

תוכן עניינים

| | |
|----|--|
| 2 | הקדמה (+ סוף שיעור 3): הקדמה והסביר על התקנים השונים |
| 8 | שיעור 4: מבנה החבילות וארQUITטורת 802.11 |
| 12 | שיעור 5: WEP |
| 18 | שיעור 6: המשך WEP |
| 21 | שיעור 7: המשך WEP |
| 24 | שיעור 8: WPA, WPA2 |

הקדמה (+ סוף שיעור 3):

הקדמה וסיכום ("על רגאל אחת"):

Wi-Fi הוא קישור של Wireless Fidelity, הוא התקן שידור של גלי רדיו וմבוסס על 802.11 Wi-Fi, מכשירים רבים מתחברים לאינטרנט ע"י Wi-Fi, מחשבים ניידים, מחשבים נייחים, קונסולות משחק, טלפונים סולריים ועוד.

בהקדמה זו נסביר על הצורות השונות של Wi-Fi, התקנים שונים בדגש על Router ביתית או AP ארגוני או ביתי.

ראוטר ביתי מכיל כמה רכיבים, Modem, Wi-Fi, Switch ואחראי על ההתחברות אל הספקית.icut נעבור על ההגדרות השונות הקיימות בראוטר וב-Wi-Fi עצמו.

קליטה: הקליטה של Wi-Fi נמדדת ב dBm, ככל ברזל, ככל שהdBm נמוך יותר, כך הקליטה טובת יותר. תמיד הקליטה תציג כMINUS 20- ועד ל-90-. הטוווחים הינם:

- 20- ועד -30: הקליטה מצוינת וכנראה אתם מרחק של מטר בודד מרכיב Wi-Fi במקרה שלטן AP או Router ביתי.
- -50 : קליטה מצוינת גם, אך אתם מרחק של כמה מטרים מהנקודה.
- -60 : קליטה סבירה, זאת אומרת שבouceמה זו תוכלו לגלוש באינטרנט ולא להבחן באיטיות שימושית.
- -70 : אומר כי הקליטה פחות מסבירה ולא תוכלו לראות סרטונים באיכות גבוהה או לטעון דפים \ סרטונים בmahירות סבירה.
- -80- או -90: עצמת הקליטה נמוכה מאוד ולרוב לאצליח לגלוш באופן סביר ואם בכלל.

טיפים נוספים: כאשר נקנה ראוטר או AP נבחן כי לכל אנטנה יש עצמת dB הבדל בין dbi ל-dbm הוא ש-db_i הוא כמה מקסימום של עצמת השידור תהיה -dm_b והוא כמה "כח" משדר עצם האנטנה (Wi-Fi)

לכן, אם נבדוק למשל באתר של Tp-link את הראוטר הבא: WA901ND-TL נוכל להבחן כי רשום שהאנטנות למשהן הן 3 אנטנות שכל אחת 5dbi זאת אומרת, זה שיש לנו 3 אנטנות לא אומר שהעצמה תהיה גדולה יותר. Antenna Type 3 * 5dBi Detachable Omni Directional

לכן יש צורך לבדוק אם האנטנה של הראוטר היא יותר מ-5dbi וכך נוכל להשיג קליטה חזקה יותר במכשירים מרוחקים יותר מהנקודה בה נמצא הראוטר.

כלי לבדיקת עצמת השידור של Wi-Fi באזרור הוא NetSpot, שניתן להוריד מוגול.

SSID - הוא השם של "החברה" אותו יפיק הראוטר, למשל WiFi חלקנו נכון להיום רגילים לראות HOTBOX וכו' של חברות הטלוויזיה והכבלים, שכן הרבה חברות בתים קונים "Bundle"

טלוויזיה + ספק + תשתית וכו', למעשה, בעצם, אותה החברה מספקת גם ראוטר והוא זה שמניף את ה Wi-Fi. דוגמה לSSID המוצגים על ידי הטלפון הסולרי, אותן SSID שמצוין הטלפון הסולרי בכך שחייב רשותות Wi-Fi ואלו הם היחידים שבתווח הקליטה שלו.

סוג הצפנות:

- כאשר אנו מגדירים את הרואוטר, חובה להגדיר סיסמת התחרבות ל SSID שכן, אם הרשות תהיה פתוחה, כל תוקף יוכל להתחבר לרשות ולבצע התקפות מגוונות שכבר נלמדו פה באתר, החל מ MITM או שינוי DNS וכו'ayan. لكن חובה علينا להגדיר סיסמא חזקה, וכך הצפנה חייב להיות לפחות WPA2, עצת נסביר על סוג ההצפנות הקיימות ברכיב ה-Wi-Fi:
- WEP – הוא קיצור של Wired Equivalent Privacy והוא פרוטוקול הישן ביותר והחלש ביותר מבין פרוטוקולי האבטחה של Wi-Fi, נכון להיום אין להשתמש בו שכן תוקף, בקבילות יתרה יכול לפרק את הרשות ולסכן את המשתמשים בה.
 - WPA – הוא קיצור של Wireless Protected Access והוא פותח את התאזרחות ה-Wi-Fi, הפרוטוקול משתמש במפתח זמן מסוג TKIP והוא נחשב לפרוטוקול ביןיהם אשר מטרתו היא להחליף את פרוטוקול ה-WEP.
 - WPA2 – הוא התקן הסטנדרטי שיש להשתמש והוא הגרסה החדשה יותר של WPA, הוא משתמש במפתח זמן מסוג CCMP או בקיצור WPA2\PSK הוא השימוש הביתי של WPA2 (Persona).
 - Enterprise WPA2 – הוא השם השני של 802.1x והוא יכול לבדוק את הרכיב המתחבר אליו על ידי כך שהרכיב שורצוה להתחבר יאשר על ידי שרת RADIUS.

סטנדרטים ב-Wi-Fi:

- לכל Wi-Fi יש סטנדרט שונה, ה-802.11 מגיע בתצורה של N\G\B:
B – הוא עד מהירות של 11Mbps וnochesh ליחסית איטית בתדר של 2.4Ghz
G – תומך עד קצב של 54Mbps בתדר של 2.4Ghz
N – תומך עד 300Mbps ויכול להגיע ל450Mbps בתדרים של 2.4Ghz ו-5Ghz
AC – הוא המהיר ביותר, קצב העברה של 1Gbps

תדרים בעולם Wi-Fi קיימים 2 תדרים, 2.4Ghz ו-5Ghz ההנחה של אנשים היא ש5Ghz הוא גדול יותר וכן מגיע רחוק יותר מאשר 2.4Ghz אך זו טעות. לתדר ה-2.4Ghz יש 13 ערוצים, העוצמים המומליצים לבחירה הם: 1, 6, 11, 1, 6, 11, הסיבה היא שעוצמים אלו לא חופפים לגלי רדיו שקיים ברכיבים אחרים ולכן לבחור בהם (לרוב הרואוטר יבחר בלבד את העורץ ואין צורך להגדיר לו)

2.4Ghz הוא תדר נמוך יותר וכן "חודר" קירות ומחסומים אחרים בקלות יותר מאשר 5Ghz אז למה שנבחר בתדר 2.4Ghz או ב-5Ghz? לתדר ה-5Ghz הוא תדר פחות עmmo, אך הוא נוחש מהיר יותר ויכול לספק מהירות גבוהה יותר. אבל! רוב הרואוטרים תומכים ב-Dual Band, זאת אומרת שיש לרואוטר 4 אנטנות, 2 אנטנות בתדר 2.4Ghz ו-2 אנטנות בתדר 5Ghz, מדובר שיש 2 אנטנות לכל תדר? אחת משדרת ואחת קולטת וכן יוצרת פ煦ות "עומס".

[מזכיר]

מושגים נוספים (תזכורת מתקשורת):

DHCP: פרוטוקול תקשורת המשמש להקצאה של כתובות IP ייחודיות למחשבים ברשת מקומית (LAN). בנוסף לכטבות ה-IP, שירות DHCP בדרך כלל יספק למוחשב גם נתונים כמו ה-Subnet mask, כתובת שרת DNS וכתובת שער הגישה (Gateway), כך שהמחשב יוכל להתחיל ל��ק ברשת ללא צורך בנזtones נוספים.

DNS: בamilim פשוטות, Domain Name System הוא אוסף של מסדי נתונים המתרגם "שמות مواقع" (Hostnames) לכטבות IP. ניתן להתייחס לDNS כאל "ספר הטלפונים של האינטרנט" מכיוון והוא ממיר שמות مواقع קלים לזכור כמו com www.duckduckgo.com לכטבות IP כמו 40.114.177.156.

הבדלים בין הידר של רשות אלחוטית (802.11) לרשות קוית (802.3)

:802.3

```
> Frame 42: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on interface 0
  ▾ Ethernet II, Src: Cimsys_33:44:55 (00:11:22:33:44:55), Dst: Powercom_3c:7a:00 (00:05:9a:3c:7a:00)
    > Destination: Powercom_3c:7a:00 (00:05:9a:3c:7a:00)
    > Source: Cimsys_33:44:55 (00:11:22:33:44:55)
    Type: IPv4 (0x0800)
```

:802.11

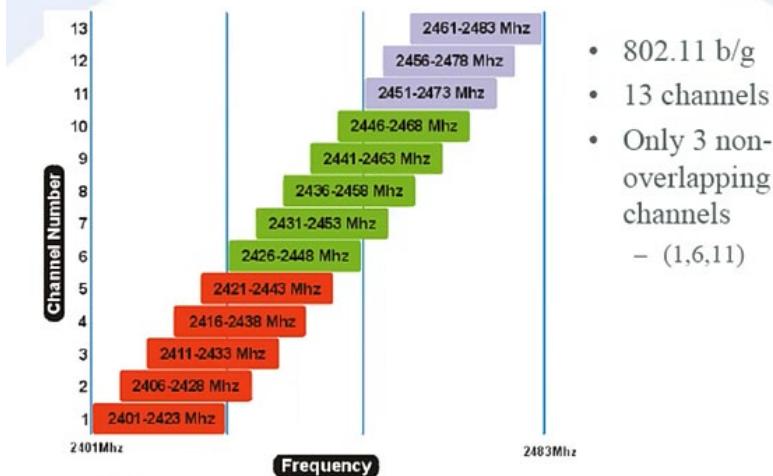
```
▼ IEEE 802.11 Beacon frame, Flags: .....
  Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: fa:8f:ca:37:71:7c (fa:8f:ca:37:71:7c)
    Source address: fa:8f:ca:37:71:7c (fa:8f:ca:37:71:7c)
    BSS Id: fa:8f:ca:37:71:7c (fa:8f:ca:37:71:7c)
    ..... 0000 = Fragment number: 0
    1000 0010 0011 .... = Sequence number: 2083
    Frame check sequence: 0xf6ef3bd0 [incorrect, should be 0x7e761ebc]
```

ברשת אלחוטית ישנו הידר נוסף בשם **RadioTap**: כותרת זו מספקת מידע נוספת שמתווסף לכל מסגרת 802.11 בעת לכידת מסגרות. רק כדי להיות ברור - אלה אינם חלק מפורמט הפרטאים הסטנדרטי 802.11, אלא הם מידע שנוסף בזמן הלכידה כדי לספק עוד נתונים על הפרטאים שנלכדו. לדוגמה, בלכידת תעבורת רגילה 802.11, אין מידע לגבי רמת אות הקבלה של המסגרת בזמן הלכידה אבל זה נמצא בהידר RadioTap, מה שיכל להיות שימושי מאוד. דוגמה נוספת, אין מידע על איזה ערוץ נמצא בשימוש על ידי תחנה שיצרה את המסגרת אבל זה נמצא בהידר RadioTap, וזה שוב יכול להיות מאוד שימושי.

מידע נוסף: <https://dalewifisec.wordpress.com/2014/05/17/the-to-ds-and-from-ds-fields>

כל שטדר יותר גבוהה אזי האורך גל יותר קטן, וככל שאורך גל יותר קטן אזי החדרות שלו (חדרה דרך מכשולים) יותר קטנה
ערכאים הם תחומי תדרים (לדוגמה, 2.4 GHz הרץ) או במילימטרים, הקזאה של טווח תדרים

WiFi: 2.4 GHz Bands and Channels



- 802.11 b/g
- 13 channels
- Only 3 non-overlapping channels
 - (1,6,11)

בשביל לנצל את כל רוחב הפס, מצופה שאף מכשיר אחר לא ישמש בחלק מהתווך (לדוגמה, התווך בתמונה לעיל)

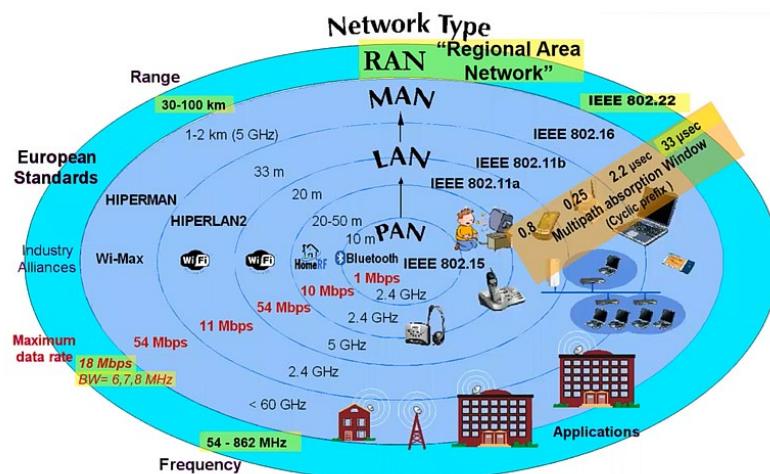
תזכורת מודל השכבות:

| מספר השכבה | שם השכבה | מטרה (בקיצור) | פרוטוקול לדוגמה | שם של גוש מידע | הערות המידיע ביט אחר ביט – 0 או 1 בכל פעם |
|------------|------------------------------------|------------------------|-----------------|---|---|
| 1 | השכבה הפיזית (Physical Layer) | ביט (bit, סיבית) | | | |
| 2 | שכבת הקשר (Data Link) | מסגרת (frame) | Ethernet | תקשרות בין יישויות סמוכות זו לזו | |
| 3 | שכנת הרשת (Network Layer) | .packet (帧) (חבילה) | IP | השלטה על המסלול שתעביר חבילת מידע בין המקור אל היעד | |
| 4 | שכנת התעבורה (Transport Layer) | סרגמנט (segment) | TCP | ריבוב אפליקציות על +אותה ישות (תמייד) +מתן אמינות ל קישור (אופציונלי) | |
| 5 | שכנת האפליקציה (Application Layer) | * אין שם מיוחד * | HTTP | שימושים שונים בהתאם לאפליקציה | |

תקן אומר איזה תדרים עובדים, ובאיזה צורה עובדים ואיך יוצרים את החבילות שעובדים איתם תקן 802.11 זה wireless WLAN IEEE 802.11 נמצא בתפר בין Data Link Layer ו-Network Layer (Layer 2 ו-Layer 3 בהתארכות התחנות)
כלומר, אינו מדובר על Network Layer ומטה

יש כל מיני תתי תקנים כמו 802.11ac שהם תיקוני בטחה וכו'

wifi זה תקן (גוף עסק) וזה לא wifi 802.11



| | Personal Area Network (PAN) | Local Area Network (LAN) | Metropolitan Area Network (MAN) | Wide Area Network (WAN) |
|---------------|---|---|--|--|
| Technology | <ul style="list-style-type: none"> Bluetooth Ultra-wideband (UWB) | <ul style="list-style-type: none"> WiFi (802.11a/b/g/n/ac) WiGig (802.11ad) | <ul style="list-style-type: none"> WiMAX (802.16) | <ul style="list-style-type: none"> GSM GPRS W-CDMA HSPA LTE |
| Data Transfer | Low data rates | High data rates | Medium data rates | Low to high data rates |
| Range | Very short range | Short range | Medium range | Long range |
| Connectivity | Notebook to PC to peripheral devices to systems | Computer to computer or peripheral devices and the Internet | LAN or computer to high-speed wire line Internet | Smartphones and other mobile devices to WANs and the Internet |

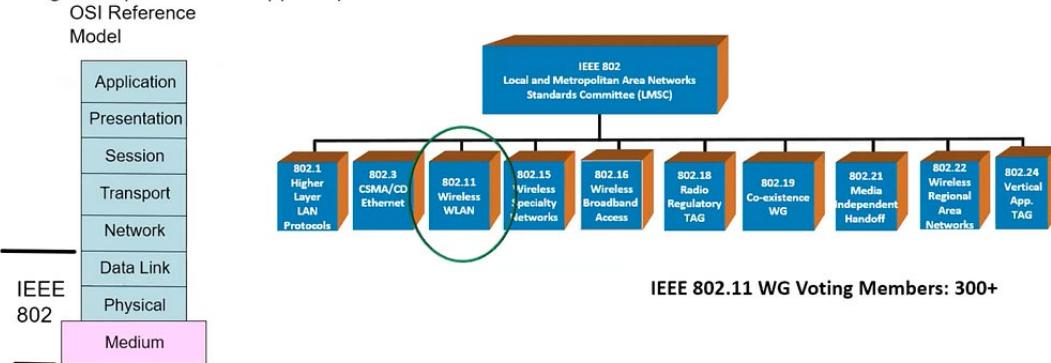
נשים לב כי wifi לא יכול להיות בכלל תקן כי מי שקבע את זה הוא קבוצה של גופים מסחריים שהסתכימו על דרך להעביר תקשורת אלחוטית. לעומת זאת, יצרו מוצר ע"י כך שלקחו מה שטוב להם.
נקרא wifi alliance = ברית/שיתוף פעולה (modulatia rates וכו')

הבדלים בין המהירויות אלו הבדלים במודולציה וככל שהמודול יותר מורכב יש יותר סיכוי להפרעות (מודולציה של rates וכו')

כל החלק הנ"ל (של המודולציות וכו') הוא החלק הפיזי.

The IEEE 802.11 Working Group is one of the most active WGs in 802

- Focus on link and physical layers of the network stack
- Leverage IETF protocols for upper layers



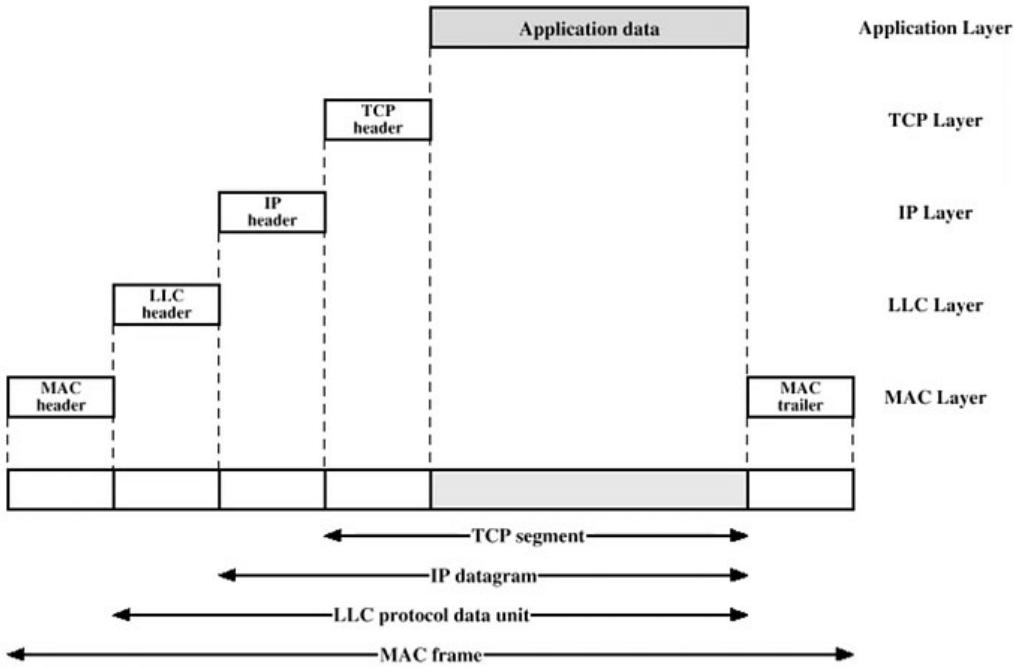
מבחינת בסיס הפרטוקול כאשר נרצה להקים רשת אלחוטית נצטרך לשלוח אותן על מנת
שמכשירים אחרים יזהו אותנו
הארQUITקטורה שלנו היא צזו שטמיד מנהלת ולא מבוזרת (מבוזרת הכוונה שככל רכיב מנהל את עצמו
אבל תלוי ברכיב אחר)
נשים לב כי בתקשורת קוית כי כל אחד מנהל את עצמו אך התקשרות מועברת בהסכם
בארQUITקטורת 802.11 יש רכיב מרכזי שמנהל וכל השאר עוברים דרכו

ראוטר מנהל נקודת גישה. נקודת הגישה, בין היתר, מאפשרת תקשורת בין עמדות קצה שלא יכולות
لاتקשר בעצמן בגל המרחק

בשלב זה של הקורס, אנחנו עוסקים בנLAN wifi alliance. אנחנו צריכים לדעת שישוב בהםים לבין
GSM הייתה קיימת בתיאוריה אבל לא מתקיים כי אי אפשר לחיב בתשלום כשוואקים בנLAN וко'

שיעור 4:

נעסק במבנה החבילות עצמן:



הידר MAC הוא תחילת ההודעה
הידר LLC מאפשר לדעת איזה חבילה חבוייה בפנים
הידר IP מאפשר לגעת איזה IP או איזה גרסה IP (4 או 6) וכו'
הידר TCP
הידר החומר

הסביר על LLC: שכבת המשנה של LLC מספקת מגוון ריבוי המאפשרים למספר פרוטוקולי רשת (למשל IPX, IP, DECnet ו-IPX) להתקיים במקביל בתוך רשת מרובת נקודות ולהיות מועברים על אותן מדיהם רשת. הוא יכול גם לספק מגוון ניהול שגיאות של בקרת זרימה ומנגנון ניהול שגיאות של בקשה חוזרת אוטומטית (ARQ).

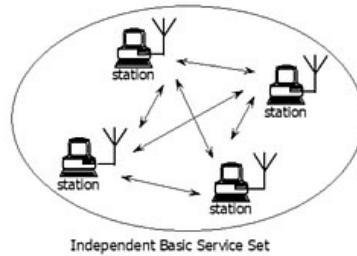
מטרת חבילת Beacon היא לידע שקיימת רשת [חביבה כזו היא Management (מודגדר בرمמת MAC)] וכל אחד יכול ליצור אותה (גם למטרות לא טובות כמו Evil Twin)

BSS היא סט שירותי בסיסיים (מקומיים) הניתנים ע"י נקודת AP
ESS היא סט שירותי מורחב, כמו AP מאפשר גישה לשאר האינטראנט

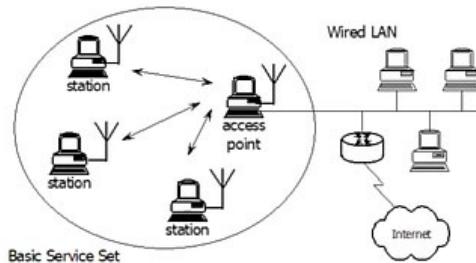
בגדול AP מיצרת Distribution System שאפשר לקטול כב BSS או ESS שזה בעצם רעיון של מתן שירות לקוחות של רכיבים

אצלנו הקופסה של הראטור מכילה מגוון שירותי, היא גם AP וגם רואטור וגם פורטל וגם מספקת שירותי אבטחה ועוד

- ארכיטקטורת 802.11 (אלו בעצם מודים של הרכבים רשות ברמת התקן):
- Peer-To-Peer, מספק תקשורת לوكלית, מאפשר Authentication וגם Ad hoc mode •
 - (בפועל לא משתמשים באחרונים) Registration



In Infrastructure Mode: מאפשר forwarding לתקשורת קוית, מאפשר ESS, בדר"כ מי שנמצא במצב **AP** הוא Infrastructure (כי מצב זה מאפשר לו תקשורת עם נקודות קצה אחרות ויכול לעשות Authentication וגם [בשביל לקשר Registration] (associate) בין לעמודות קצה) ויכול לעשות forwarding לתקשורת קוית)



גם אם אנו נמצאים במצב Infrastructure אז נדרש עוד רכיבים המאפשרים התמודדות עם דברים שאנו מוצפים לקבל ברשות בין היתר, הרכיבים: (רכיבים אלו מייצרים את BSS או ESS)

- Distribution of messages within a DS, מאפשר לדעת מי שלח למי ולשלוח את זה להלאה
- Transition typed based on mobility, מאפשר לדעת אם מעבירים לרשות נוספת או לאינטרנט. ככלומר, היכולת לעבור בין DS (BSS או ESS או BSS אחר)
- Association related services, מאפשר לדעת אם מישחו חבר ברשות הזאת.
- Disassociation או Reassociation. עוזר להתחבר במהירות ולהתנתק כי אנו רוצים מצד אחד להיות תמיד בהזנה אבל גם לא לבזבז אנרגיה.
- Authentication, Access and privacy services או Deauthentication
- Privacy. ככלומר, אנו יודעים מי אתה ואנו רק מאבטחים אותו.

יכול לזכור מצב שעברנו את שלב ההתחנה Association אך לא את ההסכמה Authentication ואז אנו יכולים להיות מחוברים ולקבל שירותים מהרשת אבל לא לקרוא הודעה כי הם מוצפנות. מצד שני, מצב זה יכול להיות מספיק בשביל לפזר את WEP.

IEEE 802.11 Medium Access Control (MAC), הוא שימוש בmedium אחר וכן זה אומר שהוא פגיע (ולא מוגן יותר כמו כבל חשמל) וכן אנו בודקים בעזרת גישות שונות שיש גישה ואבטחה ושנעברת המידע תעשה בצורה מהימנה

Reliable Data Delivery, מאפשר לשולח את המידע בצורה מהימנה, לדוגמה אם יש חפיפת בין כמה AP אז צריך להגדיר לכלום שימושו הולך לשדר [כי אם לדוגמה יש לנו 3 תחנות מסרה אחת אחרי השניה כך שככל אחת שומעת רק את הסמוכה לה, אז אם התחנה הראשונה תרצה לשולח הודעה לתחנה השניה יכול לקרטות מצב שהשניה לא תוכל לשימוש כי השלישי גם משדרת (כלומר, השניה מנסה לשולח את גם לראשונה וזה יש רעש) והתחנה הראשונה לא יודעת את זה. זה נקרא **hidden terminal** [CTS / RTS / CTS / RTS]. כל זה ברמה פיזיקלית יכול לקרטות מצב של retransmit גם אם משתמשים בCDPS (בתקן 802.11)

Access control, אלו טכניקות ניהול

Medium access control, מתקבע כאשר אין RTS / CTS ואנו צריכים לנהל את עצמנו

(הסביר למטה)

-
-
-

מצב מוניטור מאפשר לשמעו איזה חבילות שנרצה גם אם לא מופנות אליוינו, ולכתוב איזה חבילות שנרצה (זה נקרא *passive sniffing*).

הדרך בה מקבלים את המידע:

1. מקבלים מסר בינהרי (מידע ספרי)
2. הופכים אותו למידע באמצעות carrier signal preamble
3. כמה זמן שנוו משדרים את signal משמש אותנו כ
4. משדרים את האות עם המידע

האות עם המידע היא המידע הספרתי

есאנו רוצים לקבל מידע אנו שלוחים Probe request והתשובה מהAP היא חבילת Probe response (מחזר מידע, לדוגמה את SSID) החבילות הנ"ל הינם פרוטוקול של services

Probe response דומה לBeacon, כולל מידע על יכולת, מידע אימות וכו'. ההבדל הוא שbeacon נשלחת לעיתים קרובות ותגובה Probe response רק בתגובה.

אם נרצה להתחזות ל_AP נוכל בעצם לשולח Beacon

תחת 802.11 ישנו 3 סוגי מסגרות:
Management .1
Data .2
Control .3

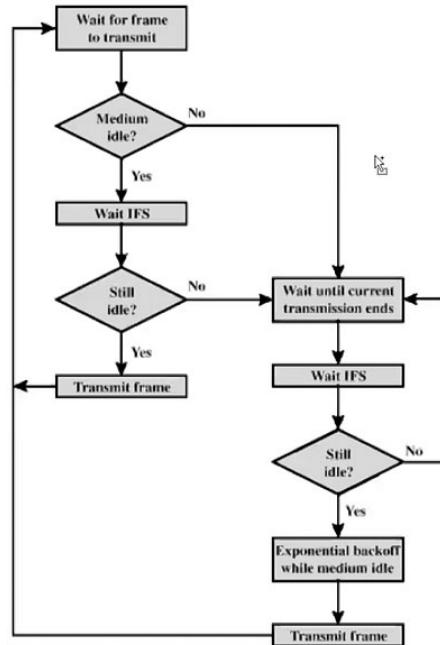
בשני הביטים הראשונים של הודעה תמיד יהיה כתוב מה הסוג ומה התת סוג להלן, חלק מהטבלה:

| Type Value B3..B2 | Type Description | Subtype Value B7 .. B4 | Subtype Description |
|----------------------|------------------|---------------------------|------------------------|
| 00 | Management | 0000 | Association Request |
| 00 | Management | 0001 | Association Response |
| 00 | Management | 0010 | Reassociation Request |
| 00 | Management | 0011 | Reassociation Response |
| 00 | Management | 0100 | Probe Request |
| 00 | Management | 0101 | Probe Response |
| 00 | Management | 0110 | Timing Advertisement |
| 00 | Management | 0111 | Reserved |
| 00 | Management | 1000 | Beacon |
| .. | .. | .. | .. |

מקור: https://en.wikipedia.org/wiki/802.11_Frame_Types#Types_and_SubTypes

(Medium Access Control Logic: ניהול התקשרות)

בסולולר יש מקור ניהול אחד בערוץ 802.11 wifi כל אחד מנהל את עצמו, אך, מי שעומד בתקן תמיד ייכה בין השילוחות ליעומת זאת, ב-802.11 wifi כל אחד מנהל את עצמו, אך, מי שעומד בתקן תמיד ייכה בין השילוחות של ההודעות כפי שניתן לראות בתמונה:



כאשר זיפזוף הוא הזמן שהתוור פנוי וכאשרIFS היא ייחdet המתנה מסוימת (פרוסת אוויר) ישן כמה ייחדות המתנה DIFS, PIFS, SIFS, כאשר האחרונה הקצרה ביותר ומשמשת כאשר עוסקים בהודעות עם עדיפות גבוהה ואז כשהתוור פנוי נחכה פחות זמן וכן נכיסים לשידור ראשונים.

גם ל-AP יש קידימות מבחינתIFS כמו לדוגמה אם מדובר בחסויוןAssociation שהוא סוג Management

לפעמים זה בלתי נמנע ובגלל זה קורה מצב בו יש קושי ל-4 אנשים לראות יוטיב בו זמינות אם עושים זאת ברשומות פשוטות כמו 2.4, כי ככל רוצים להשתמש באותו תווור.

נשים לב כי אם משתמש במכשיר שהוא אינו תחת התקן אז נוכל באמצעות חישום תקשורת כי אנו לא מתחשבים באחרים

שיעור 5:

:Subnetwork
כשמדובר בכתבאות לרשותות, אין מספר הכתובות מוחולקות כך שיישם טווים שמייעדים לרשותות/חוויות שונות, וכך בעצם מגדרים קבוצות של מחשבים בצורה לוגית לדוגמה, ב4קן נוכל להגדיר 256 קבוצות בצורה פשוטה (ב6קן נקבל יותר קבוצות ולזה משתמשים ב-BSS

הגדירות בנוגע לחבריות:

- TX הוא transmitter (שלוח)
- RX הוא receiver (מקבל)

כשנעביר חברות תחת כמה תחנות מסמר אז האז, אך משתנים אבל החסונים קבועים

תחת 802.11 כל מסגרת (frame) שאנו נשלח נصفה לקבל ack

כאשר נתקיים בעיות אז הרכיב עובר לשדר במודולציה נמוכה (כמו 1.2 מגה בית פר שנייה)
וכשמשדרים במודולציה נמוכה אז תופסים יותר זמן אויר זהה נקרא avalanche rate
הפתרון הוא שליחת ack על מנת לדעת מתי לבצע שליחה חוזרת

עד כאן למדנו את ניהול התווך האלחוטי (הSDS בצורה שתהיה אמינה)

:Mac Frame Format

אינו שיר ספציפית ל-802.11 אלא מגעEthernet (שהוא תקן 802.3)

| | |
|------------------|---|
| Frame Control | Control flags |
| Duration/ID | Timing control |
| Addresses | Various MAC entities |
| Sequence Control | Sequence/Fragment number for error/flow control |
| Frame Body | 0 or more data bytes (SDU) |

| | | | | | | | | |
|---------------|-----------------|-----------|-----------|-----------|---------------------|-----------|--------------|---------|
| Frame Control | Duration/ ID | Address 1 | Address 2 | Address 3 | Sequence Control | Address 4 | Frame Body | FCS |
| 2 bytes | 2 bytes | 6 bytes | 6 bytes | 6 bytes | 2 bytes | 6 bytes | 0-2312 bytes | 4 bytes |

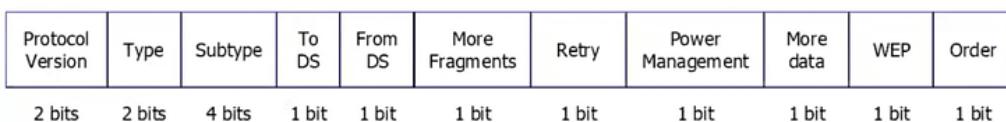
רק שכן ב-802.11 מה שעשו להשתנות הוא המשמעות של הדברים
 נשים לב כי כתוב בשדה השני Duration או ID כי זה תלוי בסוג החברה

- נשים לב כי כתוב בשדה השני Duration או ID כי זה תלוי בסוג החברה
 - receiver: Address 1
 - (transmitter: Address 2
 - destination: Address 3
 - source: Address 4

ובמקרה של Ethernet אין את ערכי "שלוח" ו"מקבל" כי יש Layer אחר עבורם שנקרו ע"י הסוויצ'

כasher מוגדר בצורה הבאה:

| | | | | | | | | | | |
|------------------|---|--|--|--|--|--|--|--|--|--|
| Type and Subtype | Data, Control, Management with subtypes | | | | | | | | | |
| To DS/From DS | Access Point (AP) is destination/source | | | | | | | | | |
| More Fragments | Part of fragmented LLC packet | | | | | | | | | |
| Retry | Indicates re-transmission of bad packet | | | | | | | | | |
| Power Management | STA alerts AP of its mode Value of 1 STA will be in power-save mode Value of 0 STA will be in active mode | | | | | | | | | |
| More Data | AP alerts STA (in power-save mode) of buffered frames | | | | | | | | | |
| WEP | Indicates WEP encrypted data | | | | | | | | | |
| Order | Indicates Strictly Ordered service class | | | | | | | | | |



כasher, אם נשלח מ_AP איז שני הפלגים יהיה 1 (From DS וגם To DS)

:Control Frame Subtypes
כפי שהזכרנו לעיל את RTS / CTS, הם תת-סוגים והם שייכים לסוג Control
גם ack הוא תת-סוג ושיך לסוג Control

Power save – poll (PS-Poll)

Request to send (RTS)

Clear to send (CTS)

Acknowledgment

Contention-free (CF)-end

CF-end + CF-ack

הסוגים מצויים בתוך ה-FC (Frame Control) כפי שנראה בתמונות למטה

עד כאן הבנו באופן כללי את החבילות
מכאן והלאה נלמד איך נוצרת רשות ואיך מקבלים שירות רשות

בשביל להבין איך נוצרת רשות נעבור לשכבה ה-link

תמיד נצטרך תאמיות לאחר עبور תקנים קודמים גם ברמת link כדי שיתאים גם ל-Ethernet שהוא 802.3

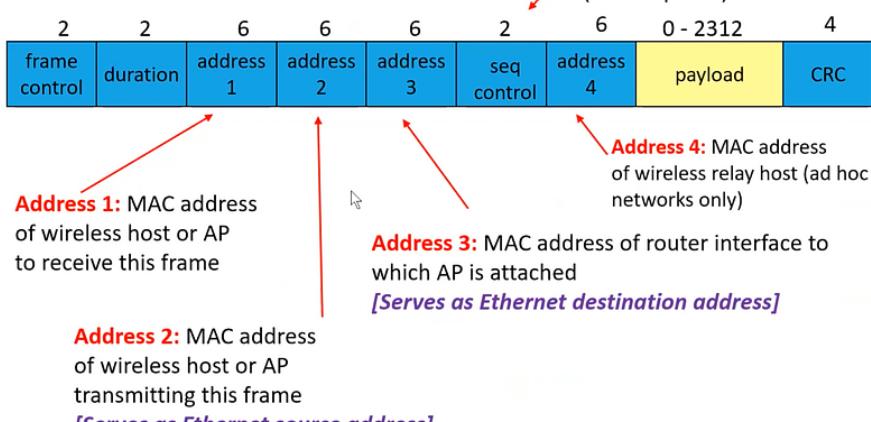
:WEP

בנוגע לmac frame איז אם נבייט ethernet נקבל את המבנה:

| Layer | Preamble | Start frame delimiter | MAC destination | MAC source | 802.1Q tag (optional) | Ethertype (Ethernet II) or length (IEEE 802.3) | Payload | Frame check sequence (32-bit CRC) | Interpacket gap |
|-------------------------------|--------------------|-----------------------|--------------------|------------|-----------------------|--|----------------|-----------------------------------|-----------------|
| | 7 octets | 1 octet | 6 octets | 6 octets | (4 octets) | 2 octets | 46-1500 octets | 4 octets | 12 octets |
| Layer 2 Ethernet frame | | | ↔ 64–1522 octets ↔ | | | | | | |
| Layer 1 Ethernet packet & IPG | ↔ 72–1530 octets ↔ | | | | | ↔ 12 octets ↔ | | | |

אר כshedobar ב11.802 המבנה הינו:

Sequence No.: needed for ARQ (ACK required) mode.



לומר, ב ethernet אין שימוש ב sender, transmitter כי מדובר בראשת חוטית שבה כלם מחוברים לאוטו מוקם ואז לא צריך לציין למי משדרים. לעומת ethernet בtoken:

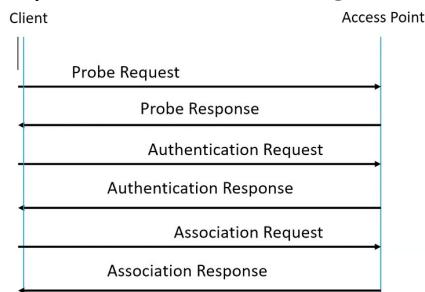
(destination) הוא היעד Address 2
(source) הוא המקור Address 3

לעומת זאת, ב-802.11

(receiver) הוא המקלט Address 1
(transmitter) הוא השולח Address 2
(destination) הוא היעד Address 3

משמש אותנו בתור BSSID או דברים אחרים שהם עוד כתובות Address 4

תהליך ההתחברות לרשת: (באמצעות active sniffing שמבצע הלוקה [cano, ע' בקשת probe])



1. ליקוי מחפש את כל APs בטוח הרדיו שלו שמתאים לקצב-תעבורה של - Shallow. probe req.
 2. כל ה-APs שעונים לדרישות עננים. -> probe res. יש מידע סינכרון והעומס על ה-AP וה-SSID שלו.
 3. הליקוי בוחר איזה AP המכמתים לו. (לפי קצב התעבורה והעומס) ומאמת עצמו לו.
 4. AP reply auth reply
 5. כחוט אינטואיטיבי, הליקוי שולח בקשה קישור (association req.)
 6. AP reply association reply

לאחר הקישור, הליקוי יכול להעביר תקשורת ל-AP.

זכור כי לכל חבילה מהשיטה הנ"ל יש אפקט

זכור כי יש חמישה מצבים למתאים הרשות:

1. Infrastructure
2. Ad hoc
3. Management
4. Monitor
- 5.

SSID הוא שם מזווה של הרשות וה**מקום היחידי** שמויע השם של הרשות הוא בחבילת Beacon
BSSID הוא כתובות המק המיצגת את הרשות

בדרכ'ן על מנת לזהות רשותות נקשר ל**Beacons** אבל Apple שולחת תמיד probe requests

Association אומר שאנו שיכים ל_AP מסויים ואז לאחר Association נוכל לקבל שירות רשות. אם עברנו את שלב ה-Association אז זה אפשרי לחבר פיזי ברשת חוטית לאחר מכן יישו 3 שיטות:

1. Open authentication (standard)

2. Shared Key authentication (standard)

3. MAC address authentication (commonly used)

שהגדכנו מראש. זו בעיה כי נוכל להתחזות. נשים לב כי אין שום הצפנה על כתובות MAC.

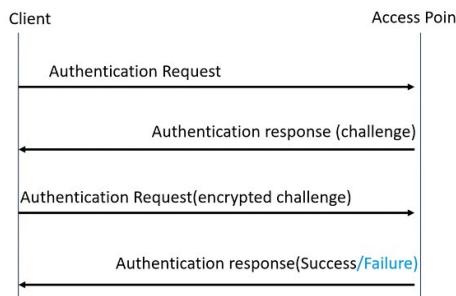
נוכל אפילו לדעת איזה MAC עבר את שלב האימות ע"י ההידר (ההידר לא מוצפן) שבו כתוב

את הסוג וההת סוג ולפי זה נסיק אם עבר את שלב האימות]

באותה Frame Control כתוב לנו האם קיימ WEP ונדרש אתגר או שלא. זה כתוב בBeacon וגם בProbe Response

Shared Key Authentication

Requires that the client configures a static WEP key



נשים לב כי AP שולח את האתגר, הלקוח עונה לאתגר בצורה מוצפנת, ואז מקבלים מענה אם הצלח או לא.

האתגר לא היה עניין של האם לחבר או לא, אלא האתגר היה עניין של הצפנה וזאת הסיבה שWEPA לא בדיק עובד.

מה שלא עבד בWEPA זה שהביסוס שלו זה נתו הצפנה, ושלב הAssociation הוא משני וכתוצאה לכך אנחנו עדיין יכולים לקבל שירותים אבל לא לקרוא Data. כלומר, אנו מוצפינים אבל לא בודקים עוד דברים כמו לדוגמה, אם החבילות הם לפי סדר.

==== מסגרות 802.11 ===

נראה דוגמאות מסווגי Control ו-Management (ולא סוג Data):
מסגרות Management:

מסגרות ניהול מאפשרות תחזקה, או הפסקה, של תקשורת. נראה כמו תת-סוגים נפרדים:

- מסגרת Authentication: אימומות 802.11 מתחילה בכך שהכרטיסים רשות שולח מסגרת אימות לנקודת הגישה את זהותה (והתשובה היא בהתאם לאחד משלושת השלבים שמוצגים בסעיף 5 [כמו לדוגמה, תשובה ע"י אטגר]).
- מסגרת Association: נשלחת מתחנה, היא מאפשרת לנקודת הגישה להקצות Mbps ו-SSID של הרשת שאליה התמונה רוצה לשער. אם הבקשה מתקבלת, נקודת הגישה שומרת זיכרון ומקיים מזהה שיור עבור הcrcטיס רשות (נקרא WNIC).
- מסגרת Tagging Association: נשלח מנוקודת גישה לתמונה המכילה את הקבלה או הדחיה לביקשת שיור. אם מדובר בקבלת, המסגרת תכיל מידע כגון מזהה שיור וקצבית נתונים נתמכים.
- מסגרת Beacon: נשלח מעת לעת מנוקודת גישה כדי להכריז על נוכחותה ולספק את ה-SSID, ופרמטרים אחרים עבור WNIC בטוויה.
- מסגרת Deauthentication: נשלח מתחנה המעוניינת לסיים חיבור מתחנה אחרת.
- מסגרת Disassociation: נשלח מתחנה המעוניינת לסיים את החיבור. זהה דרך אלגנטית לאפשר לנקודת הגישה לוותר על הקצאת זיכרון ולהסיר את ה-WNIC מטבלת השיר.
- מסגרת Probe request: נשלח מנוקודת גישה המכילה מידע על יכולת, קצבית נתונים נתמכים וכו', לאחר קבלת מסגרת Probe request.
- מסגרת Reassociation: WNIC שלוח בבקשת שיור מחדש מחדש כאשר הוא נופל מטווח נקודות הגישה המשויכות כתע ומוסץ נקודת גישה אחרת עם אותן זכירות. נקודת הגישה החדשת מתאמת את העברת כל מידע שעדיין עשוי להיות כולל במאגר של נקודת הגישה הקודמת.
- מסגרת Tagging Reassociation: נשלחה מנוקודת גישה המכילה את הקבלה או הדחיה לביקשה לשער מחדש מחדש של WNIC. המסגרת כוללת מידע הנדרש לשער כגון מזהה השיר וקצבית נתונים נתמכים.
- מסגרת Action: הרחבת מסגרת ניהול לשיליטה בפעולה מסוימת. חלק מקטגוריות הפעולה הן Block Ack, Radio Measurement, Fast BSS Transition, RTS, Radio Measurement, וכו'. פרימרים אלו נשלחים על ידי תחנה כאשר היא צריכה לומר לעמידה כדי לבצע פעולה מסוימת. לדוגמה, תחנה יכולה לומר לתמונה אחרת להגדיר אישור חסימה על ידי שליחת מסגרת פעולה "ADDBA". התמונה השנייה תגיב עם מסגרת פעולה "ADDBA Response".

מסגרות Control:

מסגרות בקרה מקלות על חילופי מסגרות נתונים בין תחנות. כמו מסגרות בקרה נפרדות:

- מסגרת אישור (ACK): לאחר קבלת מסגרת נתונים, התמונה מקבלת תשליך מסגרת ACK בתוך תחנת השולחת אם נמצא שגיאות. אם התמונה השולחת לא קיבל מסגרת ACK בתוך פרק זמן שנקבע מראש, התמונה השולחת תשליך מחדש את המסגרת.
- מסגרת בקשה לשיליחה (RTS): מסגרות RTS ו-CTS מספקות תכנית הפתחת התגובה אופציונלית עבור נקודת גישה עם תחנות סטרכות. תחנה שולחת מסגרת RTS כשלב ראשוני בלחיצת יד זו כיוונית הנדרשת לפני שליחת מסגרות נתונים.
- מסגרת Clear to send (CTS): תחנה מגיבה למסגרת RTS עם מסגרת CTS. הוא מספק אישור לתמונה המבקשת לשולח מסגרת נתונים. ה-CTS מספק ניהול בקרה התגובה על-ידי הכללת ערך זמן שעבורו כל שאר התחנות אמורים לעמוד לידור בזמן שהתחנה המבקשת משדרת.

מקור: https://en.wikipedia.org/wiki/IEEE_802.11#Management_frames

מתקפת Deauthentication היא מתקפה בו שלוחים בפשטות חבילה המכריזה על ניתוק מתקפת Probe request שלוחת מלא הודעות בקשה Probe עד **להשbetaה של הקורבן**

hostapd זו בעצם התוכנה שנותנת את כל השירותים (service set) וגם את האינטראנט

בשביל לדעת שאנו אכנ passive sniffing אז נזכה לראות Wireshark **חבילות Data מוצפנות**. גם אם רואים ack זה אומר שאנו תחת passive sniffing (כלומר, במצב מוניטור) כי לא אמורים לראות אותן.

שיעור 6:

כשנרצה לפרוץ רשות אלחוטית תמיד נדרש להיות בסביבה שלה. ההגנה הינה מתוגרת יותר כי אנו צריכים להגן על רשות ניידת.

אנו נראה בהמשך (כשנדבר על WPA) שבWPA משתמשים בין היתר בCCMP שמעיד על הצפנה אם מופיע בחיבור (מהרCCMP ומטה [כלומר, שכבת הNetwork וה-Transportation וכו']). איןום קריאים כי הם כבר מוצפנים באמצעות CCMP. בפרט, לא יוכל לראות את IP'ם כי ה-Network מוצפן) לעומת זאת, בWEП אין CCMP אלא יש ווקטורים כפי שנראה גם בהמשך.

משמעות מצב מוניטור היא שיש אפשרות לבצע sniffing active ו גם sniffing passive . בשורה התחתונה, על מנת לבדוק שאנו תחת sniffing active נרצה לחפש חבילות מוצפנות. על מנת לבדוק שאנו תחת sniffing active יוכל לכתוב קוד עם scapy שמייצר ושולח חבילות ואז לנסוט להבין אותם, או שנוכל להקשיב לחבילות אחרות ולשם כך צריך כמה כרטיסי רשות.

בDemo של Scapy ניתן לראות איך החבילות בנויות ולהזות איר Scapy עובד.

קישור: <https://scapy.readthedocs.io/en/latest/introduction.html#probe-once-interpret-many>

בסוף, יש צורך לדעת את הLayers בScapy לדעת מהו השדה Dot11MacFields ולמה זה עובד

| Scapy 802.11 Layers | Dot11 Layer Fields / Default Values |
|---|--|
| <pre>>>> ls() Dot11 : 802.11 Dot11ATIM : 802.11 ATIM Dot11AssoReq : 802.11 Association Request Dot11AssoResp: 802.11 Association Response Dot11Auth : 802.11 Authentication Dot11Beacon : 802.11 Beacon Dot11Deauth : 802.11 Deauthentication Dot11Disas : 802.11 Disassociation Dot11Elt : 802.11 Information Element Dot11ProbeReq: 802.11 Probe Request Dot11ProbeResp: 802.11 Probe Response Dot11QoS : 802.11 QoS Dot11ReassoReq: 802.11 Reassociation Request Dot11ReassoResp: 802.11 Reassociation Response Dot11WEP : 802.11 WEP packet RadioTap : RadioTap dummy</pre> | <pre>>>> ls(Dot11) Field Type Default Value ----- subtype : BitField = (0) type : BitEnumField = (0) proto : BitField = (0) FCfield : FlagsField = (0) ID : ShortField = (0) addr1 : MACField = ('00:00:00:00:00:00') addr2 : Dot11Addr2MACField = ('00:00:00:00:00:00') addr3 : Dot11Addr3MACField = ('00:00:00:00:00:00') SC : Dot11SCField = (0) addr4 : Dot11Addr4MACField = ('00:00:00:00:00:00')</pre> |

קישור: <https://scapy.readthedocs.io/en/latest/api/scapy.layers.dot11.html>

על מנת לבדוק אם חיבור ה-802.11 איז נבדק אם הוא קיים אבל לא ע"י שדות ספציפיים של Scapy כי שדות שונים של Scapy וכרטיסי רשות שונים נתונים תוצאות שונות.

בחזרה לWEП:

ראינו שכל הנראות של רשות וכל השימושים השונים שאנו עושים תלויות בשכבה שיש לנו על שכבת Network וה-Transportation וזה בעצם השכבה של 802.11.

ראינו מה 802.11 Frame מכיל (את ה-Frame Control בתחילת הheader וכל השאר) ואיך הם משתנים בהתאם לתפקידו שאנו רוצים לעשות וכך נדע איך לפענה את המידע כי לכל חיבור יכול להיות מבנה אחר

איך מבצעים את ה-"אגטגר" של Authentication מתחת WEП:
נרצה להשתמש בהצפנה בשבייל לתקוף הצפנה צריך לתקוף את Privacy (ולא Authentication שמאפשרת לדעת שאתה מי אתה)

אנו נרצה לחתת מפתח כי יתכן שתהיה לנו קבוצת משתמשים גדולות. מצד שני זה די פרוץ שזה אותו מפתח. כמו כן, נרצה שהוא רנדומלי כדי "למנוע" ניחושים.
נרצה לעשות Authentication למשתמש ואז להצפן. (ברשת פתוחה יש Authentication וזהו).

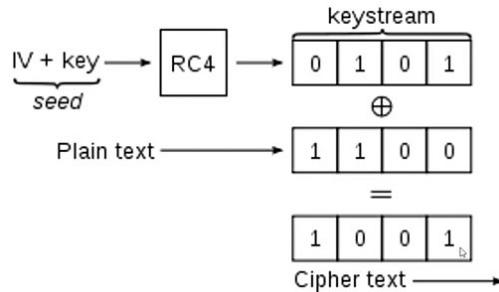
בזמן שהWEП היה מוגדרת, הייתה גישה של הצפנה ד' חכמה שנקראת RC4 והוא בסיס של הרבה גישות הצפנה, אך הדרך שהשתמשו בה לא הייתה ממש טובה.

הרעין ההגיוני הוא לקחת מספר רנדומלי ואת המפתח עצמו וליצור פונ' Hash. קר AP ישלח את המספר הרנדומלי והלקוק ייצור את Hash עם המפתח שיש ברשותו ויחזיר לAP את Hash לצורך אימות. (ככה בעצם נמנע Replay Attack בין היתר). במקרה זה AP ידע שהלקוק הוא מי שהוא, אך הלקוק לא יודע אם AP הוא מי שהוא.

שוב.. הרעיון לא רע אך המימוש הוא הבעייתי. בעצם זה שמצפינים את payload עצמו ולא את כל השאר זה בעייתי

איך זה בעצם מתבצע:

| | | |
|---|--|--|
| <p>Message הוא הודעה עצמה נועד לבדיקת לוודא את integrity (יושרה) של Message</p> <p>Message + CRC הוא Plaintext</p> <p>או וקטור האתחול 24bit והוא רכיב רנדומלי התחלתי שאיתו מתחילהים לעבוד (יש לו 2 שימושים כפי שנראה)</p> <p>Key הוא באורך 40bit או אחרי הרחבה באורך 104bit, והוא המפתח המצורף לו</p> <p>Keystream הוא קומבינציה מסוימת של IV וה-Key</p> <p>שנoused להצפין את Plaintext כiphertext</p> <p>Ciphertext הוא התוצאה הסופית שאותה שלוחים</p> | <ul style="list-style-type: none"> • • • • • • • • | |
|---|--|--|



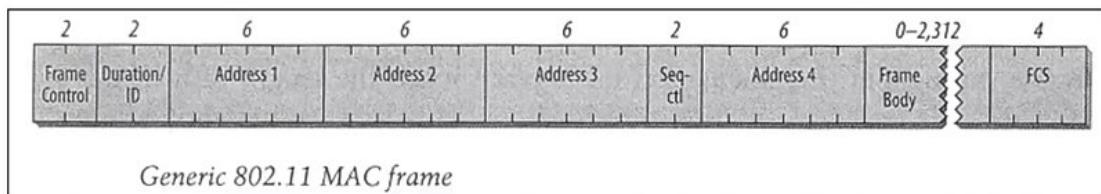
בפועל ניתן לנקוט במסלול אחד: RC4 שמאפשר להפעיל על מחזורת 64bit או (128bit) מיצרים איזהキー (key), keystream מיצרים איזהseed (seed), לאחר מכן עושים XOR עם plaintext וכך נקבל את התוצאה הסופית (Ciphertext). בסוף נצמיד את IV לתוצאה הסופית.



(נזכיר כי אנו נמצאים בתפר בין Network Layer ל-Data Link Layer ולכן כל מה שב-Network והלאה הוא מוצפן וכך בין היתר הIP גם מוצפן)

אנו נראה שלפי שיטה זו כל הצפנה של חבילה היא בפני עצמה וכן בשבייל לנסות לעונח אותה לא צריך באמת לדעת מה היה לפני ומה אחריו

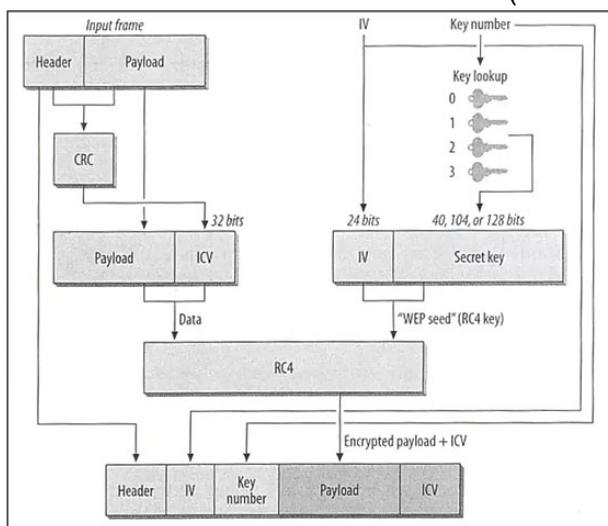
נשים לב כי הגודל של IV הוא 2^{24} ואלו כמות המפתחות הצפנה שאנו יכולים להשתמש בהם ככלומר, 2^{24} . Keystreams.



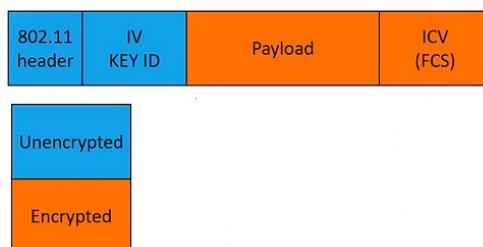
בחלק של ה-Frame Body נכנסת הרצפנה

איפה נמצאת הבעה:
הרצפנה הזאת היא פשוטה כי פועלת XOR פשוטה, ופה בדיק נמצאת הבעה כיוון שנוכל לחת את ה-IV וויסמה שניחסנו אז לבצע XOR להודעה ולאמת את התוצאה עם CRC

תהליך הרצפנה עצמו (בתרשים):



ה-Header לא מוצפן רק ה-Payload וה-ICV (נקרא CAN ICV) מוצפנים
בנוסף לכך, ה-IV קוצר מידי והוא-CRC (Checksum) פשוט מדי [זה-Header מידי] וזה-Header נוצר ה-CRC **חשוף**
מכאן אם המידע שחרס לנו הוא קוצר אז נוכל להשלים אותו
(נקודה נוספת: האורכים של הרכיבים שעושים בניהם XOR אינם בהכרח שוים ולכן משתמשים באופן
מחזרי ברכיב של המפתח)



וכאן התחלנו לראות את הפגיעות של ה-WEP

שיעור 7:

חזרה על השיעור הקודם בעיקר ומבנה החבילות ב-WiFi, לדוגמה, עבור Beacon:

```
> Frame 1: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface wlx6c5ab03ad5c0, id 0
> Radiotap Header v0, Length 26
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....
> IEEE 802.11 Wireless Management
```

הזכיר כי בSeanior Virtual Machine לא בהכרח נראה את כל החבילות, ובעצמן, גם כשנעשה Packet Injection יבודג גם אם זה כתוב שכן

קוד שראינו בשיעור המשמש להסנהה: (הסנהה של רשות אלחוטיות שקיימות בסביבה)

```
1 #!/usr/bin/env python
2
3 from scapy.all import Dot11, sniff
4
5
6 ap_list = []
7
8 def PacketHandler(packet):
9     if packet.haslayer(Dot11):
10        if packet.type == 0 and packet.subtype == 8:
11            if packet.addr2 not in ap_list:
12                ap_list.append(packet.addr2)
13                print("Access Point MAC: %s with SSID: %s" %(packet.addr2, packet.info))
14
15
16 sniff(iface="wlp2s0", prn = PacketHandler)
```

הקוד בודק אם קיימת שכבה Dot11 (רלוונטי אליו) ואז בודק אם הסוג הוא 00 (Management) וההת סוג הוא 8 (כלומר, 1000 ביביארי) זהה אומר חבילת Beacon. במידה וכן הוא שומר את ה-Transmitter שנמצא תחת addr2 (802.11).

אפשר גם להשתמש ב-sniff של Scapy

```
>>> sniff(iface="wlx6c5ab03ad5c0", count=1)
<Sniffed: TCP:0 UDP:0 ICMP:0 Other:1>
>>>
```

[קרנו לפונ' עם flag של count=1 (כלומר, אנו רוצים להסניף רק רשות אחת)].

שים לב כי כתוב שלא מדובר בכלל ב-TCP/UDP/ICMP, וזאת בגלל שלושת אלו [בפרט] נמצאות בשכבות שאחרי ה-Network Manager, ובגלל שאנו נמצאים בתפר בין Data Link Layer ל-Network Layer לא מכך והלא הכל מוצפן [בדרכ' הרשותות מוצפנות] וכן אין לו אפשרות לדעת לגבי TCP/UDP/ICMP.

כפי שהסבירנו בשיעור הקודם, כשנרצה לדעת אם קיבלנו הודעה Dot11 אז נבודק באופן כללי אם השכבה Dot11 נמצאת בפנים (ע"י Scapy כפי שעשינו לעיל, או אחרת) אבל לא ע"י **שדות ספציפיים** של Scapy כי שדות שונים של Scapy וcrc32 רשות שונים תוצאות שונות.

לא בכל סביבה עבודה מה שנראה לנו עובד (למרות שנראה חבילות), לכן, הדריך הכי טובה לבדוק זאת היא ליצור חבילות ב-Scapy ולראות אותן ב-Scapy ואם משווה לא מצליח אז זה לא עובד.

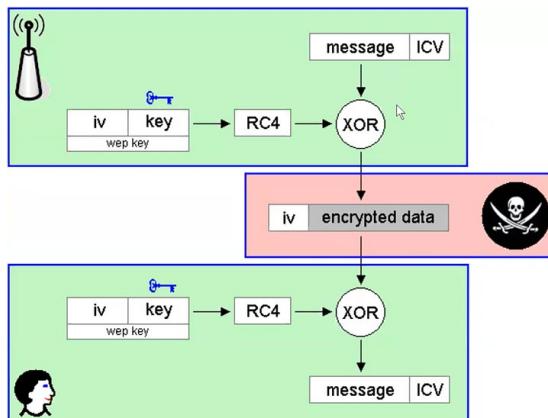
.broadcast נשלחה לכטובת ff:ff:ff:ff:ff:ff אז מדובר בהודעתה
.destination RA=DA הכוונה שהמקבל הוא היעד [option]

```
###[ 802.11 ]###
subtype = Beacon
type   = Management
proto  = 0
FCfield = 1
ID    = 0
addr1 = ff:ff:ff:ff:ff:ff (RA=DA)
addr2 = 64:64:4a:2f:43:fe (TA=SA)
addr3 = 64:64:4a:2f:43:fe (BSSID/STA)
SC    = 28144
```

על מנת לדעת תחת איזה AP נמצאים לkusothot az נחשף את הכתובת של ה-AP תחת שדה receiver transmitter אבל לא תמיד ידוע אם זה באמת **לקוח או DS** (Distribution system), כלומר From DS / To DS שנמצאים תחת שדה Frame Control.

בchnerה ל-WEP (ויאם לפני שנתחיל לדבר על WPA):

תזכורת הצפנה WEP:



ישנו כמה סוג התקפות WEP:

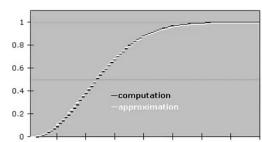
- ההתקפה הכי פשוטה היא ניסיון למצוא את המפתח
- דרך אחרת היא לקבל את המידע מבלי לקבל את המפתח (כלומר, תלויים בתקשורת ולא במפתח)
 - דרך סטטיטית היא גם ללא תקשורת לגיטימית של לקוח עם ה-AP
 - דרך דינאמית היא עם תקשורת עם ה-AP

:The Birthday Paradox
(כמו שובר הינוים)

מה ההסתברות של 2 אנשים מתוך 23 אנשים בחדר יהיה יום הולדת?
מי שהו כבר עשה את החישוב בשביבנו והතשובה היא 50.70%

23 people in a room

How likely that two people share the same birthday?



$$\begin{aligned} p(n) &= 1 \times \left(1 - \frac{1}{365}\right) \times \left(1 - \frac{2}{365}\right) \cdots \left(1 - \frac{n-1}{365}\right) \\ &= \frac{365 \times 364 \cdots (365-n+1)}{365^n} \\ &= \frac{365!}{365^n (365-n)!} \end{aligned}$$

Roughly: $p(n) \approx 1 - e^{-n^2/(2 \times 365)}$,
Answer: 50.7%!

נניח **n** אנשים ו**m** אפשרויות

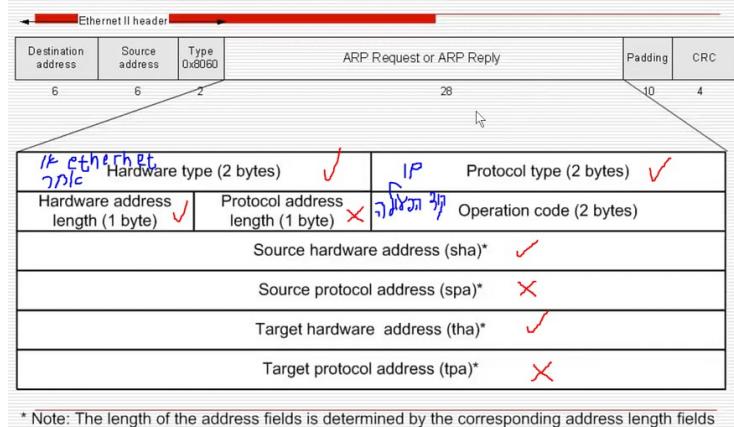
For **m** people and **n** days, the probability is about $1 - e^{-\frac{m^2}{2n}}$

במקרה שלנו (WEП) יש 2^{24} אפשרויות שזה יוצא 16,777,216 מכאן, $M = 16$ והסיכוי להתנגשות לאחר 4,823 פקודות הוא 50%. באופן דומה, הסיכוי להתנגשות לאחר 12,430 פקודות הוא 99% לרשף במהירות 11Mbps יקח 3 שניות!

铭记 כי אם יהיה שימוש חוזר באותו IV אז תהיה יותר פגיעות זאת הסיבה שהגדילו את ה-Key (הצמוד לו)

בקורס תקשורת למדנו על ARP שמחבר אותנו בין כתובת IP לכתובת MAC

ARP Packet Format



כאשר מה שמופיע בו הוא מה שאנחנו יודעים
ומכאן ניתן לראות שם על plaintext יש מספיק מידע כולמר, נותר לנו קצת מידע בשבייל לנוסות
לנחש ואז לבדוק אם הצלחנו לפצח את ההצפנה (בדיקה ה-CRC)

ל-CRC יש בעיה נוספת והיא שהוא לא ינארו, כלומר, גם היא מקבל CRC חדש שהוא לאomi ק הוא
עדין יכול להיות לגיטימי מבחינת ההצפנה ואז יהיה אפשר לפתח אותה ולזרוק אותה (אם ה-CRC
לא באמת נכון) ואם ה-CRC נכון הוא שולח הודעה חזרה

از בתור התחלת, אם אנחנו מקבלים מספיק חבילות של VII אז אנחנו יכוליםגלות מחדש את
המפתח וזאת ההתקפה הכיו פשטota שיש

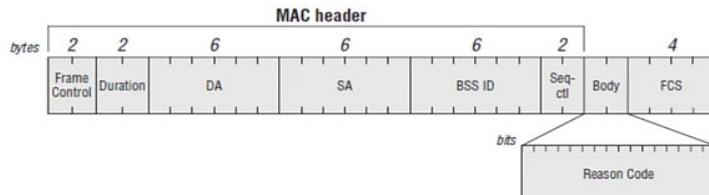
אחרי זה יש לנו גישה נוספת שאומרת שם יש לנו מספיק חבילות אז אנחנו יכולים ביצורה סטטית
לשחזר את המפתח ממש זהה מה שדיברנו עליו

מתבצע על כך שלפעמים שולחים חבילה בחתיות קטנות ואז יש לנו בעצם
שימוש חוזר באותו VII ואז אנחנו יכולים למוד מהצורה בה ה-AP פיצח אותה כשהוא שולח אותה
ל-Host
(MTU הוא גודל שמן והלאה צריך Fragmentation)

שיעור 8:

כפי שהסבירנו, מתקפת Deauthentication היא מתקפה בו שולחים בפשטות חבילה המכריזה על ניתוק. זה קורה כי אין authentication לחבילהnihol (כלומר, אין דרך לדעת שחבילה כזו לגיטימית) ולאחר ניתוק התקשרות בין ה-AP והלקוח מפסיקה והלקוח נחשב זר ונחוסם

כך נראה ההידר של Deauthentication:



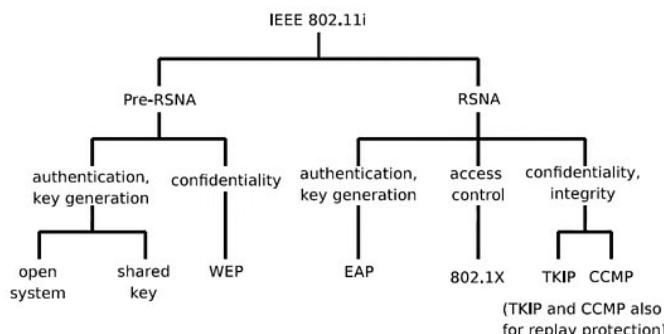
בין היתר, ברור כי $SA=TA$ (השלוח הוא המקור)

יש הרבה Reason Codes כאשר נהוג להשים את 7 Reason.

בדרכ' נשתמש בזה כשרצה לבצע מתקפת Twin Evil. לאחר מכן הקורבן מתישחו יתחבר לרשת המזוייפת שהקמננו (אלא אם כן שעינוי מתקפת Karma ואז הוא אוטומטית יתחבר)

לאחר שראו את החולשה ב-WEP רצוי ליציר שלב ביניים שהוא קונספט מסוים הנקרא RSNA

IEEE 802.11i היא מפת הדרכים שיש לנו אחרי שתתקן יתקבל



כאשר, confidentiality נותנת את החזנה (פרטיות) [נשים לב בכך ימין מיותר integrity (יושרה)] או בקרה הגישה. EAP נותנת יותר וודאות לגבי מי נגד מי. WEP לא היה שימוש ב-Access control (זה היה קיים אבל Wifi Alliance החליטה לא להשתמש בו)

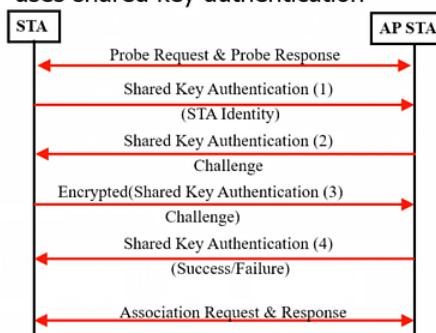
Open system אומרים שאין סיסמה (פחות מעניין אותו)

תקן 802.11w מאפשר לחתול גם לחבילות ניהול תחת validation ו-authentication

תקן 802.11s זה Mesh

תזכורת WEP: (לפני שנעבור לדבר על WPA)

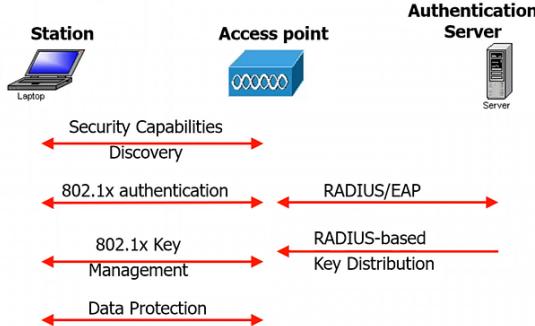
- WEP uses shared key authentication



:WPA

כאמור, ה-WEP פרוץ ולכן Wifi Alliance רצוי לפתח משזה יותר מאובטח במידע מוביל "לשבור את הכלים". لكن הם רק שידרגו את מה שהיא מקודם והთוצרת הוא WPA ב-WPA הוסיף 4-way handshake group key handshake ואלו השינויים המרכזיים (בנוסף לAuthentication)

הAuthentication מתבצעת ע"י radius Eap או Radius הוא עבר enterprise זהה שרת חיצוני (authentication) לאימות. במקרה של שימוש ביתי, אז הרואוטר משתמש גם כשרת ההאינטראציית (authentication)



נרצה לדעת איך מתבצע Eap

Authentication

- Mutual authentication
- The AS and station derive a Master Key (MK)
- A Pairwise Master Key (PMK) is derived from MK
- The AS distributed PMK to the AP
- In PSK authentication, the authentication phase is skipped
 - PMK = PSK

Mutual authentication אומר שגם אני יודע שאתה הסוד וגם אתה יודע שגם יודע את הסוד. וזה מתבצע ע"י בקשת אתגר דו צדדי.

(בWEП-AP שלח ליקוח אתגר והוא היה עונה עליון בצוירה מוצפנת באמצעות הסוד, אך הליקוח לא היה יודע אם ה-AP יודע את הסוד וזה לא טוב כי אפשר להקים AP מזויף שמקבל כל ליקוח [ambil לבדוק שום דבר] והוא אינו יודע שה-AP שהקמננו מזויף)

Master Key הוא קבוע ומשמש לייצור pairing שהם לאו דווקא קבועים

Pairwise Master Key (PMK) נגזר ממה MK ובו משתמשים

ניתן להבין מכאן שיש לנו כמה מפתחות (כיוון שאינם קבועים) ולכן נרצה לנצל את זה התחילה:

- Key management and establishment
 - PMK is sent to AP by AS
 - Key management is performed between AP and the peer – four-way handshake
 - The four-way handshake can also be used for mutual authentication between AP and the peer in PSK mode
 - A set of keys are derived from PMK to protect group key exchange and data
 - Group key exchange allows AP to distribute group key (for multicast) to the peer

את הPMK אנו שלוחים ל-AP ואז מתבצע אתגר דו צדדי בתהליך 4-way handshake לאחר מכן נגזר מהPMK מפתחות המשמשות להצפנה המידע מכאן ולהלאה broadcast/multicast

TKIP (Temporal Key Integrity Protocol) הוא החלק של הפרוטוקול כפוי שנitinן לראות בתמונה של מפת הדרכים למעלה כאשר TKIP מתייחס ל-WPA-1 CCMP מתייחס ל-WPA2.

- Optional IEEE802.11i protocol for data confidentiality and integrity
 - TKIP is designed explicitly for implementation on WEP legacy hardware
- TKIP three new features:
 - A cryptographic message integrity code (MIC)
 - A new IV sequencing discipline
 - The transmitter increments the sequence number with each packet it sends
 - A per-packet key mixing function

היעוד של TKIP הוא עבור חומרות המתאמת ל-WEP.

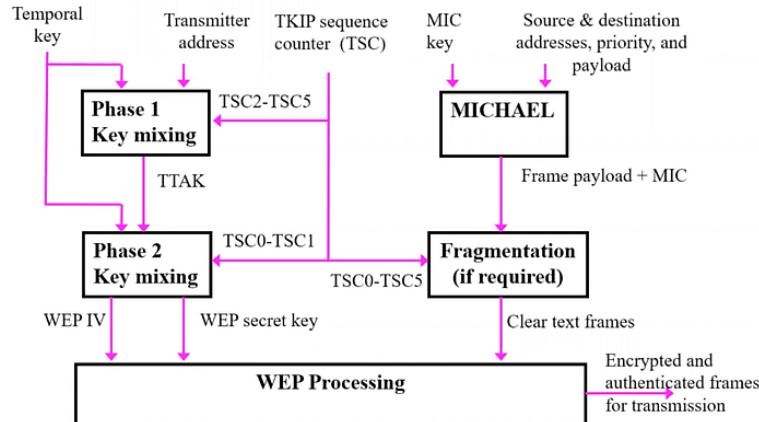
נוסף ב-TKIP 3 תכונות:

1. MIC המאפשר בדיקת הוגה והם נדע באיזה שלב אנו נמצאים (אם זו תגובה או משהו אחר). עם זאת אנו נמנעים מ-m-Reply attack כי לפני זה (ב-WEP) יכלנו לנקח כל IV ו-Payload מוצפן ולשלוח הודעה לגיטימית [זה יתאפשר] אבל כאן יש חשיבות לסדר ולכן לא יתאפשר
2. כאן ה-IV משתנה כי הגודל משתנה וגם הדרך שמשתמשים בו משתנה וגם יש לו sequence .3.

כלומר, ראיינו כבר 2 מכשולים. הראשון זה handshaking 4 והשני הוא MIC.

תהליך TKIP:

■ TKIP frame processing



כאן יש שניים, כי את המפתח שהינו משתמשים בו ב-WEP (לפני שעושים את ה-XOR) אנו מערבלים עם כתובות transmitter ורך לאחר מכן מוסיפים את ה-WEP ואת ה-key-secret key וכאן יש לנו יותר אלמנטים (שמשתנים כי כתובות transmitter-transmitter משתנה) ולכן, המפתח שנוצר עכשו הוא יותר זמני וכל זה מתבצע עם אותה חומרה כמו ב-WEP.

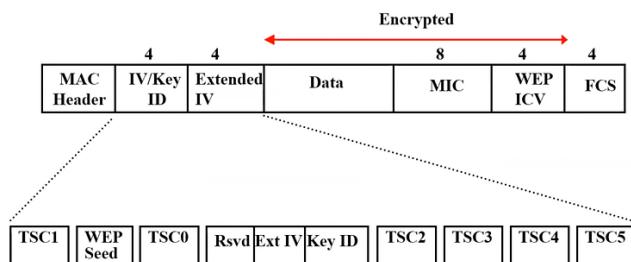
בצד ימין יש עוד תוספת, כשהאנו בונים את החבילה אנחנו לא בונים אותה בפני עצמה אלא מוסיף מפתח שיעזר לדעת אם החבילה אוטנטית או לא ב-WEP הינו שלוחים IV+Payload+WPA+B-A וכאן שלוחים MIC+Payload+IV

(כאן אנו עוסקים בהצפנה עצמה ולא במפתחות, אנו אמנים משתמשים במפתח ה-TKIP Confidentiality-**Replay Attack** [מניעת סודיות])

- Defeating weak key attacks: key mixing
 - Transforms a temporal key and packet sequence number into a per packet key and IV
 - The key mixing function operates in two phases
 - Phase 1: Different keys used by different links
 - Phase 1 needs to be recomputed only once every 2^{16} frames
 - Phase 2: Different WEP key and IV per packet
 - Phases 1 and 2 can be pre-computed
- Defeating replays: IV sequence enforcement
 - TKIP uses the IV field as a packet sequence number
 - The transmitter increments the sequence number with each packet it send
 - A packet will be discarded if it arrives out of order
 - A packet is out-of-order if its IV is the same or smaller than a previous correctly received packet
- Defeating forgeries: New MIC (Michael)
 - MIC key is 64-bits
 - security level of 20 bits

בעזרת MIC נוכל למנוע זיווף חבילת. כאמור, באמצעותו אנו יכולים לבדוק אם החבילת אוטנטית, כמובן, אנו מונעים זיווף כי על מנת ליצור את-h-MIC יש צורך לדעת את-h-Payload עצמו (ראינו שב-Arp זה כמעט מטהאפשר אבל בכלל, שכן יש הגנה מסויימת) וגם צריך לדעת את-h-MIC Key שקשה לנחש אותה כל זה חלק אחד החלק השני הוא אי אפשר להשתמש באותו IV כי הוספנו את-h-sequence

- TKIP encapsulation



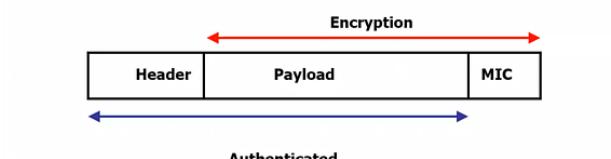
:WPA2

כעת, נתקדם לתקן 802.11i שבו משתמשים ב-CCMP עם מצב CBC-MAC

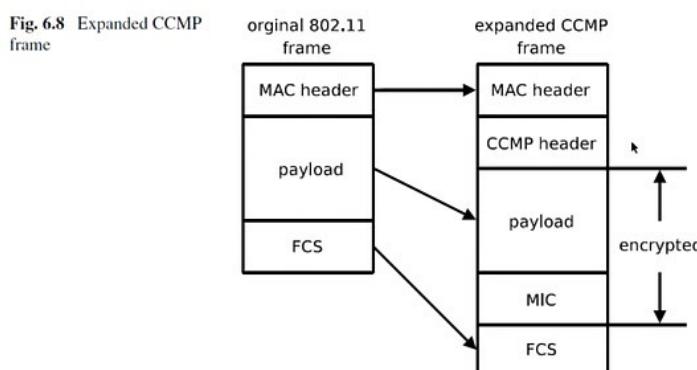
RC4 הוא אלגוריתם הצפנה שעומד ביכולות חומרה מסוימות AES הוא תקן הצפנה וכך משתמשים בו ולא ב-RC4 כמו מקודם

גם כאן משתמשים ב-C-MIC כי זה נותן טביות אבטחה ומונע זיופים

- Both encryption and MIC use AES
 - Uses counter Mode (CTR) to encrypt the payload and MIC
 - Uses CBC-MAC to compute a MIC on the plaintext header and the payload
 - Both encryption and authentication use the same key



כלומר, אלו אותן עקרונות כמו מקודם רק שכן ה-Input Inn של ה-CCMP שונה ניתן לקורט שבאמת המסגרת של CCMP והמסגרת של WEP שונות כי זה תקן:



מכאן, אם אנו רואים הידר של CCMP אז בהכרח מדובר בחבילת WPA

עד כאן רأינו שקיים את ה-C-MIC שמונע זיופים אבל לא דיברנו על Replat Attacks ועל החלק של ההצפנה לפי מפתח הדרכים-ה-Confidentiality הוא ה-AES וה-Integrity-ה-MIC הוא ה-C-MIC

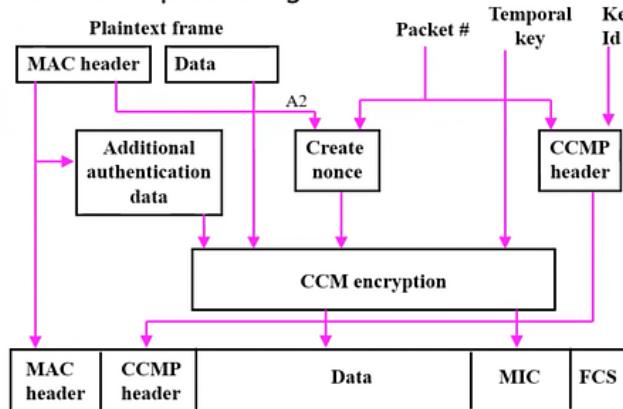
כאן, לא רק ה-7ו תלו依 ב-sequence אלא גם ההצפנה עצמה. בנוסף יש לנו את ה-C-MIC [כפי שניתן לראות בתמונה למטה, גם תהליך האימות וגם ההצפנה משתמשים באותו מפתח]:

- Both encryption and MIC use AES
 - Uses counter Mode (CTR) to encrypt the payload and MIC
 - Uses CBC-MAC to compute a MIC on the plaintext header and the payload
 - Both encryption and authentication use the same key



כלומר, אנו מצפינים את ה-MIC ואת ה-Payload עם AES והרכיבים שלנו להצפנה הם בעצם גם ה-Counter

■ CCMP data processing

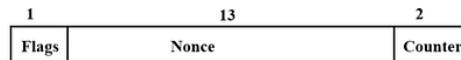


סמלול sequence, כלומר, מספר חבילה

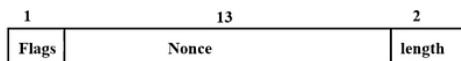
.plaintext. stream cipher key stream נתון, ומצפין plaintext עם key stream XOR עם ה- גוזל ה- key stream cipher מוחלט לבלוקים, ו-XOR מבוצע על כל בלוק בנפרד. **CBC-MAC** תתוחזור המודול הפישוט (Electronic Code Book) שבו הצפנה טקסטים זהים תיתן תוצאות זהות. פורמואט IV או mode cipher-block feedback. הפערין השני ב-IV מושך ב-IV ומכה נראה רק את הראשון.

כאן, הביסוס הוא על בלוקים ולא סטרימ. כלומר, מחלקים את הודעה לגדים קבועים ואוטם מצפינים כר של בלוק תליי בקדום (משרשרים אוטם) וכך יש לנו Counter (CTR)

- Each message block has the size of 16 octets
 - For CTR encryption, A_i has the following format (i is the value of the counter field):

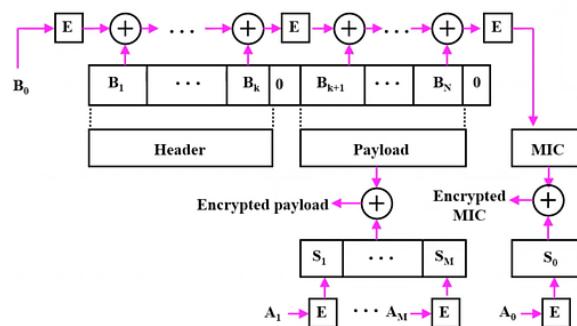


- For the CBC-MAC authentication, B_0 has the following format (length := size of the payload):



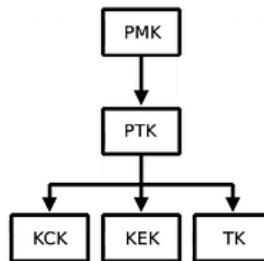
רקע הבלוק ההתחלתי (למטה בתמונה) מכיל את האור

- CCM encryption



ולאחר כל זה נקבל את ההידר CCMP

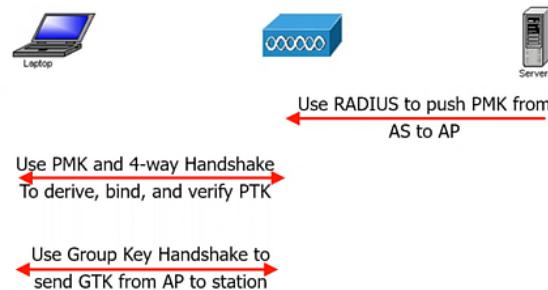
היררכיה המפתחות:



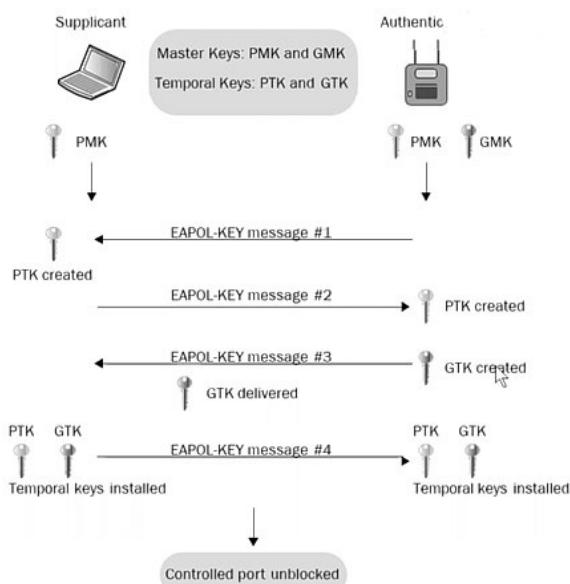
- EAPOL-key key confirmation key (KCK)
- EAPOL-key key encryption key (KEK)
- Temporal key (TK)

ה-PMK הוא ה-Pairwise Key שיצרנו בין הלקוח ל-AP
את ה-TK אנו מכירים כבר מה-TKIP

■ 802.1x key management



בשלבי ה-4-way handshake 2 (כולל) הכל מוצפן ולן לאחר הודעה 3 [שבה מקבלים את ה-GTK] גם הלקוח יודע
שה-AP יודע את הסוד

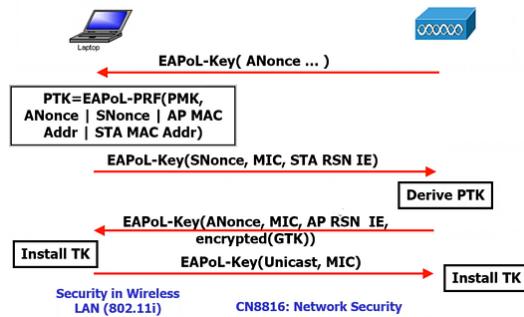


הרחבת על תהליך 4-way handshake

<https://wlan1nde.wordpress.com/2014/10/27/4-way-handshake/comment-page-1>

<https://www.wifi-professionals.com/2019/01/4-way-handshake>

ה-4-way handshake (בו נוצרם המפתחות):
 ■ 4-Way Handshake



שימושים של המפתחות:

- $\text{PTK} := \text{KCK} \mid \text{KEK} \mid \text{TK}$
 - KCK used to authenticate Messages 2, 3, and 4
 - KEK unused by 4-way handshake – used for the encryption of group key
 - TK installed after Message 4 – used for data encryption
- The discovery RSN IE exchange from alteration protected by the MIC in Messages 2 and 3
- The MIC carried in the messages are also used for mutual authentication

דוגמאות לדברים שיכל לשאול בהצגה:

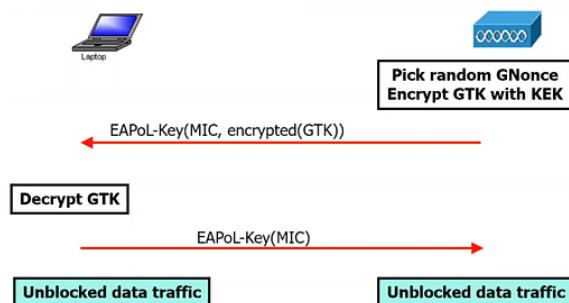
- איך מונעים חבילות (שזה בעזרת MIC)
- איך מונעים Replay Attacks (ע"י sequence [פעם ב-TKIP ופעם ב-CCMP])

לסיכום:

מבחינת ההצפנה ראיינו שיש 2 דרכי להצפנה
 מבחינת הדרכ שلنנו לניהול ה-4-way handshakeauthentication אז אנחנו הבנו שיש לר' דרך אחרת
 (4-way handshake)

כשמדוברים על GTK אז ככלם יש SNonce וזה אומר שיש לנו משחה שחזור על עצמו וזה חולשה

- Group Key Handshake



אבל החולשה לא צאת חזקה כי יש לנו MIC שמנוע מאיתנו לזייף את החבילות ולשלוח אותן שוב
 ויש לנו Counter פנימי לבЛОקים וגם Counter חיוני ולכן התתקפה לא באמת קלה

בשורה התחתונה, אם לא עברו את ה-4-way handshake אז לא יוכל לפעול את ה-Payload למרות
 שראאים את ההידר של ה-MAC

צריך לזכור את הקטע של ה-4-way handshake והקטע של ה-Keys.