

תקשורת מחשבים ואלגוריתמים מבוזרים

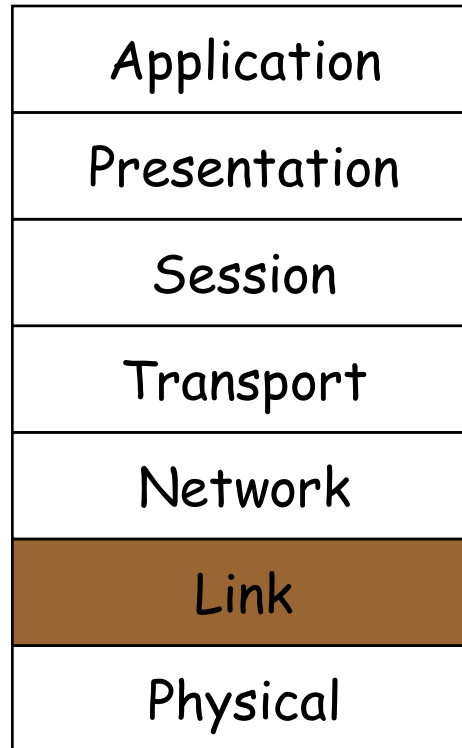


קורס מס' 202-2-1131

מתרגל: ד"ר גיא לשם leshemg@cs.bgu.ac.il

הרצאה שלישית – שכבת קישור הנתונים

שכבת קישור הנתונים



The 7-layer OSI Model

שכבת קישור הנתונים

המטרה שלנו:

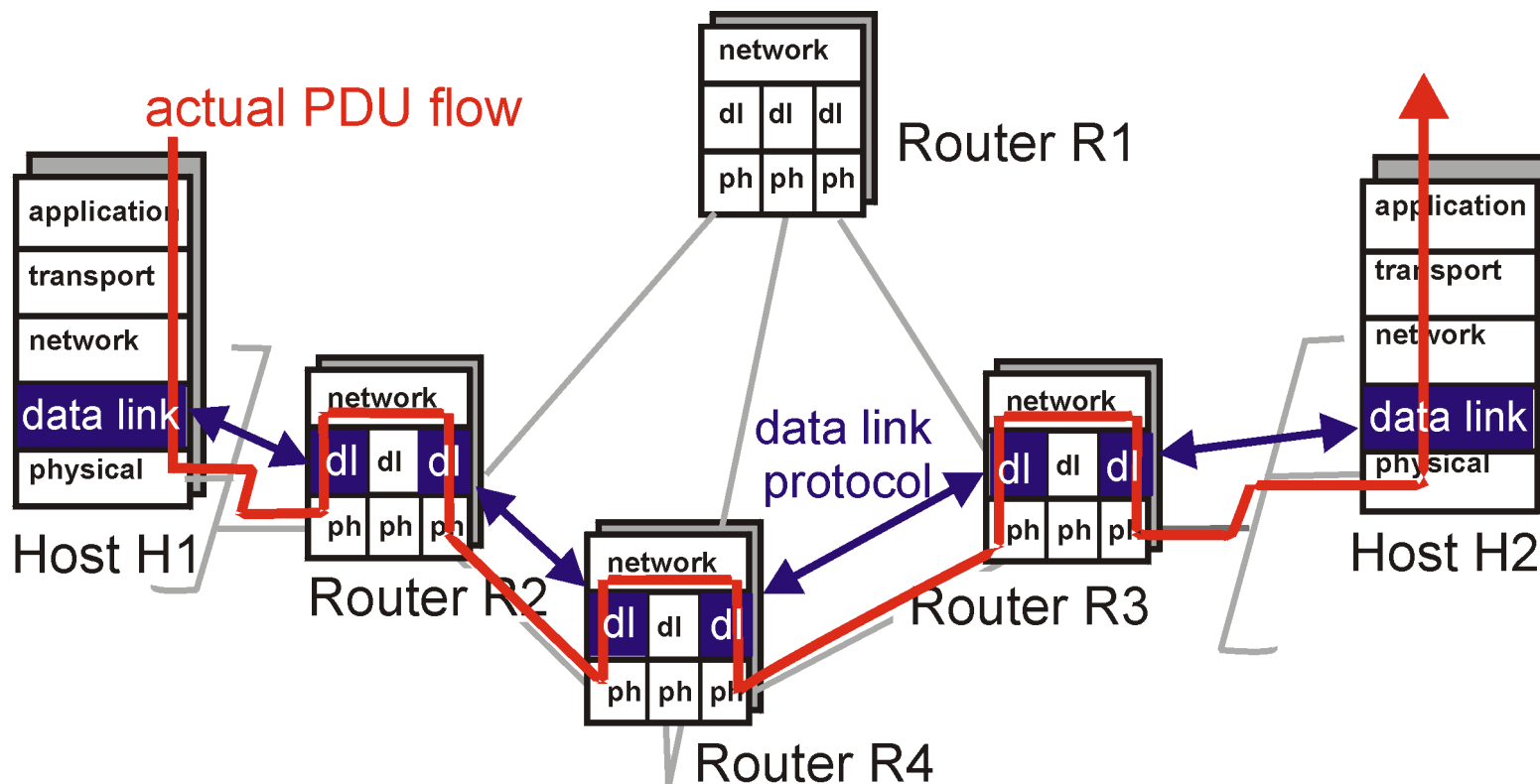
- להבין את העקרונות מאחורי השירות שמספקת שכבת קישור הנתונים:
 - גילוי שגיאות, תיקון שגיאות.
 - חלוקה של ערוץ שידור: גישות מרובות.
 - שיטת פנייה למשאבים ברשת באמצעות שכבת הקישור.
- ייצוג וביצוע של טכנולוגיות שונות של שכבת קישור הנתונים.

מבט על:

- שירותים של שכבת הקישור.
 - גילוי שגיאות, תיקון שגיאות.
 - פרוטוקלי גישות מרובות ו-רשתות מקומיות (LANs).
 - שיטת פנייה למשאבים ברשת באמצעות שכבת הקישור.
- טכנולוגיות של שכבת קישור הנתונים:
 - אתרנט (Ethernet), תקן של רשת תקשורת מקומית.

שירותים של שכבת הקישור

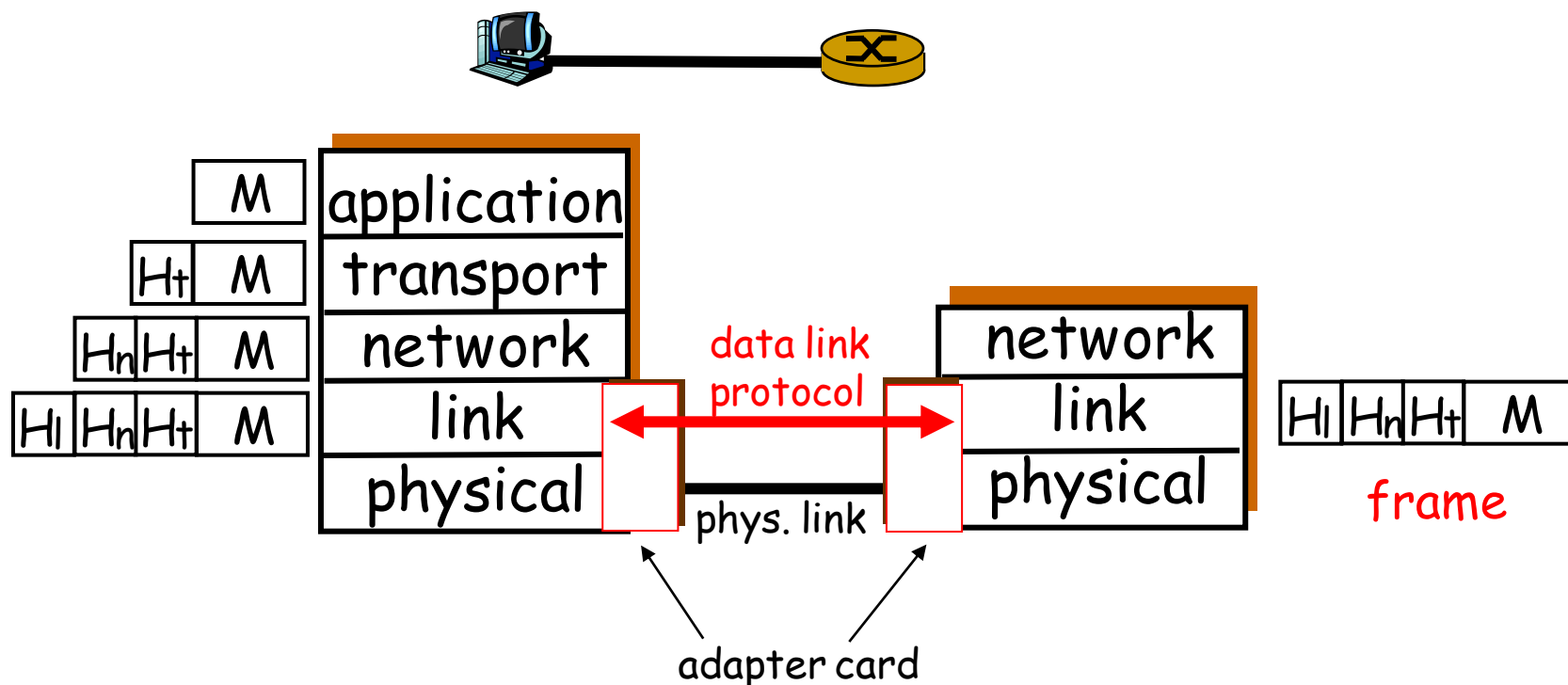
שכבת קישור נתונים: מסלול ההקשר



PDU (protocol data unit) – המידע המועבר כיחידה אחת בין ישויות הרשת יכול להכיל מידע של בקרה, מידע של כתובת, או של נתונים.

שכבת קישור נתונים: מסגרת ההקשר

- חיבור של שני התקנים בצורה פיזית.
- host-router, router-router, host-host
- יחידה של הנתונים : מסגרת - חבילות נתונים (*frame*).



שרותי שכתב קישור הנתונים

□ חלוקה להודעות בדידות, גישות לערוץ:

- עטיפה של הנתונים לתוך מסגרות (frame - חבילות נתונים), הוספה של "ראש" (header) ו-"זנב" (trailer).
- חיבור גישה לערוץ תקשורת.
- "כתובת פיסיית" לכל ראש של מסגרת לזיהוי מקור ויעד.
- "הכתובת הפיסיית" שונה מכתובת ה-IP.

□ מישלוח אמין של נתונים בין שני התקנים פיסיים מחוברים ביניהם:

- לעתים רחוקות נשתמש בבערוץ בעל קצב שידור נמוך (זוג שזור לדוגמא) עם מיעוט שגיאות במהלך השידור.
- בד"כ נשתמש בערוץ תקשורת אלחוטי עם הרבה שגיאות במהלך השידור.

שרותי שכבת קישור הנתונים (המשק)

□ בקרת זרימה (flow control):

- בקרה על העברת הנתונים בין שני מחשבים (השולח והמקבל).

□ גילויי שגיאות (error detection):

- שגיאות נגרמות ע"י היחלשות האות עם עליית אורך הכבלים ברשת, רעש.
- הקולט (receiver) מגלה נוכחות של שגיאות.
- שולח האות (sender) שולח את החבילה מחדש.
- הקולט מתגבר בעצמו על הבעיה.

□ תיקון שגיאות (error correction):

- הקולט מזהה ומתקן את שגיאות הביטים ללא שימוש בשליחה חוזרת.
- השיטה נקראת FEC (forward error correction).

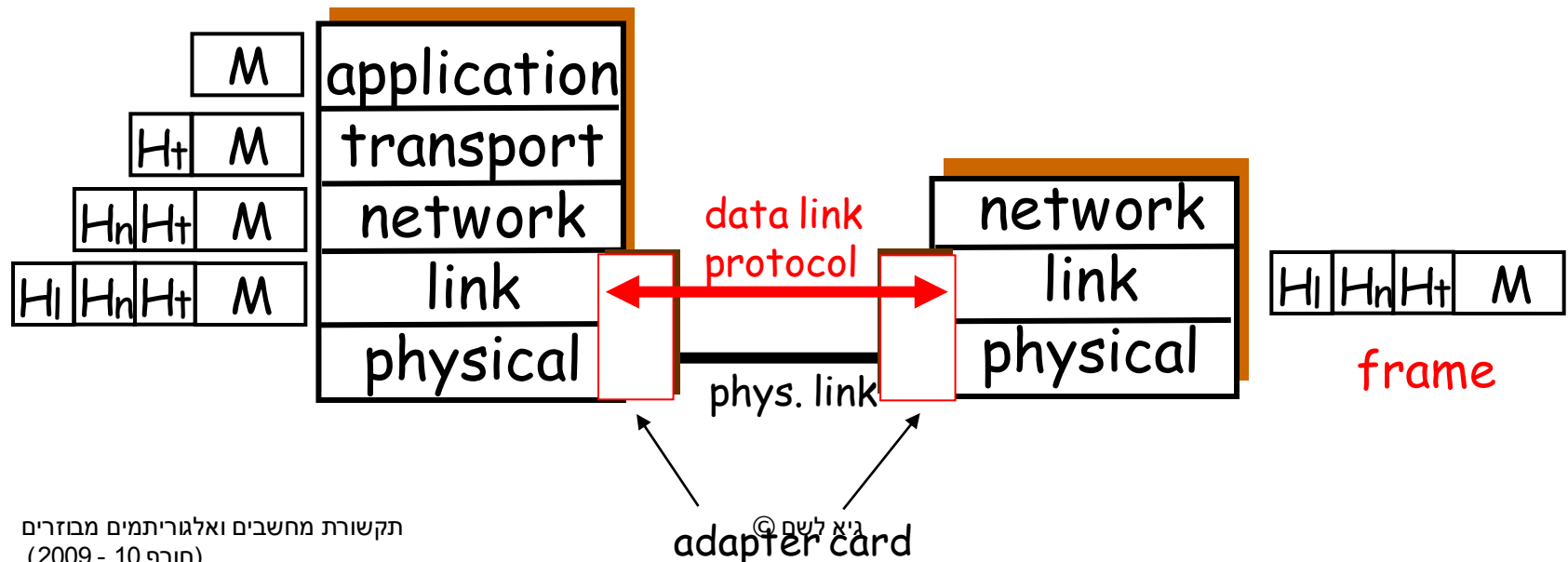
שכבת קישור הנתונים: המימוש (מערכת מחשב)

מתאם "adapter" - כרטיס המתחבר ללוח האם ומאפשר ביצוע פעולות שונות



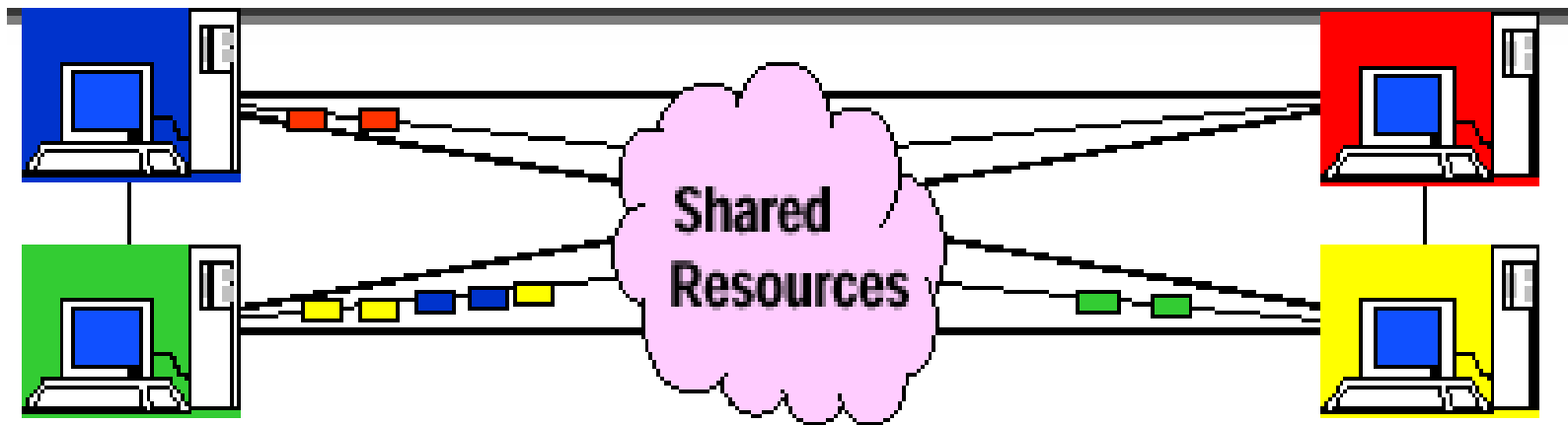
לדוגמא: כרטיס, כרטיס Ethernet.

בד"כ כולל RAM, DSP PCMCIA chips, host bus, interface ו- link interface.



(Frames) מסכת

מוטיבציות החביאה



■ במקום לשולח את הנתונים בבלוק יחיד, נשבור אותו לסידרה של מסגרות (חבילות מידע):

- יכולת האיחסון הזמני (buffer size) של הקולט יכולה להיות מוגבלת.
- ככל שזמן השידור ארוך יותר, הסבירות לשגיאות גדלה ונזדקק לבצע שליחה חוזרת.
- שיפור במשאבים המשותפים (לדוגמא שידור מרובב - העברת מספר הודעות בו זמנית בערוץ אחד)

שיטות לזיהוי אסכרות

□ ספירת בייטים (יחידת מידע בסיסית הכוללת 8 סיביות).

■ שיטה זו משמשת לזיהוי frame באופן כללי.

□ Byte stuffing - שיטת ה-byte stuffing שולחת תווים מיוחדים לזיהוי התחלה/סיום של החבילה.

□ Bit stuffing - שיטת ה-bit stuffing שולחת דגל בינרי בתחילת וסיום החבילה.

■ כאשר שתי השיטות משמשות לזיהוי של תחילה וסיום של חבילה המשודרת.

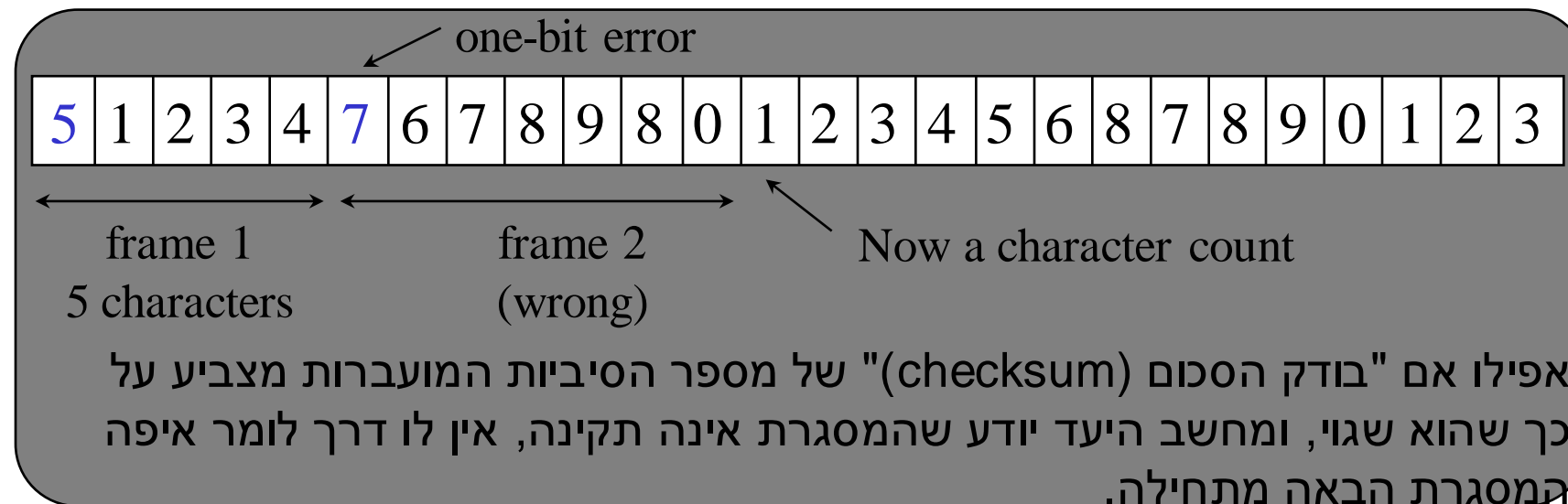
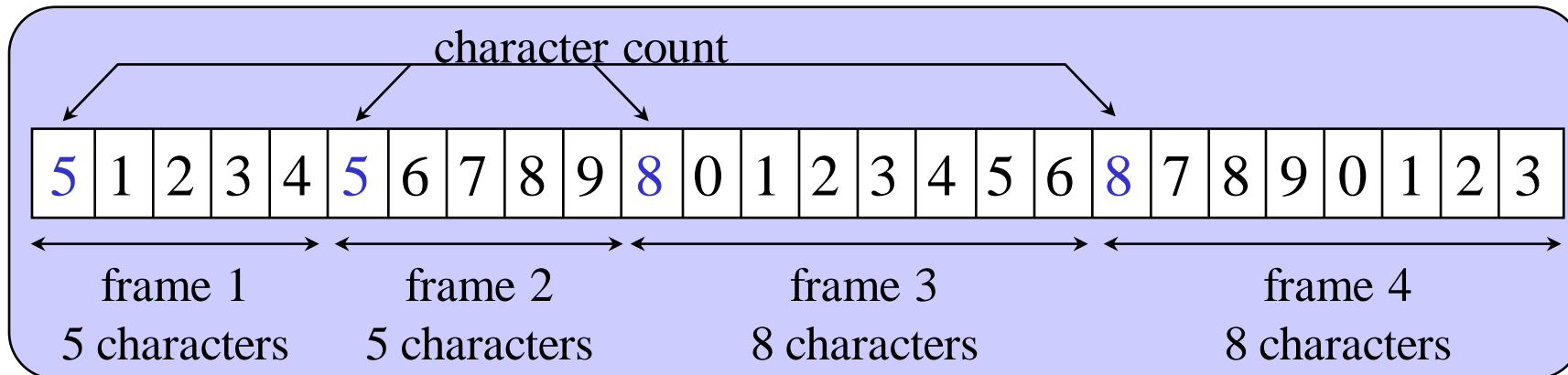
מסכרות (חבילות איזע)

□ נתחיל ונסיים את החבילה עם ייצוג ספרתי מיוחד
(**byte/character stuffing**).

□ נתחיל ונסיים עם דגל בינארי (**bit stuffing**).

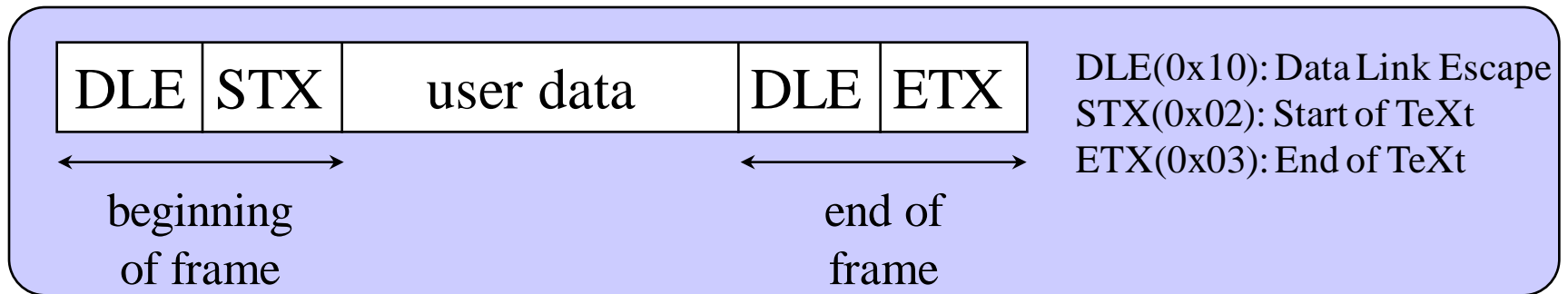


Character Count



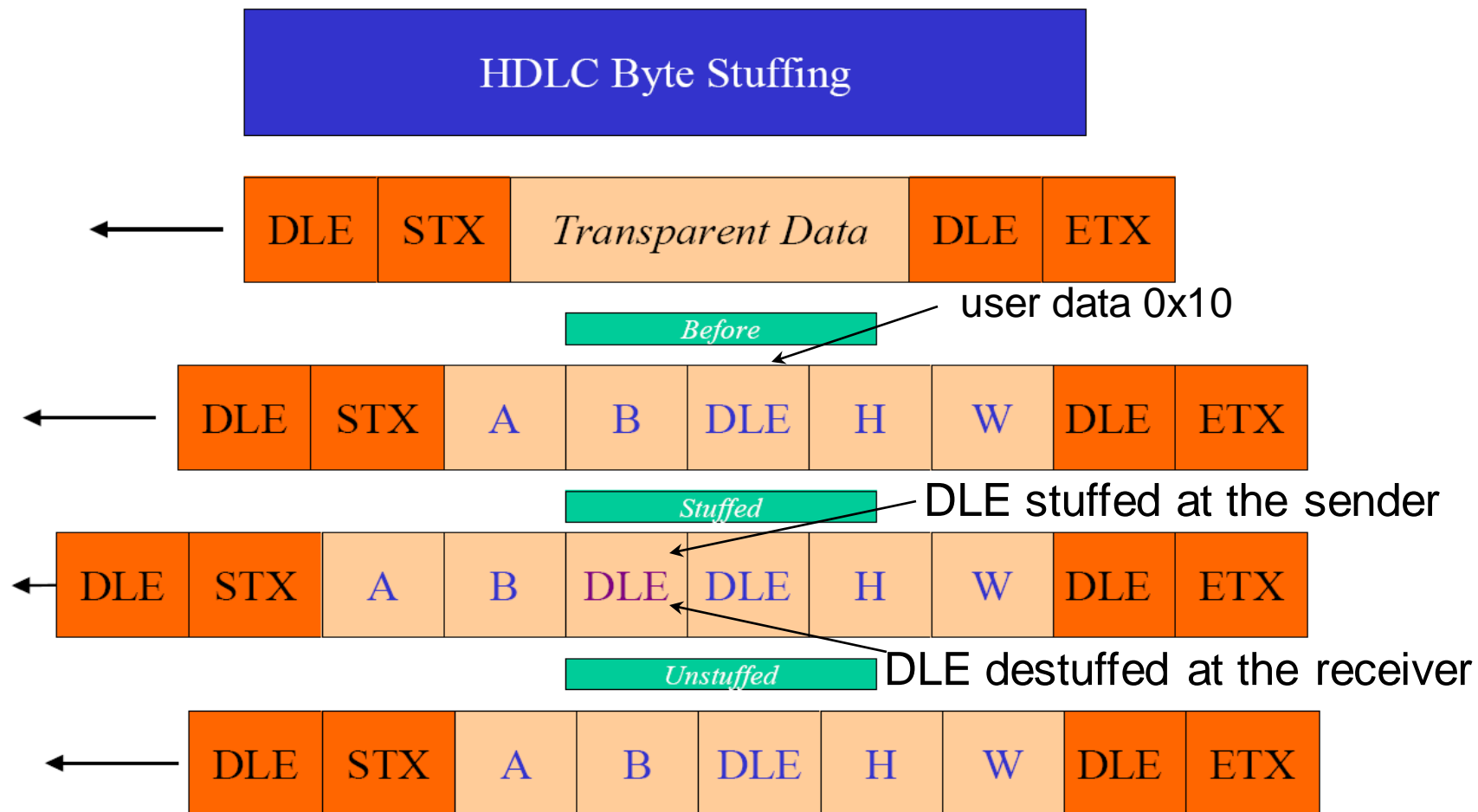
Byte Stuffing

- מתיחס גם ל- Character Stuffing.
- תוי ASCII משמשים כתוחמי המסגרת, לדוגמא: DLE STX ו- DLE ETX



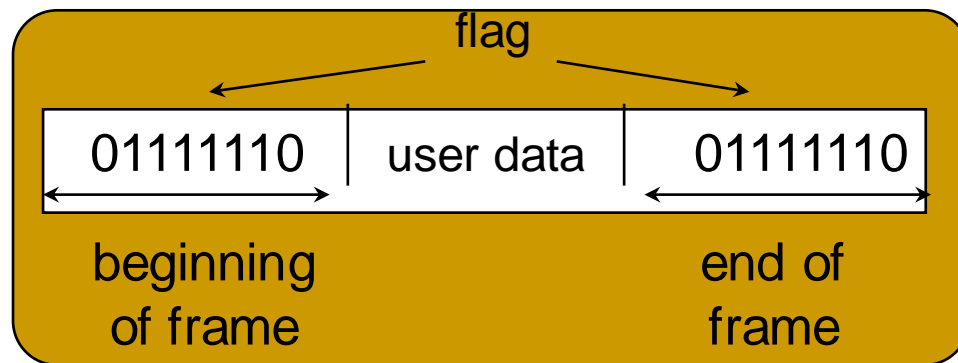
- הבעיה: מה קורה אם תבניות אותיות האלה (DLE) קורות בתוך טקסט?
- פתרון: השולח "ממלא" DLE נוספים לתוך זרם הנתונים, לפני כל מקרה של DLE "מקורי" בזרם הנתונים.
- הקולט "מרוקן" את ה-DLE הנוספים לפני שהוא שולח את המידע לשכבת התקשורת.

Byte Stuffing



Bit Stuffing

- כל מסגרת (frame) מתחילה ומסתיימת בתבנית מיוחדת הנקראת דגל בייט (flag byte) <-- [01111110].

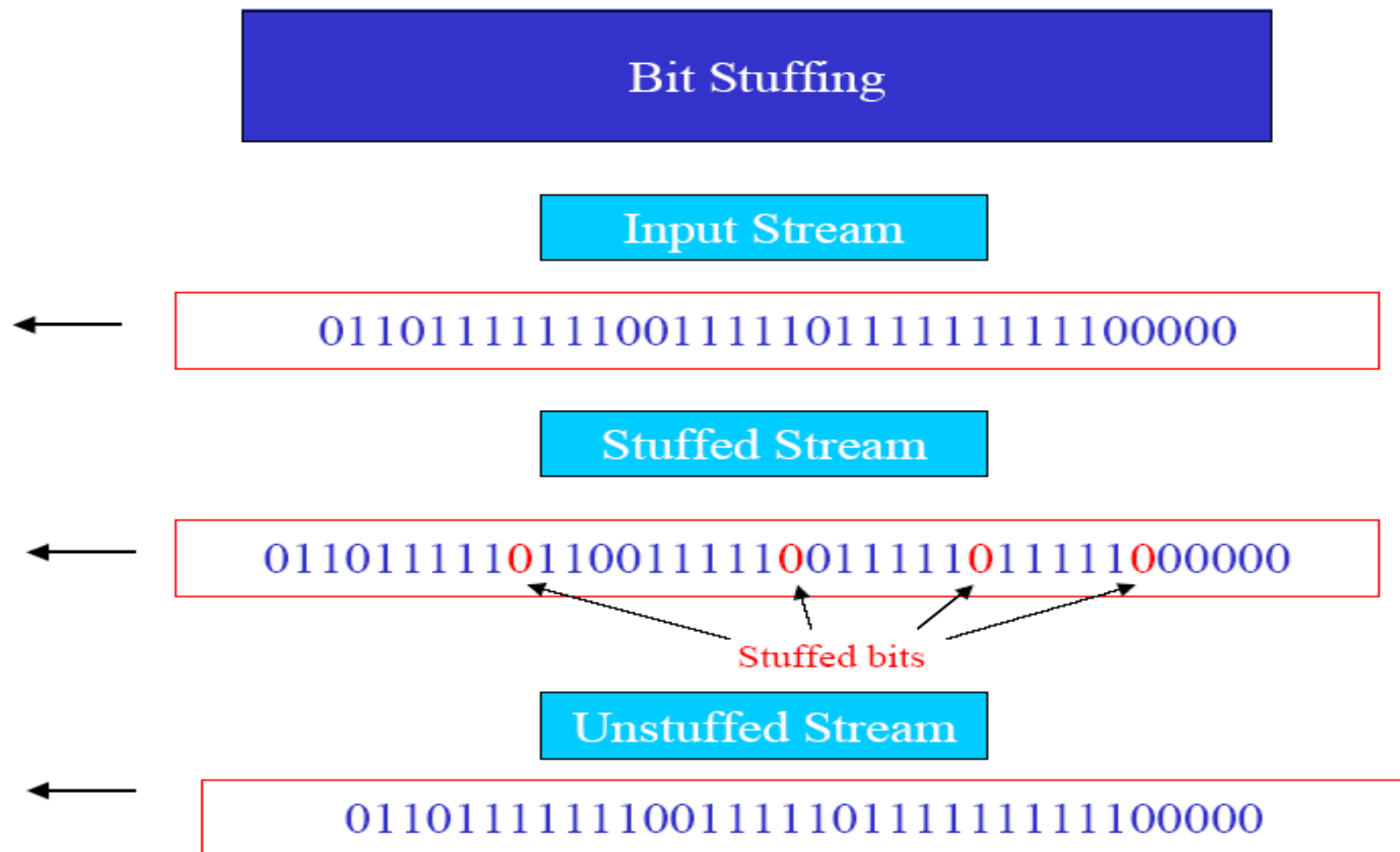


- בעיה: תבנית הדגל יכולה להופיע בתוך זרם המידע.

פתרון:

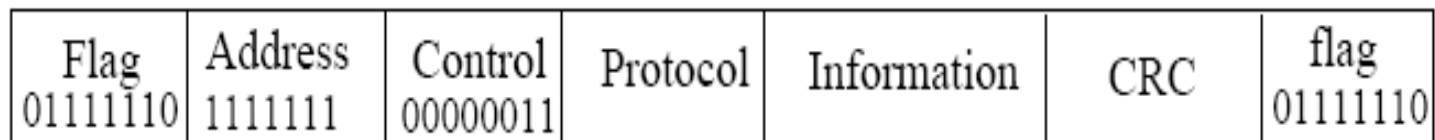
- בכל זמן שהוא, שכבת קישור הנתונים השולחת נתקלת בחמשה אחדים רצופים ([11111]) בזרם הנתונים היא באופן אוטומטי מוסיפה את הסיבית (ביט) 0 לתוך הזרם היוצא.
- בכל זמן שהוא, כשהקולט "חואה" חמישה אחדים באופן אוטומטי הוא מסיר את הסיבית 0 לפני שהוא מעביר את הנתונים לשכבת הרשת.

Bit Stuffing



PPP פרוטוקול

PPP (Point-to-Point Protocol) Frame Format



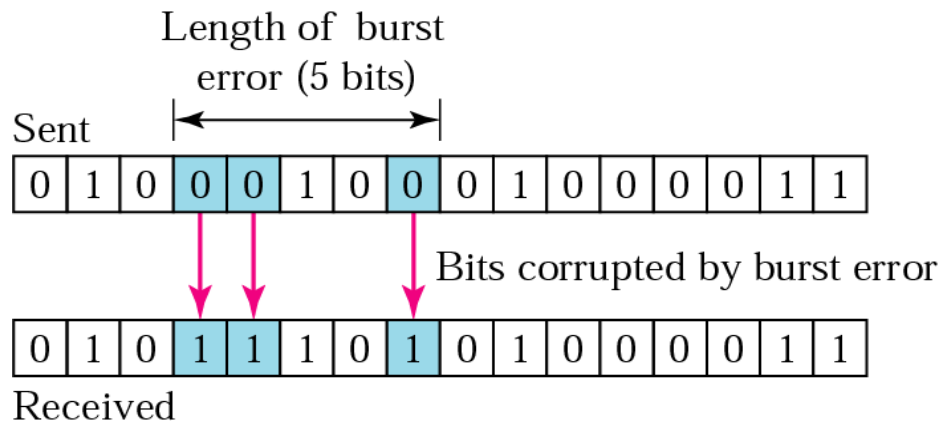
↖
All stations are to
accept the frame

⋮
Unnumbered
frame

↖
Specifies what kind of packet is contained in the
payload, e.g., LCP, NCP, IP, OSI CLNP, IPX

סיכוף ואיפוי ע'א'א'א'א'

- לדוגמא פרץ של טעויות:



□ חבילות הנתונים (Frames) כוללת

מידע נוסף:

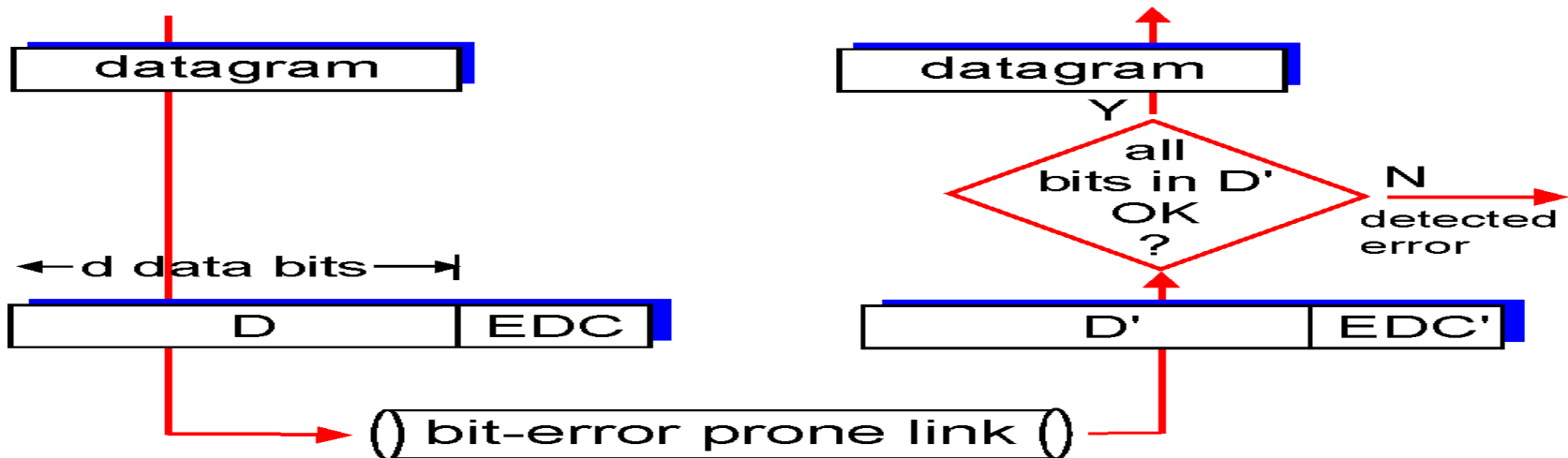
- לגלות שגיאות או נכונות.
- קביעת מידע על הנתונים ע"י השולח.
- ביצוע בדיקה ע"י המקבל.
- לערוב לנכונות ע"י סטטיסטיקה (לא אבסולוטי).

גילוי שגיאות

EDC (Error Detection and Correction bits) - גילוי שגיאות וסיביות התיקון.

D נתונים המוגנים ע"י בדיקת שגיאות ויכולות לקלוט בנוסף שדה של ראש (header).

- שיטת גילוי שגיאות אינה אמינה ב-100%! **שאלה:למה?**
- הפרוטוקול יכול להחמיץ מספר שגיאות, אבל זה קורה לעיתים רחוקות.
- שדה EDC ארוך יותר יניב גילוי שגיאות ותיקון טובים יותר



שיטה 1 לאיפוי שגיאות: בדיקת זוגיות (Parity Checking)

דוגמאות להוספת סיבית זוגיות		
7 סיביות נתונים		בית עם סיבית זוגיות
זוגית	אי-זוגית	
00000000	00000001	
10100001	10100010	
11010010	11010011	
11111111	11111110	

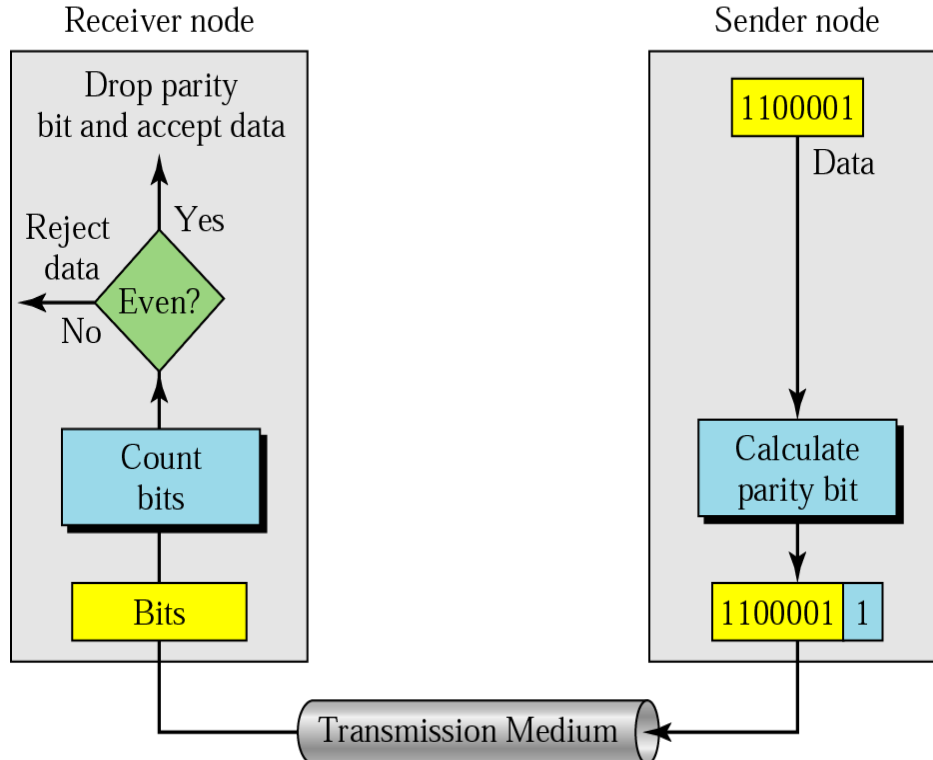
- סיבית זוגיות או סיבית ביקורת זוגיות היא סיבית המשמשת כספרת ביקורת, שערכה מסמן האם מספר הסיביות באוסף נתון שערך 1 הוא זוגי או אי-זוגי. כלומר מוסיפים לכל מילת קוד סיבית בכדי ליצור מספר זוגי של '1'ים. קיימים שני סוגים של סיביות זוגיות:

- סיבית זוגיות זוגית, ששווה ל-0 אם ורק אם מספר האחדות בסיביות הנבדקות הוא זוגי, ושווה ל-1 עבור אי זוגי.
- סיבית זוגיות אי-זוגית ששווה ל-0 כאשר מספר האחדות בסיביות הנבדקות הוא אי-זוגי, ושווה ל-1 עבור זוגי.

- הוספת סיבית ביקורת לרצף של סיביות מאפשר לגלות שגיאה אחת בהעברת המידע, אך לא מאפשר לתקן אותה.

בדיקת זוגיות - Parity Checking

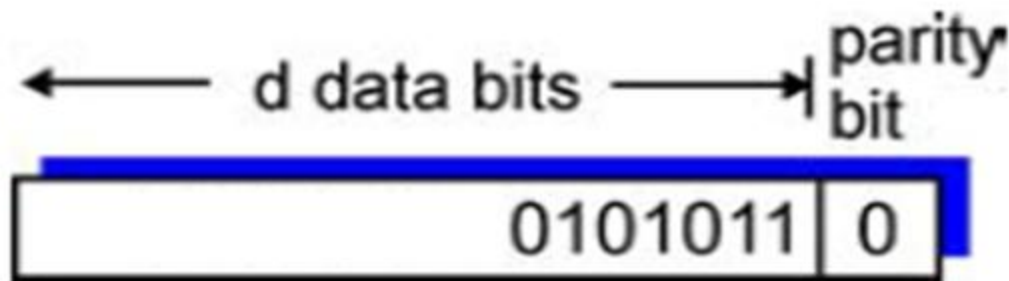
□ סיבית בדיקת הזוגיות נוספת לכל יחידת מידע, כך שהמספר מוחלט של האחדים הוא זוגי (או אי זוגי עבור סיבית בדיקת זוגיות אי זוגית)



Parity Checking - *בדיקת זוגיות*

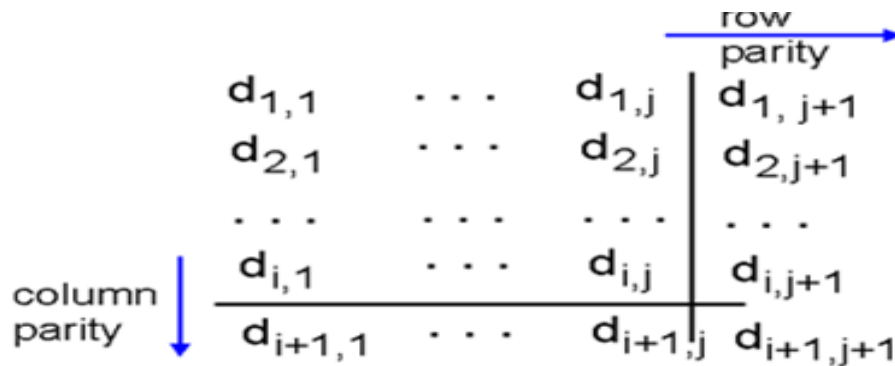
□ בדיקת זוגיות חד-מימדית: הרעיון הוא להוסיף ביט אחד לכל בית (7 ביטים) באופן שישלים למספר זוגי של אחדות.

Single Bit Parity:
Detect single bit errors



בדיקת זוגיות דו-מימדית

בדיקת זוגיות דו-מימדית: נבצע בדיקת זוגיות לפי קו-אורך (LRC) ולפי קו אנכי ונבדוק:



1	0	1	0	1	1
1	1	1	1	0	0
0	1	1	1	0	1
0	0	1	0	1	0

no errors

1	0	1	0	1	1
1	1	1	1	0	0
0	1	1	1	0	1
0	0	1	0	1	0

parity error

parity error

correctable single bit error

VRC

1	0	1	1	0	1	1	1
1	1	0	1	0	1	1	1
0	0	1	1	1	0	1	0
1	1	1	1	0	0	0	0
1	0	0	0	1	0	1	1
0	1	0	1	1	1	1	1
0	1	1	1	1	1	1	0

LRC

שיטה 2 לאיפוי שגיאות: סיכום ביקורת (Checksum)

- ❑ **סיכום ביקורת (Checksum)** הוא קוד לזיהוי שגיאות, המאפשר זיהוי של שגיאות ותיקון במקרים מסוימים, והוא סוג של "פונקצית יתירות" (redundancy check).
- ❑ אופן הפעולה מתבצע על ידי הוספת חלק נוסף להודעה שהוא תוצאה של פונקציה ידועה מראש המופעלת על ההודעה.
- ❑ לאחר מכן, ניתן להפעיל את הפונקציה שוב על ההודעה ולוודא שהתוצאה שהתקבלה זהה לתוצאה שצורפה להודעה, אחרת, יש להסיק שנפלה שגיאה במידע.
- ❑ יעילות המנגנון של פונקצית יתירות תלויה בבחירת הפונקציה לחישוב היתירות. פונקצית היתירות הפשוטה ביותר לחישוב היא פונקצית הזהות: בהינתן הודעה M , הפלט של הפונקציה יהיה ההודעה עצמה.

סיכום ביקורת (המשק)

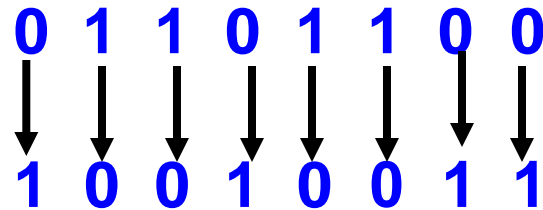
- פונקציה זו מאפשרת זיהוי שגיאות באופן יעיל, אך לא מאפשרת תיקון השגיאות כיוון שלא ניתן לדעת אם הטעות נמצאת בהודעה עצמה או בחלק שהתווסף לה כסיכום ביקורת.
- פונקציה אחרת פשוטה גם היא לחישוב היא בהינתן הודעה M הפלט של הפונקציה יהיה MM ואז כאשר נשלחת ההודעה בצירוף סיכום הביקורת יש שלוש גרסאות להשוות ואז במקרה של שגיאה ניתן להשוות את ההודעה עם שתי הגרסאות הנוספות ולתקן לפי הרוב.
- בסיכום ביקורת נקבע קוד היתירות הנקבע על ידי סיכום של כל הבתים בהודעה. לדוגמה: נניח שישנם 4 בתים בהודעה: $0x25$, $0x52$, $0x3F$, $0x62$ מסכמים את כל הבתים ומקבלים $0x118$. מורידים את הביט הנושא ומקבלים $0x18$. **מחשבים משלים ל-2** ומקבלים $0xE8$. זהו סיכום הביקורת.

חישוב הנפח f – 1:

נרצה לייצג מספרים שליליים באופן פשוט שיאפשר
חיסור ע"י חיבור השלילי של מספר.

חישוב המשלים ל-1:

הפוך "1" ל – "0" ו – "0" ל – "1".



נרצה שחיבור השלילי של מספר יתן 0.

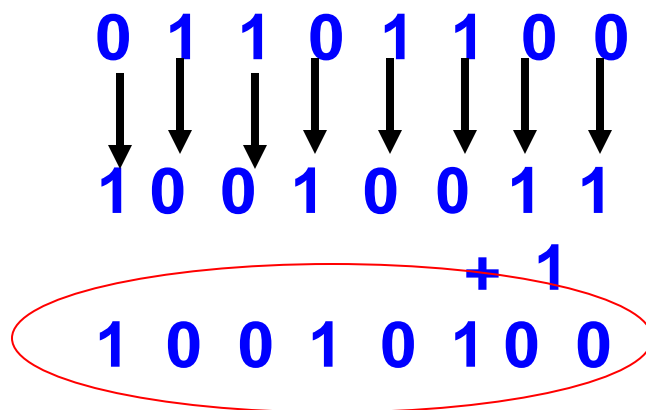
חישוב המעלה f - 2:

הפתרון: נחשב את המשלים ל-1 נוסף 1 לתוצאה.

חישוב המשלים ל-2:

1. הפוך "1" ל- "0" ו- "0" ל- "1".

2. נוסף לתוצאה 1



חיסור בעזרת 2^n - 1

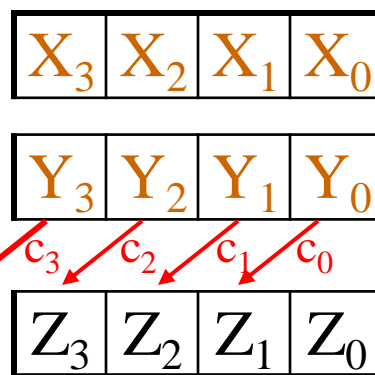
קלט: X, Y מספרים בעלי "גודל" של n סיביות, מיוצגים ע"י משלים ל-1 בעזרת $n+1$ סיביות.

חשב: $X + Y$ והשאר התוצאה ב-1's comp.

ביצוע: א. חבר $X + Y$.

ב. אם יש נשא סופי חבר אותו אל התוצאה (נשא מעגלי)

דוגמא ע"י $n=3$:



← נשא סופי C

נכונות:

ע"י חלוקה

למקרים

בדומה ל-

2's comp.

$$\begin{array}{r}
 \underline{5 - 3} \\
 0101 \\
 + 1100 \\
 \hline
 10001 \\
 + 10001 \\
 \hline
 0010
 \end{array}$$

-0011

$$\begin{array}{r}
 \underline{2 - 4} \\
 0010 \\
 + 1011 \\
 \hline
 1101 \\
 - 0010 = -2
 \end{array}$$

-0100

← שלילי

דוגמאות לחיסור בעזרת משלים ל-1

$$\begin{array}{r} 1\ 1\ 0\ 1\ 0 \\ - \\ 1\ 0\ 0\ 0\ 0\ 0 \\ \hline \end{array}$$

דוגמא לתרגיל
חיסור:

$$\begin{array}{r} 1\ 1\ 0\ 1\ 0 \\ -\ 1\ 1\ 0\ 1 \\ \hline \end{array}$$

דוגמא לתרגיל
חיסור:

חיסור בעזרת המשלים ל-1 : המשלים ל-1 של 100000 הוא 011111.

חיסור בעזרת המשלים ל-1: המשלים ל-1 של 01101 הוא 10010.

$$\begin{array}{r} 0\ 1\ 1\ 0\ 1\ 0 \\ + \\ 0\ 1\ 1\ 1\ 1\ 1 \\ \hline 1\ 1\ 1\ 0\ 0\ 1 \end{array}$$

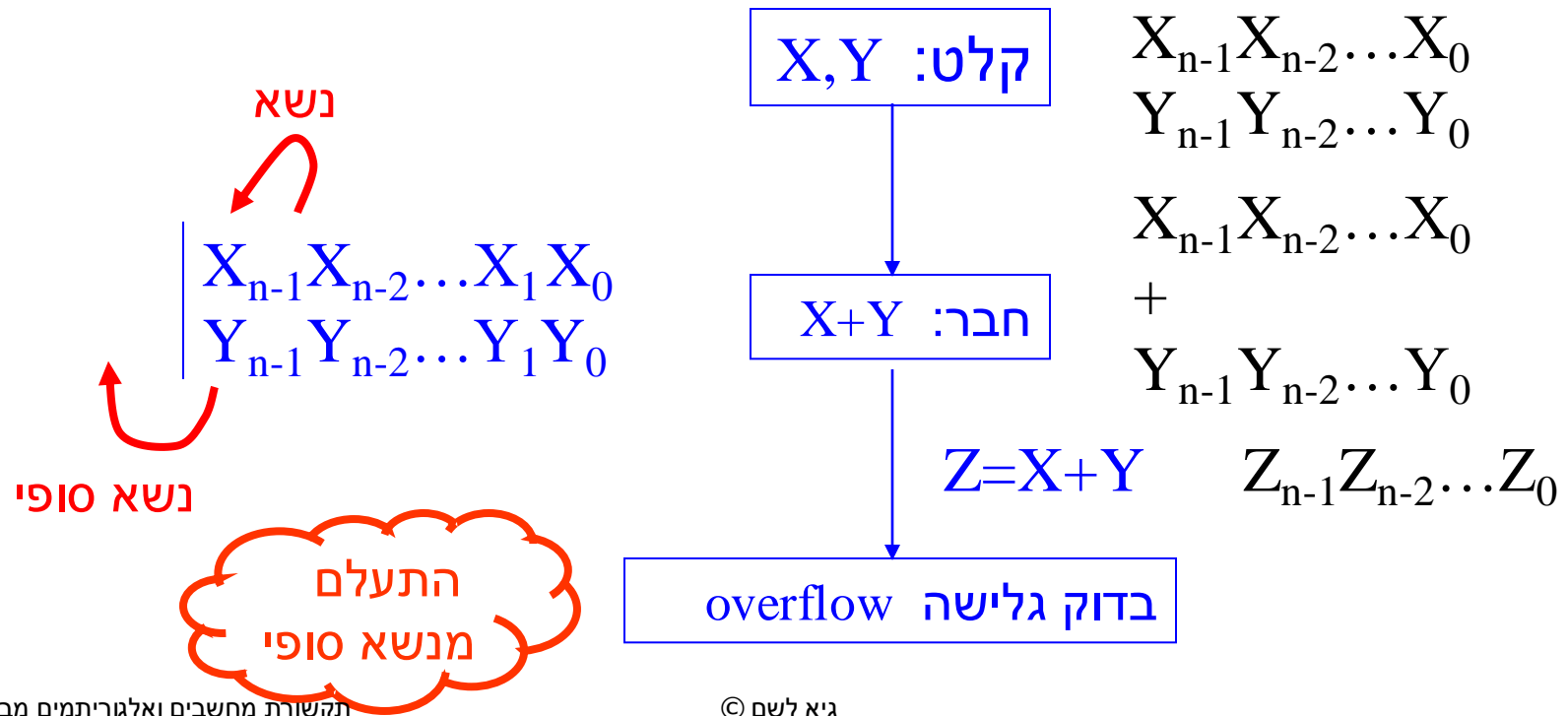
$$\begin{array}{r} 1\ 1\ 0\ 1\ 0 \\ + \\ 1\ 0\ 0\ 1\ 0 \\ \hline 0\ 1\ 1\ 0\ 0 \\ + \\ 0\ 1\ 1\ 0\ 1 \\ \hline \end{array}$$

אין נשא. שלילת המשלים ל-1 של התוצאה היא:
-000110

(יש נשא)

חיסור בעזרת $2's$ Complement

קלט: X, Y מספרים בינאריים בעלי n ספרות וספרת סימן $(n+1)$ מיוצגים ע"י $2's$ Complement



דוגמא : $n=3$, חשב $3-5 \Leftarrow -5 + (3) \equiv 3-5$ נזדקק ל-4 סיביות (+1) ביט סימן.

$$\begin{array}{r}
 3 = 0011_2 \\
 + 0011 \\
 \hline
 1110 \quad \text{שלייל} \leftarrow \text{2's Comp.} \\
 -2 \equiv -0010_2
 \end{array}
 \qquad
 \begin{array}{r}
 -5 = 0101_2 \\
 \downarrow \downarrow \downarrow \downarrow \\
 1010_2 \\
 + 1 \\
 \hline
 1011_2
 \end{array}
 \qquad
 \begin{array}{r}
 3-5
 \end{array}$$

$$\begin{array}{r}
 5 = 0101_2 \\
 + 1101 \\
 \hline
 0010 \quad \text{נשא סופי "התעלם".} \\
 \text{"1"} \leftarrow
 \end{array}
 \qquad
 \begin{array}{r}
 -3 = 0011_2 \\
 \downarrow \downarrow \downarrow \downarrow \\
 1100_2 \\
 + 1 \\
 \hline
 1101_2
 \end{array}
 \qquad
 \begin{array}{r}
 5-3
 \end{array}$$

פעולות סיכום ביקורת

השולח מבצע את הפעולות הבאות:

□ יחידת המידע מחולקת ל- k חלקים, כל אחד עם n סיביות.

□ מחברים את כל החלקים ומשתמשים במשלים ל-1 לקבלת הסכום.

□ הסכום הוא המשלים והוא הופך לסיכום הביקורת (checksum).

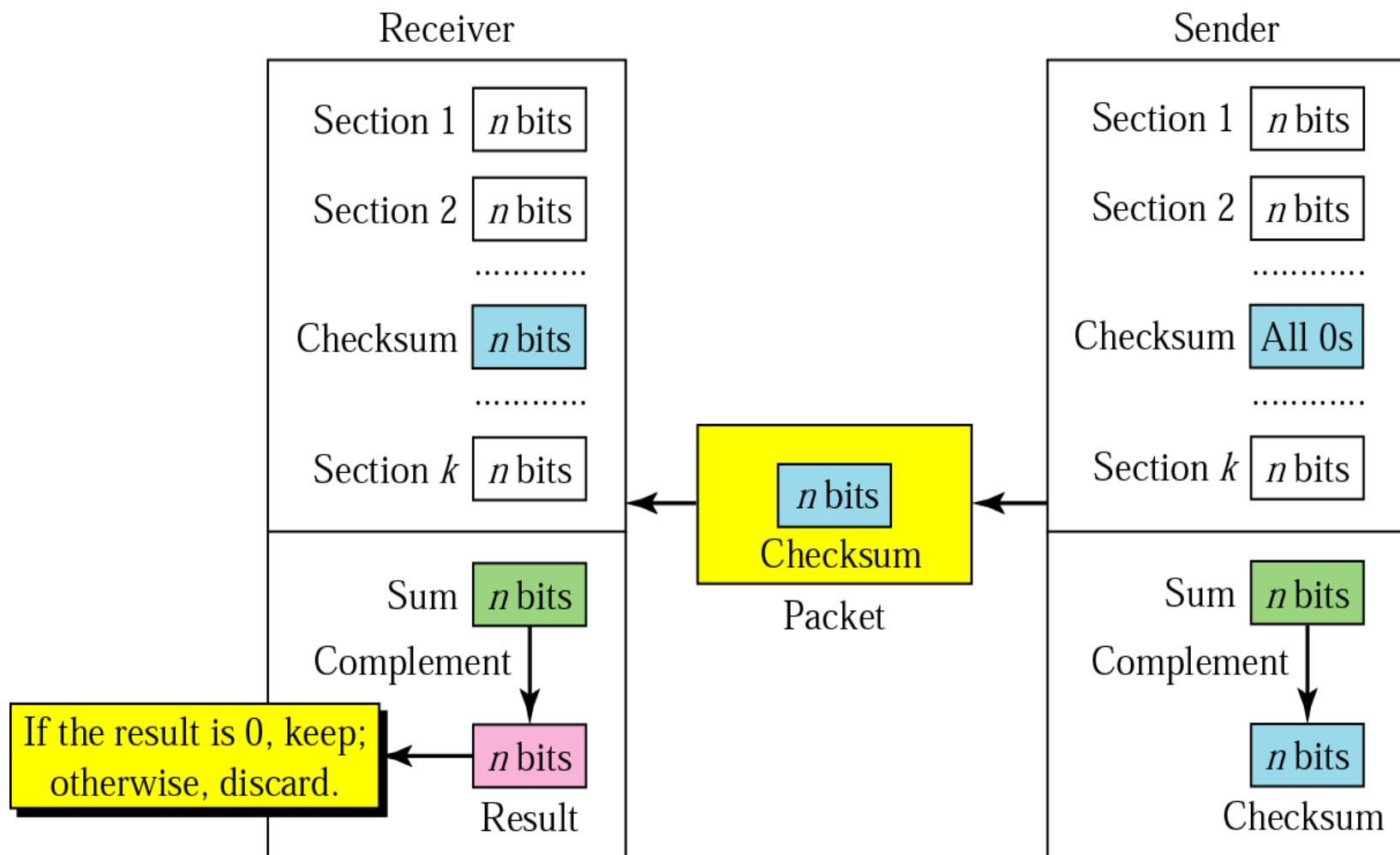
□ סיכום הביקורת (checksum) נשלח עם הנתונים.

פעולות סיכום ביקורת (checksum)

הקולט מבצע את הפעולות הבאות:

- יחידת המידע המתקבלת מחולקת ל- k חלקים, כל אחד עם n סיביות.
- מחברים את כל החלקים ומשתמשים במשלים ל-1 לקבלת הסכום.
- הסכום הוא המשלים והוא הופך לסיכום הביקורת (checksum).
- נפחית את ה-checksum של השולח מה-checksum של המקבל, אם התוצאה אפס, הנתונים שנשלחו התקבלו, אחרת ידחו.

סיכום ביקורת (המשק)



דואנא פסיכוס ביקורת

נניח שהבלוק הבא מכיל 16 סיביות (ביטים) הנשלחים ומשתמשים בסיכום ביקורת (checksum) של 8 סיביות.

10101001 00111001

נחבר את המספרים תוך שימוש בשיטת המשלים ל-1 (one's complement).

10101001

00111001

11100010 Sum

סיכום

סיכום ביקורת

00011101

התבנית אשר תשלח: 00011101 00111001 10101001

דואנא פסיכוס ביקורת (המשק)

עתה שהקולט מקבל את התבנית שנשלחה ואין שגיאות שנוצרו בשידור נניח

10101001 00111001 **00011101**

כאשר הקולט מבצע סיכום של שלושת הקטעים שנשלחו, הוא אמור לקבל רצף של 1-ים, ואחרי חישוב המשלים ל-1 נקבל רצף של 0-ים אשר יראה כי לא נוצרו שגיאות בשידור.

10101001

00111001

00011101

Sum

11111111

Complement

00000000 means that the pattern is OK.

דואל אפסיכום ביקורת (המשק)

נניח אתה כי יש פרץ של שגיאות באורך 5 אשר משפיעות על 4 סיביות.

10101111 11111001 00011101

כאשר הקולט מסכם את שלושת הקטעים שנשלחו, הוא מקבל

10101111

11111001

00011101

Partial Sum 1 11000101

Carry 1

Sum 11000110

Complement 00111001 the pattern is corrupted.

סיכום ביקורת (המשק)

יתרונות: □

■ קל לחישוב

■ גודל

חסרונות: □

■ לא מגלה את כל הטעויות הנפוצות

□ לדוגמא: הסיבית השניה נהפכת בכל קבוצת נתונים

שיטה 3 לאיפוי שגיאות: בדיקת יתרונות מחזורית

(Cyclic Redundancy Check (CRC))

□ טכניקה פופולרית לגילוי שגיאות שידור.

□ מחרוזת נתונים בינארית באורך $K \leq$ יוצרת פולינום בדרגה K , כאשר k הביטים משמשים כמקדמים עבור הפולינום, $G(x)$ עם k מונחים הנעים מ- x^{k-1} ל- x^0 . לדוגמא 110001 יכול ליצג את הפולינום $G(x) = x^5 + x^4 + x^0$.

□ יצירת פולינום מחולל אפשרי:

- $G(x) = x^{16} + x^{15} + x^2 + 1$ CRC-16 (16 סיביות בדיקה)
- $G(x) = x^{16} + x^{12} + x^5 + 1$ CRC-16 ITU (16 סיביות בדיקה)
- $G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ CRC-32 (32 סיביות בדיקה)

□ שיטה זו מבטיחה גילוי כל שגיאה, שתי שגיאות, כל מספר אי זוגי של שגיאות, כל השגיאות באורך עד 16, 99.997% שגיאות באורך 17, 99.998% שגיאות באורך 18 ומעלה.

בדיקת יתירות מחזורית (CRC)

- **בדיקת יתירות מחזורית (Cyclic redundancy check או בקיצור CRC)** היא סוג של קוד לאיתור שגיאות או פונקציית גיבוב (hash function) המשמשת לאיתור שגיאות בהעברת נתונים. לפני העברת המידע מחושב ה-CRC ומתווסף למידע המועבר.
- לאחר העברת המידע, הצד המקבל מאשר באמצעות ה-CRC שהמידע הועבר ללא שינויים. השימוש ב-CRC נפוץ בעיקר בשל קלות המימוש שלו בחומרה בינארית, קלות החישוב המתמטית שלו, ובמיוחד היעילות שלו בגילוי שגיאות נפוצות הנובעות כתוצאה מערוצי תקשורת רועשים.
- **אופן הפעולה**

- שמסתכלים על כל וקטור באורך n כפולינום שמקדמיו הם קואורדינטות הווקטור. CRC משתמש בפולינום המוגדר בפולינום יוצר מדרגה r . סוגים שונים של קוד CRC משתמשים בפולינומים יוצרים שונים.
- בהינתן פולינום יוצר מדרגה r ובהינתן הודעה M שברצוננו לקדד, עלינו לבצע את הפעולות הבאות:
 1. נוסף r אפסים מימין להודעה.
 2. נחלק בפולינום (תוך שימוש בחילוק של השדה מודולו 2)
 3. נחסר את השארית תוך שימוש ב-**xor** במקום בחיסור רגיל.
- נצרף את התוצאה שקיבלנו מימין להודעה המקורית ונשלח.
- כמו בכל קידוד Checksum, הצד המקבל יבצע את שלבים 1 ו-2 ויוודא ש- r הביטים האחרונים שנשלחו זהים לתוצאה שהתקבלה.

אלגוריתם בקידוק יתירות מחזורית

□ לשולח יש d סיביות של הנתונים שאותם הוא רוצה לשלוח, $D \leq$, מוגדר במספר בינארי.

□ השולח והמקבל בוחרים תבנית של $r+1$ סיביות (הנקרא המחולל), $G \leq$.

□ המטרה: בחר r סיביות, $R \leq$, כך ש:

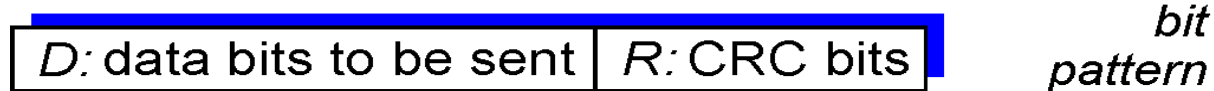
■ $\langle D, R \rangle$ בדיוק מתחלק על ידי G (מודולו 2).

■ הקולט יודע את G , מחלק את $\langle D, R \rangle$ ע"י G . אם לא נשאר אפס: טעות גילתה!

■ יכול לגלות כל פרץ של טעויות הקטן מ- $r+1$ סיביות.

□ שימוש רחב בשיטה זו הלכה למעשה (ATM, HDCL).

← d bits → ← r bits →



$$D * 2^r \text{ XOR } R$$

mathematical formula

p	q	$p + q$
0	0	0
0	1	1
1	0	1
1	1	0

□ טבלת XOR:

CRC -f kNd1?

$D=101110, d=6, G=1001, r=3$

=> **<D,R>** = 101110000

Want:

$$D \cdot 2^r \text{ XOR } R = nG$$

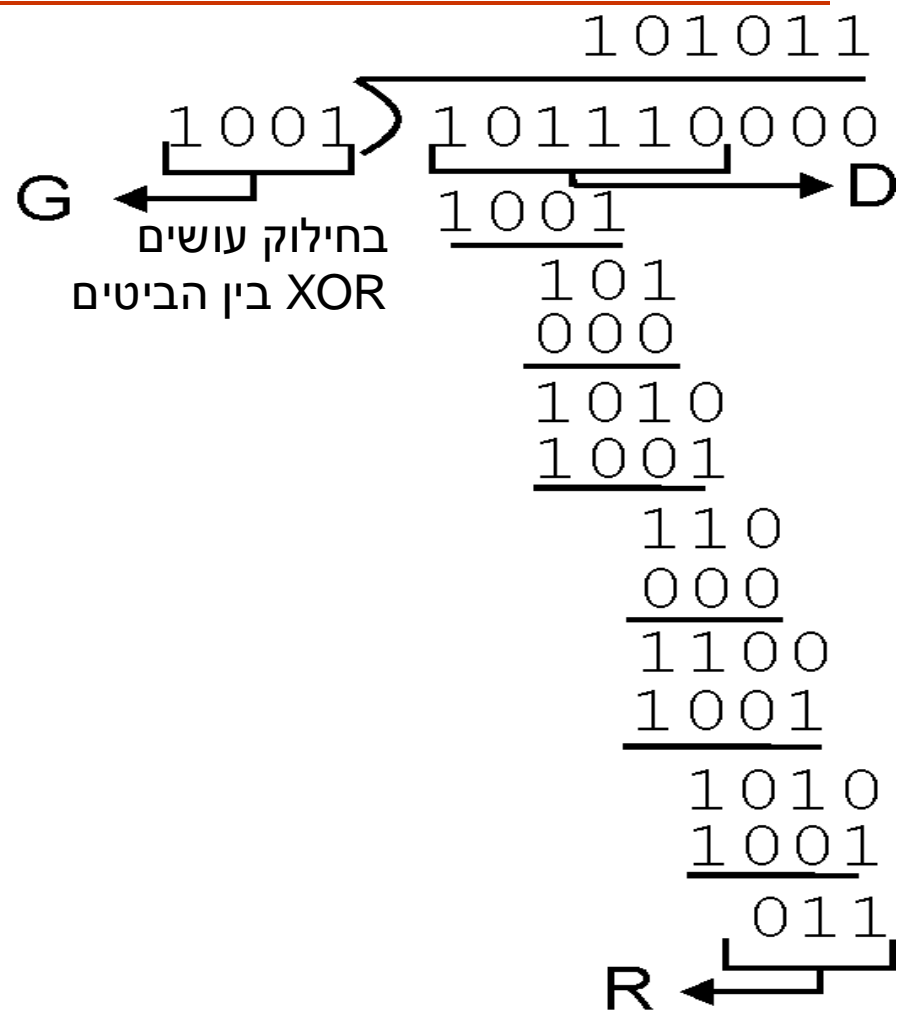
equivalently:

$$D \cdot 2^r = nG \text{ XOR } R$$

equivalently:

if we divide $D \cdot 2^r$ by G ,
want remainder R

$$R = \text{remainder}\left[\frac{D \cdot 2^r}{G}\right]$$



פרוטוקלי גישות מרובות

פרוטוקולי MAC (Multiple Access Control)

נחלק לשלושה סוגים:

■ חלוקת הערוץ (Channel Partitioning)

- חלוקת הערוץ "לחלקים" קטנים בהתייחסות לחלוקת זמן, תדירות.
- הקצאת "חלקים" לצומת עבור לשימוש בלעדי.

■ גישה אקראית (Random Access)

- לאפשר התנגשויות.
- התאוששות לאחר ההתנגשות.

■ החלפות ("Taking turns")

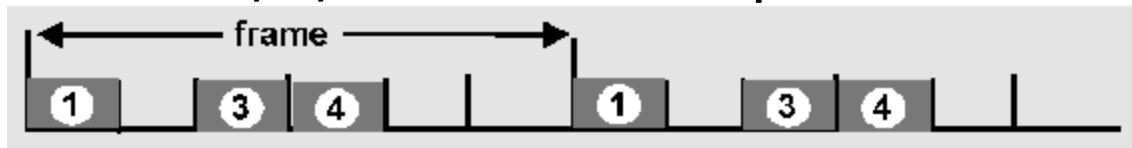
- באופן הדוק נתאם פעולות בערוץ המשותף כדי להמנע מהתנגשויות.

המטרה: יעילות, שיוויוניות, פשטות, ביזור.

פרוטוקול MAC לחלוקת הערוץ: TDMA

TDMA: time division multiple access

- הגישה לערוץ היא לפי תור - תחנות משדרות בתור, כל תחנה מקבלת זמן מוקצב שבו היא מקבלת את רוחב הפס המלא ושלאחריו תשדר התחנה הבאה בתור.
- כל תחנה מקבלת חריץ בגודל קבוע (אורך=זמן מעבר של חבילה) בכל סבב - הערוץ מחולק לקבוצות של חריצי זמן רצופים בגודל קבוע. בכל קבוצה כזו של חריצי זמן משודרת מסגרת אחת.
- חריצים לא ממומשים מתבזבזים.
- דוגמא: רשת מקומית עם 6 תחנות, לתחנות 1,3,4 יש חבילות לשליחה, אבל החריצים שמוקצים לתחנות 2,5,6 נותרות ללא שימוש.



פרוטוקול MAC לחלוקת הערוץ: FDMA

FDMA: frequency division multiple access

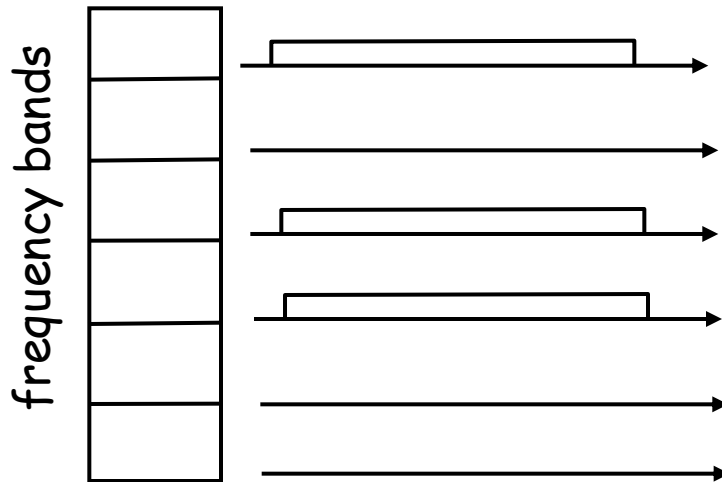
ב- FDMA (ריבוב בחלוקת תדר) - כל רוחב הסרט מחולק לחלקים שווים, לדוגמא תתי-ערוצים (כאשר בין כל שני תתי ערוצים סמוכים מגדירים מרווח בטחון) תחום תדרים לא מנוצל שנועד למנוע הפרעה הדדית בין שני תתי הערוצים.

כל תחנת מקבלת תת-ערוץ משלה בעל תחום תדירות קבוע.

זמן שידור לא מנוצל בתחום התדירות יורד לאבדון.

דוגמא: רשת מקומית עם 6 תחנות, לתחנות 1,3,4

יש חבילות לשליחה והן נשלחות, אבל תחומי התדרים שמוקצים לתחנות 2,5,6 נותרים ללא שימוש.



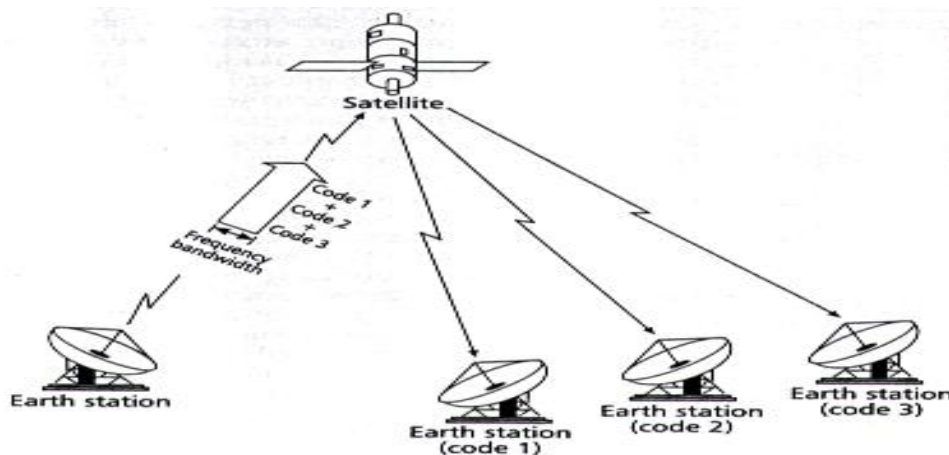
פרוטוקול MAC אחלוקת הערוץ: CDMA(Code Division Multiple Access)

ב-CDMA, השידורים מכל התחנות מופרדים במישור התדר-זמן ע"י קידוד. ה-CDMA בנוי בטכנולוגיית ה-Spectrum Spread כלומר, הוא מפזר את המידע באות מסוים על פני רוחב-פס גדול יותר מהאות המקורי.

תחנת המקור לוקחת את האות המקורי עם רוחב הפס הצר, מוסיפה לו קוד (בעזרת chipping sequence) לפי תחנת היעד, מפזרת את המידע על פני רוחב פס גדול ומשדרת אותו לכל תחנות. בתחנות הקולטות מופרד הקוד מהמידע והתחנה שקוד הזיהוי שייך לה מפענחת את המידע ע"י הקוד שלה (own chipping sequence) ומעבירה את הנתונים אל היעד (שימושי בעיקר לתקשורת לווינית, וסלולרית).

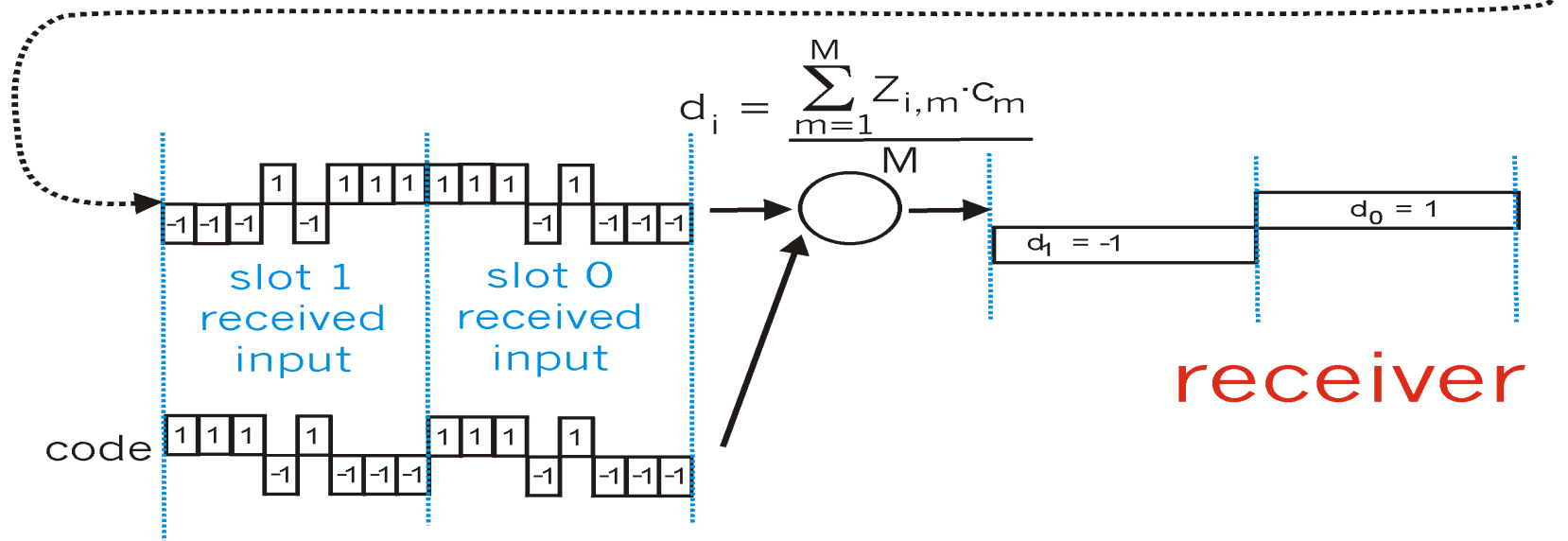
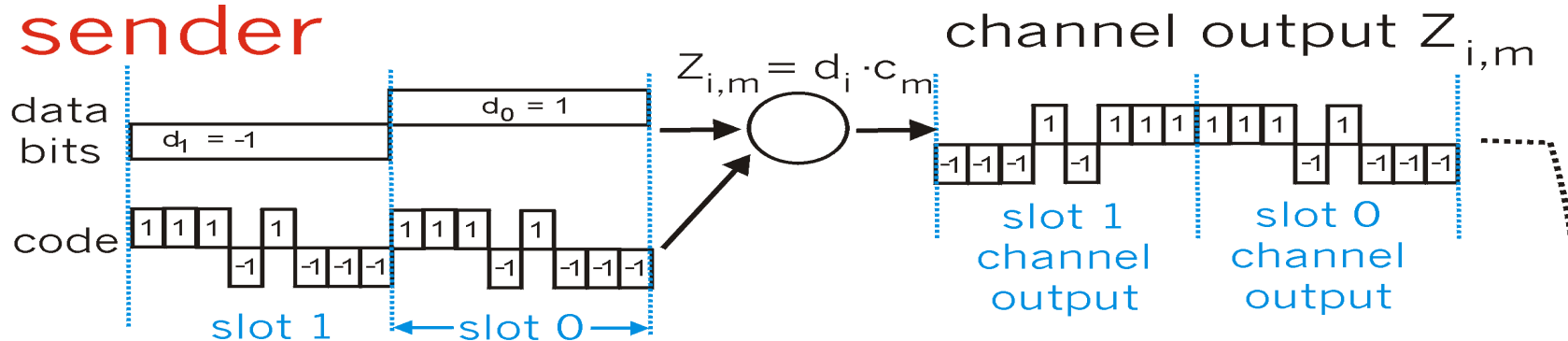
קידוד האות (encoded signal) = המידע המקורי (original data) \times סידרת מעבדים (chipping sequence).

פענוח (decoding) = מכפלה סקלרית של האות המקודד (encoded signal) וסידרת המעבדים (chipping sequence).



CDMA Encode/Decode

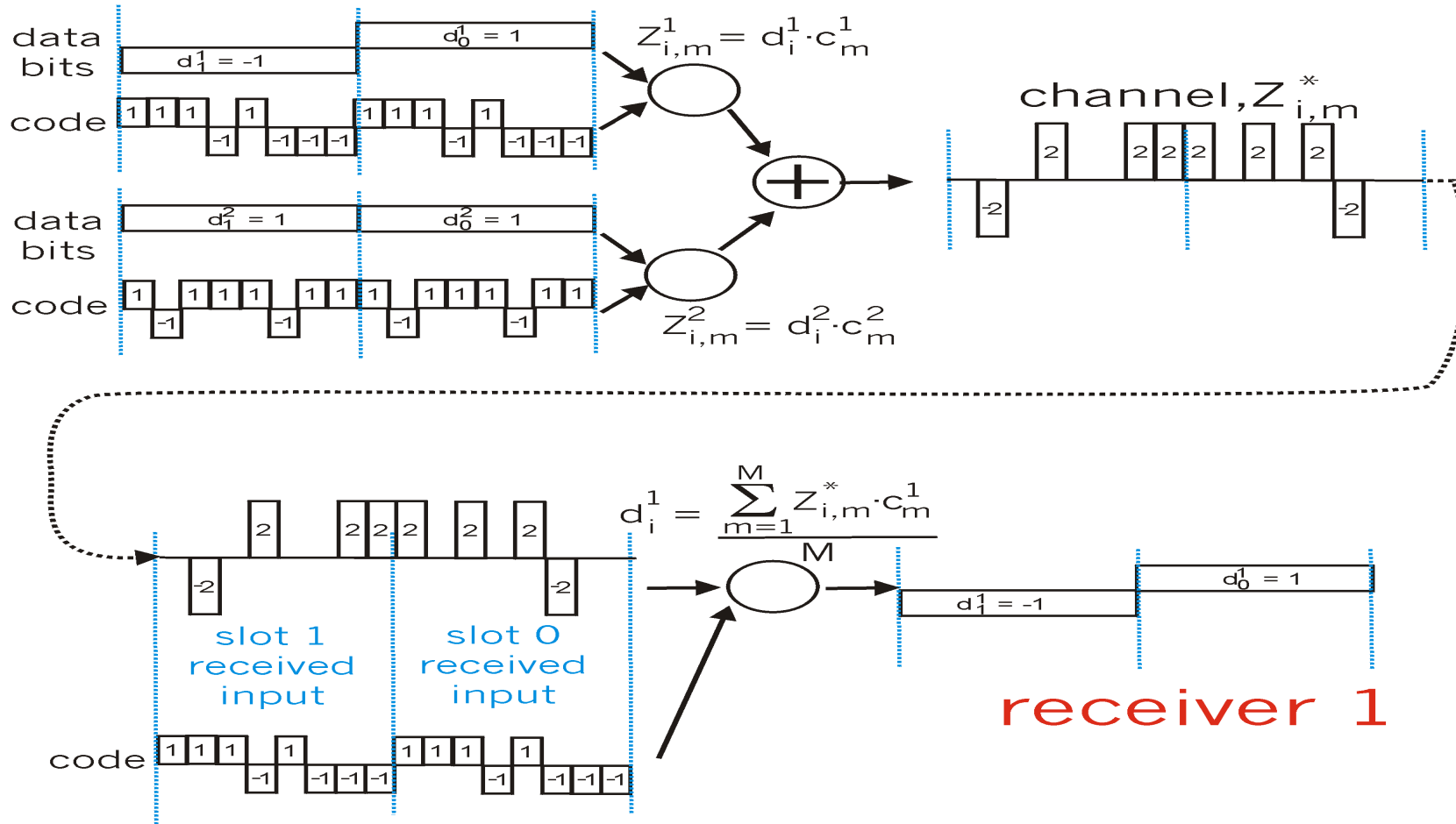
sender



receiver

CDMA: two-sender interference

senders



פרוטוקולי גישה אקראית (Random Access protocols)

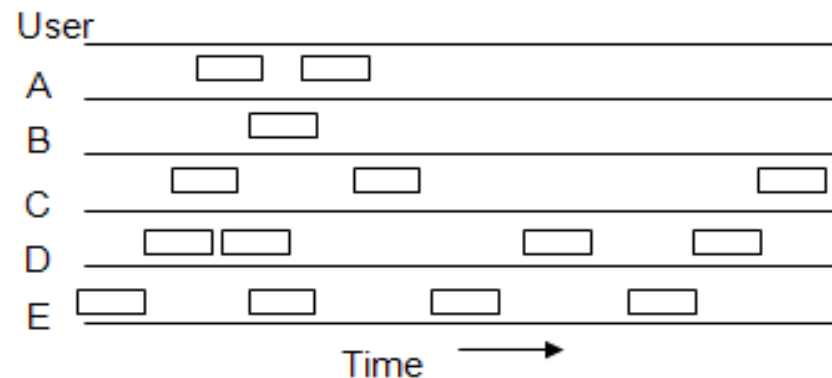
- כאשר תחנה (צומת) יש חבילה (packet) לשליחה
 - התחנה תשלח את החבילה ברוחב פס מלאה של הערוץ בקצב R.
 - אין עדיפות כלשהיא לתחנה מסוימת הרשת.
- שתים או יותר תחנות משדרות ביחד \leq "התנגשות".
- פרוטוקול **MAC** לגישה אקראית מפרטים:
 - אך מגלים התנגשויות.
 - אך מתאוששים מהתנגשויות (לדוגמא השהייה ושליחה מחדש).
- דוגמא לפרוטוקולי MAC לגישה אקראית:
 - ALOHA
 - slotted ALOHA
 - CSMA and CSMA/CD

פרוטוקול ALOHA

רקע - בשנות ה-70 פותח באוניברסיטת הוואי פרוטוקול לפתירת בעיית הקצאת הערוץ. קיימות שתי גרסאות לפרוטוקול זה: Pure Aloha ו-Slotted Aloha. ההבדל ביניהן הוא בחלוקת הזמן. בפרוטוקול Pure Aloha אין חלוקת הזמן למקטעים בידיים, ואילו ב-Slotted Aloha קיימת חלוקה כזו.

Pure Aloha - הרעיון הבסיסי של פרוטוקול זה פשוט: המשתמשים משדרים כשיש להם מידע לשדר. כמובן, שיהיו התנגשויות, כאשר המסגרות המתנגשות יהרסו. קיים משוב מהערוץ, ולכן התחנה המשדרת יודעת לזהות התנגשות על ידי האזנה לערוץ. במידה והמסגרת נהרסה, המשדר מחכה פרק זמן אקראי, ושולח את המסגרת שוב. (ברור שזמן ההמתנה צריך להיות אקראי, אחרת המסגרות יתנגשו שוב ושוב). מערכות בהן מספר משתמשים חולקים ערוץ משותף בצורה שיכולה להוביל לבעיות, נקראות מערכות תחרות (Contention).

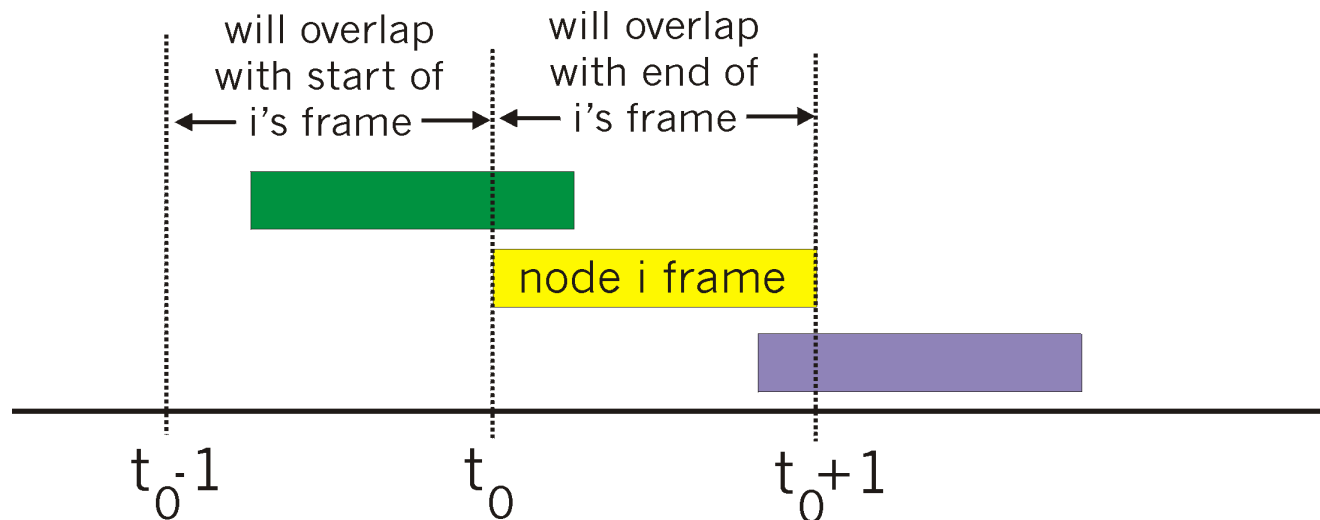
סכמה של שידור מסגרות במערכת ALOHA:



מספר משתמשים המשדרים מסגרות באורך קבוע. (אורך המסגרות באיור קבוע כי התפוקה של מערכת ALOHA מקסימאלית במקרה זה). כאשר שתי מסגרות נמצאות בערוץ באותו זמן, תהיה התנגשות ושתייהן יאבדו. יש לשים לב, כי גם אם הביט הראשון של המסגרת החדשה חופף עם הביט האחרון של המסגרת שכמעט הסתיימה, שתי המסגרות יהרסו וישודרו מחדש אחר כך.

סיכום Pure ALOHA

- Pure Aloha: פשוט יותר, והוא ללא תאום לביצוע בו-זמני (סינכרוניזציה).
- מסגרת (חבילה) צריכה להישלח:
 - נשלחת ללא המתנה לתחילת חריץ (slot) הזמן.
 - ההתנגשויות יגדלו קרוב לודאי:
 - מסגרת שנשלחה בזמן t_0 תתנגש במסגרת שנשלחה בזמנים $[t_0-1, t_0+1]$



ניתוח יציאות Pure ALOHA

ננתח את יעילות הערוץ המשתמש בפרוטוקול זה. כלומר, מהו אחוז המסגרות המשודר המגיע ליעד (כלומר, לא מתנגש), ע"פ ההגדרות הבאות: זמן מסגרת – frame time – כמות הזמן הנדרשת להעברת מסגרת באורך קבוע.

$$t = \text{זמן מסגרת} = \frac{\text{אורך מסגרת (בסיים)}}{\text{קצב שידור}}$$

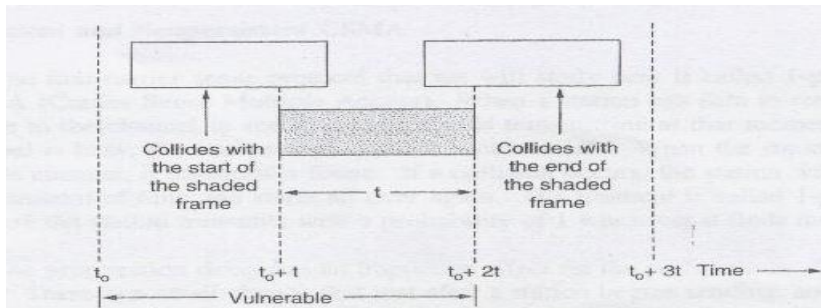
S - קצב היווצרות מסגרות בממוצע - קצב השידור (λ) – נניח קצב פואסוני. כאשר $S > 1$ קצב היווצרות המסגרות גבוה מקיבולת הערוץ וכמעט כל מסגרת תסבול מהתנגשות. עבור תפוקה סבירה, יש לדרוש כי $0 < S < 1$.

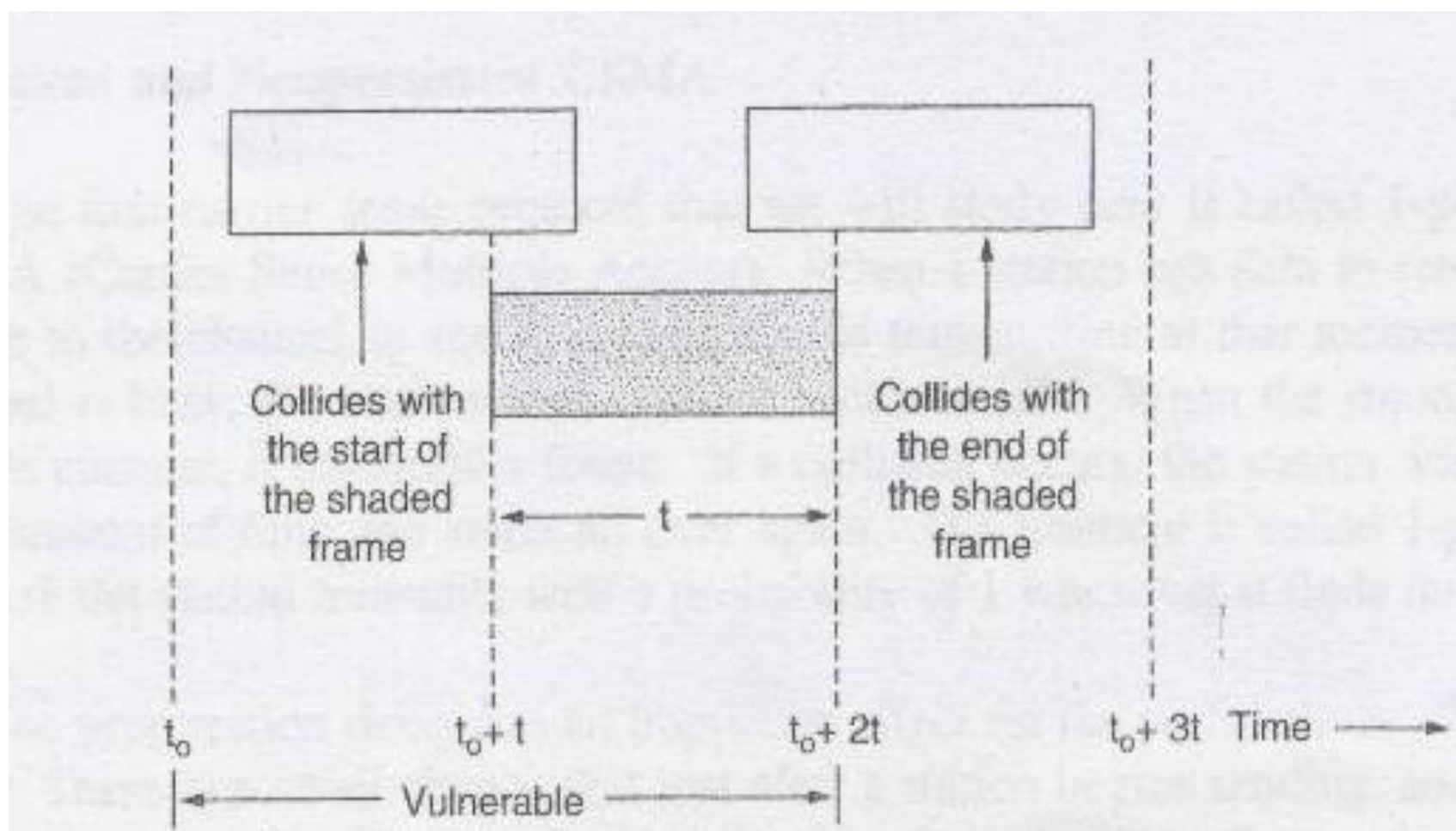
G - קצב ניסיונות השידור – נניח קצב פואסוני. (ברור כי בחלק מהמקרים יהיו התנגשויות, ולכן לא כל מה שמנסים לשדר, בסופו של דבר ישודר). ברור כי $G \geq S$, כיוון שיש יותר ניסיונות לשידור משידור. בעומס נמוך $G \approx S$, מספר ההתנגשויות יהיה נמוך ולכן $S \approx 0$ בעומס גבוה, מספר ההתנגשויות יהיה גבוה ולכן $S = G \cdot P_0$.
 P_0 - הסתברות לשידור מוצלח (כלומר, הסתברות לחוסר התנגשות).

ההנחה היא כי אם נוצרת מסגרת, מסגרת חדשה לא נוצרת עד שהקודמת לא שודרה.
 t - הזמן הדרוש לשליחת מסגרת.

t_0 - זמן שליחת מסגרת.

אם משתמש ייצור מסגרת חדשה בין זמן t_0 לזמן $t_0 + t$ סוף המסגרת תתנגש עם ההתחלה של המסגרת האפורה. כנ"ל בין זמן $t_0 + t$ לבין $t_0 + 2t$





ניתוח יציאות (המשק)

□ האינטרוול השקט (quiet interval) הוא $2t$ - מרווח זמן הדרוש כדי שלא נקבל התנגשות. (זמן זה נובע מחוסר ודאות לגבי מיקום המסגרת שברצוני לשדר לעומת המסגרת שנוצרה). ההסתברות להיווצרות K מסגרות במשך זמן מסגרת, נתון על ידי התפלגות פואסון:

$$P[K] = \frac{G^K e^{-G}}{K!}$$

ולכן, ההסתברות להיווצרות 0 מסגרות הוא: $P[0] = e^{-G}$.

□ במשך זמן $2t$, קצב ניסיונות השידור הוא $2G$, ולכן ההסתברות להיווצרות 0 מסגרות כעת היא: $P[0] = e^{-2G}$. מכאן נקבל כי קצב היווצרות מסגרות הוא: $S = G \cdot P[0] = G \cdot e^{-2G}$.

□ ניתן להראות ע"י הצבת מספרים בנוסחה כי התפוקה המקסימאלית מתרחשת כאשר $G = 0.5$, ואז $S = \frac{1}{2e} = 0.184 = 18.4\%$.

□ כלומר, התפוקה המקסימאלית היא 18%. תפוקה זו נמוכה מאד.

□ קיימת יכולת לבצע אופטימיזציה על ידי שינוי קצב ניסיונות השידור (הגדלת G), אך אם ננסה לשדר בקצב גדול מדי, ההסתברות לחוסר התנגשות תקטן – מעין עסקת חליפין (Tradeoff).

אנרץ קצב היווצרות אסכרות כנאד קצב ניסיונות השידור

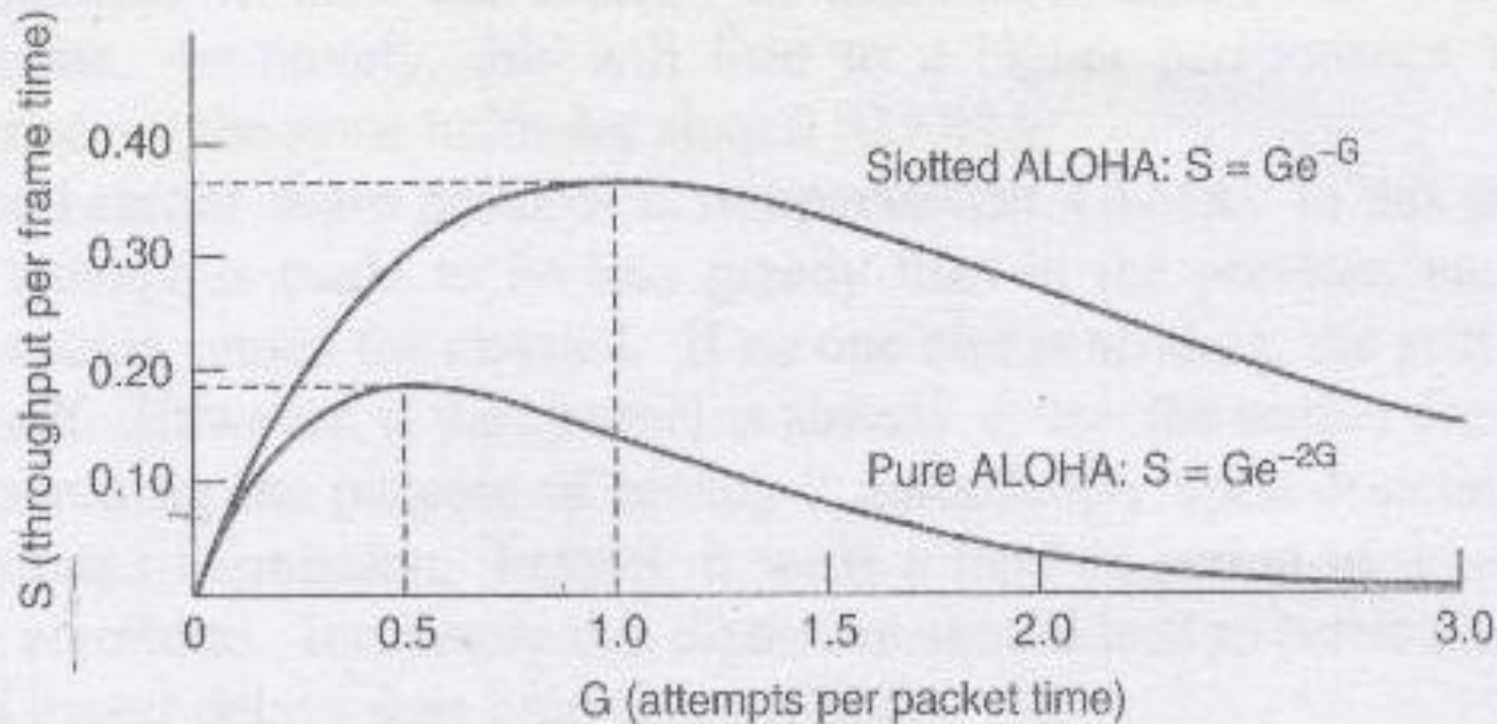
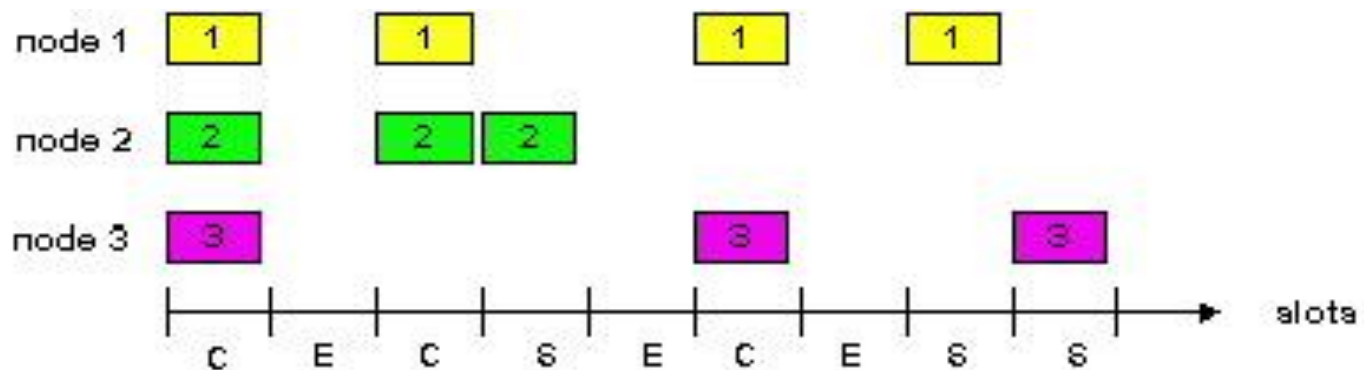


Fig. 4-3. Throughput versus offered traffic for ALOHA systems.

Slotted Aloha

בשנת 1972, פורסמה שיטת ה-Slotted Aloha, אשר נועדה להכפלת הקיבולת של מערכת Aloha.

- ההצעה הייתה לחלק את הזמן לאינטרוולים בדידים, כאשר כל אינטרוול מתאים למסגרת אחת.
- גישה זו דורשת את הסכמת המשתמשים על גבול המקטע. (דרך אחת ליצירת סנכרון היא לגרום לתחנה מיוחדת ליצור קוֹק (צפצוף) בתחילת כל אינטרוול, כמו שעון).
- השיטה עובדת כך:
 - הזמן מחולק לחלקים (חריצים) שווים בגודלם (=זמן שידור חבילה).
 - הצומת (התחנה המשדרת) עם הגעת החבילה: משדרת בתחילת החריץ הזמן הבא.
 - אם נוצרה התנגשות: משדר מחדש בחריץ זמן עתידי עם הסתברות P , עד להצלחה בשידור.



ניתוח יציאות Slotted Aloha

בשיטה זו, התחנה אינה רשאית לשלוח מידע כל הזמן. התחנה נאלצת לחכות לתחילת מקטע הזמן הבא. אינטרוול השקט קטן פי 2 והוא כעת t בלבד.

ההסתברות לחוסר התנגשות כעת היא $P[0] = e^{-G}$ ולכן $S = e^{-G} \cdot G$.

כפי שניתן לראות, Slotted Aloha מגיע לשיא כאשר $G=1$, בתפוקה מקסימאלית

של $\frac{1}{2} = 0.368$, פעמיים מהתפוקה המקסימאלית של pure Aloha.

במקרה האופטימאלי נוכל להגיע בפרוטוקול זה להסתברות של 37% למקטעים ריקים (אי-שידור), הסתברות של 37% הצלחות.

עבודה ב- G גבוה יותר תקטין את מספר המקטעים הריקים, אך תגדיל את מספר ההתנגשויות. הסתברות לכך ששידור ידרוש K ניסיונות (כלומר, $K-1$ התנגשויות, הצלחה אחת):

$$P_K = \underbrace{e^{-G}}_{\text{חוסר התנגשות פעם אחת}} \underbrace{(1 - e^{-G})^{K-1}}_{\text{התנגשות } K-1 \text{ פעמים}}$$

מספר ניסיונות ממוצע לשידור (תוחלת): $E = \sum_{k=1}^{\infty} k P_k = \sum_{k=1}^{\infty} k e^{-G} (1 - e^{-G})^{k-1} = e^G$

מספר השידורים הממוצע תלוי בצורה מעריכית ב- G , ולכן עלייה קטנה בעומס, תגרום עלייה אקספוננציאלית במספר ניסיונות השידור ובכך תוריד את הביצועים בצורה חדה.

Carrier Sense multiple Access – CSMA

- ראינו כי בשיטת ה-Slotted Aloha ניתן להגיע לתפוקה מקסימאלית של $\frac{1}{e}$. התפוקה בשיטה זו נמוכה מאד, כיוון שללא יכולת להבחין אם הערוץ פנוי או תפוס, נגרמות התנגשויות רבות.
- ברשתות תקשורת מקומיות רבות, התחנות יכולות לזהות מה תחנות אחרות עושות ולשנות את התנהגותן בהתאמה. רשתות אלו יכולות להשיג ביצועים גבוהים יותר מביצועי ה-Slotted Aloha.
- בחלק זה, נדון במספר פרוטוקולים שנועדו לשיפור הביצועים. פרוטוקולים בהם תחנות מאזינות לשידור ומתנהגות בהתאם נקראים Carrier sense protocols.

Persistent and Non-persistent CSMA

1 Persistent CSMA □

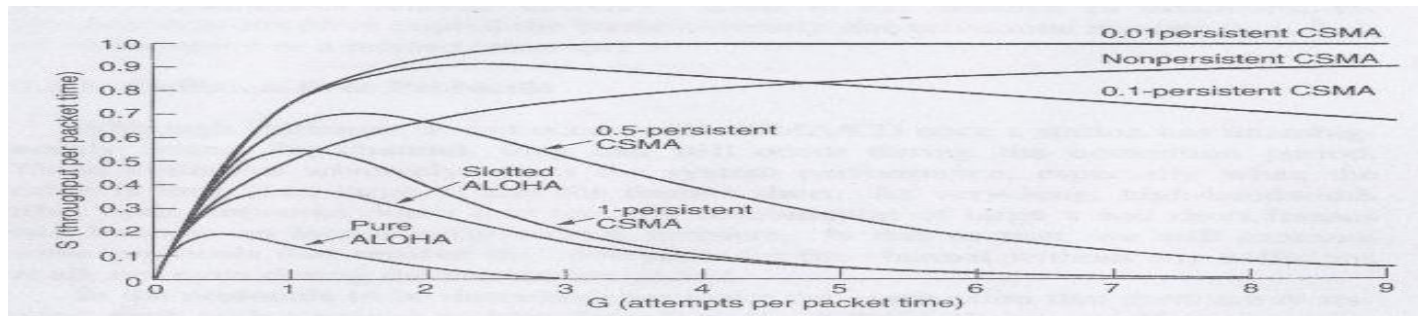
- כאשר לתחנה יש מידע לשדר, ראשית, היא מאזינה לערוץ ובודקת האם מישהו אחר משדר באותו הרגע. אם הערוץ תפוס, התחנה מחכה עד שהוא מתפנה. כאשר תחנה מזהה שהערוץ פנוי, היא משדרת מסגרת. במידה ויש התנגשות – התחנה מחכה פרק זמן אקראי ומתחילה את הכול שוב.
- פרוטוקול זה נקרא 1 Persistent כיוון שתחנה משדרת בהסתברות 1 במידה וגילתה שהערוץ פנוי. **לזמן ההתפשטות** יש השפעה חשובה על ביצועי הפרוטוקול. כיוון שקיים סיכוי כי אחרי שתחנה התחילה לשלוח Packet לשידור, תחנה נוספת גם מעוניינת לשלוח והיא בודקת את הערוץ. אם הסיגנל של התחנה הראשונה עדיין לא הגיע לתחנה השנייה, התחנה תחוש שהערוץ פנוי ותתחיל לשדר, דבר שיגרום להתנגשות. ברור כי ככל שזמן ההתפשטות ארוך יותר, ביצועי הפרוטוקול יורדים.
- אם זמן ההתפשטות הוא אפס, עדיין יהיו התנגשויות, כי אם שתי תחנות רוצות לשדר באמצע זמן שידור של תחנה שלישית, שתיהן ימתינו עד לסיום השידור ויתחילו לשדר בדיוק יחד, דבר שיגרום כמובן להתנגשות. ולמרות זאת, פרוטוקול זה טוב בהרבה מ-Pure Aloha, כיוון שהתחנות מחכות לפחות עד סיום השידור של התחנה השלישית.

CSMA (המשק)

- מבחינה אינטואיטיבית, זה יוביל לביצועים טובים יותר מ-Pure Aloha, ומאותן הסיבות גם לביצועים טובים יותר מ-Slotted Aloha. הרחבה לפרוטוקול זה היא פרוטוקול ה- p persistent CSMA.

□ p persistent CSMA

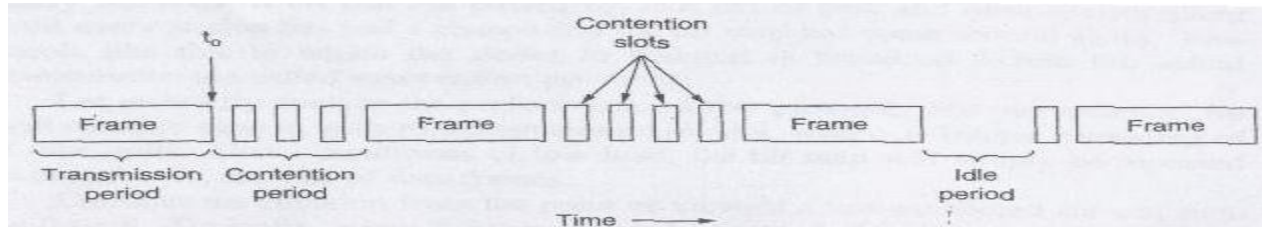
- פרוטוקול זה מיועד לשימוש בערוצי Slotted. כאשר תחנה מוכנה לשידור, היא בודקת את הערוץ. אם הערוץ פנוי, היא משדרת בהסתברות p , ומחכה עד המקטע הבא בהסתברות $1-p$. אם המקטע הבא פנוי, היא משדרת בהסתברות p , וממתינה בהסתברות q וכן הלאה.... תהליך זה חוזר על עצמו עד שמסגרת משודרת, או עד שתחנה אחרת התחילה לשדר.
- באיור הבא מוצגים גרפים של מס' הניסיונות לשידור כפונקציה של התפוקה עבור פרוטוקולים שונים. יש לשים לב כי בגרף זה לא בא לידי ביטוי עניין ההשהיה (delay).



- עבור תעבורה גדולה מאד, מתחילים להיווצר תורים והחוצץ (buffer) מתחיל לגדול. התעבורה שהייתה מתפרצת הופכת לתעבורה אחידה, וניתן לטפל בה בעזרת TDM. נוצר מצב בו בכל מקטע זמן יש שידור, והתעבורה במוצא הופכת ל-100%. כלומר, אנו מגיעים לנצילות תעבורה של 100% (מבלי לקחת בחשבון גם את פרמטר ההשהיה). ראינו כי קיים שיפור בתפוקה תוך שימוש בפרוטוקולים בעלי Carrier Sense. נראה בהמשך כי בעזרת פרוטוקול מתקדם יותר ניתן לשפר את הביצועים אף יותר.

CSMA/CD - CSMA with Collision Detection

- שיפור נוסף בביצועים ניתן להשיג כאשר תחנות יפסיקו את השידור ברגע שמזהה התנגשות.
- במילים אחרות, אם שתי תחנות מרגישות שהערוץ פנוי ומתחילות את השידור בו זמנית, שתיהן יזהו את התנגשות כמעט מיד. במקום לסיים את שידור המסגרות (אשר אובדות מיידית ממילא), התחנות יפסיקו את השידור ברגע שיזהו ההתנגשות.
- הפסקת שידור מהירה חוסכת זמן ורוחב פס.
- פרוטוקול זה הידוע בשם CSMA/CD, נמצא בשימוש נרחב ברשתות LAN בתת שכבת ה-MAC.
- CSMA/CD משתמש במודל הבא:



- בנקודת זמן t_0 , תחנה סיימה לשדר. כל תחנה יכולה לנסות לשדר כעת. אם שתי תחנות או יותר מחליטות לשדר יחד, תהיה התנגשות. תחנה יכולה לזהות התנגשות על ידי צפייה בהספק או ברוחב הפולס של האות המגיע למקלט והשוואתו לאות ששודר.
- לאחר שתחנה מסוימת מזהה התנגשות, היא מפסיקה את השידור, מחכה פרק זמן אקראי ומנסה לשדר שוב, בהנחה שאף תחנה לא התחילה לשדר בינתיים. לכן, המודל של CSMA/CD מכיל זמני תחרות וזמני שידור לסירוגין. כאשר זמני השקט מתקבלים כאשר כל התחנות שקטות (לא משדרות).

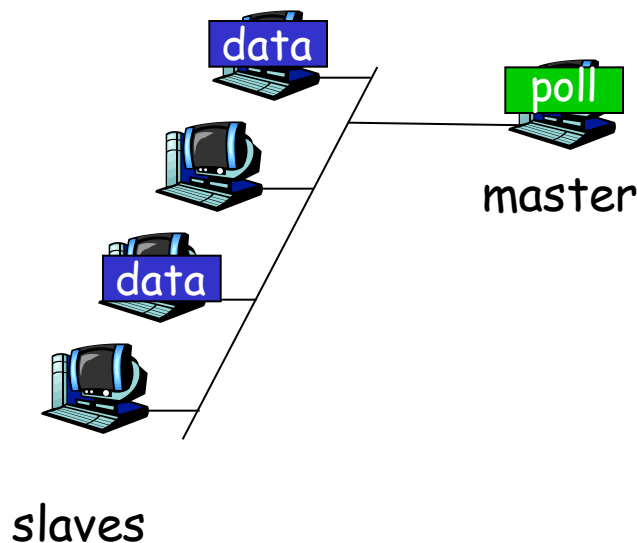
סיכום CSMA/CD

:CSMA/CD

- התנגשויות מתגלות תוך זמן קצר.
- שידור שמתנגש מופסק, ומפחית את האובדנים בערוץ.
- מתעקשים או לא מתעקשים על שידור מחדש.
- גילוי התנגשויות (collision detection):
 - פשוט ב-LANs עם כבלים: מודדים את עוצמת הסיגנל, משווים לאותות של השידור והקליטה כאשר משדרים בערוץ.
 - קשה ב-LANs ללא כבלים: מכיון שהקולט מופסק במהלך השידור.
 - באופן פרקטי לרשת יש זמן של "שיבוש שידור (jamming)" להבטיח שכל אחד יקבל את ההתנגשות.

פרוטוקול MAC "Taking Turns"

בחירות (Polling):



■ הצומת השולט (master) "מזמין" את הצמתים הנשלטים לשדר לפי תור.

■ בצורה אופיינית נשתמש בהתקנים נשלטים "אילמים".

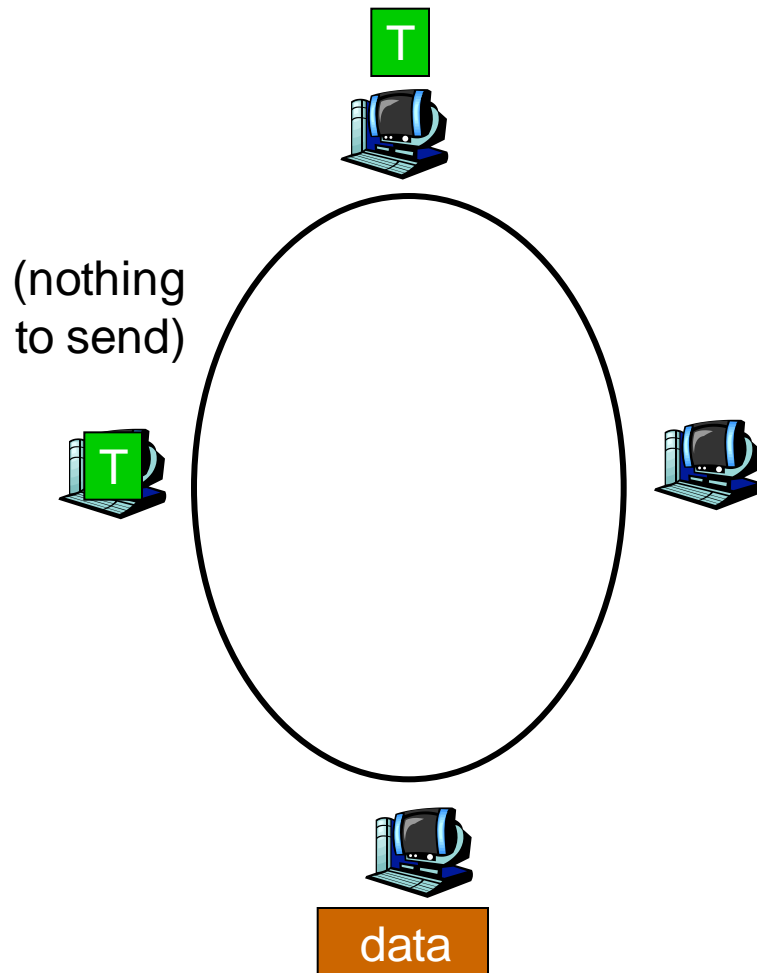
■ דאגות:

■ תקורה – זמן מבוזבז.

■ זמן תגובה - הזמן שלוקח בין שליחת ההזמנה לשידור לבין התחלת השידור.

■ נקודה יחידה של כישלון – בעיות של הצומת השולט.

פרוטוקול “Taking Turns” MAC



אסימון עובר (Token passing):

- אסימון עם בקרה עובר מצומת אחת לשניה באופן סידרתי.
- הודעת האסימון (token message).
- דאגות:
 - תקורת האסימון – זמן מבוזבז.
 - זמן תגובה - הזמן שלוקח בין שליחת ההזמנה לשידור לבין התחלת השידור.
 - נקודה יחידה של כישלון – בעיות של האסימון.

סיכום פרוטוקולי MAC

■ מה עושים עם תווך משותף ?

■ חלוקת הערוץ, לפי זמן, תדירות, או קוד,

■ חלוקת זמן, תדירות וקוד.

■ חלוקה אקראית (ודינמית),

■ ALOHA, S-ALOHA, CSMA, CSMA/CD

■ carrier sensing: קלה למימוש בחלק מן הטכנולוגיות (כבלים),

וקשה למימוש באלחוטי.

■ CSMA/CD משמש בטכנולוגית האתרנט.

■ Taking Turns,

■ בחירת הצומת המשדרת ע"י אתר מרכזי, אסימון עובר בין צמתים.

■ Bluetooth, FDDI (Fiber Distributed Data Interface),

IBM Token Ring

סיכום פרוטוקולי MAC (המשק)

פרוטוקולי MAC לחלוקת הערוץ (channel partitioning):

- יעילות גבוהה של הערוץ המשותף בעומסים גבוהים.
- לא יעיל בעומסים נמוכים: עיכוב בגישה לערוץ, רוחב פס של $1/N$ מוקצה אפילו אם רק מחשב אחד פעיל.

פרוטוקולי MAC לגישה אקראית (Random access):

- יעיל בעומסים נמוכים: צומת בודדת יכולה לנצל באופן מלא את כל הערוץ.
- לא יעיל בעומסים גבוהים: ריבוי התנגשויות.

פרוטוקולי “taking turns”:

- הכי יעילים לשני העולמות (עומסים גבוהים ונמוכים).

טכנולוגיות LAN

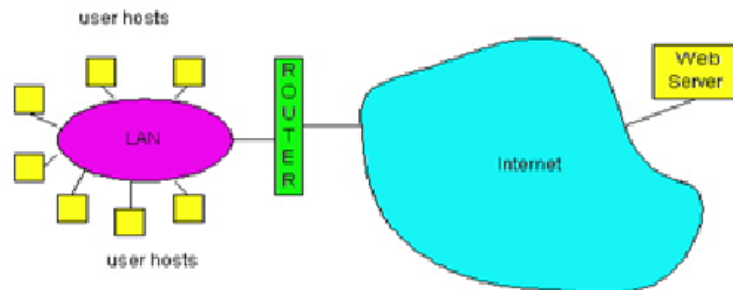
מקרה לימוד – טכנולוגיית LAN

עד עכשיו הראינו כי שכבת קישור הנתונים עוסקת ב:

- שירותים (services), גילוי שגיאות ותיקונם (error detection/correction), ריבוי גישות בערוץ (multiple access).

שלב הבא: טכנולוגיית LAN

- מיעון (Addressing) - שיטת פנייה למשאבים ברשת.
- אתרנט (Ethernet) - תקן של רשת תקשורת מקומית
- התקני רשת הקובעים את נתיבי חבילות הנתונים אל יעדיהן - hubs, bridges, switches.
- IEEE - 802.XX פיתחו מספר סטנדרטים לרשתות LAN ביניהם 802.11.



- PPP - פרוטוקול נקודה לנקודה.
- ATM - פרוטוקול להעברת נתונים בקצב גבוה.

מיצון ק-LAN

כתובות IP 32-bit:

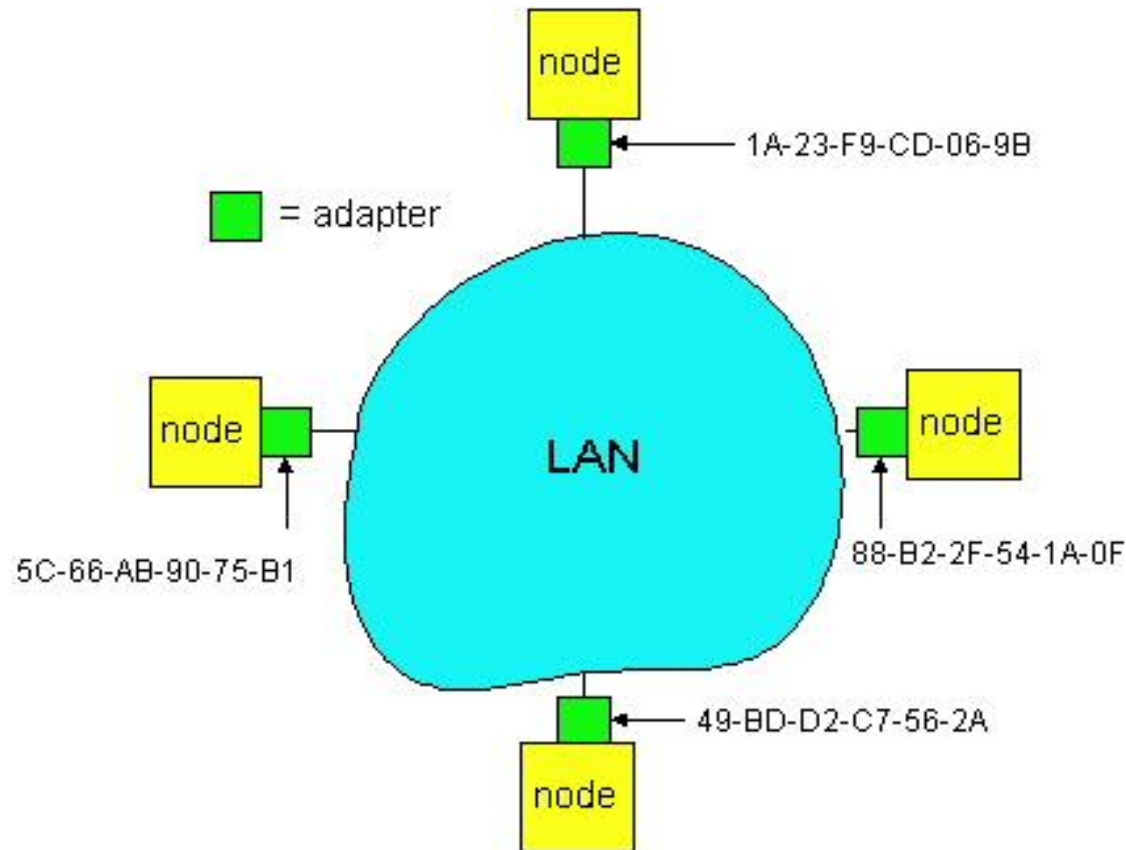
- כתובות שכבת הרשת (network-layer address).
- משמש לקבלת נתונים (חבילה) הכולל מידע ומועבר ברשת עם כתובות מקור ויעד.
- דוגמא: 192.168.32.201

כתובות LAN (או MAC או physical)

- **MAC = Media Access Control** או בקרת גישה למדיה, מזהה ייחודי המוטבע על כל רכיב תקשורת לרשתות מחשבים בעת הייצור.
- משמש לקבלת נתונים ממשק פיסי אחד לממשק פיסי שני באותה רשת.
- כתובות MAC עם 48 bit עבור רוב ה-LANs הצרובות בזכרון כרטיס התקשורת.
- דוגמא: 00:1D:0F:E5:A9:5A

מיצון ק-LAN

לכל כרטיס תקשורת יש כתובת LAN יחודית הצרובה עליו.



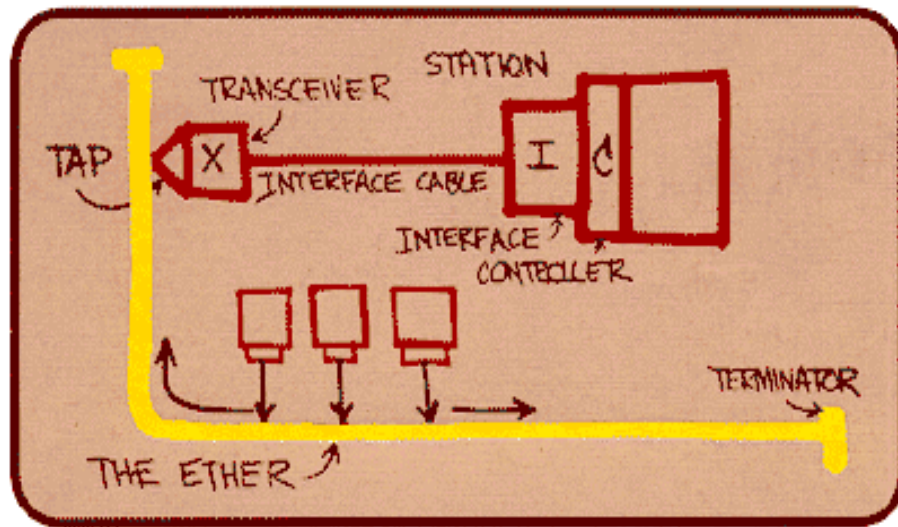
מיצון ק-LAN

- כתובות MAC מוקצות ע"י IEEE.
- היצרנים קונים "מנות" של מרחב כתובות MAC (על מנת להבטיח יחודיות).
- אנלוגיה:
- (a) כתובת MAC: כמו מספר מספר זהות, ביטוח לאומי.
- (b) כתובת IP: כמו כתובת דואר.
- כתובת MAC ניידת
- בעבר ניתן היה להעביר כרטיס תקשורת ממחשב אחד למשנהו (היום הוא חלק מלוח האם ולכן זו הערה שהיתה נכונה בעבר).
- הירארכית כתובות ה-IP אינה ניידת
- תלויה ברשת אליה המחשב מחובר.
- פרוטוקול ARP מתרגם את כתובות IP לכתובות MAC.

אתרנט - Ethernet

דומיננטיות טכנולוגית ה-LAN:

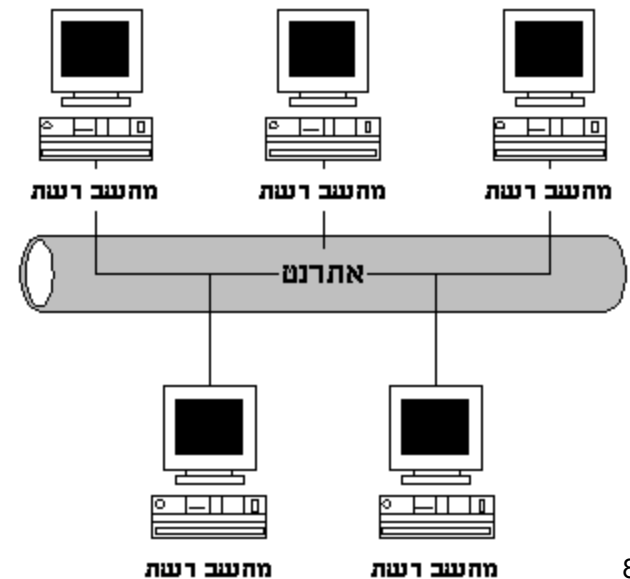
- זול – כ- 20\$ עבור 100Mbps.
- האתרנט הכי נפוץ בטכנולוגית ה-LAN.
- האתרנט יותר פשוט וזול מאשר טכנולוגיות האסימון ו-ATM.
- קצב העבודה בטכנולוגיה זו: 10, 100, 1000 Mbps



Metcalfe's Ethernet sketch

תקשורת מחשבים ואלגוריתמים מבזרים
(חורף 10 - 2009)

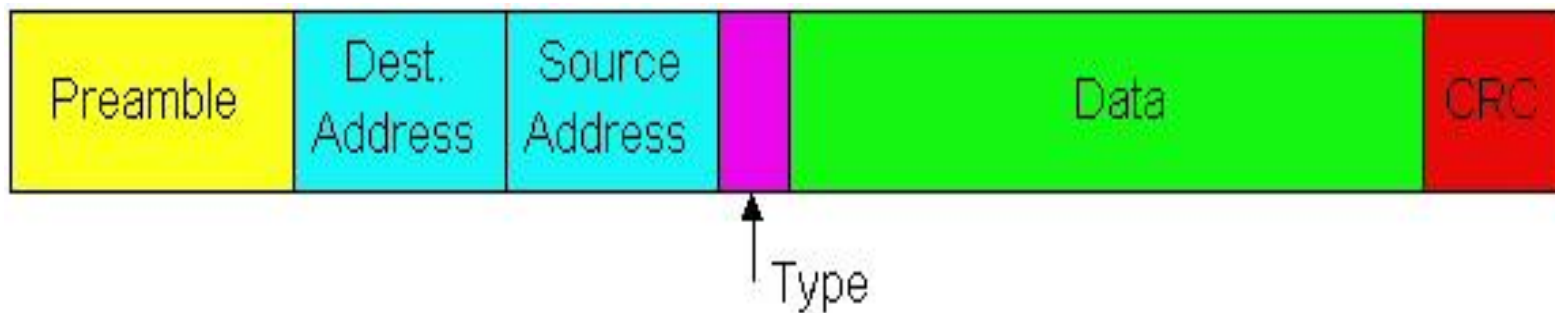
גיא לשם ©



מבנה האתחול

□ פעולת אריזת ההודעות כוללת את הפריטים הבאים:

- מסגור: זיהוי תחילת הודעה וסופה.
- מיעון: שדות המכילים כתובת מקור וכתובת יעד.
- איתור שגיאות: קודים מבוססי יתירות, המיועדים לגילוי שגיאות העברה בערוץ.

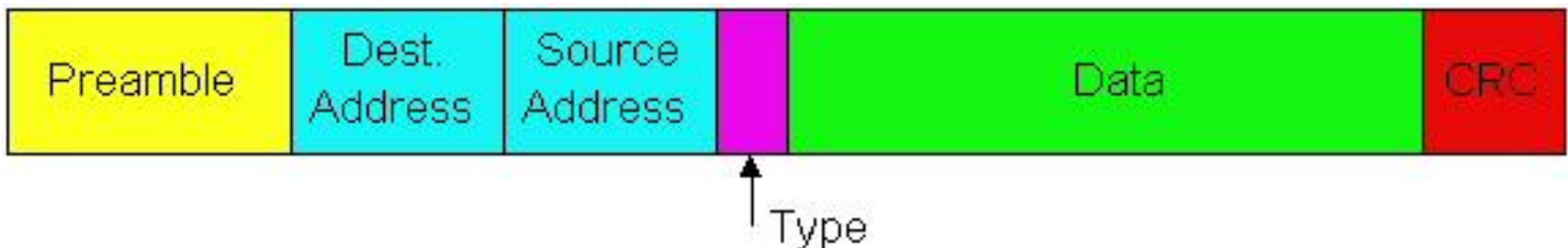


הקדמה (Preamble):

ההקדמה, המורכבת מסדרת הסיביות 101010 משמשת להכרזה על קיומה של המסגרת.

מבנה המסגרות של האתריט

- **מיעון (Addresses):** 6 בייטים, המסגרת מתקבלת ע"י כל התקני התקשורת ב-LAN ונזרקת אם הכתובת לא תואמת.
- **הסוג (Type):** שדה ה-TYPE מציין איזה סוג של מידע יש בשדה ה-DATA, זה מאפשר לנו לעבוד עם מס' פרוטוקולים בשכבות הגבוהות, IP, DECNET, או IPX.
- **המידע (Data):** גודל שדה המידע נע בין 46 ל-1500 בתים.
- **בדיקת CRC:** ההתקן הקולט בודק אם יש שגיאות, במידה ויש המסגרת נזרקת.



שיטת העבודה ברשת

Carrier Sense Multiple Access/Collision) - CSMA/CD Detection (איתור נושא/גילוי התנגשויות – הארכיטקטורה של אתרנט מבוססת על התפיסה שיושמה ברשת ALOHA לתקשורת שפותחה באוניברסיטת הוואי. מערכת ALOHA מאפשרת למספר התקנים מבוזרים להתקשר זה עם זה.

□ תהליך הגישה לרשת מורכב מ- 4 שלבים:

1. שלב ההאזנה – התחנה בודקת (SENSE) אם קיים ברשת גל נושא כלשהוא (CARRIER) או במילים אחרות אם מישהו משדר כרגע ברשת.
2. התחנה ממתינה פרק זמן של 9.6 מיקרו-שניות, ואם במשך זמן זה אין שידור ברשת, התחנה מתחילה לשדר אך ממשיכה להאזין לרשת.
3. המסגרת (FRAME) שהתחנה משדרת מופצת לכל התחנות האחרות ברשת. ייתכן שבאותו זמן תחנה אחרת ברשת שהמתינה אף היא 9.6 מיקרו-שניות תרצה לשדר. במקרה כזה שתי התחנות מגלות התנגשות (Collision) ושתיהן מפסיקות לשדר.
4. שתי התחנות תנסינה לשדר שנית במועד מאוחר יותר. הסיכוי שהן תשדרנה שנית בדיוק באותו הזמן מוקטן ע"י שימוש באלגוריתם מיוחד, הנקרא: **אלגוריתם BACK-OFF**, המיושם בכרטיס הרשת (NIC).

אלגוריתם CSMA/CD-ק סימול

A: sense channel, **if** idle (סרק)

then {

transmit (שדר) and monitor (האזן) the channel;

If detect another transmission

then {

abort and send **jam signal**;

update # collisions;

delay as required by exponential **backoff** algorithm;

goto A

}

else {done with the frame; set collisions to zero}

}

else {wait until ongoing transmission is over and **goto A**}

Ethernet's CSMA/CD *פאזן*

:Jam Signal

□ ודא כי כל המשדרים אחרים מודעים להתנגשות; 48 סיביות;

:Exponential Backoff

□ *מטרה*: התאם שליחה מחדש של המידע המנסה להערך לעומס הנוכחי.

■ עומס כבד: זמן ההמתנה האקראי ארוך יותר.

□ התנגשות ראשונה: בחר K מ- $\{0,1\}$; ההמתנה היא $512 \times K$ סיביות זמן השליחה (בקו תקשורת שהקיבולת שלו 10Mbps, זמן השידור של מסגרת כזו הוא 51.2 מיקרו שניות).

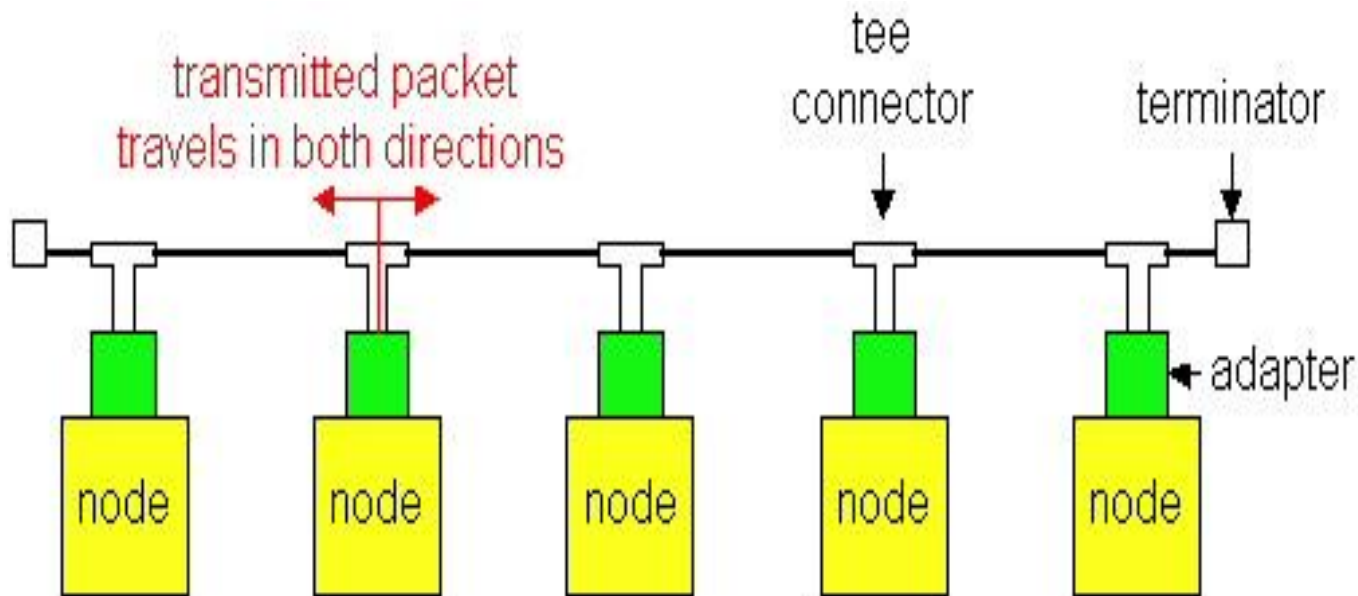
□ אחרי n התנגשויות: בחר K מ- $\{0,1,\dots, 2^n-1\}$.

□ אחרי 10 או יותר התנגשויות בחר K מ- $\{0,1,2,3,4,\dots,1023\}$.

טכנולוגיית האתרנט: 10Base2

□ 10Mbps; 2: מקסימום אורך כבל של 200 מטר.

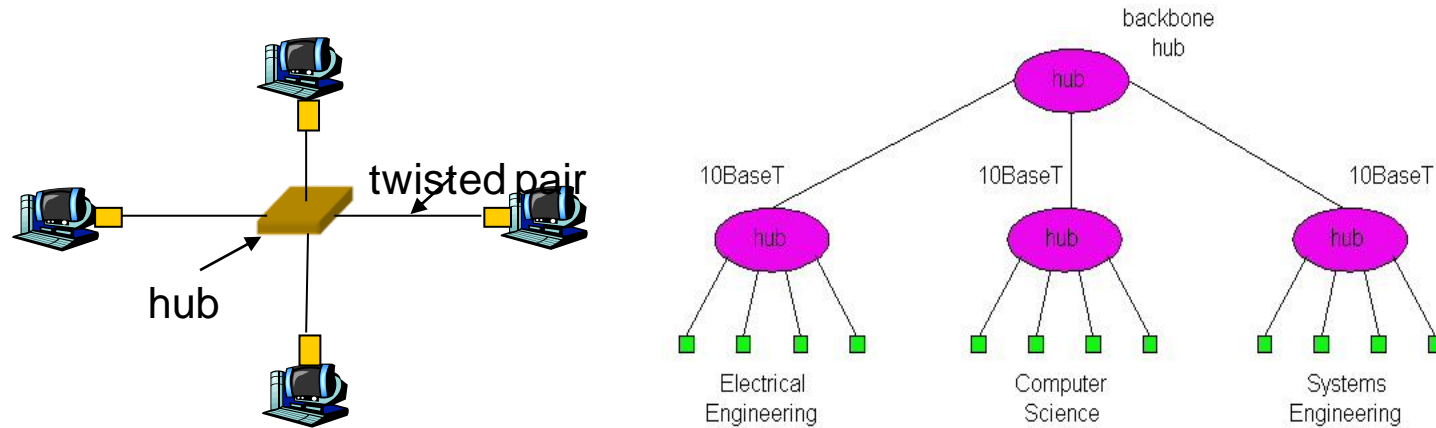
□ כבל קואקסיאלי דק בטופולוגיית bus.



□ מגברים משמשים לחיבורים של מקטעים רבים.

טכנולוגיית האתרנט 10BaseT- / 100BaseT

- קצב של 10/100 Mbps נקרא אתרנט מהיר ("fast ethernet").
- מסמל זוג שזור (Twisted Pair).
- **משתמשים ב-Hub** על מנת לחבר בין מחשבים באמצעות זוגות שזורים, לכן נקרא לטופולוגיה זו "טפולוגית כוכב (star topology)".
- טכנולוגית CSMA/CD מושתלת ומוצאת לפועל ע"י ה-hub.



- המרחק המקסימאלי בין המחשב ל-Hub היא 100 מטר.
- Hub יכול לנתק התקנים "פטפונים".
- Hub יכול לבצע ניטור מידע, סטטיסטיקה עבור מנהל הרשת.

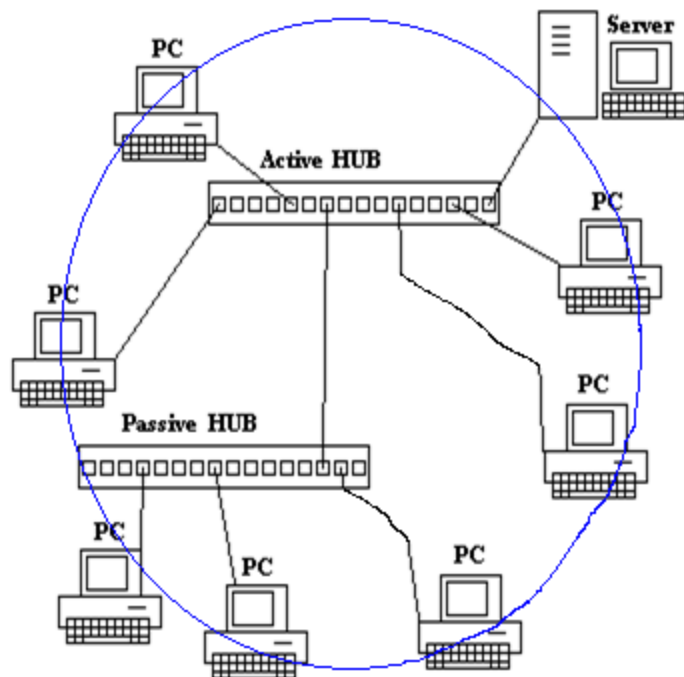
טכנולוגיית האתרנט Gbit

- משתמש במסגרת (frame) של האתרנט הסטנדרטי.
- מאפשר קישור נקודה לנקודה וערוצי הפצה לכל (broadcast) השותפים.
- התווך המשותף, משתמשים ב-CSMA/CD; מרחקים קצרים בין הצמתים על מנת להשיג יעילות גבוהה.
- נשתמש ב-hubs, הנקראים כאן "Buffered Distributors".
- נדרשת תקשורת דו-כיוונית מלאה (Full-Duplex) עבור 1Gbps עבור קישור נקודה לנקודה.
- half duplex - תקשורת חצי דופלקס, תקשורת שמסוגלת להעביר מידע בכיוון אחד בלבד בו-זמנית.
- Full-Duplex - תקשורת דו-כיוונית מלאה, תקשורת שמסוגלת להעביר מידע בשני הכיוונים בו-זמנית.

רשתות טבעת אסימון – Token Ring

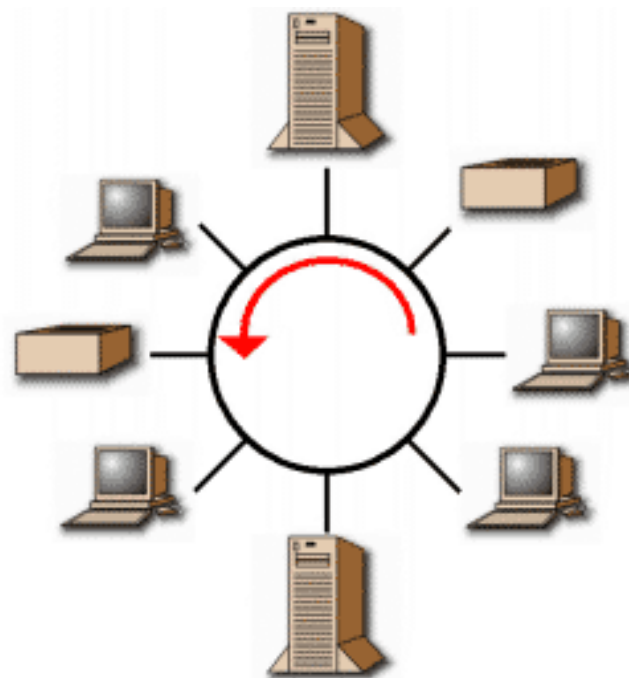
- לאור העובדה שגישה אל רשת מבוססת CSMA כרוכה בקיום מידה מסוימת של תחרות בין תחנות המנסות להעביר הודעות בעת ובעונה אחת. רשתות העברת אסימון משתמשות בשיטת גישה שונה.
- הגישה אל הרשת נקבעת ע"פ הקביעה בידי איזה תחנה מצוי האסימון. כלומר, ברגע נתון מתאפשר רק לתחנה אחת, זו שבידיה מצוי האסימון, לתפוס את הערוץ. אז מועבר האסימון מתחנה לתחנה, עד שהוא מגיע לתחנה הממתינה לשגר את ההודעה. לאחר שיגור ההודעה מועבר האסימון אל התחנה הבאה.
- קיימות שתי טופולוגיות עבור רשתות העברת אסימון: **טבעות העברת אסימון (Token passing rings)** ו**אפיקי העברת אסימון (Token passing busses)**. **בטבעת העברת אסימון**, מגדירה הטופולוגיה בעלת הצורה של הלולאה הסגורה את הטופולוגיה הלוגית (כלומר את סדר העברת האסימון בין התחנות). **אפיק העברת אסימון** מתאפיין ביתר גמישות תפעולית מפני שסדר העברת האסימון בין התחנות נקבע על-ידי טבלאות הנמצאות בכל תחנה. אם קיימת תחנה (כגון מדפסת), שאינה יוזמת אף פעם תקשורת כלשהיא, היא תהווה תחנה המשמשת אך ורק לסיום מעגל, והיא לא תיכלל בסדר התשאול של התחנות. אם תחנה כלשהיא זקוקה לעדיפות גבוהה, היא יכולה להופיע מספר פעמיים בסדר התשאול.

טבעות העברת אסימון ואפיקי העברת אסימון



אפיקי העברת אסימון (Token passing)
busses): תחנות מקושרות באורח פסי על ידי
bus משותף, אבל התחנות מאורגנות ע"י
התוכנה כטבעת.

תקשורת מחשבים ואלגוריתמים מבזרים
(חורף 10 - 2009)



טבעת העברת אסימון (Token passing)
(rings),
מגדירה טופולוגיה בעלת הצורה של הלולאה
הסגורה את הטופולוגיה הלוגית (כלומר את
סדר העברת האסימון בין התחנות).

נתחיל בהרחקה f-LAN

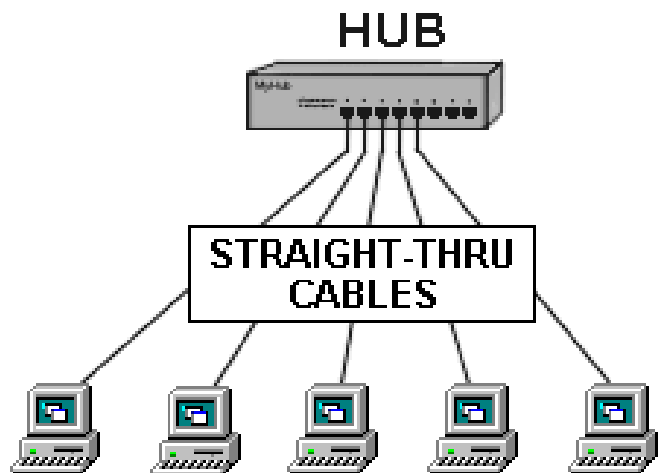
□ מוטיבציה:

- מגבלת מרחק (Distance limitation).
- ירידה בביצועים ככול שמיספר משתמשים מתרבה.

□ נדון ב:

- Hub
- Repeater
- Bridge
- Switch

Hub - מרכזיה

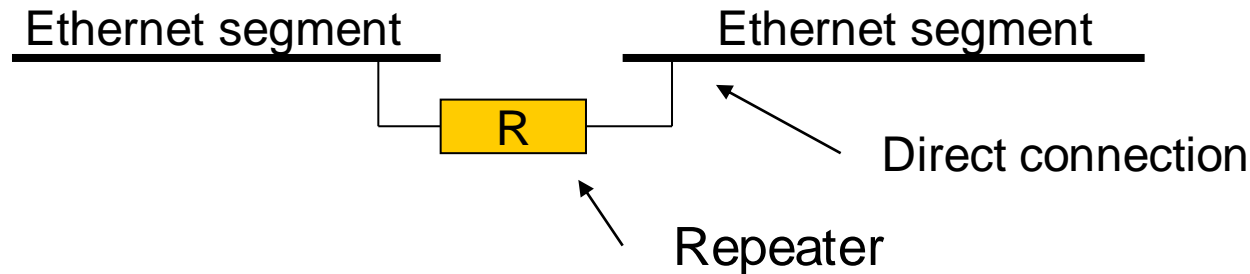


המרכזייה (HUB) מהווה נקודה מרכזית לכל הרשת, כאשר מחשבים מחוברים למרכזיה (HUB) ממנה עובר כבל נפרד לכל מחשב

לסיכום:

- התקן חומרה.
- יוצר מקטע LAN אחד.
- כל "מסגרת" אתרנט מתקבלת מממשק (port) אחד ונשלחת לכל הממשקים (ports) האחרים.
- מבחינה לוגית פועלת על אותות ומופצת.
- כל אות נכנס לכל החיבורים.
- יוצר תחום התנגשויות אחד.

מגבר משחזר - Repeaters



■ מגבר משחזר (Repeater) - הוא רכיב ברשת מחשבים המחובר בין שני מקטעים של אותה הרשת ומאפשר להגדיל את המרחק בין שני קצותיה. המשחזר נכנס לפעולה כאשר מתקבלת תשדורת באחד מקצותיו, הוא מנקה את התשדורת מהפרעות, מחזק את האות אם יש צורך בכך ומעביר אותו הלאה אל הקצה השני. משחזר לא מגביל מתחמי שידור או מתחמי התנגשות. לכל מדית תקשורת מותאם משחזר ייחודי, וקיימים רכיבים עבור כל סוגי המדיות ובין השאר כבלים מוצלבים, סיבים אופטיים ואף לתקשורת אלחוטית.

■ לסיכום: ניתן להאריך את הרשת בעזרת משחזר וכך גם לחדש את האות שנחלש.

■ התקן חומרה.

■ מחבר בין שני מקטעי LAN.

■ מעתיק אות (סיגנל) ממקטע אחד למשנהו.

■ מגביר אות ממקטע LAN אחד ושולח אותו למקטע LAN שני.

■ מרבה גם רעשים והתנגשויות.

■ עובד בשני הכיוונים בו-זמנית.

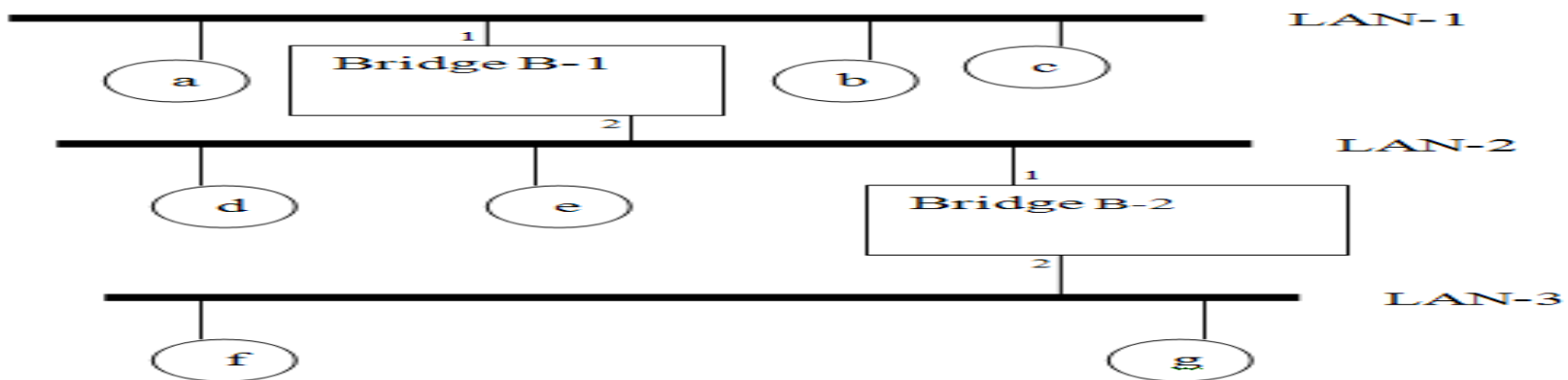
Bridges

□ Bridge הוא מכשיר אשר מחבר בין רשתות LAN.

□ ה-bridge, בניגוד ל-Hub, מפריד את מרחב ההתנגשויות של כל תת-רשת, לומד את הרשת ויודע לנתב חבילות למוצא המתאים לפי כתובת ה-MAC ועל פי טבלת bridging המקשרת בין כתובת לפורט מוצא.

□ הלימוד נעשה בצורה דינאמית וה-bridge שקוף לתחנות האחרות. כאשר חבילה מתקבלת, ה-bridge שומר את כתובת המוצא של החבילה ביחד עם הפורט בו היא התקבלה (אם כבר לא שמורה בטבלה) והזמן הנוכחי.

□ באם כתובת היעד לא נמצאת בטבלה, ה-bridge ישלח עותק של החבילה לכל אחד מהפורטים האחרים (לפי CSMA/CD) אחרת החבילה תנותב לפורט המתאים. ה-bridge ימחק כניסות עבור כתובות מהן לא התקבלה חבילה מעבר לזמן נתון (Aging Time).



Bridges (המשק)

- חומרה ברמת קישור הנתונים.
- מחבר בין שני מקטעי LAN.
- שליחת מסגרות (frames)
 - מאחסן ושולח מסגרות איתרנט.
 - בוחן את ראש המסגרת (frame header) ובאופן סלקטיבי שולח את המסגרת על בסיס כתובת ה-MAC של היעד.
 - כאשר המסגרת נשלחת למקטע LAN המתאים, נשתמש ב-CSMA/CD (פרוטוקול גישה לערוץ משותף) לגשת למקטע.
- אין שליחה של רעש או התנגשויות.
- לומד את הכתובות ומבצע פילטור.
- מאפשר שליחה עצמאית.
- שקוף וברור
 - המחשבים לא מודעים לנוכחות של ה-bridge.
 - הכנס והפעל (plug-and-play), לימוד עצמי (self-learning).
 - ה-bridge לא נזקק ל"קינפוג".

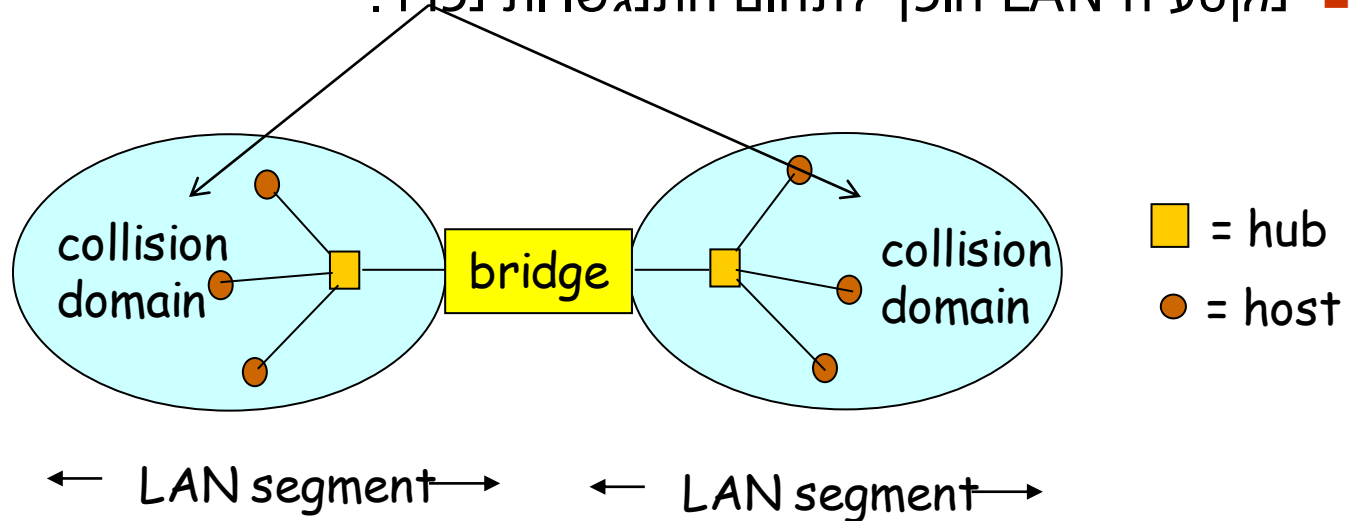
ה-Bridges מאחד את התצורה

□ התקנת ה-Bridge שוברת את הרשת מקומית לתוך קטעים של רשת מקומית קטנים יותר.

□ ה-Bridge מסן חבילות מידע (packets):

■ מסגרות של אותו מקטע LAN בד"כ לא נשלחות למקטעי LAN אחרים.

■ מקטע ה-LAN הופך לתחום התנגשויות נפרד.



אלגוריתמי אימות ה-Bridge

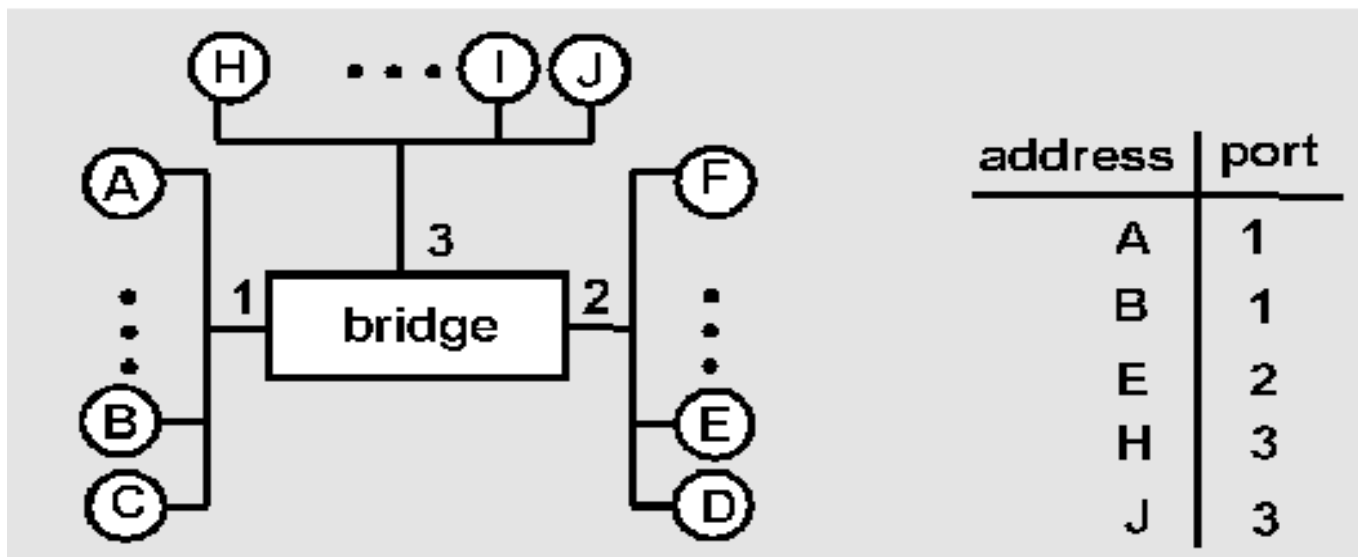
- מקשיב במוד מעורבב (כאשר כל המסגרות (frames) מועתקות ומנותחות).
- מסתכל על כתובת המקור השולח של המסגרות הנכנסות.
- מכין רשימה של המחשבים על כל מקטע (segment).
- רק מעביר הלאה אם נדרש.
- תמיד מעביר הלאה ב-broadcast/multicast.

אפלטוןית אימוץ fe ה-Bridge (המשק)

- ל-bridge יש את טבלת ה-bridge (bridge table).
- רישום ב- טבלת ה-bridge:
 - כתובות LAN של הצמתים (מחשבים), ממשקי ה-bridge (ports), והזמן הנוכחי.
 - כניסות ישנות בטבלה נזרקות (זמן חיים בטבלה כ- 60 דקות).
- ה-bridges **לומד** איזה מחשבים ניתן להשיג דרך הממשקים
 - כאשר מסגרת מתקבלת, ה-bridges "לומד" את המיקום של השולח: מקטע של רשת מקומי נכנסת.
 - תיעוד של הזוג השולח/מיקום השולח בטבלת ה-bridge.

Bridge-*f* אנדל

נניח ש-C שולח מסגרת ל-D ו-D מחזיר חזרה עם מסגרת ל-C.



ה-Bridge מקבל מסגרת מ-C

שימו לב על טבלת ה-Bridge ש-C מחובר ללמשק 1 ב-Bridge.

מכיון ש-D לא נמצא בטבלת ה-Bridge, ה-Bridge שולח מסגרת לממשקים (ports) 2 ו-3

המסגרת מתקבלת ע"י D

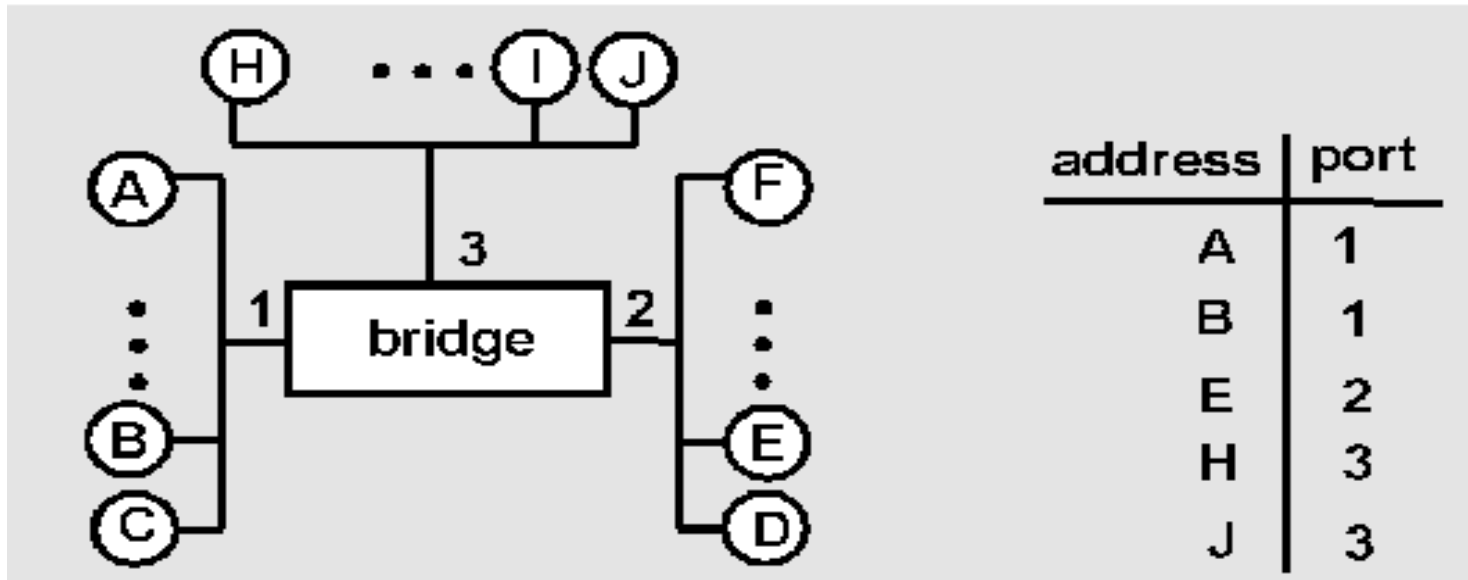
Bridge- \mathcal{F} $\kappa\mathcal{N}\mathcal{C}\mathcal{I}\mathcal{Z}$

□ D יוצר מסגרת עבור C, ושולח

□ ה-Bridge מקבל את המסגרת

■ שים לב שכעת בטבלת ה-Bridge, D נמצא בממשק 2

■ ה-Bridge יודע ש-C נמצע על ממשק 1, לכן באופן סלקטיבי הוא מעביר הלאה את המסגרת לממשק 1



אלגוריתם של עץ מרחב

Spanning Tree Algorithm

□ רשת של bridges הוא גרף.

■ בד"כ הגרף נבנה בדרך הירארכית

□ אם ה- bridges בקצה ההירארכי נכשל -- LAN יכול להיות מנותק.

□ לכן ה-LAN בד"כ מחובר עם יותר מאשר נקודת חיבור אחת (יתירות).

□ אם ניתן לגרום לאותו מידע להיות מועתק הרבה פעמים מעל הרשת מקומית --
< זה אפילו יכול לרסק את הרשת.

□ פרוטוקול עץ פורש יכול למצוא תת-גרף שפורש את כל הצמתים
שלו ללא לולאה.

■ פריסת צמתים (Spanning) == כל מקטעי LAN נכללים.

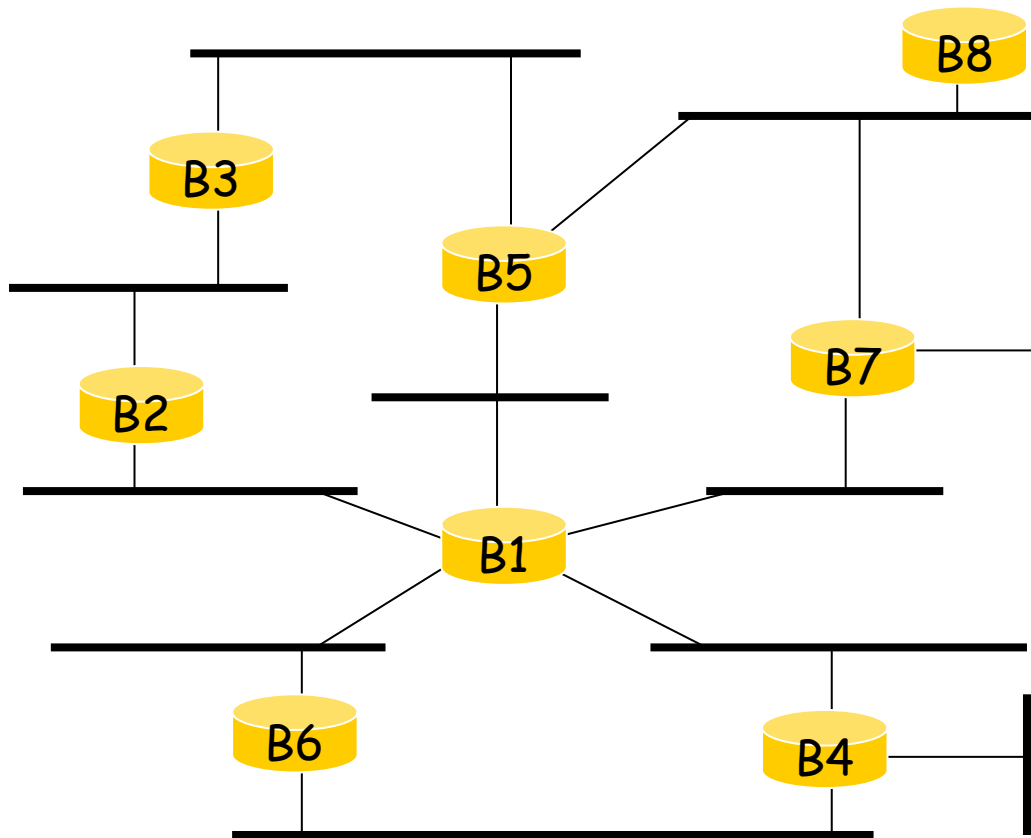
■ עץ (Tree) == טופולוגיה ללא לולאות.

□ פרוטוקול הביזור עובד באופן הבא:

■ קובע איזה bridge יהיה בשורש העץ,

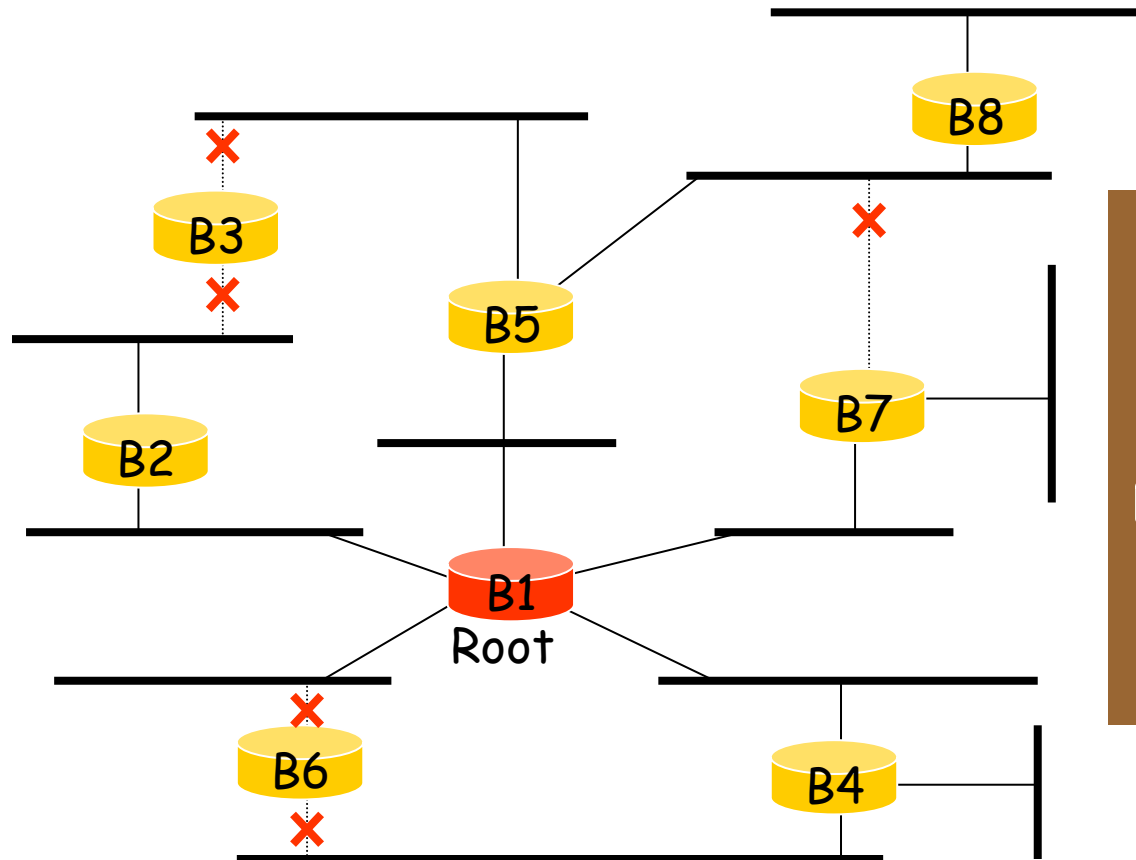
■ כל bridge מפנה לדרך אחרת ממשקים (ports) שאינם חלק מן העץ.

דואנא ףאצ כורע (Spanning Tree)

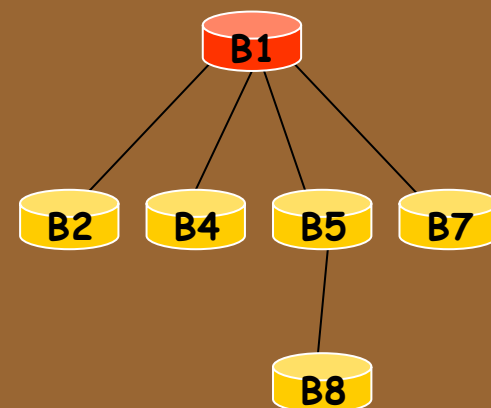


- פעולת הפרוטוקול:
1. בוחר שורש.
 2. עבור כל LAN, בוחר את ה-bridge שנראה הכי קרוב לשורש.
 3. כל ה-bridges על ה-LAN שולחים חבילות נתונים (packets) בכיוון השורש דרך ה-bridge הנראה הכי קרוב לשורש.

צורת קשר (המשק)



Spanning Tree:



Switch

- ביצועים גבוהים מכפיל את ממשקי ה-bridge !
- פיסית דומה ל-hub.
- לוגית דומה ל-bridge
 - פועל על חבילות המידע (packets).
 - מבין בכתובות.
 - מעביר הלאה רק אם נדרש.
 - שיטת העברה הלאה יותר מתוחכמת.
- מרשה לזוגות נפרדים של מחשבים לתקשר באותו זמן (full duplex).

תצורה אופינית

