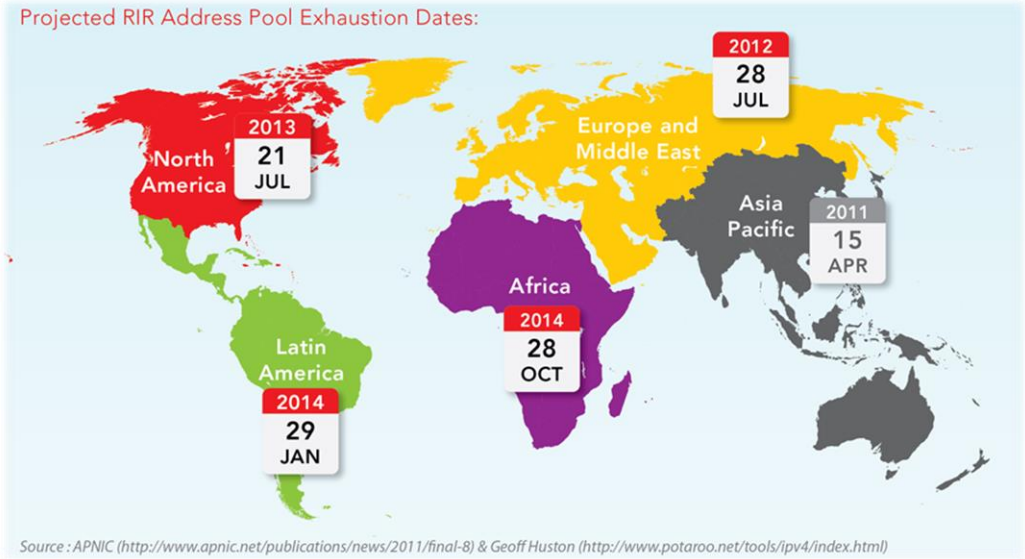
NAT

Network Address Translation

Introduction

- בתחילת שנות השמונים נוצר הפרוטוקול IPv4 עם 4.3 מיליארד כתובות. כמות כתובות שעל דעת כולם הייתה צריכה להספיק, אבל מהר מאוד כולם ראו כיצד רשתות המחשבים צומחות ומתרחבות בקצב מסחרר. בעקבות מצב זה ארגון ה-IETF פיתח פתרונות שונים, בינהם NAT. אחת השיטות העיקריות של NAT היא תרגום כתובות פרטיות רבות לכתובת ציבורית אחת, בצורה זו NAT חוסכת ומעכבת את אוזלת הכתובות. בסביבות 2012 כתובות ה-IPv4 הציבוריות אזלו.
  - IPv6 הוא פתרון נוסף (נולד להחליף את הפרוטוקול הישן).



IPv4 Address Space

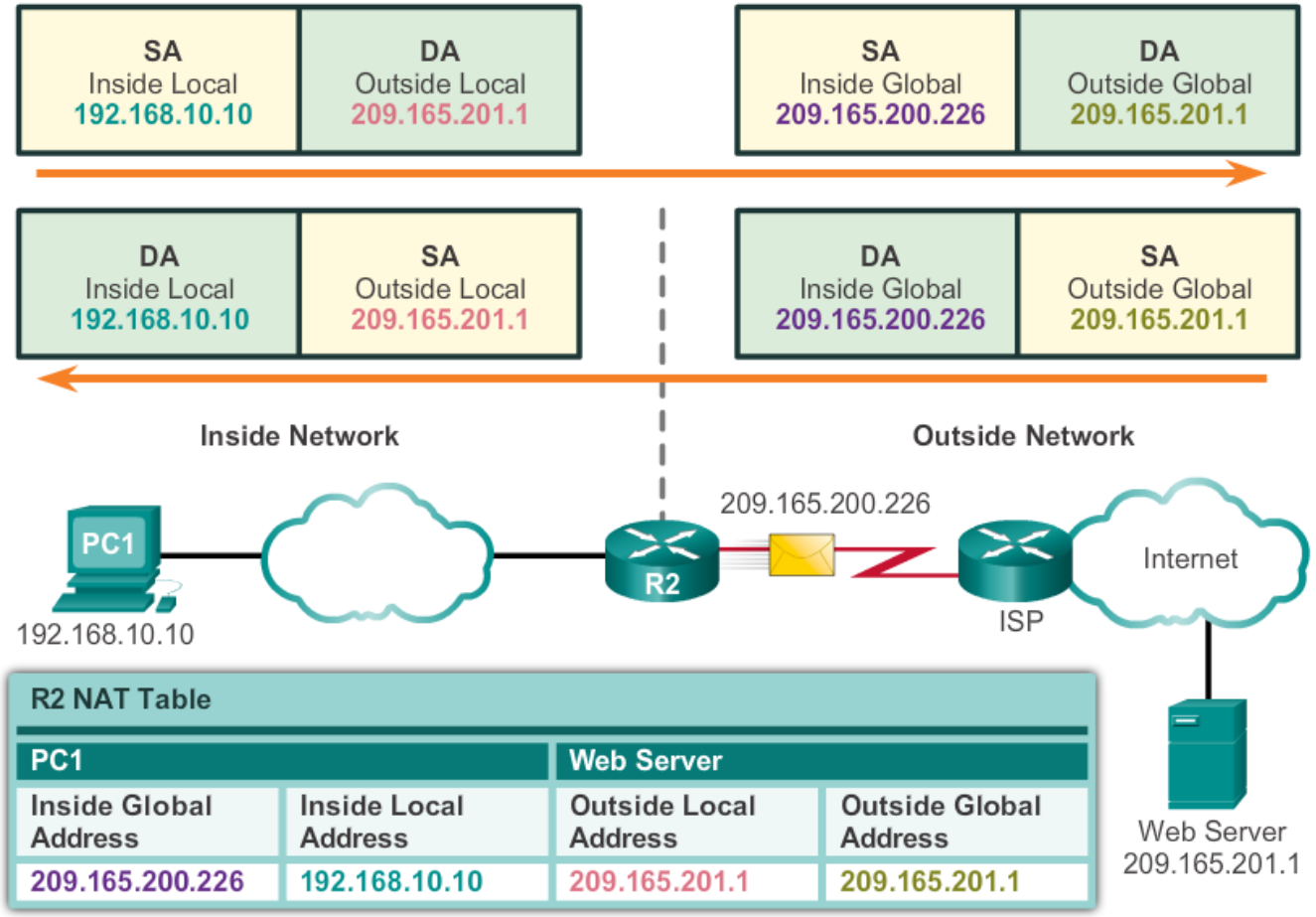
- פרוטוקול ה-NAT מבצע פעולה פשוטה למידי, תרגום כתובות פרטיות לכתובות ציבוריות, על פעולה זה נרחיב בהמשך.
- בעקבות אוזלת הכתובות המהירה, עלתה מסקנה שלא תתאפשר חלוקת כתובות ייחודיות לרכיבי הרשת השונים בעולם. בעקבות כך חולקו הכתובות לשני סוגים: כתובות פרטיות וכתובות ציבוריות.
- כתובות פרטיות משמשות לזיהוי משתמשים ורכיבים ברשת הפנימית (פנים ארגון). מטרתן לאפשר תקשורת בין רכיבים שונים ברשת הפנימית אבל הם אינן ייחודיות וניתן להגדיר את אותן כתובות בכל רשת פנימית אחרת (RFC 1918 מתאר בצורה מלאה את קונספט הכתובות הפרטיות).
- כתובות ציבוריות משמשות לזיהוי רשתות שונות ברשת הציבורית (חוץ ארגון). מטרתן לאפשר תקשורת בין רשת פנימית אחת לרשת פנימית אחרת והן ייחודיות, זאת אומרת אין 2 כתובות ציבוריות זהות.
- רשתות פנימיות עם עשרות עד אלפי משתמשים יכולות להשתמש באותן כתובות פרטיות אבל כל רשת מיוצגת ע"י כתובת ציבוריות אחת, כך שלא נוצרות כפילויות באינטרנט.

Class	Private Address Range	Prefix
A	10.0.0.0-10.255.255.255	/8
B	172.16.0.0-172.31.255.255	/16
C	192.168.0.0-192.168.255.255	/24

NAT Terminology

- ל-NAT מספר מונחים שמתארים את תהליך תרגום הכתובות בצורה מלאה.
- לאורך תהליך התרגום (מיפוי) NAT מתאר את הכתובת במונחים שונים, בהתאם לשלב בתהליך:
  - Inside local address
  - Inside global address
  - Outside local address
  - Outside global address

NAT Operation



R2 NAT Table

PC1		Web Server	
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

Advantages vs. Disadvantages

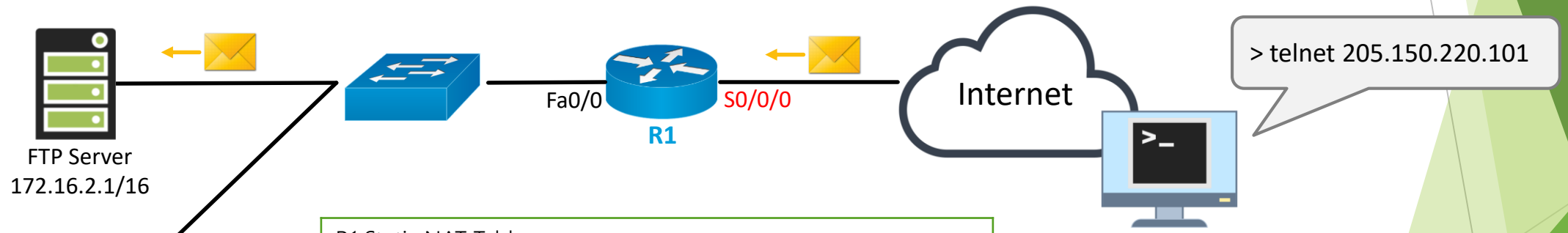
- היתרונות:
  - חסכון בכתובות ציבוריות (בשיטת PAT).
  - שכבת אבטחה נוספת, משתמשים ברשת הפנימית מוסתרים מהרשת הציבורית (ע"י נתב ה-NAT).
  - מספק גמישות בתכנון הרשת הפנימית וסכמת הכתובות הפרטיות, התרחבות הרשת אינה בעיה.
- חסרונות:
  - הגדרת ותחזוקת NAT לעיתים פעולות מורכבות.
  - ביצועי הרשת פוחתים בעקבות תהליך התרגום שהמידע עובר.
  - פרוטוקולי אבטחה ו-Tunneling כמו IPsec אינם פועלים כשורה בגלל אופן הפעולה של NAT.
  - קישוריות קצה לקצה אינה מתאפשרת, דבר שפוגע ביכולות של פרוטוקולים מסויימים.

Types of NAT

- קיימים שלושה סוגים של NAT:
- Static address translation (static NAT)-מיפוי מכתובת פרטית אחת לכתובת ציבורית אחת ולהפך.
- Dynamic address translation (dynamic NAT)-מיפוי מספר כתובות פרטיות למספר כתובות ציבוריות ולהפך.
- Port Address Translation (PAT)-מיפוי מספר כתובות פרטיות לכתובת ציבורית אחת ולהפך. שיטה זו נקראת גם NAT Overload.

Static NAT

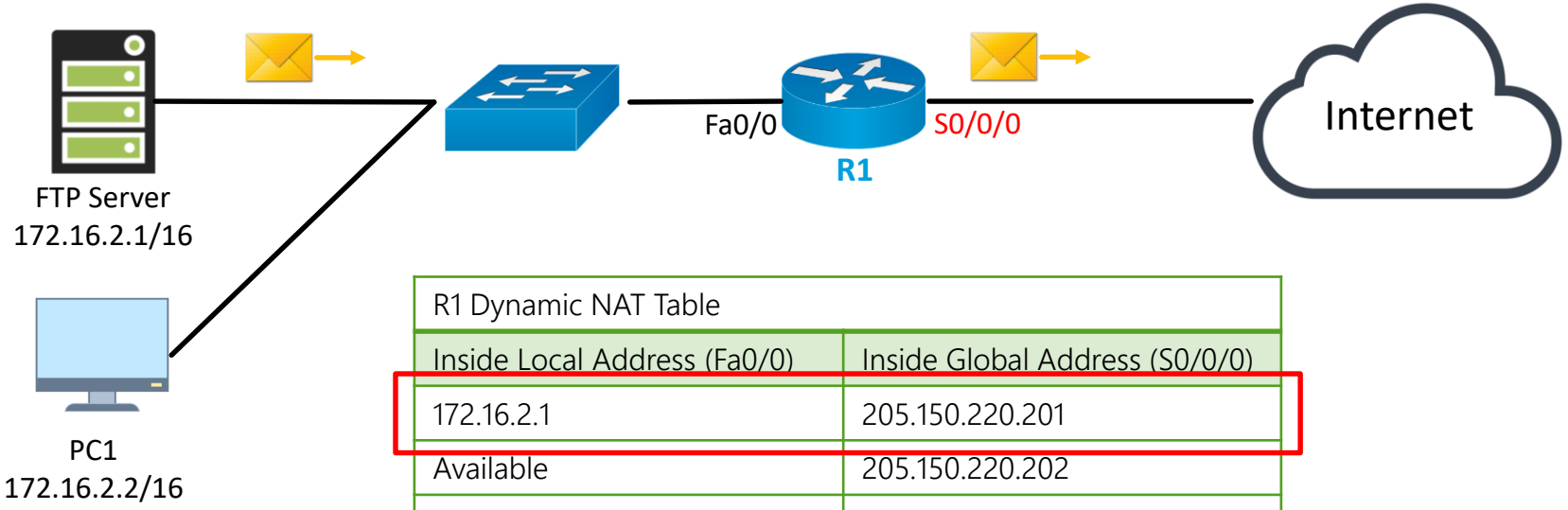
- NAT סטטי ממפה כתובת פרטית אחת לכתובת ציבורית אחת ולהפך, או במילה One-to-One.
- שיטת זו מאוד יעילה כשצריך לאפשר גישה מהרשת הציבורית אל שירותים ברשת הפנימית, כמו שרתי Web או שליטה מרחוק על רכיב רשת. כך לדוגמה ניתן לתקשר עם שרת או כל רכיב ברשת הפנימית מכל מקום בעולם, מכיוון שהנתב מוודא שהמידע ממקור חיצוני יגיע לרכיב ספציפי פנימי.



R1 Static NAT Table	
Inside Local Address (Fa0/0)	Inside Global Address (S0/0/0)
172.16.2.1	205.150.220.101
172.16.2.2	205.150.220.102
172.16.2.3	205.150.220.103

Dynamic NAT

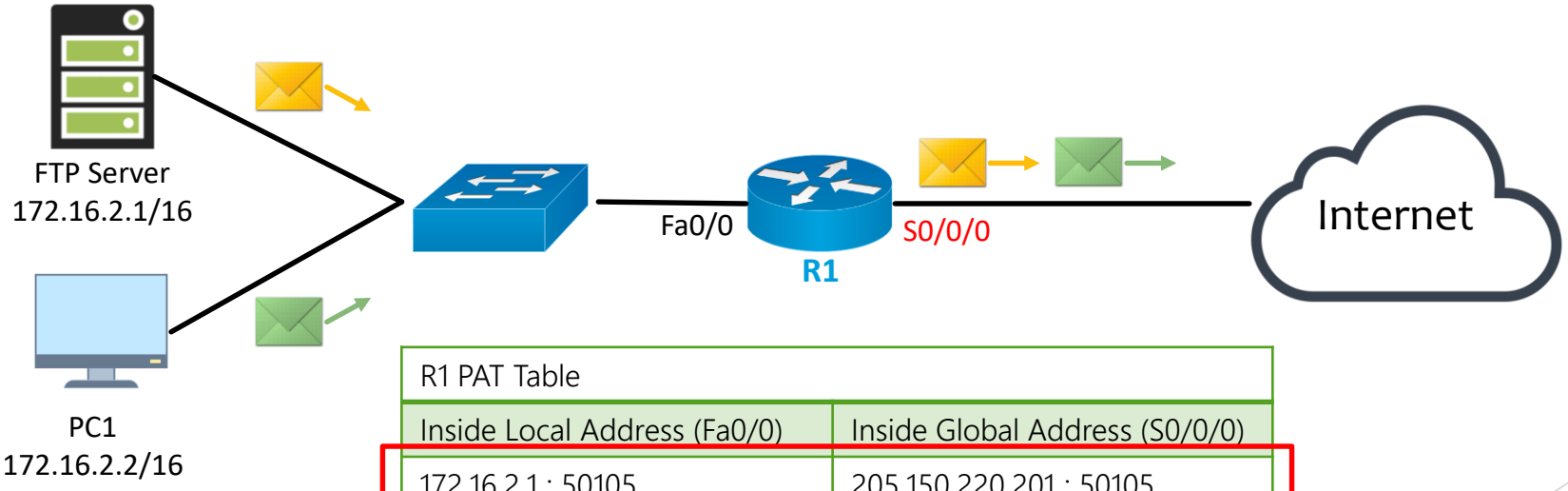
- NAT דינמי ממפה מספר כתובות פרטיות למספר כתובות ציבוריות ולהפך, או במילה Many-to-Many
- NAT מסוג זה משתמש במאגר (Pool) של כתובות ציבוריות, כשרכיב ברשת הפנימית מעוניין לפנות החוצה אל הרשת הציבורית, NAT ממפה אותו לכתובת ציבורית פנויה מהמאגר (בדר"כ הראשונה).



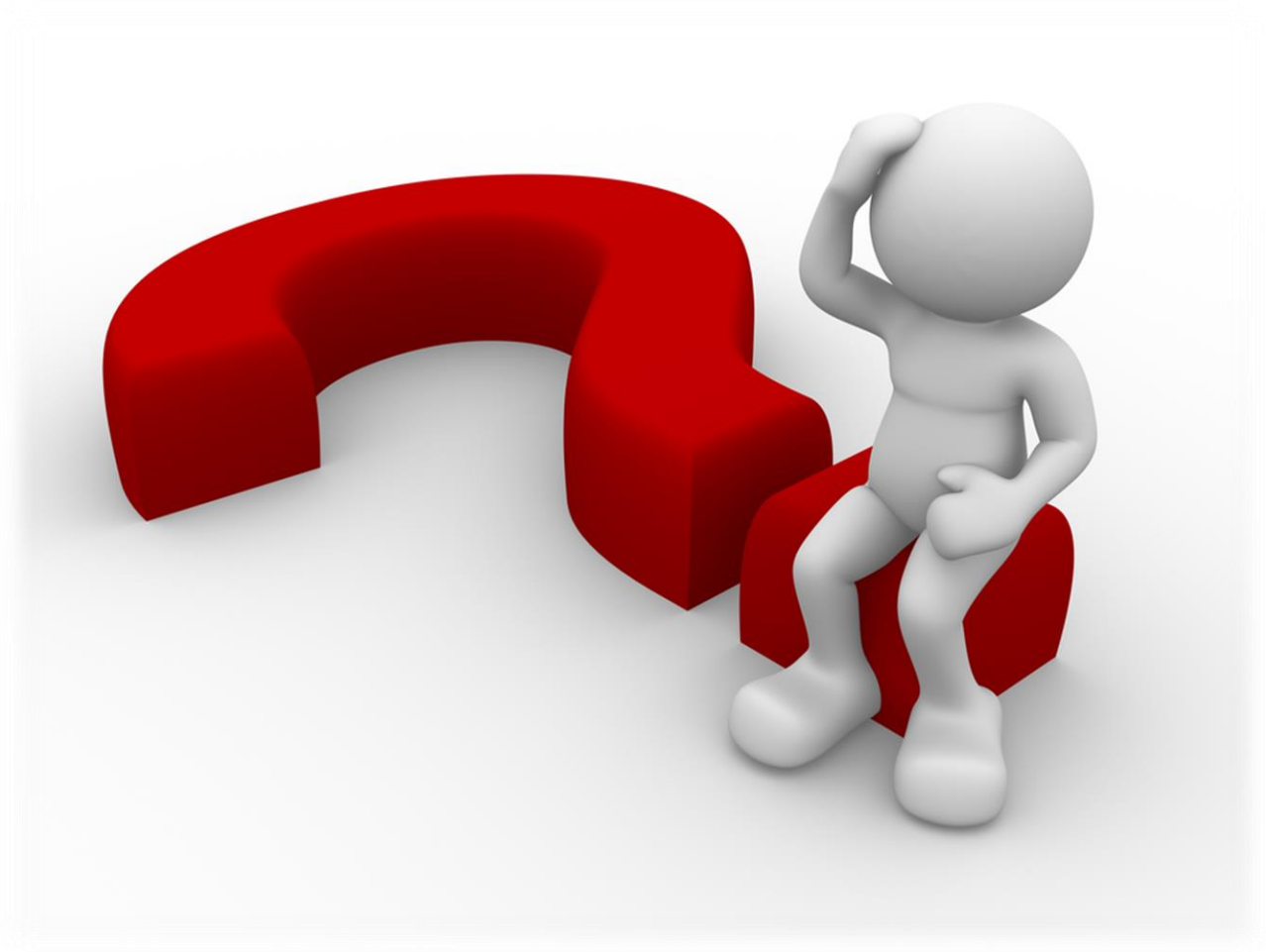
R1 Dynamic NAT Table	
Inside Local Address (Fa0/0)	Inside Global Address (S0/0/0)
172.16.2.1	205.150.220.201
Available	205.150.220.202
Available	205.150.220.203

PAT

- PAT נקרא גם NAT Overload ממפה מספר כתובות פרטיות לכתובת ציבורית אחת, או במילה Many-to-One
- שיטה זו היא הנפוצה ביותר והחסכונית ביותר. PAT מצליח להשיג את מטרתו בעזרת כתובת ציבורית אחת! PAT דואג למפות גם מספרי פורטים, זאת אומרת בכל פעם שרכיב ברשת הפנימית מעוניין לפנות החוצה לרשת הציבורית, הרכיב מצרף לכתובת המקור גם מספר פורט מקור (לרבות מהטווח הדינמי 49,152-65,535). PAT ממפה את הכתובת הפרטית לכתובת הציבורית כולל מספר הפורט. בצורה זו PAT מצליח לשמור על ייחודיות ושוני בין המשתמשים למרות השימוש בכתובת ציבורית זהה.



R1 PAT Table	
Inside Local Address (Fa0/0)	Inside Global Address (S0/0/0)
172.16.2.1 : 50105	205.150.220.201 : 50105
172.16.2.2 : 50106	205.150.220.201 : 50106



Command Page

- רשימת הפקודות המלאה והסבר, נמצאת בקובץ Command Page NAT.