

# קורס CCNA

## שיעור מס' 10

נושא הלימוד:

NAT

PAT

IPV6

מרצה: אלי בפלר

Version 2

כל הזכויות שמורות לאלי בפלר © beflereli@gmail.com  
תודה ליקי בן ניסן על תרומת חלק נרחב מחומר הלימוד

# מבוא

בפרוטוקול ה-IPv4 קיימים מספר מוגבל של כתובות IP אפשריות, ליתר דיוק - בגרסה זו ניתן לחלק 4,294,967,295 כתובות - (ארבעה מיליארד מאתיים תשעים וארבעה מיליון תשע מאות שישים ושבעה אלף מאתיים תשעים וחמשה).

כל אחד מאיתנו צורך עד 10 כתובות IP (טלפון, מדפסת, מצלמת רשת, מחשב, שעון חכם, טלויזיה ועוד) ובשנות ה-80 העריכו שיוצר מחסור בכתובות ומתוך כך נולד הצורך למצוא פתרון לנושא.

הארגון האחראי על הסדר בכתובות IP הוא ארגון IANA (Internet Assigned Numbers Authority)

הפתרון הראשון הוא כתובות פרטיות לכל הרשת הפנימית וכתובת יציאה אחת לרשת החיצונית, על פתרון זה נרחיב כרגע.

פתרון נוסף שמצאו, הוא יצירת פרוטוקול חדש IPv6 המאפשר מספר רב יותר של כתובות מה-IPv4 ועליו נלמד בהמשך.

# פרוטוקול NAT

NAT (Network Address Translation) שמשמעותו הוא תרגום כתובת רשת. הוא פרוטוקול ברשת המחשבים, המתרגם את כתובות ה-IP מכתובת ציבורית לכתובת פרטית ולהיפך.

פעולה זו מאפשרת לנו לחבר מחשבים רבים לרשת האינטרנט באמצעות **כתובת IP אחת**.

להזכירכם, אנו שוכרים קו אינטרנט מספק האינטרנט ISP ומקבלים ממנו כתובת IP ציבורית אחת או יותר.

איך זה עובד? יש נתב אחד שיושב בנקודת החיבור בין ה-LAN לבין ה-WAN ותפקידו לבצע את התרגום של הכתובות מהכתובות הפרטיות 10.0.0.1 לכתובת הציבורית לדוגמה: 84.94.114.7.

למידע נוסף באתר Cisco

[http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/nat\\_dynamic.html#wp1078939](http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/nat_dynamic.html#wp1078939)



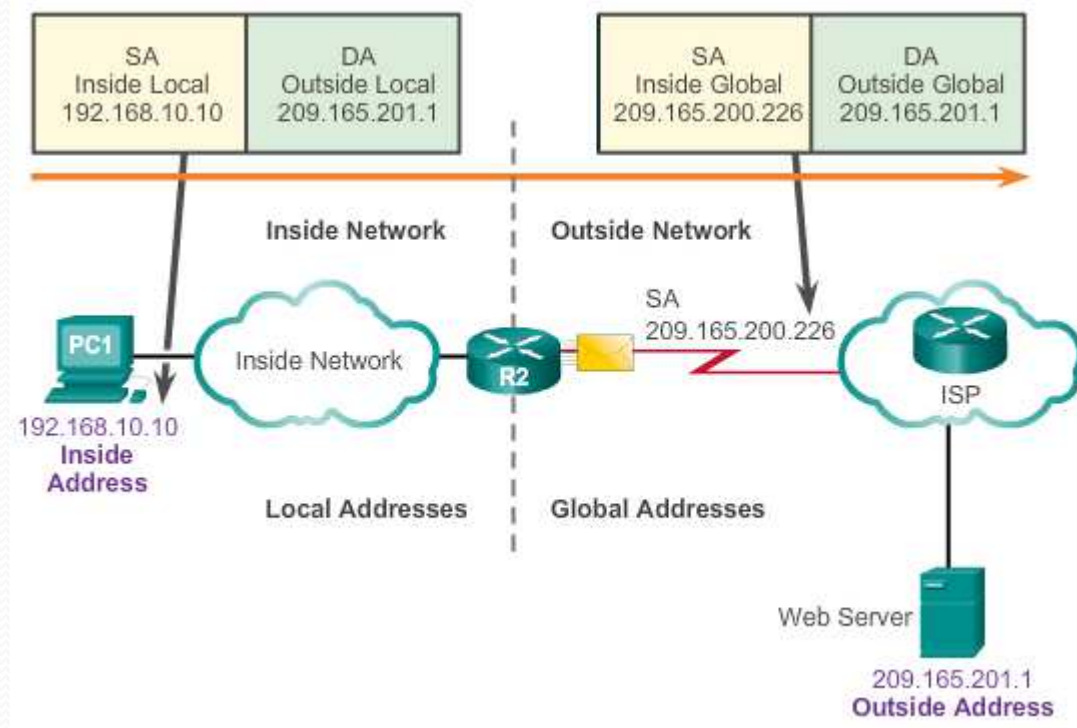
## ישנם 4 סוגים של כתובות NAT:

Inside local - כתובת המקור לפני התרגום (כתובת פרטית).

Inside global - כתובת המקור לאחר התרגום (כתובת ציבורית).

Outside local - כתובת היעד (כתובת ציבורית).

Outside global - כתובת היעד (כתובת ציבורית).



## סוגי ה-NAT:

- One-to-one – Basic NAT – מחשב אחד לאחד, ברשת הביתית היוצא לאינטרנט ומקבל כתובת ציבורית חוקית.
- One-to-many NAT \ NAT \ PAT – אחד להרבה, מספר מחשבים ברשת היוצאים דרך כתובת ציבורית אחת.
- Many-To-Many Dynamic NAT – הרבה להרבה, ארגונים גדולים עם מספר רב של משתמשים ירכשו מספר כתובות ציבוריות לצורך יציאה לאינטרנט.



# Static NAT

ממפה כתובת פרטית אחת, לכתובת ציבורית אחת. לדוגמה: אם תרצו להגיע מהאינטרנט לשרת ה-WEB ותקלידו את הכתובת 84.54.150.170 נצטרך ליצור הפניה מכתובת זו לכתובת המקומית 192.168.1.20 של שרת ה-WEB.

הגדרת התרגום

```
Router(config)#ip nat inside source static {local-ip} {global-ip}
```

או הגדרת Port Forward

```
Router(config)#ip nat inside source static {local-ip} {port} {global-ip} {port}
```

צפייה בטבלת התרגומים

```
Router#show ip nat translations
```

```
R2#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 209.165.200.225:16642 192.168.10.10:16642 209.165.200.254:80 209.165.200.254:80
tcp 209.165.200.225:62452 192.168.11.10:62452 209.165.200.254:80 209.165.200.254:80
```

## תרגול

פתח את הקובץ שבכונן ופתור אותו לפי ההוראות המצורפות.

### 11.2.1.4 Packet Tracer - Configuring Static NAT.pka

# Dynamic NAT

ממפה כתובות פרטיות, לכתובות ציבורית מתוך מאגר כתובות ציבוריות. Many-To-Many

**הגדרת מאגר כתובות ציבוריות**

```
Router(config)#ip nat pool {pool name} {starting IP} {ending IP} {netmask}
```

**הגדרת הכתובות שמיועדות לתרגום** - יצירת access-list שמגדיר את הכתובות הפנימיות

```
Router(config)#access-list {acl-number} permit {source} {source-wildcard}
```

**הגדרת התרגום** – שיוך access-list למאגר הכתובות הציבוריות לצורך התרגום.

```
Router(config)#ip nat inside source list {acl-number} pool {pool name}
```

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

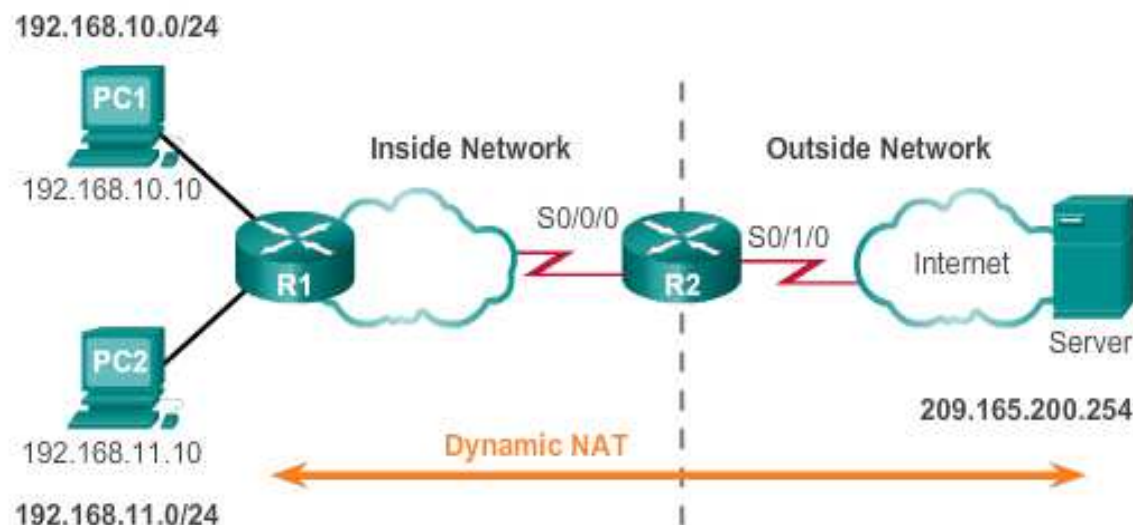
הגדרת הממשק החיצוני

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

הגדרת הממשק הפנימי



## דוגמה :



Defines a pool of public IPv4 addresses under the pool name NAT-POOL1.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226
209.165.200.240 netmask 255.255.255.224
```

Defines which addresses are eligible to be translated.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Binds NAT-POOL1 with ACL 1.

```
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

Identifies interface serial 0/0/0 as an inside NAT interface.

```
R2(config)# interface Serial0/0/0
```

```
R2(config-if)# ip nat inside
```

Identifies interface serial 0/1/0 as an outside NAT interface.

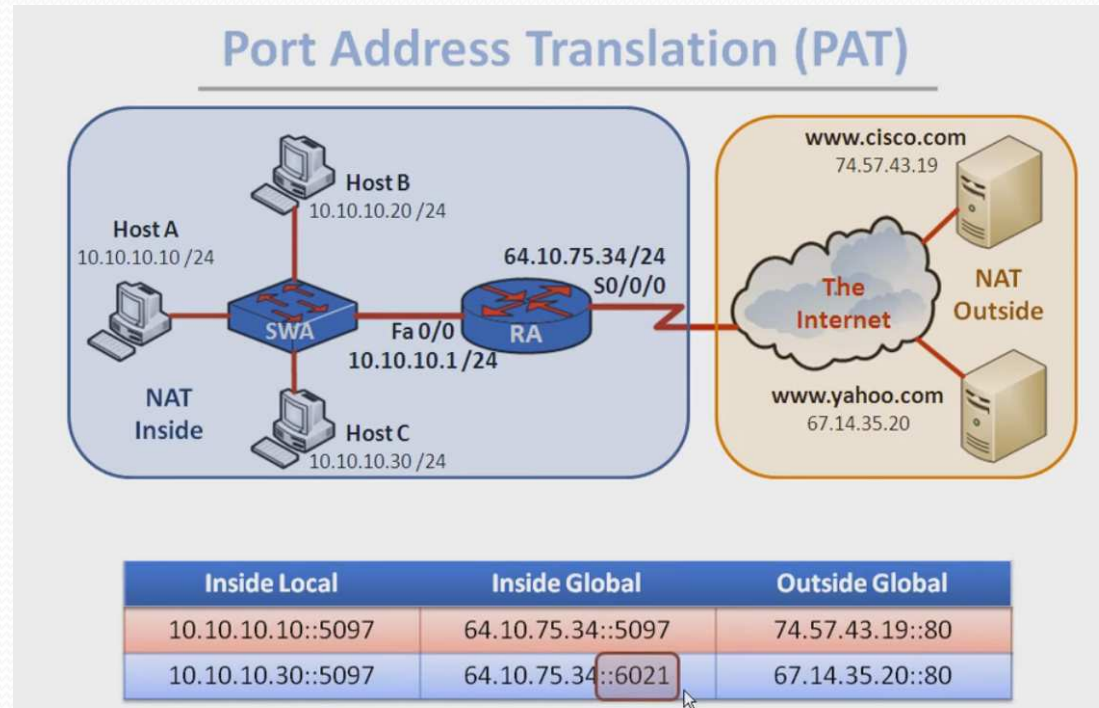
```
R2(config)# interface Serial0/1/0
```

```
R2(config-if)# ip nat outside
```

### פתח את הקובץ שבכונן ופתור אותו לפי ההוראות המצורפות. 11.2.2.5 Packet Tracer - Configuring Dynamic NAT.pka



# NAT Overload (PAT)



Host A פנה לאינטרנט לאתר Cisco והנתב עדכן את כתובת ה- Inside global שלו, והכניס מידע בטבלה שהוא מחזיק שהמידע שיחזור בפורט 5097 שייך ל-Host A. Host C גם יצא לאינטרנט לאתר של Yahoo והנתב עדכן את כתובת ה- Inside global שלו עם פורט שונה 6021, והכניס מידע בטבלה שהוא מחזיק שהמידע שיחזור בפורט 6021 שייך ל-Host C, בעצם בוצע שינוי של ה- Port ומכאן שמו.



מתרגם כתובות פרטיות רבות, לכתובת ציבורית אחת - One-to-many

PAT (PORT ADDRESS TRANSLATION) הנתב מתרגם את פורט המקור (ומכאן שמו) ומחזיק את המידע בטבלת תרגומים, על מנת שידע לאן לנתב את המידע לכשיחזור.

צפייה בטבלת התרגומים Router#show ip nat translations

הגדרת הכתובות שמיועדות לתרגום – יצירת access-list (Standard\Extended) שמגדיר את הכתובות הפנימיות שמותר להן לצאת לאינטרנט

Router(config)#access-list {acl-Number} permit {source} {source-wildcard}  
(במקרה זה הגדרנו Standard ACL – תזכורת במצגת שיעור 7)

הגדרת התרגום – שיוך ה- access-list לממשק היציאה לאינטרנט מהנתב

Router(config)#ip nat inside source list {acl-number\Name} interface {interface} overload

**לשים לב: המילה Inside מבלבלת פה כי הכוונה להמיר את כתובות הרשימה הפנימית, ואילו ב-**

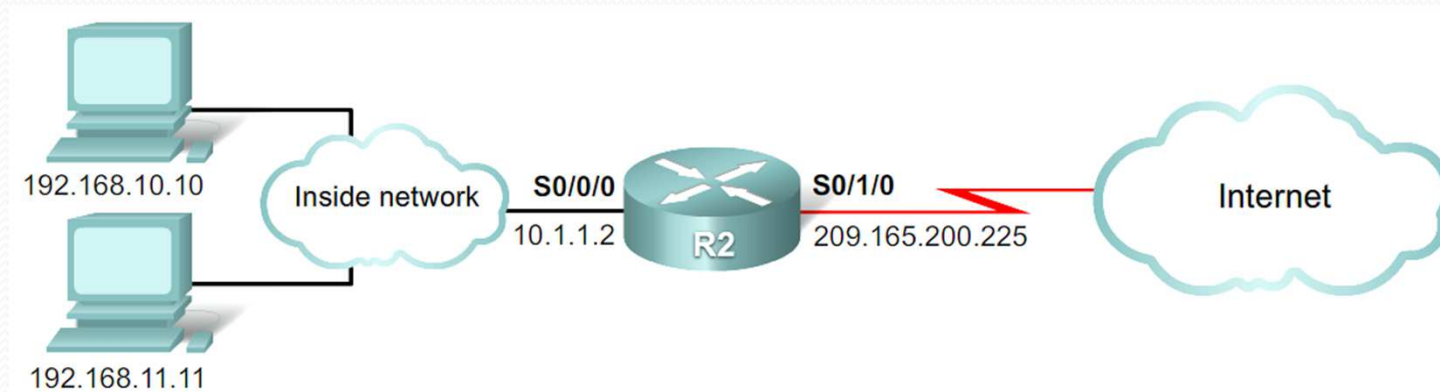
**Interface יש להגדיר ממשק יציאה והפקודה overload מאפשרת את ה-PAT**

**ולסיום יש להגדיר את ממשק הכניסה וממשק היציאה** Router(config-if)# ip nat inside\outside

דוגמה נוספת - <http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/260-cisco-router-nat-overload.html>

לדוגמה:

כתובות פרטיות ברשת 192.168.0.0/16 יתורגמו לכתובת הציבורית 209.165.200.225



```
access-list 1 permit 192.168.0.0 0.0.255.255
!Defines which addresses are eligible to be translated
ip nat inside source list 1 interface serial 0/1/0 overload
!Identifies the outside interface Serial 0/1/0 as the inside global address to be overloaded
interface serial 0/0/0
    ip nat inside
!Identifies Serial 0/0/0 as an inside NAT interface.
interface serial 0/1/0
    ip nat outside
!Identifies Serial 0/1/0 as an inside NAT interface.
```



## תרגול

פתח את קובץ ה-PDF שבכונן והקם את הרשת לפי ההוראות.

### 11.2.3.7 Lab - Configuring Port Address Translation (PAT)

תרגול נוסף

### 7.2.8 Scaling Networks with NAT.pka



## Question 1

Which two statements about static NAT translations are true? (choose two)

- A. They are always present in the NAT table.
- B. They allow connection to be initiated from the outside.
- C. They can be configured with access lists, to allow two or more connections to be initiated from the outside.
- D. They require no inside or outside interface markings because addresses are statically defined.

## What are two benefits of using NAT? (choose two)

- A. NAT protects network security because private networks are not advertised.
- B. NAT accelerates the routing process because no modifications are made on the packets.
- C. Dynamic NAT facilitates connections from the outside of the network.
- D. NAT facilitates end-to-end communication when IPsec is enable.
- E. NAT eliminates the need to re-address all host that require external access.
- F. NAT conserves addresses through host MAC-level multiplexing.

## תשובות E+A



# Internet Protocol Version 6 (IPv6)

כמו שהסברנו במבוא, יותר מחשבים והתקנים מתחברים כיום לאינטרנט. כדי לחבר את כולם לאינטרנט, נדרשת כמות גדולה יותר של כתובות IP. כמות הכתובות הציבוריות הולכת ואוזלת, וזאת למרות השימוש ב-NAT/PAT שמאפשרים לחסוך בכתובות IP. קיים פתרון נוסף והוא המעבר לשימוש בפרוטוקול IPv6, כרגע אין עדיין תאריך יעד אך בעתיד הוא צפוי להחליף לחלוטין את הפרוטוקול IPv4. לצורך ההשוואה, זהו מספר הכתובות האפשריות בכל פרוטוקול:

| Version | Supported Addresses                                 |
|---------|-----------------------------------------------------|
| IPv4    | 4,294,967,296                                       |
| IPv6    | 340,282,366,920,938,463,463,374,607,431,768,211,456 |

## יתרונות IPv6:

- כתובת IP מסוג IPv6 היא באורך 128bit לעומת 32bit של כתובת מסוג IPv4. המשמעות היא שתיאורטית לכל אדם ניתן לספק מספר כתובות השווה לכל הכתובות הציבוריות הקיימות ב-IPv4. לכן IPv6 מבטל את הצורך בשימוש ב-NAT \ PAT.
- יתרון נוסף הוא באבטחה - בכתובות IP מסוג IPv6 קיים IPsec מובנה, ולכן שימוש ב-IPsec פשוט יותר ותעבורת הרשת בטוחה יותר.
- Subnet mask קבוע של 64bit, כלומר מחצית מכתובת IP היא כתובת רשת. ניתן לשנות את ה-subnet mask ברמת הנתב אך לעמדות הקצה הוא קבוע.

# מבנה כתובת IPv6

כתובת IPv6 מורכבת מ 128Bit המחולקים ל-8 קבוצות מספרים של 16Bit בכל קבוצה. הכתובת מתורגמת למספר הקסדצימלי.

0010000000000001:0000110110111000:000000000100001:0000000100010001:0010000010000001:0000110110101000:0000100000100001:0000000101010001

8421 8421 8421 8421 : 8421 8421 8421 8421 etc  
0010 0000 0000 0001 : 0000 1101 1011 1000 : etc  
=2 =0 =0 =1 =0 =D =B =8  
2 0 0 1 : 0 D B 8

| Decimal | Binary | Hex |
|---------|--------|-----|
|         | 8421   |     |
| 9       | 1001   | 9   |
| 10      | 1010   | A   |
| 11      | 1011   | B   |
| 12      | 1100   | C   |
| 13      | 1101   | D   |
| 14      | 1110   | E   |
| 15      | 1111   | F   |



# כתיבת הכתובת בצורה מקוצרת

קיימים 2 חוקים המאפשרים לצמצם את הכתובת לכתובת קצרה יותר:  
**חוק ראשון:** ניתן להוריד את האפסים שבתחילת כל מספר (אבל להשאיר לפחות אחד)

|                                         |
|-----------------------------------------|
| 2001:0DB8:0000:1111:0000:0000:0000:0200 |
| 2001: DB8: 0:1111: 0: 0: 0: 200         |

|                                         |
|-----------------------------------------|
| FE80:0000:0000:0000:0123:4567:89AB:CDEF |
| FE80: 0: 0: 0: 123:4567:89AB:CDEF       |

**חוק שני:** ניתן להחליף אפסים רצופים בסימן :: (ניתן לביצוע רק פעם אחת בכל כתובת)

|               |                                         |
|---------------|-----------------------------------------|
| Preferred     | 2001:0DB8:0000:0000:ABCD:0000:0000:0100 |
| No leading 0s | 2001: DB8: 0: 0:ABCD: 0: 0: 100         |
| Compressed    | 2001:DB8::ABCD:0:0:100                  |
| or            |                                         |
| Compressed    | 2001:DB8:0:0:ABCD::100                  |

Only one :: may be used.

## תרגילים:

2001 : 0000 : 0DB8 : 1111 : 0000 : 0000 : 0000 : 0200

2013 : 0000 : 0123 : 4567 : 89AB : CDEF : 0000 : 0001

1111 : 0000 : 0000 : 0000 : 0000 : 0000 : 0101 : 1111

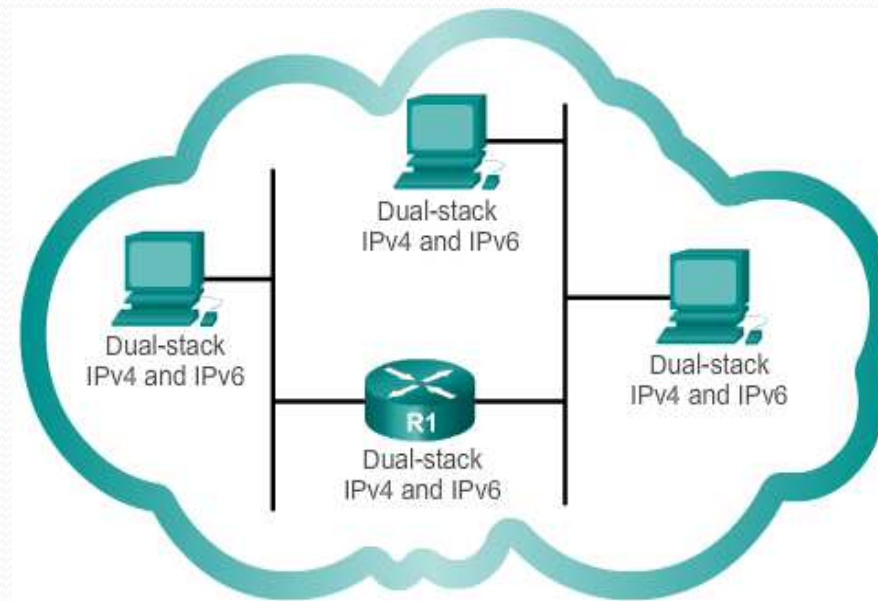
0000 : 0000 : 0000 : 1234 : 6678 : 9101 : 0000 : 34AB

# מעבר כתובות IP מ-IPv4 ל-IPv6

Internet Engineering Task Force (IETF) פיתח שלוש שיטות למעבר מ-IPv4 ל-IPv6:

## שיטה ראשונה - Dual Stack

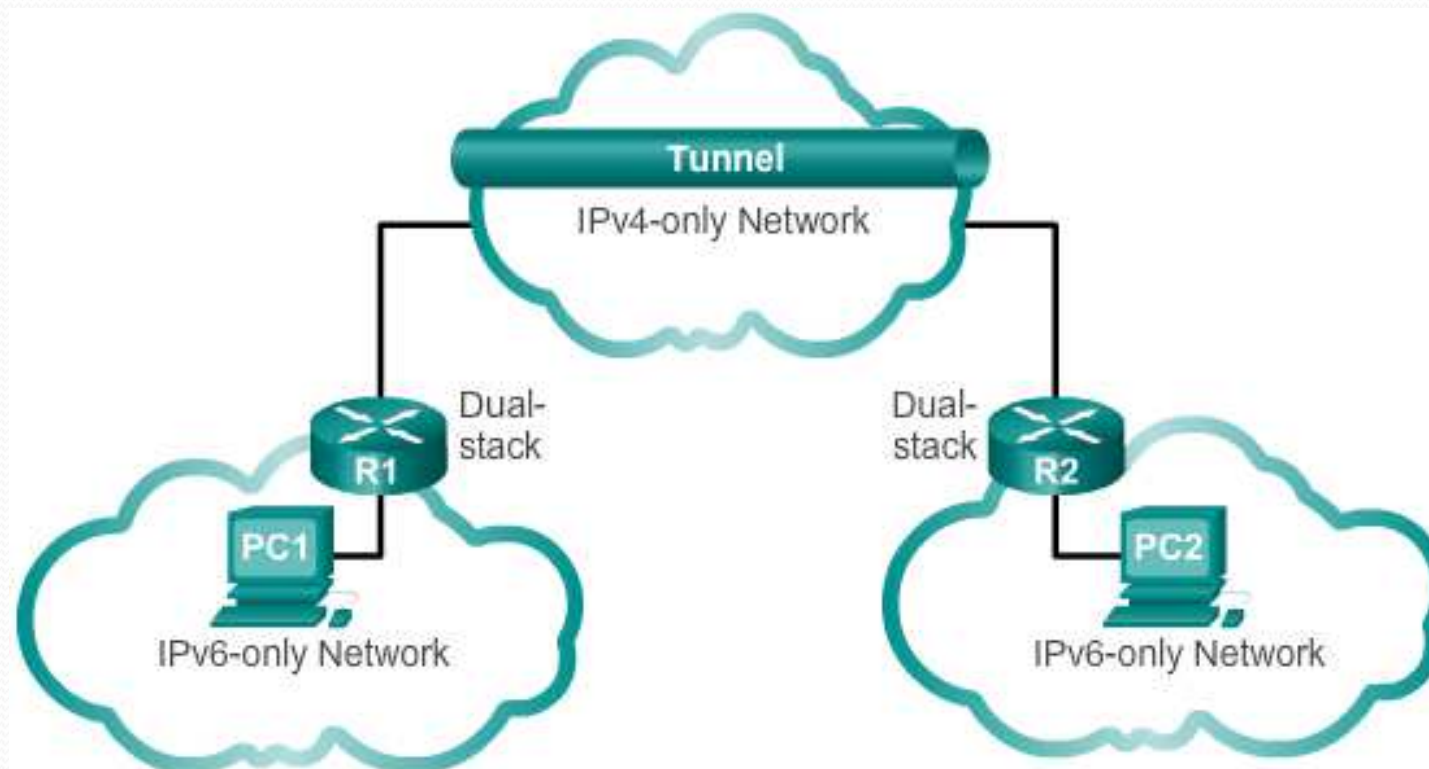
זו השיטה הקלה ביותר. השיטה מאפשרת תמיכה כפולה של IPv6 ו-IPv4 באותו כרטיס רשת. כך פועלים על הכרטיס רשת שני מחסניות פרוטוקול של TCP/IP, ולכרטיס הרשת יש שתי כתובות IP. הבעיה היא שלא כל התקן תומך ב-IPv6.





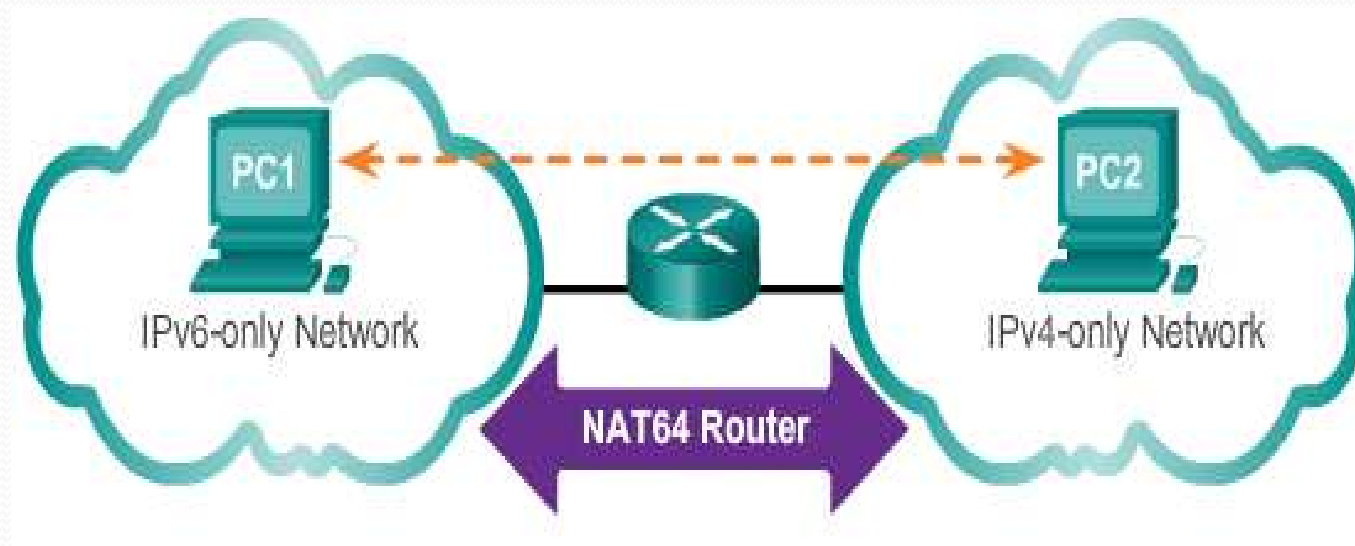
## שיטה שניה - Tunneling

בשיטה זו, Packet מסוג IPv6 נארז מחדש לתוך Packet מסוג IPv4



## שיטה שלישית – Translation

בשיטה זו, טכנולוגית Network Address Translation 64 (NAT64) מאפשרת תרגום כתובת IPv6 לכתובת IPv4 ולהפך.

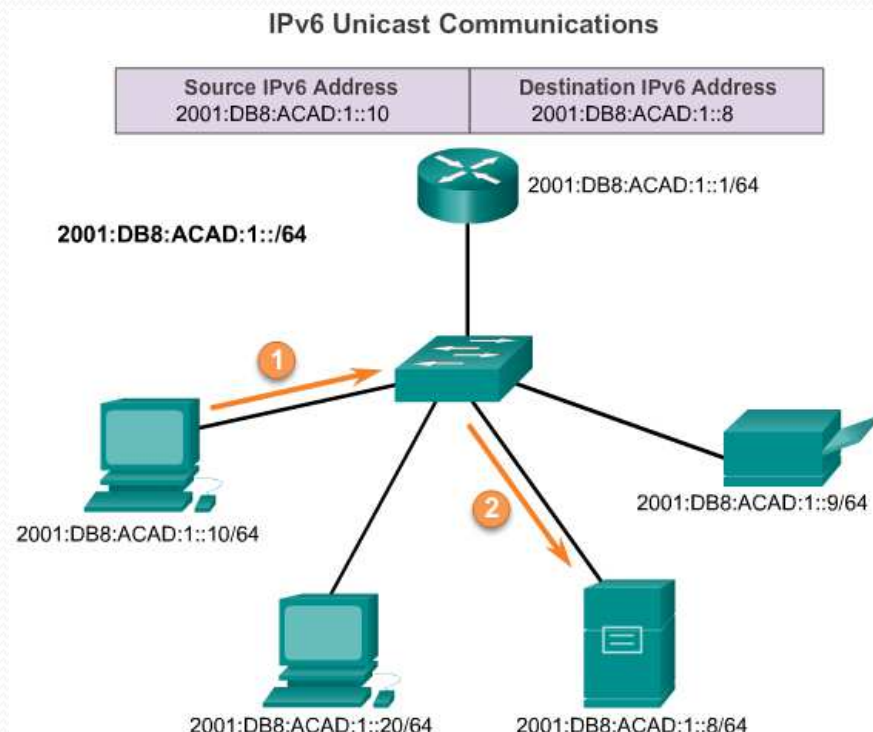


# סוגי כתובות

ב- IPv6 קיימים שלושה סוגי כתובות, יש יותר כתובות מסוג Broadcast.

## Unicast

תקשורת מסוג אחד לאחד, כמו ב- IPv4.





## Multicast

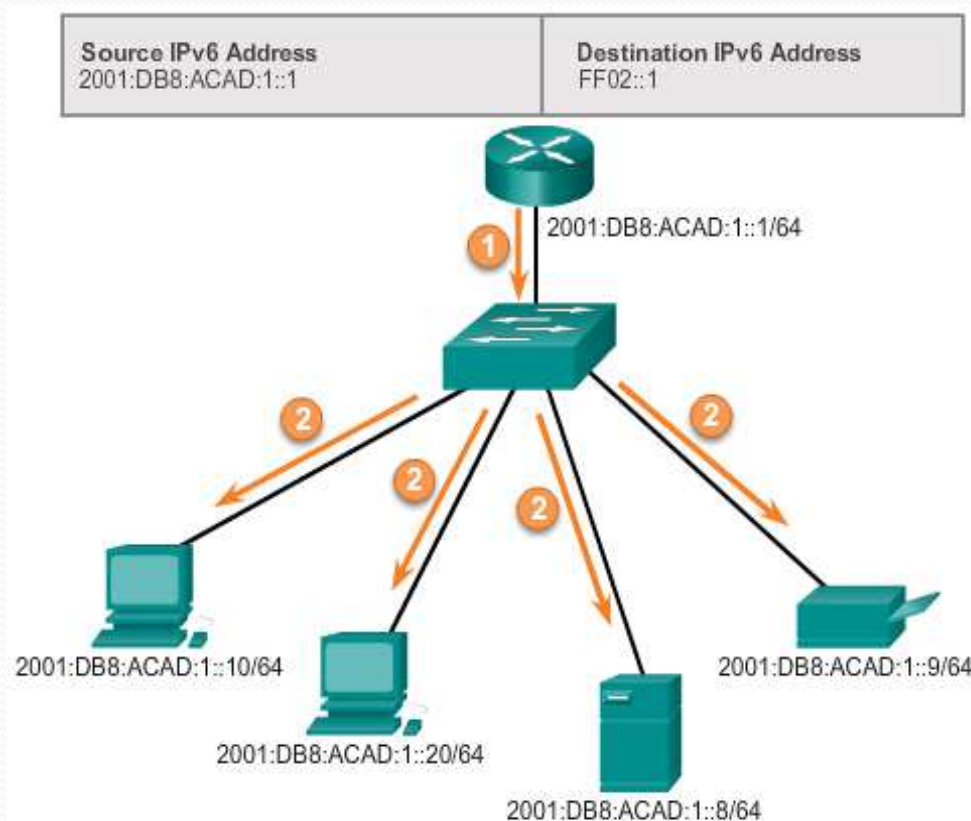
תקשורת אחד לרבים.

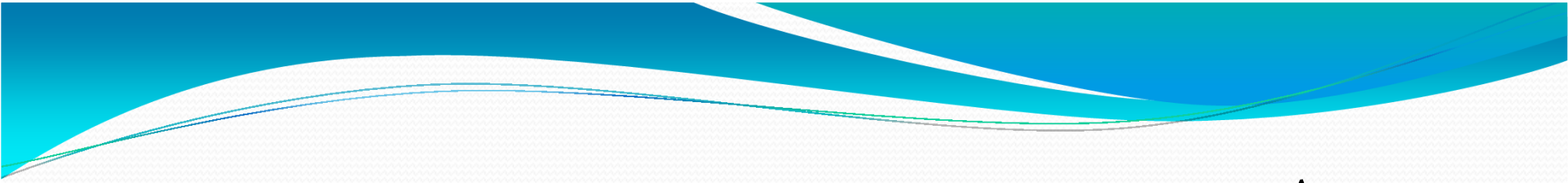
הכתובות מתחילות ב- FF00::/8.

ישנם כתובות שמורות כמו :

– FF02::1 כל ההתקנים

– FF02::2 כל הנתבים





## Anycast

זו תקשורת מסוג אחד לאחד הקרוב ביותר מתוך קבוצה (one to nearest)  
לדוגמה: אם יש קבוצת שרתים זהים שמשתמשים עם כתובות Anycast  
התקשורת תתבצע לשרת הקרוב ביותר.

# Unicast Addresses יוגי

## Global Unicast

כתובת ייחודית באינטרנט (זהה לכתובת ציבורית).

הכתובת מתחילת ב- 2000::3 או ב- 3000::3.

הספק שרות מספק ללקוח כתובת עם 48/ Network ID, וזה משאיר ללקוח 16 bits כדי ליצור תתי רשתות.

## Link-Local

כתובת פנימית שלא ניתנת לניתוב (דומה ל- (APIPA לכל כרטיס רשת שתומך ב- IPv6 חייבת להיות כתובת מסוג Link-Local. כלומר לכל כרטיס רשת יכולים להיות כמה כתובות.

אם הכתובת לא ניתנה לכרטיס בצורה ידנית, המערכת הפעלה לא פונה לשרת DHCP אלא נותנת כתובת לכרטיס בצורה אוטומטית. הכתובות מתחילות ב- FE80::/10.

## Loopback

כמו 127.0.0.1. הכתובת היא ::1

## Unique local

כמו כתובות פרטיות, כלומר לא ניתן לנתב אותם באינטרנט.

הכתובות בטווח FDFF::/7 - FC00::/7.



# הגדרת כתובת IPv6 לנתב

## הגדרת כתובת בצורה ידנית

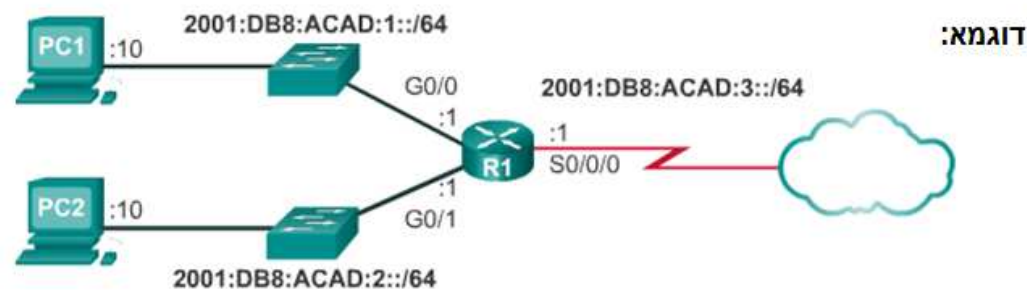
כברירת מחדל IPv6 לא מאפשר בנתבים.

כדי לאפשר שימוש ב- IPv6 בנתב השתמש בפקודה זו:

```
Router(config)#ipv6 unicast-routing
```

הגדרת הכתובת לממשק:

```
Router(config-if)#ipv6 address {2001:db8:3c4d:1:0260:d6ff:fe73:1987}/{64}
```



```
R1 (config)#interface gigabitethernet 0/0
R1 (config-if)#ipv6 address 2001:db8:acad:1::1/64
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#interface gigabitethernet 0/1
R1 (config-if)#ipv6 address 2001:db8:acad:2::1/64
R1 (config-if)#no shutdown
R1 (config-if)#exit
R1 (config)#interface serial 0/0/0
R1 (config-if)#ipv6 address 2001:db8:acad:3::1/64
R1 (config-if)#clock rate 56000
R1 (config-if)#no shutdown
```

### הגדרת Static Link-Local Address

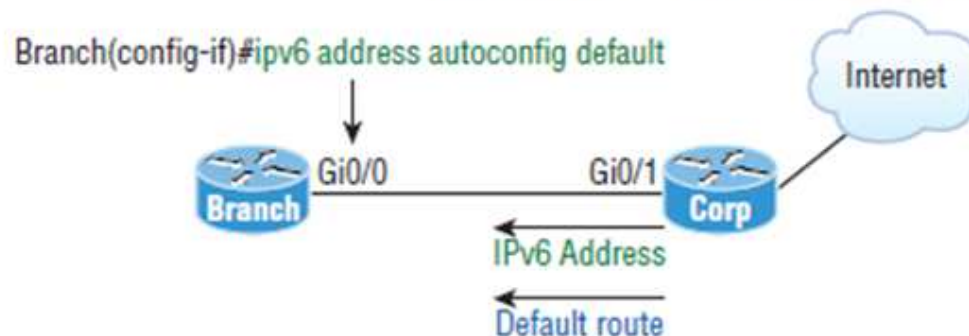
הכתובת משמשת את הנתב בתקשורת מול התקנים שמחוברים לאותה המקטע של הנתב. הכתובת משמשת לזיהוי הנתב באותו מקטע בלבד ולכן לנתב יכולים להיות כמה ממשקים עם כתובת זהה. היתרון במתן כתובת ידנית זה מתן כתובת פשוטה.

Router(config-if)#**ipv6 address {link-local-address} link-local**

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
    link-local    Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#
```

הגדרת נתב לקבלת כתובת בצורה אוטומטית:  
שיטה זו מתאימה רק אם הנתב נמצא בקצה הרשת.



שימוש בשיטת eui-64 כדי לקבוע בצורה אוטומטית את ה-ID :interface  
`Router(config-if)#ipv6 address {2001:db8:3c4d:1}::<64} eui-64`

במקום לתת כתובת ניתן להגדיר שהממשק יקבל אוטומטית כתובת (link-local addresses)  
`Router(config-if)#ipv6 enable`

### בדיקת תקינות ההגדרות

`Router(config-if)# show ipv6 interface brief`

`Router(config-if)# show ipv6 route`



## תרגול

פתח את הקובץ שבכונן ופתור לפי ההוראות

### 8.2.5.3 Packet Tracer - Configuring IPv6 Addressing.pka