

Network Fundamentals: Part 1

השפה של האינטרנט – איך העולם מחובר?

מה נלמד היום?

01

סוגי מדיה

איך מידע עובר פיזית ברשתות קוויות ואלחוטיות

02

חומרת רשת

ההבדל הקריטי בין Switch ל-Router ותפקידם

03

זהות ברשת

כתובות MAC ו-IP - מה ההבדל וכיצד הן עובדות

04

פרוטוקולים

השפה של הרשת - TCP, UDP ופורטים

המטרה שלנו: להבין לעומק איך מידע עובר מנקודה A לנקודה B ברשת המחשבים.

למה איש סייבר חייב להבין רשתות?

ההגנה

רוב מתקפות הסייבר מגיעות דרך הרשת. הבנת הרשת היא הבסיס לאיתור איומים ומניעת פריצות.

ההתקפה

כדי לפרוץ למערכת, צריך למצוא "דלת פתוחה" - פורט פתוח, שירות פגיע, או נקודת חולשה ברשת.

החקירה

כדי להבין מה קרה באירוע אבטחה, צריך לדעת לקרוא ולנתח תעבורת רשת ולעקוב אחר חבילות מידע.

"אי אפשר לאבטח את מה שלא מבינים איך הוא עובד."



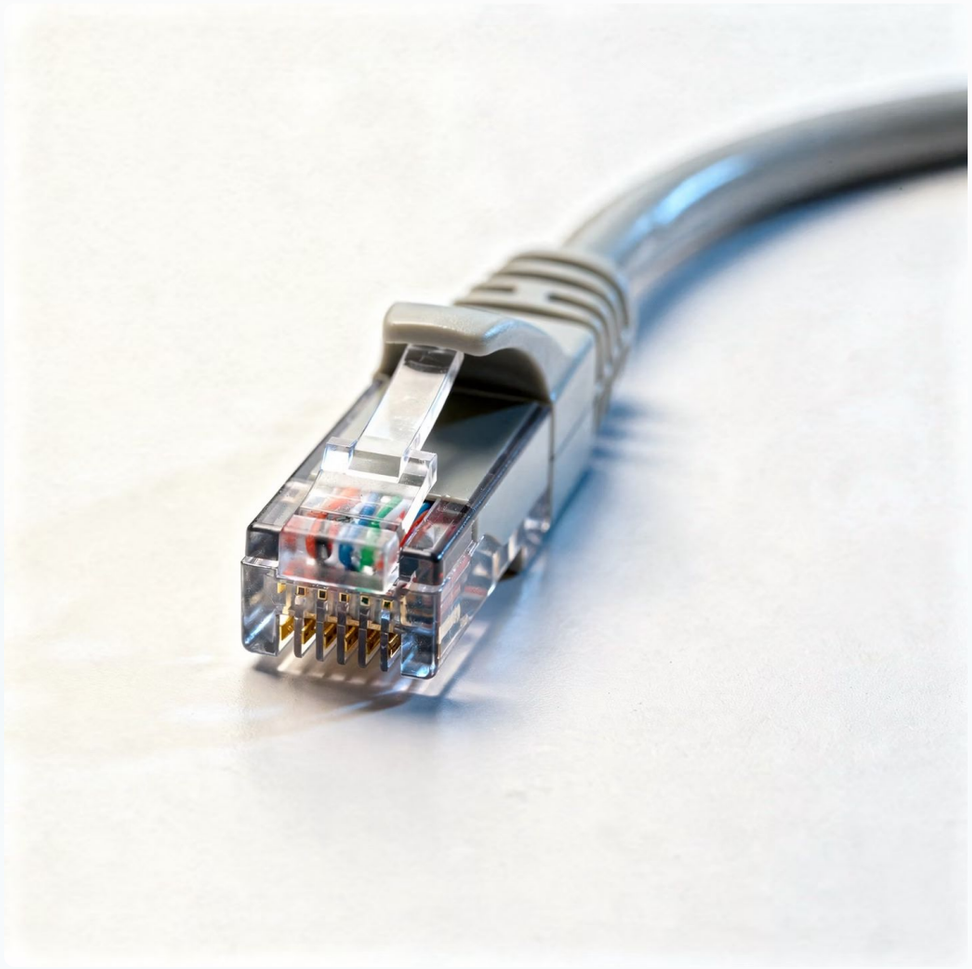
המדיה הפיזית – רשתות קוויות

סיב אופטי (Fiber Optic)



- משתמש באותות אור במהירות עצומה
- מתאים למרחקים ארוכים (עשרות קילומטרים)
- רוחב פס אדיר - גיגהביטים לשנייה
- תשתית האינטרנט העולמית - כבלים תת-ימיים

כבל רשת (Ethernet/Copper)



- הנפוץ ביותר ברשתות מקומיות (LAN)
- משתמש באותות חשמליים להעברת מידע
- מוגבל במרחק - עד 100 מטר בלבד
- זול וקל להתקנה

המדיה האלחוטית – Wireless Networks

Wi-Fi

רשתות אלחוטיות מקומיות המבוססות על גלי רדיו לטווח קצר. מספקות נוחות וגמישות (Mobility) על חשבון יציבות ואבטחה. נפוצות בבתים, משרדים ומקומות ציבוריים.

- תקני 802.11 (a/b/g/n/ac/ax)
- טווח: עד כ-50 מטר בתנאים טובים
- רגישות להפרעות ומכשולים פיזיים

רשתות סלולריות (4G/5G)

רשתות רחבות טווח המבוססות על אנטנות סלולריות. מאפשרות חיבור לאינטרנט מכל מקום בכיסוי הרשת, תוך כדי תנועה.

- כיסוי רחב - קילומטרים רבים
- מספקת מהירויות עד גיגהביט לשנייה 5G
- דורשות מנוי ותשלום לספק סלולרי



כרטיס הרשת – Network Interface Card



כרטיס הרשת (NIC - Network Interface Card) הוא הרכיב בחומרה שמחבר את המחשב או המכשיר לרשת. זהו "השער" שדרכו כל המידע נכנס ויוצא מהמכשיר שלנו.

סוגי כרטיסי רשת

- **פיזי (Wired):** חיבור ישיר לכבל Ethernet
- **אלחוטי (Wireless):** מכיל אנטנה לחיבור Wi-Fi
- **משולב:** תומך בשני סוגי החיבורים

עובדה חשובה: לכל כרטיס רשת יש "תעודת זהות" ייחודית שנצרבת בחומרה במפעל - כתובת MAC. זו זהותו הפיזית של המכשיר ברשת.



המתג – The Switch

הוא "שוטר תנועה" חכם ברשת המקומית. הוא מחבר מכשירים בתוך **אותה** רשת - למשל, כל המחשבים והמדפסות במשרד או בבית שלכם Switch.

קבלת חבילה

המתג מקבל חבילת מידע ממחשב אחד

זיהוי יעד

הוא בודק את כתובת ה-MAC של היעד

העברה חכמה

שולח את החבילה **רק** למכשיר המיועד

היעילות: בניגוד ל-Hub ישן, Switch לא משדר את המידע לכולם - הוא יודע בדיוק לאן לשלוח. זה חוסך רוחב פס ומגדיל את האבטחה.



הנתב – The Router

שעובד בתוך רשת אחת, הראוטר Switch-הוא "שער" המחבר בין **רשתות שונות**. בניגוד ל Router מתמחה בחיבור בין רשתות מרוחקות.

הדוגמה הקלאסית

הראוטר הביתי שלכם מחבר בין הרשת הפרטית בבית (x.x.192.168) לבין רשת האינטרנט העולמית הענקית.

קבלת החלטות נתיב

הראוטר מחליט מה הדרך הטובה והמהירה ביותר (Routing) להעביר מידע ליעד רחוק - תהליך הנקרא Routing.

תרגום כתובות

הראוטר מבצע NAT - מתרגם בין הכתובות הפרטיות של המכשירים בבית לכתובת הציבורית אחת שלכם באינטרנט.

ההבדל הקריטי – Switch vs Router

קריטריון	Switch (מתג)	Router (נתב)
תפקיד	חיבור מכשירים באותה רשת	חיבור בין רשתות שונות
היקף פעילות	רשת מקומית (LAN)	בין רשתות (WAN/Internet)
סוג כתובות	עובד עם כתובות MAC	עובד עם כתובות IP
החלטות	החלטות פשוטות - שליחה ישירה	החלטות מורכבות - בחירת נתיב
אנלוגיה	אינטרקום בין חדרים בבניין	שירות דואר בינלאומי

זכרו: Switch = תוך הבית, Router = בין הבית לעולם

נקודת גישה – Access Point



הוא המכשיר שהופך את הרשת הקווית לאלחוטית, ומאפשר למכשירים (Access Point (AP להתחבר באמצעות Wi-Fi.

בסביבת הבית

ה"ראוטר" הביתי שלכם הוא למעשה מכשיר משולב המכיל שלושה רכיבים:

- **Router** - לחיבור לאינטרנט
- **Switch** - לחיבור כבלים
- **Access Point** - לשידור Wi-Fi

בסביבה ארגונית

ארגונים משתמשים במכשירי AP נפרדים המפוזרים בתקרה לכיסוי אחיד. כל AP מתחבר לרשת הקווית ומשדר Wi-Fi באזור מוגדר.



כתובת MAC – הזהות הפיזית

כתובת MAC (Media Access Control) היא מספר סידורי ייחודי שנצרב על כרטיס הרשת במפעל. זוהי "תעודת הזהות" הפיזית והקבועה של המכשיר ברשת.

המבנה

12 תווים הקסדצימליים (0-9, A-F) המחולקים לזוגות

דוגמה: 00:1A:2B:3C:4D:5E

החצי הראשון

מזהה את היצרן (OUI - Organizationally Unique Identifier)

למשל: Intel, Apple, Dell

החצי השני

מזהה את הכרטיס הספציפי של אותו יצרן

קבוע ויניקודי בעולם

שימוש: כתובת MAC משמשת לזיהוי מכשירים בתוך הרשת המקומית בלבד. היא לא עוברת מעבר לראוטר.



כתובת IP – הזהות הלוגית

כתובת IP (Internet Protocol) היא כתובת לוגית שמוקצית למחשב כשהוא מתחבר לרשת - דומה למספר טלפון או כתובת דואר פיזית.

למה צריך שתי כתובות?

- מזהה את החומרה הפיזית **MAC**.
- מזהה את המיקום הלוגי ברשת **IP**.

זה כמו שיש לכם תעודת זהות (MAC) וכתובת מגורים (IP) - התעודה לא משתנה, אבל הכתובת כן.

ההבדלים מ-MAC

- כתובת IP **משתנה** כשעוברים רשת
- כתובת MAC **קבועה** בחומרה
- משמש לניתוב ברשת העולמית IP
- משמש לזיהוי ברשת המקומית MAC

פרוטוקול IPv4

192.168.1.15

IPv4 (Internet Protocol version 4) היא הגרסה הנפוצה ביותר של כתובות IP, עדיין רוב האינטרנט עובד איתה בשימוש כיום. למרות שהיא ישנה (משנות ה-80).

01

ארבעה חלקים (Octets)

הכתובת מורכבת מ-4 מספרים המופרדים בנקודות. כל מספר הוא בין 0 ל-255.

02

32 ביטים

מאחורי הקלעים, כל octet הוא 8 ביטים בבינארי. סך הכל 32 ביטים לכל כתובת.

03

המגבלה הגדולה

קיימות רק כ-4.3 מיליארד כתובות IPv4 אפשריות. עם מיליארדי מכשירים בעולם - הכתובות נגמרות!

בגלל המחסור, נוצר פתרון ביניים שנקרא NAT שמאפשר לרשת שלמה לחלוק כתובת ציבורית אחת.



העתיד של האינטרנט – IPv6

זוהי הגרסה .IP הוא הפתרון הסופי למחסור בכתובות (Internet Protocol version 6) IPv6 .IPv4 המודרנית שתחליף בהדרגה את

היתרונות

- **מספר אדיר:** 340 ונדציליון כתובות (36 אפסים!)
- **אבטחה מובנית:** IPsec מוטמע בפרוטוקול
- **ניתוב יעיל:** מבנה היררכי טוב יותר
- **עתיד מובטח:** מספיק לכל מכשיר בעולם

המבנה החדש

דוגמה לכתובת IPv6:

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

- 128 ביטים (במקום 32)
- 8 קבוצות של 4 תווים הקסדצימליים
- מופרדים בנקודותיים (:)

למרות היתרונות, המעבר ל-IPv6 איטי כי דורש שינוי בכל התשתיות. כרגע, האינטרנט תומך בשני הפרוטוקולים במקביל.

Public vs Private IP



כתובת ציבורית (Public IP)

הכתובת של הבית או העסק שלכם כלפי העולם. זו הכתובת שדרכה האינטרנט מזהה אתכם. היא ייחודית בכל האינטרנט - לא יכולות להיות שתי כתובות זהות.

דוגמאות לטווחים ציבוריים: כל כתובת שאינה בטווח הפרטי



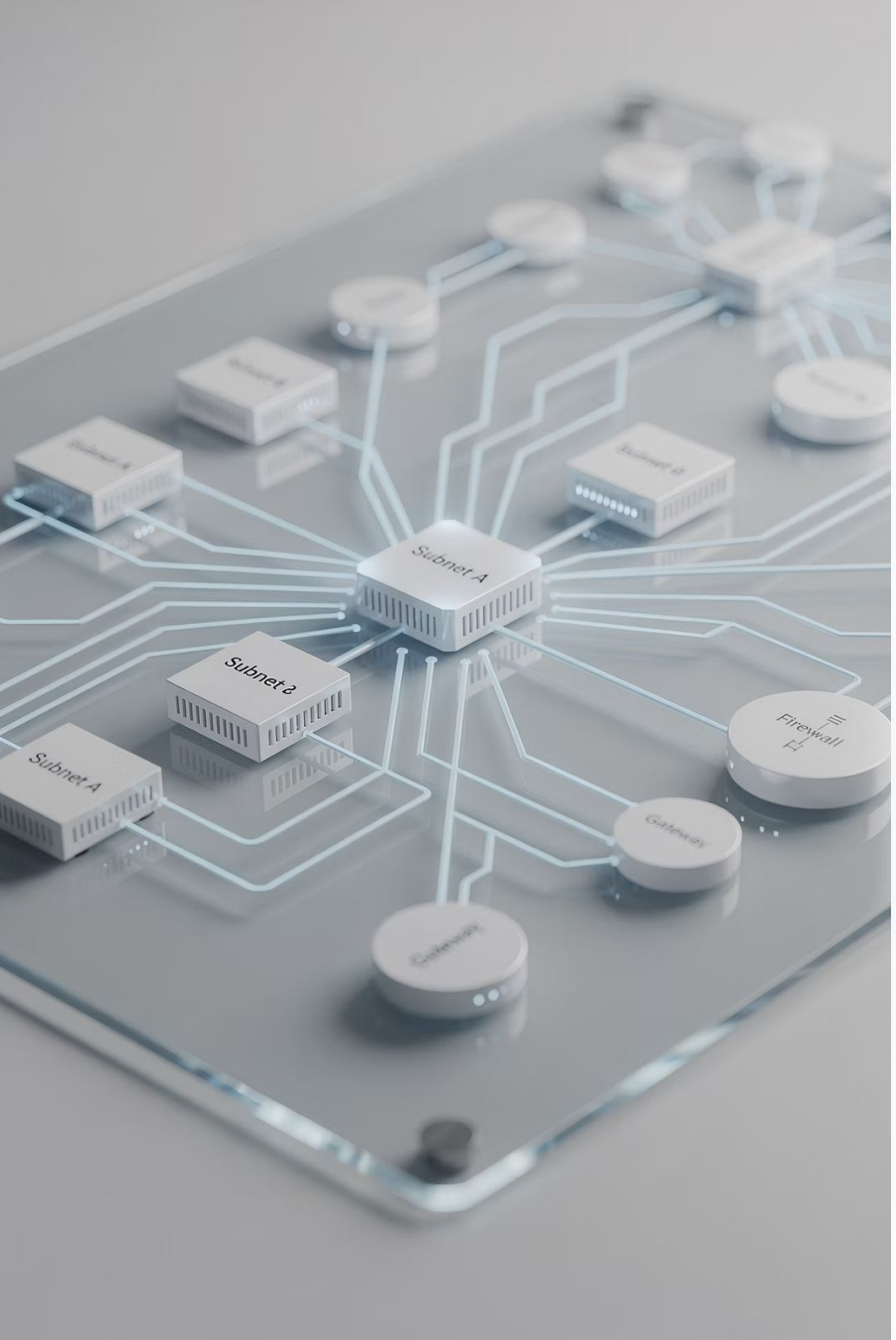
כתובת פרטית (Private IP)

הכתובת של המכשיר הספציפי בתוך הרשת הפנימית שלכם. מכשירים רבים יכולים לחלוק את אותו טווח פרטי ברשתות שונות.

טווחים שמורים:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

NAT (Network Address Translation): הראוטר מתרגם בין הכתובות הפרטיות הרבות בבית לכתובת הציבורית האחת שלכם.



חלוקת הרשת – Subnet Mask

איך המחשב יודע אם המכשיר שאיתו הוא רוצה לדבר נמצא "בבית" (ברשת המקומית) או "בחוץ" (באינטרנט)? התשובה: Subnet Mask.

מהי מסכת רשת?

היא "מסכה" מתמטית Subnet Mask שמחלקת את כתובת ה-IP לשני חלקים נפרדים בעלי משמעות שונה.

Network ID

החלק הראשון מזהה את הרשת עצמה - כמו שם הרחוב. כל המכשירים באותה רשת יחלקו את אותו Network ID.

Host ID

החלק השני מזהה את המכשיר הספציפי ברשת - כמו מספר הבית ברחוב. זה מה שמבדיל בין מכשיר למשנהו.

דוגמה מעשית ל-Subnet

הנתונים

כתובת IP:

192.168.1.10

Subnet Mask:

255.255.255.0

הפענוח

Network ID (הרחוב)

192.168.1

כל המחשבים בבית שלכם יתחילו עם אותם שלושת המספרים הראשונים.

Host ID (מספר הבית)

10

זה המזהה הייחודי של המחשב הספציפי שלכם ברשת הביתית.

המשמעות המעשית: כשהמחשב שלכם רוצה לשלוח מידע ל-192.168.1.25, הוא יודע שזה באותה רשת (אותו רחוב) ושולח ישירות דרך ה-Switch. אבל כשהוא רוצה לשלוח ל-8.8.8.8 (גוגל), הוא מבין שזה רשת אחרת ושולח דרך הראוטר.



ה"מלצר" האוטומטי – DHCP

הוא הפרוטוקול שחוסך לנו את הצורך להגדיר DHCP (Dynamic Host Configuration Protocol) לכל מכשיר שמתחבר לרשת IP ידנית כתובת.

1

Discovery

המכשיר החדש משדר: "היי! אני חדש פה, מישהו יכול לעזור לי?"

2

Offer

שרת ה-DHCP עונה: "שלום! יש לי כתובת IP פנויה בשבילך: 192.168.1.25"

3

Request

המכשיר מאשר: "מעולה, אני לוקח את הכתובת הזו!"

4

Acknowledge

השרת מאשר: "הכתובת שלך! בנוסף, הנה Subnet Mask, Gateway וכו'."

מידע נוסף שה-DHCP מספק: Subnet Mask, Default Gateway (כתובת הראוטר), DNS Servers, ועוד. כל מה שהמכשיר צריך להתחיל לעבוד ברשת!

הדלתות של המחשב – Ports

יש לנו כתובת IP שמזהה את המחשב, אבל איך המחשב יודע לאיזה תוכנה או שירות להעביר את המידע? התשובה: **פורטים**.



מהו Port?

הוא מספר ייחודי (בין 0 ל-65,535) שמזהה תוכנה או שירות ספציפי במחשב. כל תוכנה Port ש"מקשיבה" לרשת פותחת פורט משלה.

למה זה נחוץ?

המחשב שלכם מריץ המון דברים במקביל: דפדפן, תוכנת מייל, Zoom, משחק. הפורט מבטיח שכל מידע שמגיע מהרשת יועבר לתוכנה הנכונה.

אנלוגיה: כתובת IP היא כמו כתובת הבניין, והפורט הוא מספר הדירה.

פורטים מפורסמים (Well-Known Ports)

פורטים מסוימים שמורים לשירותים סטנדרטיים ומוכרים. חשוב לזכור אותם - זה חלק בסיסי בכל מבחן סייבר!

Port 80 – HTTP

גלישה רגילה באינטרנט (לא מוצפנת). כשאתם מקלידים http://example.com, הדפדפן מתחבר לפורט 80.

Port 443 – HTTPS

גלישה מאובטחת ומוצפנת באינטרנט. זה הפורט שרואים כשיש "מנעול" ליד הכתובת בדפדפן.

Port 53 – DNS

"ספר הטלפונים" של האינטרנט. תרגום שמות אתרים (google.com) לכתובות IP (142.250.185.46).

Port 22 – SSH

חיבור מאובטח למחשב מרחוק. משמש מנהלי מערכות לשליטה בשרתים.

טיפ למבחן: חייבים לדעת את המספרים האלו בעל פה! הם מופיעים כמעט בכל מבחן רשתות וסייבר.



שכבת התעבורה – Transport Layer

כשאתם שולחים מידע ברשת - למשל, תמונה או סרטון - הוא לא עובר כגוש אחד גדול. במקום זאת, המידע מחולק ל**חבילות** (Packets) קטנות שנשלחות בנפרד.

1

למה לחלק לחבילות?

יעילות - מספר חבילות יכולות לנסוע במקביל בנתיבים שונים. גמישות - אם חבילה אחת הולכת לאיבוד, לא צריך לשלוח הכל מחדש.

2

שתי דרכים לשליחה

יש שני פרוטוקולים עיקריים לשליחת חבילות: TCP ו-UDP. כל אחד מתאים למטרה שונה.

האמין והאחראי – TCP

.הוא הפרוטוקול שמבטיח שכל המידע יגיע ליעד, שלם ובסדר הנכון - כמו שליח אמין שלא עוזב עד שמקבלים את החבילה (Transmission Control Protocol) TCP



אישור קבלה

לכל חבילה שנשלחת, הצד המקבל שולח אישור חזרה. אם האישור לא מגיע, החבילה נשלחת שוב.



שמירת סדר

החבילות עשויות להגיע בלבלול, אבל TCP מסדר אותן בחזרה לפי המספר שלהן.



בקרת זרימה

מתאים את קצב השליחה ליכולת של TCP הצד המקבל - לא מציף אותו במידע.

שימושים: כל מקום שבו דיוק קריטי - טעינת דפי אינטרנט, שליחת מיילים, הורדת קבצים, העברות כספיות. כל מקום שבו אי אפשר לאבד אפילו ביט אחד.



לחיצת היד המשולשת – Way-3 Handshake

לפני שמעבירים מידע ב-TCP, המחשבים מבצעים "טקס היכרות" קצר שנקרא Way-3 Handshake. זה מבטיח ששני הצדדים מוכנים לתקשורת.

1

שלב 1: SYN

הלקוח: "שלום שרת, אפשר לפתוח חיבור?" (SYN = Synchronize)

2

שלב 2: SYN-ACK

השרת: "כן, אני מוכן! גם אני רוצה לפתוח חיבור איתך." (SYN + ACKnowledge)

3

שלב 3: ACK

הלקוח: "מצוין, החיבור פתוח. מתחיל לשלוח מידע!" (ACKnowledge)

רק אחרי השלבים האלה, המידע האמיתי מתחיל לזרום. זו הסיבה שחיבור TCP לוקח רגע קצר להתבסס.



המהיר והעצבני – UDP

UDP (User Datagram Protocol) הוא הפרוטוקול ש"שוגר ושוכח" - שולח את המידע הכי מהר שאפשר, **בלי** לבדוק אם הוא הגיע.

אין לחיצת יד

הוא פשוט לא מבצע 3-Way Handshake. UDP מתחיל לשלוח מידע מיד, ללא הכנות.

אין אישורי קבלה

אחרי ששלח חבילה, UDP לא מחכה לאישור. הוא לא יודע ולא אכפת לו אם היא הגיעה.

אין בקרת סדר

החבילות עשויות להגיע בלבלול, והמערכת צריכה להתמודד עם זה (או להתעלם).

היתרון הגדול: מהירות אדירה ועיכוב מינימלי. כשמהירות חשובה יותר מדיוק מוחלט, UDP הוא הבחירה.

מתי משתמשים ב-UDP?

.מושלם לכל יישום שבו **זמן אמת** חשוב יותר מדיוק מושלם. אם איבדנו חתיכת מידע קטנה, עדיף להמשיך הלאה מאשר לעצור ולחכות UDP



שיחות וידאו

-כולם משתמשים ב - Zoom, Teams, Google Meet
אם כמה פיקסלים הלכו לאיבוד, זה לא נורא. אבל UDP.
.עיכוב של שנייה הורס את השיחה



סטרימינג

אם פריים אחד חסר, .YouTube, Netflix, Twitch
העין לא תשים לב. אבל אם הסרטון ייעצר כל פעם
.לבקש חבילה מחדש - זה בעיה



גיימינג אונליין

במשחקים, תגובה מהירה קריטית. אם מיקום השחקן לא
עודכן בדיוק אחד, אפשר לתקן בעדכון הבא. אבל lag
הורס את החוויה.

השוואה מלאה – TCP vs UDP

תכונה	TCP	UDP
חיבור	מבוסס חיבור (3-Way Handshake)	ללא חיבור (Connectionless)
אמינות	גבוהה - מבטיח הגעת כל הנתונים	נמוכה - אין ערבות להגעה
מהירות	איטי יותר בגלל הבדיקות	מהיר מאוד - overhead מינימלי
סדר חבילות	מסודר - מבטיח סדר נכון	לא מסודר - חבילות עלולות להתבלבל
גודל Header	20 בייטים (יותר מידע בקרה)	8 בייטים בלבד (קל וזריז)
שימושים	קבצים, בנקאות ,Web, Email	וידאו, אודיו, משחקים, DNS

כלל אצבע: TCP לדיוק, UDP למהירות!

כלי הדיאגנוסטיקה – ICMP

ICMP (Internet Control Message Protocol) הוא פרוטוקול מיוחד שלא מעביר מידע של משתמשים, אלא **הודעות שגיאה ובקרה** בין מכשירי רשת.

תפקידים עיקריים

- **דיווח על שגיאות:** "היעד לא זמין", "הרשת לא נגישה"
- **בדיקת קישוריות:** האם מכשיר מסוים מחובר וחי?
- **דיאגנוסטיקה:** מדידת זמני תגובה, מציאת בעיות בנתיב

הכלי המפורסם: Ping

פקודת Ping משתמשת ב-ICMP כדי לבדוק קישוריות. היא שולחת "Echo Request" ומקבלת "Echo Reply".




```
C:\> ping 8.8.8.8

Reply from 8.8.8.8:
 bytes=32 time=15ms
Reply from 8.8.8.8:
 bytes=32 time=14ms
```

פקודות רשת בסיסיות

כל איש סייבר חייב להכיר את פקודות הבסיס האלה. הן כלים יומיומיים לבדיקה, דיאגנוסטיקה ופתרון בעיות.

ipconfig / ifconfig

הצגת מידע על כרטיסי הרשת שלך: IP, Subnet Mask, Gateway.

`ipconfig /all` (Windows)

`ifconfig` (Linux/Mac)

ping

בדיקת קישוריות למכשיר. "האם אתה שם? כמה זמן לוקח להגיע אליך?"

`ping google.com`

nslookup

בדיקת שרתי DNS ותרגום שמות אתרים לכתובות IP.

`nslookup google.com`

traceroute / tracert

עוקב אחרי המסלול שהמידע עובר דרכו עד ליעד. רואים כל ראוטר בדרך.

`tracert google.com`

בוחן מהיר – בדקו את עצמכם!

1

איזה פרוטוקול משמש לשיחות וידאו?

תשובה: UDP - כי מהירות חשובה יותר מדיוק מוחלט בזמן אמת.

2

מהו מספר הפורט של HTTPS?

תשובה: 443 - גלישה מאובטחת ומוצפנת באינטרנט.

3

איזה רכיב רשת מחבר בין רשתות שונות?

תשובה: Router (נתב) - בניגוד ל-Switch שעובד בתוך אותה רשת.

4

האם כתובת MAC משתנה כשעוברים דירה?

תשובה: לא! כתובת MAC צרובה בחומרה וקבועה. רק כתובת ה-IP משתנה.

5

מהו תפקיד ה-DHCP?

תשובה: הקצאה אוטומטית של כתובות IP למכשירים שמתחברים לרשת.

סיכום ומה הלאה?

מדיה

למדנו על כבלים, אלחוט, וכיצד המידע עובר פיזית

חומרה

הכרנו Switch, Router, Access Point והבדלים ביניהם



פרוטוקולים

שלטנו ב-TCP, UDP, פורטים ושפת הרשת

זהויות

הבנו MAC, IP, Subnet והבדלים בין ציבורי לפרטי

בשיעור הבא: Network Fundamentals Part 2

נצלול לעומק פרוטוקולי היישום: **DNS** (איך הדפדפן יודע לאן להגיע), **HTTP/HTTPS** (השפה של הווב), ו-**Email Protocols**. נבין איך כל הרכיבים שלמדנו היום עובדים ביחד כשאתם גולשים באינטרנט.

משימה לבית: פתחו את ה-Command Prompt/Terminal ובדקו מה ה-IP של המחשב שלכם (ipconfig). נסו לעשות Ping לשרתי גוגל (8.8.8.8) ורשמו את זמן התגובה. האם יש הבדל בזמנים?

המשך ללימוד חלק 2