצעות הדפדפן ע"י רישום של כתובת IP של הנתב בשורת URL איך יודעים מה כתובת הנתב שלי?

כתיבת הפקודה ipconfig בממשק cli )בכדי להגיע לממשק הפקודה לוחצים על win+r לאחר מכן כותבים את הפקודה cmd למי ששכח(



בשורה השלישית כתוב Default Getaway זהו כתובת הנתב שלי 11.1.1.138 לאחר כתיבת הכתובת בדפדפן אנו נקבל שם משתמש וסיסמא בדרך כלל רשום על הנתב )אם לא אפשר להיכנס לאתר היצרן ולחפש את הגדרות ברירת מחדל(

לאחר ההגדרות הרגילות של הנתב לחיבור עם isp את הפרטים המדויקים אנו צריכים לקבל מהספק בקישור שלפניכם יש את ההגדרות של רוב ספק הISP <http://www.netcheif.com/Articles/BrdBandDefs/BrdBandDefs.htm>

אנחנו צריכים להכיר את דרכי הפעולה של הנתב איך בדיוק הוא יודע לאן להעביר הודעה איך זה שאנחנו לא משלמים על כל מחשב ברשת על שימוש באינטרנט ואיך זה בכלל עובד

**מה זה NAT?**

מי שיודע למה יש צורך ב-NAT, מה זה כתובת IP לא חוקית, DHCP, ומושגים

,source port אחרים כמו

הפרק הראשון עוסק במבוא ומושגי יסוד. מדובר במושגים שקשורים לנושא וחובה להכיר אותם כדי להבין מה זה NAT.

כדי להבין מדוע פותח ה-NAT, יש לחזור להיסטוריה של האינטרנט עצמו. ניתן לומר שהאינטרנט התפתח מעבר לצפוי. הרשת תוכננה למטרות מחקריות וצבאיות והפרוטוקול TCP/IP שמשתמשים בו היום )גרסה 4 או IPv4(, לא תוכנן להכיל כ"כ הרבה משתמשים או תחנות קצה. בנוסף, ישנם כתובות רבות שמבוזבזות. דוגמה מעולה לבזבזנות שכזו מתקיימת כאשר ברצונך לרכוש כתובת IP אחת. במקרה הגרוע ביותר, בעצם הרכישה, הינך מבזבז בעצם 3 כתובות: עפ"י התקן, כתובת אחת מייצגת את הרשת )היא מהווה בעצם את "השם של הרשת"(, כתובת אחת מייצגת את ה-Broadcast )מעין רשימת תפוצה של **כל** הרשת(, כתובת אחת הולכת לספקית שלך וכתובת אחת הולכת אליך. בקיצור בזבזני

כדי להתגבר על הבעיה, נכתב תקן [)RFC1918](http://tools.ietf.org/html/rfc1918)( שאומר שישנם כתובות חוקיות וישנם כתובות לא חוקיות וניתן לתרגם ביניהם. וכך, ניתן להקצות כתובות שאינם חוקיות על מנת שלא לבזבז כתובות חוקיות. למשל, אם יש לנו בבית 5 מחשבים, במקום לרכוש מהספקית שלנו 5 כתובות חוקיות ויקרות. משתמשים ב-NAT לתרגם כתובות לא חוקיות לכתובת חוקית אחת. מה שחוסך מאיתנו רכישה יקרה של מספר כתובות )אני אסביר עוד בהמשך(.

מכאן קיבל NAT את שמו. NAT הם ראשי תיבות של Network Address Translation – תרגום כתובות רשת.

ראשית ברצוני להבהיר: המושג "כתובת לא חוקית" אינו קשור לפלילים, משפט, משטרה, מאסר או כל דבר דומה.

**כתובת IP, כשמה היא, היא כתובת.**

לצורך המחשה, בעולם האמיתי, כאשר אני שולח לידיעות אחרונות מכתב שבו אני מבקש להיות מנוי על העיתונים שלהם, עלי לציין במעטפה את הכתובת של מחלקת המנויים של ידיעות, והכתובת שלי, שאליה יישלחו כל העיתונים. בצורה דומה מתבצעת התקשורת באינטרנט. כאשר אני רוצה לקרוא את ynet, המחשב שלי פונה לכתובת ה-IP של ynet )מחלקת המנויים( ומבקש את האתר הראשי. כדי שynet יידעו לאן לשלוח את המידע באתר שלהם חזרה אליי, המחשב שלי מציין את כתובת ה-IP שלו )הכתובת של הבית שלי אליו יישלחו העיתונים(.

כתובות חוקיות הם כתובות שמותר להשתמש בהם ברשת האינטרנט. מדובר בכתובת שספקית האינטרנט רוכשת עבורנו מאירגונים בינלאומיים )למשל האירגון האירופאי [ripe(](http://www.ripe.net/), ולאחר מכן מחלקת אותם ללקוחות שלה תמורת התשלום החודשי.

כתובות אלו הם כתובות שיופיעו במאפיינים של החייגן או הכתובת שתופיע אם תלחץ [כאן.](http://www.noc.co.il/)

כתובות לא חוקיות הם כתובות שהאינטרנט לא משתמש בהם. בכתובות אלו משתמשים למשל, באירגון שאינו רוצה אינטרנט )מאגר המידע של הבנקים(, ברשתות פנים-אירגוניות וגם ברשת הביתית שלנו – וזאת כדי שלא לשלם הרבה כסף על מספר כתובות חוקיות.

הכתובות הלא חוקיות הוגדרו מראש והם: **)להבין היטב כמה כתובות פנויות יש לי**

**)**

11.1.1.1 עד 11.255.255.255

172.16.1.1 עד 172.31.255.255 וגם 192.168.1.1 עד 192.168.255.255

)אנחנו נחזור על החומר שוב פעם בכתובות IP אבל זה טוב לחזרה(

אז רגע! אמרנו בעמוד הקודם שאני משתמש בכתובות לא חוקיות ברשת הביתית שלי כדי לחסוך בכסף, אבל בעמוד הזה אני אומר שאני לא יכול לגלוש עם כתובות לא חוקיות. אז איך בכל זאת אני גולש )גם אם לא רכשתי מהספקית מספר כתובות חוקיות(? או במילים אחרות, איך מחברים מחשב עם כתובת לא חוקית לאינטרנט?

והתשובה הנדרשת היא NAT!

NAT אומר בעצם, שאנחנו מתרגמים מספר כתובת לא חוקית חינמיות )למשל

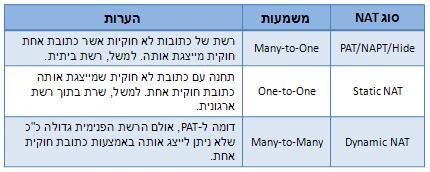
192.168.1.7( לכתובת חוקית )88.114.86.4( אחת שניתנה לנו ע"י הספקית במסגרת המנוי. באמצעות ה-NAT, מחשב ברשת בייתית יוכל לגלוש באינטרנט.

אם נחזור להמחשה הקודמת לפיה כתובת היא בית, ניתן לדמות כתובת לא חוקית לחדר. זר )מהאינטרנט( לא יידע היכן בבית שלנו )הכתובת החוקית שלנו( נמצא הסלון או חדר השינה )כתובות לא חוקיות(. תושבי הבית יידעו להגיע לחדרים הללו.

הדייר בבית לא יוכל לבקש ממחלקת המנויים של ידיעות אחרונות לשלוח לו את העיתון לסלון.

## סוגים של NAT

כאמור, NAT נועד לתרגם כתובות לא חוקיות לכתובות חוקיות. אולם, ישנם כמה סוגים של NAT:



ניתן להבין מהטבלה שלנו שההבחירה בסוג ה-NAT תלוי בצורך שלנו. למשל, ברשת הביתית שלנו נהוג למצוא את ה-PAT. בעוד שברשתות אירגוניות נהוג למצוא שילוב של PAT )כדי שהמחשבים ברשת יוכלו לגלוש( וגם Static NAT )שרתים(. ברשתות אירגוניות גדולות במיוחד נוכל למצוא שילוב של Dynamic NAT )כדי שמספר גדול מאוד של מחשבים יוכלו לגלוש( וגם Static NAT )שרתים(.

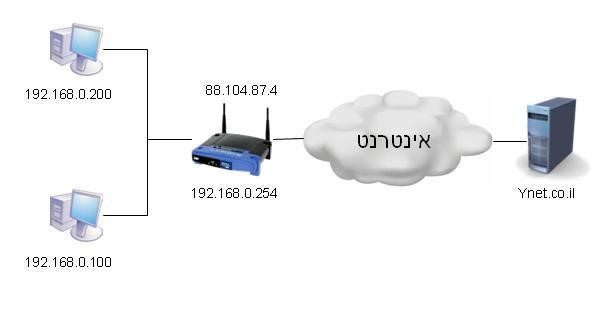
במצב זה אנחנו .Port Address Translation הינו ראשי התיבות של **PAT**

מתרגמים מספר כתובות לא חוקיות לכתובת חוקית אחת. במקומות אחדים PAT נקרא גם. בכל מקרה מדובר בשיטה שמתרגת מספר [כתובות לא חוקיות לכתובת](http://mymodemsux2.wordpress.com/%D7%94%D7%9E%D7%93%D7%A8%D7%99%D7%9A-%D7%94%D7%A9%D7%9C%D7%9D-%D7%9C-nat/%d7%9b%d7%aa%d7%95%d7%91%d7%95%d7%aa-ip-%d7%97%d7%95%d7%a7%d7%99%d7%95%d7%aa-%d7%95%d7%9c%d7%90-%d7%97%d7%95%d7%a7%d7%99%d7%95%d7%aa/)

.)many to one( [חוקית](http://mymodemsux2.wordpress.com/%D7%94%D7%9E%D7%93%D7%A8%D7%99%D7%9A-%D7%94%D7%A9%D7%9C%D7%9D-%D7%9C-nat/%d7%9b%d7%aa%d7%95%d7%91%d7%95%d7%aa-ip-%d7%97%d7%95%d7%a7%d7%99%d7%95%d7%aa-%d7%95%d7%9c%d7%90-%d7%97%d7%95%d7%a7%d7%99%d7%95%d7%aa/) אחת

**חשוב להבהיר PAT היא שיטה ספציפית שבה אנו משתמשים NAT הוא הרעיון שעומד מאחורה אז בעיקרון זה אותו דבר )מאוד דומה ל TCP\IP ומודל שבעת השכבות(**

להלן דוגמה לרשת ביתית שמשתמשת ב-PAT



נסביר את מה שאנחנו רואים….

לנתב שלנו יש בעצם שני כרטיסי רשת: אחד חיצוני שמדבר עם האינטרנט באמצעות כתובת ה-IP החוקית )88.114.87.4( וכרטיס רשת נוסף שמדבר עם הרשת הפנימית באמצעות כתובת לא חוקית )192.168.1.254(.

המחשבים ברשת הפנימית שלנו רוצים לצאת לאינטרנט )לגלוש ב-ynet למשל( אך אין ברשותנו את התקציב לקנות כתובות IP לכל מחשב. כדי לפתור את הבעיה, ניתן להגיד לנתב שלנו שיבצע תרגום של כתובות. כיצד זה יתבצע?

ראשית, המחשב שלנו קיבל כתובת משרת ה[-DHCP ש](http://mymodemsux2.wordpress.com/המדריך-השלם-ל-nat/dhcp/)נמצא בנתב )למשל

192.168.1.111(. שרת ה-DHCP לימד את המחשב שלנו שכדי לצאת לאינטרנט הם צריכים ללכת לנתב שכתובתו הפנימית, בתוך הרשת שלנו בבית, היא

192.168.1.254. הגדרה זו נקראת גם default gateway ובעברית פשוטה אומרת

"השער החוצה" . כעת, כשאנחנו מקלידים את הכתובת של ynet )וכדי לפשט את הבעיה נתעלם מהסיפור של ה-DNS אבל לא לשכוח לשנן את זה בהמשך(, מערכת ההפעלה שלנו פותחת פורט רנדומלי )למשל 1255( ופונה לנתב כדי שיספק לה את ynet בפורט של גלישה )פורט 81(. אם נציג זאת בצורה אחרת:

מבחינת המחשב

כתובת המקור היא 192.168.1.111 פורט המקור הוא 1255 כתובת היעד היא ynet.co.il פורט היעד הוא 81

הפניה לynet מכילה את הבקשה "תן לי את הדף הראשי" )get( המידע הזה מגיע לנתב. גם לנתב יש default gateway והוא האינטרנט

)בפשטות(. כיוון שאמרנו לנתב לבצע NAT, הוא יבצע תרגום של הכתובת הלא חוקית של המחשב )192.168.1.111( לכתובת החוקית שספקית האינטרנט נתנה לו )88.114.87.4(. מה הכוונה בתרגום? הנתב יוציא לאינטרנט את הבקשה של המחשב שלנו, כאילו הוא בעצמו ביקש לצפות ב-ynet )ולא המחשב שלנו(. כאשר הוא יפנה ל-ynet, הוא יחליף את כתובת המקור מ-192.168.1.111 לכתובת החוקית שהיא 88.114.87.4. כך למשל תיראה טבלת ה-NAT בנתב:

טבלאת ה-NAT בנתב

תתיחס לכתובת המקור בצורה הבאה:

192.168.1.111:1255 = 88.114.87.4:1255 כתובת היעד לא משתנה והיא עדיין ynet.co.il:80

כאשר ynet יקבלו את הבקשה, הם לא יידעו על התרגום. בעצם, הם לא יידעו שמאחורי הכתובת 88.114.87.4 יש רשת בייתית והם לא יידעו שעומד מולם נתב.

מבחינת ynet הם יחשבו שיש מחשב בודד, בכתובת 88.114.87.4, אשר רוצה לגלוש לאתר שלהם ]לכן למשל צ'קפוינט קוראים ל-PAT בשם Hide NAT - כיוון שהוא מסתיר את הרשת[.

כעת, נסתכל מה קורה מהכיוון הנגדי.

ynet מקבלים אליהם בפורט 81 בקשה. הבקשה הגיע מ-84.114.87.4 בפורט

1255. ynet מחליטים לשלוח את עמוד החדשות לנתב שלנו.

מבחינת ynet

כתובת המקור היא ynet.co.il פורט המקור הוא פורט 81 )גלישה( כתובת היעד היא 88.114.87.4 פורט היעד הוא 1255

דף האינטרנט נשלח והוא מגיע לנתב. איך הנתב יודע להעביר את דף האינטרנט למחשב שלנו? כאשר ביקשנו את דף האינטרנט נוצרה טבלת ה-NAT. בטבלה רשום לנתב כי הכתובת 88.114.87.4 בפורט 1255 שווה לכתובת

192.168.1.111 בפורט 1255. כלומר, כל תעבורה שמגיעה לנתב מהאינטרנט בפורט 1255, יש להפנות אותה למחשב שלנו )192.168.1.111( בפורט 1255.

מה יקרה אם שני המחשבים ברשת )192.168.1.111 וגם 192.168.1.211( יירצו להגיע ל-ynet בפורט מקור 1255? כיצד הנתב שלנו יידע להבדיל בין המחשבים?

הנתב בעצם יבנה את הטבלה הבאה:

88.114.87.4:1255 = 192.168.1.111:1255

88.114.87.4:**3333** = 192.168.1.211:1255

כלומר, הוא יוציא את התעבורה מפורט שונה מהפורט של אחד המחשבים כדי שלא ליצור בלבול. בצורה הזו הוא יתרגם את פורט 1255 של המחשב השני לפורט

.3131

ל-PAT יש יתרונות רבים אך גם חסרונות. port forward נותן מענה לאחד החסרונות הללו.

## Port Forward

לפני שאנחנו מתחילים בפרק, אני ממליץ לקרוא ולהבין את הפרקים שעוסקים [בפורטים](http://mymodemsux2.wordpress.com/%D7%94%D7%9E%D7%93%D7%A8%D7%99%D7%9A-%D7%94%D7%A9%D7%9C%D7%9D-%D7%9C-nat/%d7%a4%d7%95%d7%a8%d7%98%d7%99%d7%9d/), ב[-DHCP](http://mymodemsux2.wordpress.com/%D7%94%D7%9E%D7%93%D7%A8%D7%99%D7%9A-%D7%94%D7%A9%D7%9C%D7%9D-%D7%9C-nat/dhcp/) וב[-PAT](http://mymodemsux2.wordpress.com/%D7%94%D7%9E%D7%93%D7%A8%D7%99%D7%9A-%D7%94%D7%A9%D7%9C%D7%9D-%D7%9C-nat/pat/). מדובר במושגי יסוד הדרושים להבנה של הפרק הזה.

קראת? הבנת? נמשיך!

בעצם הגדרתו, ל-PAT יש חיסרון גדול הנובע מהתכנון שלו. בפרק שמדבר על [PAT](http://mymodemsux2.wordpress.com/%D7%94%D7%9E%D7%93%D7%A8%D7%99%D7%9A-%D7%94%D7%A9%D7%9C%D7%9D-%D7%9C-nat/pat/) ראינו שהנתב בונה טבלת NAT ובאמצעותה הוא יודע כיצד לתרגם. לדוגמה, מחשב ברשת הפנימית יוזם תקשורת החוצה )למשל ל-ynet(, הנתב בונה בטבלה שלו רשומה שאומרת

88.114.86.17:1255 = 192.168.1.111:1255

כאשר ynet מחזיר תשובה לנתב לפורט היעד )1255(, הנתב שלנו הולך לטבלת ה-NAT ורואה שיש לתרגם את התעבורה שנכנסה אליו מ-ynet לכתובת

.192.168.1.111:1255

כלומר, ניתן להגיד **שהתעבורה שהמחשב שלנו יוזם** **מוסיפה רשומה לטבלת ה-NAT**. אולם, מה קורה אם מגיעה לנתב שלנו תעבורה מהאינטרנט? שהמחשב שלנו ברשת הפנימית לא יזם? **כיוון שהיוזם הוא מחשב באינטרנט** )ולא ברשת הביתית( לנתב שלנו אין רשומה בטבלת הNAT, הוא לא יודע כיצד לתרגם את התעבורה שנכנסת אליו מהאינטרנט ולכן **זורק אותה**.

לכאורה, המצב תקין, שהרי אם מגיעה לרשת שלי תעבורה שלא ביקשתי, אני מעוניין שהנתב יתעלם ממנה. אולם, מה קורה אם יש לי שרת? הרי שרת אינו יוזם תקשורת בפני עצמו, אלא כשמו, נותן שרות, ואחרים יוזמים אליו תעבורה. שרת web, שיש עליו אתר אינטרנט, מחכה שייגשו אליו, הוא אינו יוזם התקשרות. בכך נוצרת תקלה משום שלא ניתן להגיע לשרת שלנו!

מכאן נובעת הבעייתיות עם PAT. כאשר יש שרת ברשת הלא חוקית, הנתב לא יודע להעביר אליו תקשורת.

**port forward**

כדי להתגבר על הבעיה, נתבים מאפשרים להוסיף רשומות לטבלת ה-NAT באופן ידני. לרשומה זו קוראים Port forward. למשל, נניח שברשת שלנו מותקן שרת web שכתובתו היא 192.168.1.211. שרת זה מחזיר דפי אינטרנט כאשר פונים אליו בפורט 81. ללא הגדרה של port forward, כאשר מישהו באינטרנט ינסה לגלוש לשרת שלנו, הוא יפנה לכתובת החוקית של הנתב )88.114.86.17:81( והנתב לא יידע שיש להעביר תעבורה שכזו את השרת. אם נבצע Port forward, נוכל להגדיר את הרשומה הבאה בטבלת ה-NAT:

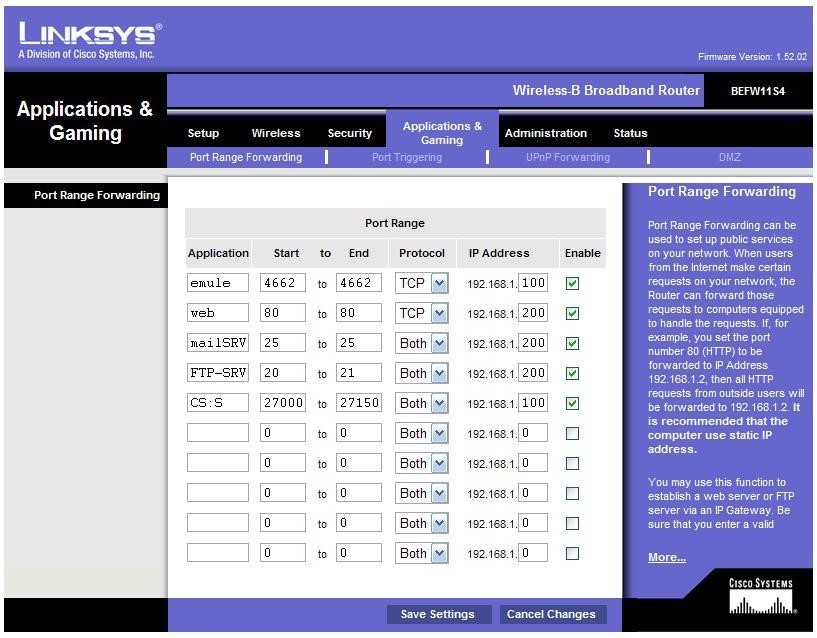
192.168.1.211:81 = 88.114.86.17:81

בצורה זו יוכל הנתב שלנו להפנות את התעבורה לשרת ה-web שלנו.

גם תוכנות שיתוף הקבצים הופכות את המחשב שלנו לשרת. הרעיון של אימיול הוא "יש לי קבצים, אתם מוזמנים לבוא ולקחת אותם ממני. אני נותן את השירות בפורט

."4662

לא מדובר בהגדרה מסובכת. להלן דוגמה להגדרות Port forward בנתב לינקסיס:



בעולם הנתבים הביתיים יש שימוש במושגים הקשורים ל-NAT באופן לא מדויק.

למשל, ישנם לא מעט נתבים )2wire למשל( שקוראים להגדרות ה-NAT של הנתב firewall באופן לא מוצדק. firewall, בדומה ל-NAT, זורק תעבורה שלא ביקשנו.

אולם ישנם שני הבדלים מהותיים: ההבדל הראשון הוא שה-firewall זורק תעבורה שאמרנו במפורש שאנחנו לא רוצים, ואילו PAT זורק תעבורה בגלל שהוא אינו יודע איך להתמודד איתה. הבדל שני הוא ש-PAT נעצר בשכבה 4 ואילו firewall יודע לבחון תעבורה בשכבה ה-7 של [מודל OSI](http://en.wikipedia.org/wiki/OSI_model). בעברית פשוטה, נתב שעושה PAT אינו מסתכל על תוכן המידע שעובר דרכו בצורה מדוקדקת והוא יכול להעביר וירוסים והתקפות בפורטים שהותרו. הוא יוכל להעביר התקפה על שרת ה-web שלנו כיוון שזו הותרה ע"י port forward בפורט 81.

firewall לעומת זאת, יודע להתסכל על התוכן של התעבורה, לנתח אותה, ולזרוק אותה אם היא מסוכנת.

**DMZ** הוא מושג שגוי נוסף בעולם ה-NAT. המושג DMZ מייצג במקור שקע נוסף בנתב שלנו המיועד לחיבור של רשת נפרדת ומאובטחת. כלומר, שקע אחד לרשת הפנימית ושקע נוסף לשרתים שלנו, ברשת נפרדת. בעולם ה-NAT, המושג DMZ אומר משהו אחר לגמרי.

הצורך ב-DMZ נולד בעצלנות

נניח שיש לנו שרת ברשת הפנימית שיש לו תפקידים רבים: הוא גם שרת FTP, יש עליו אתר אינטרנט, הוא שרת דואר, מריצים עליו אימיול ויש עליו שרתי משחקים – הכל על מחשב אחד. המשמעות היא שיש ליצור חוקים רבים של port forwarding.

הגדרת DMZ נועדה לענות על הצורך הזה בדיוק! DMZ אומר בעצם, שכל תעבורה, שהיוזם שלה מגיע מהאינטרנט, יש להפנות למחשב אחד ויחיד. בכך חסכו מאיתנו עבודה 

בנוסף, הגדרת DMZ הינה דרך מצוינת לאתר תקלה. אם אתם חושבים שבעיית התקשורת נובעת בגלל צורך בחוק port forward, ניתן להגדיר זמנית DMZ על התחנה ולבדוק אם בעיית התקשורת נפתרה!

אולם, יש חיסרון גדול ל-DMZ. אם המחשב לא מוגן כראוי, ניתן יהיה לפנות אליו בפורטים של שיתוף קבצים, remote desktop והתקפות אחרות – ובכך, לפרוץ למחשב.

**UPnP**

Universal Plug and play הינו פרוטוקול חדש יחסית המאפשר לגלות **ולהגדיר** לבד את כל מה שקשור ל-Port Forward. הפרוטוקול הוא צורך עבור כל אותם משתמשים שמסתבכים בלהגדיר פורטים. ההגדרה UPnP צריכה להיות מופעלת בשתי מקומות: שהנתב יתמוך באפשרות זו וגם, שהתוכנה על המחשב שלנו שמצריכה הפנייה של פורטים )e-mule למשל( תתמוך באפשרות הזו. כאשר הנתב שלנו מקבל אליו תעבורה שהוא אינו יודע לתרגם, הוא פונה לרשת הפנימית וסורק אחר מחשבים שיש להם UPnP. כאשר עונה מחשב כזה )למשל מחשב שיש לו emule שתומך ב-UPnP(, הנתב שואל את המחשב אם יש צורך להפנות אליו פורטים.

לכאורה למה צריך את כל מה שלמדנו מקודם פשוט נגדיר UPnP הבעיה עם UPnP היא שהוא לא מאובטח. נניח ויש לכם פרטים סודיים על המחשב שלכם ומישהו מבחוץ פונה לנתב כדי לפתוח פורטים המאפשרים להשתמש )ולמחוק( לכם את הקבצים )באמצעות SMB או Netbios(. ייתכן ובמקרה זה, הנתב יפתח גישה לעולם כך שכל אחד יוכל לחטט ולשנות לכם קבצים על המחשב!

**Port Redirect**

ניקח מצב שבו יש לנו רשת ביתית פשוטה בבית. ברצוננו לבנות שני אתרי אינטרנט ולאחסן אותם בבית. הכתובת של השרתים הם 192.168.1.111 ו-

192.168.1.211. כיוון שאנחנו עושים PAT, אנחנו יכולים לעשות הפנייה של פורט

81 רק פעם אחת. אם נפנה את פורט 81 לשרת אחד, לא נוכל להפנות את פורט

81 לשרת השני וההפך.

port redirect עונה בדיוק לבעיה זו. כפתרון, נוכל להגדיר את החוקים הבאים:

192.168.1.111:81 = 88.114.86.17:81

192.168.1.211:81 =88.114.86.17:**0303**

ניתן לראות כי כאשר הנתב יקבל אליו בקשה לפורט 8181, הוא ייתרגם אותה ויבצע redirect לפורט 81 על השרת השני שלנו. לאחר שנבצע את ההגדרה יקרה הדבר הבא:

אם נקליד בדפדפן את הכתובת 88.114.86.17:81 אנחנו נגיע לשרת הראשון )192.168.1.111( אם נקליד בדפדפן את הכתובת 88.114.86.17:8181 אנחנו נגיע לשרת השני )192.168.1.211(

**Port Trigger**

ישנם שרתים שמשתמשים ביותר מפורט אחד. אם נתקין ברשת שלנו שרת FTP, עלינו לבצע port forward לפורט 21 ולפורט 21. ב-FTP, פורט 21 משמש לבקרה )להיכנס לשרת, להכניס יוזר וסיסמה( ואילו פורט 21 משמש להעברת מידע )"אני רוצה להכנס לתיקיה X ולהוריד משם את קובץ Y"(. אולם, אם נבצע הפנייה קבועה של פורט 21, יש חשש שייפרצו לנו לשרת. מטעמי אבטחה, Port Trigger מאפשר לנו לפתוח פורטים באופן זמני. אבל מתי? מה הסיבה שהפורט ייפתח באופן זמני?

)מה ה-trigger שיפתח את הפורט?( ניתן להגדיר שפורט X ייפתח רק כשפונים לשרת בפורט Y. זה בדיוק המשמעות של הגדרת Port Trigger בנתב. אם נחזור לדוגמה שלנו, Port trigger מאפשר לנו לפתוח, במקרה זה, את פורט 21, רק אחרי שפונים לשרת שלנו בפורט 21. כלומר, רק כאשר מנסים לבצע כניסה מסודרת לשרת, ניתן יהיה להוריד ממנו קבצים.