תוכן עניינים

הקדמה (+ סוף שיעור 3):

הקדמה וסיכום ("על רגל אחת"):
Wi-Fi הוא קיצור של Wireless Fidelity, הוא התקן שידור של גלי רדיו ומבוסס על 802.11
מכשירים רבים מתחברים לאינטרנט ע"י Wi-Fi, מחשבים ניידים, מחשבים נייחים, קונסולות משחק, טלפונים סלולריים ועוד.

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

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

קליטה: הקליטה של Wi-Fi נמדדת ב dBm, כלל ברזל, ככל שהdBm נמוך יותר, כך הקליטה טובה יותר. תמיד הקליטה תוצג כמינוס 20- ועד ל90-. הטווחים הינם:

- 20- ועד 30-: הקליטה מצוינת וכנראה אתם מרחק של מטר בודד מרכיב ה Wi-Fi במקרה שלנו AP או Router ביתי.
- 50- : קליטה מצוינת גם, אך אתם במרחק של כמה מטרים מהנקודה.
- 60- : קליטה סבירה, זאת אומרת שבעוצמה זו תוכלו לגלוש באינטרנט ולא להבחין באיטיות משמעותית.
- 70- : אומר כי הקליטה פחות מסבירה ולא תוכלו לראות סרטונים באיכות גבוהה או לטעון דפים \ סרטונים במהירות סבירה.
- 80- או 90-: עוצמת הקליטה נמוכה מאוד ולרוב לא תצליחו לגלוש באופן סביר ואם בכלל.

טיפים נוספים: כאשר נקנה ראוטר או AP נבחין כי לכל אנטנה יש עוצמת dbi ההבדל בין dbi ל-dbm הוא ש-dbi הוא כמה מקסימום של עוצמת השידור תהיה ו-dbm הוא כמה "כוח" משדר כעת האנטנה (Wi-Fi)
לכן, אם נבדוק למשל באתר של Tp-link את הראוטר הבא: TL-WA901ND נוכל להבחין כי רשום שהאנטנות למעשה הן 3 אנטנות שכל אחת 5dbi זאת אומרת, זה שיש לנו 3 אנטנות לא אומר שהעוצמה 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 עוצמת השידור של Wi-Fi באזור הוא NetSpot, שניתן להוריד מגוגל.

SSID - הוא השם של "החיבור" אותו יפיץ הראוטר, למשל TalWifi חלקנו נכון להיום רגילים לראות HOTBOX וכו' של חברות הטלוויזיה והכבלים, שכן הרבה בתים קונים "Bundle"
טלוויזיה + ספק + תשתית ולכן, למעשה, אותה החברה מספקת גם ראוטר והוא זה שמפיץ את ה Wi-Fi. דוגמה לSSID המוצגים על ידי הטלפון הסלולרי, אותם SSID שמצא הטלפון הסלולרי בכך שחיפש רשתות Wi-Fi ואלו הם היחידים שבטווח הקליטה שלו

סוגי הצפנות:
כאשר אנו מגדירים את הראוטר, חובה להגדיר סיסמת התחברות ל SSID שכן, אם הרשת תהיה פתוחה, כל תוקף יוכל להתחבר לרשת ולבצע התקפות מגוונות שכבר נלמדו פה באתר, החל מ MITM או שינוי DNS וכו'
לכן חובה עלינו להגדיר סיסמא חזקה, וסוג ההצפנה חייב להיות לפחות WPA2, כעת נסביר על סוגי ההצפנות הקיימות ברכיב ה Wi-Fi:

- WEP – הוא קיצור של Wired Equivalnet Privacy והוא הפרוטוקול הישן ביותר והחלש ביותר מבין פרוטוקולי האבטחה של Wi-Fi, נכון להיום אין להשתמש בו שכן תוקף, בקלות יתרה יכול לפרוץ את הרשת ולסכן את המשתמשים בה.
- WPA – הוא קיצור של Wireless Protected Access והוא פותח את התאחדות ה -Wi Fi, הפרוטוקול משתמש במפתח זמני מסוג TKIP והוא נחשב לפרוטוקול ביניים אשר מטרתו היא להחליף את פרוטוקול ה-WEP.
- WPA2 – הוא התקן הסטנדרטי שיש להשתמש והוא הגרסה החדשה יותר של WPA, הוא משתמש במפתח זמני מסוג CCMP אך ההצפנה לרוב תהיה AES
(WPA2 – Persona) או בקיצור WPA2\PSK הוא השימוש הביתי של WPA2.
WPA2\Enterprise הוא השם השני של 802.1x והוא היכולת לבדוק את הרכיב המתחבר אליו על ידי כך שהרכיב שרוצה להתחבר יאושר על ידי שרת RADIUS.

סטנדרטים ב WI-FI:
לכל Wi-Fi יש סטנדרט שונה, ה802.11 מגיע בתצורה של B\G\N:
B – הוא עד מהירות של 11Mbps ונחשב ליחסית איטי 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 ה Wi-Fi קיימים 2 תדרים, 2.4Ghz ו 5Ghz ההנחה של אנשים היא ש5Ghz הוא גדול יותר ולכן מגיע רחוק יותר מ2.4Ghz אך זו טעות.
לתדר ה2.4Ghz יש 13 ערוצים, הערוצים המומלצים לבחירה הם: 1,6,11, הסיבה היא שערוצים אלו לא חופפים לגלי רדיו שקיימים ברכיבים אחרים ולכן עדיף לבחור בהם (לרוב הראוטר יבחר לבד את הערוץ ואין צורך להגדיר לו)
2.4Ghz הוא תדר נמוך יותר ולכן "חודר" קירות ומחסומים אחרים בקלות יותר מ5Ghz
אז למה שנבחר בתדר 2.4Ghz או ב5Ghz?
תדר ה5Ghz הוא תדר פחות עמוס, לכן הוא נחשב מהיר יותר ויכול לספק מהירות גבוהה יותר.
אבל! רוב הראוטרים תומכים ב Dual Band, זאת אומרת שיש לראוטר 4 אנטנות, 2 אנטנות בתדר 2.4Ghz ו2 אנטנות בתדר 5Ghz, מדוע יש 2 אנטנות לכל תדר?
אחת משדרת ואחת קולטת וכך יוצרת פחות "עומס".

[מקור]

מושגים נוספים (תזכורת מתקשורת):

DHCP: פרוטוקול תקשורת המשמש להקצאה של כתובות IP ייחודיות למחשבים ברשת מקומית (LAN). בנוסף לכתובת ה-IP, שרת DHCP בדרך כלל יספק למחשב גם נתונים כמו ה-Subnet mask, כתובת שרת ה-DNS וכתובת שער הגישה (Gateway), כך שהמחשב יוכל להתחיל לתפקד ברשת ללא צורך בנתונים נוספים.

DNS: במילים פשוטות, Domain Name System הוא אוסף של מסדי נתונים המתרגם "שמות מארח" (Hostnames) לכתובות IP. ניתן להתייחס ל DNS כאל "ספר הטלפונים של האינטרנט" מכיוון והוא ממיר שמות מארח שקל לזכור כמו www.duckduckgo.com לכתובת IP כמו 40.114.177.156.

הבדלים בין הידר של רשת אלחוטית (802.11) לרשת קווית (802.3):

802.3:

```
> Frame 42: 317 bytes on wire (2536 bits), 317 bytes captured (2536 bits) on interface 0
v 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)
```

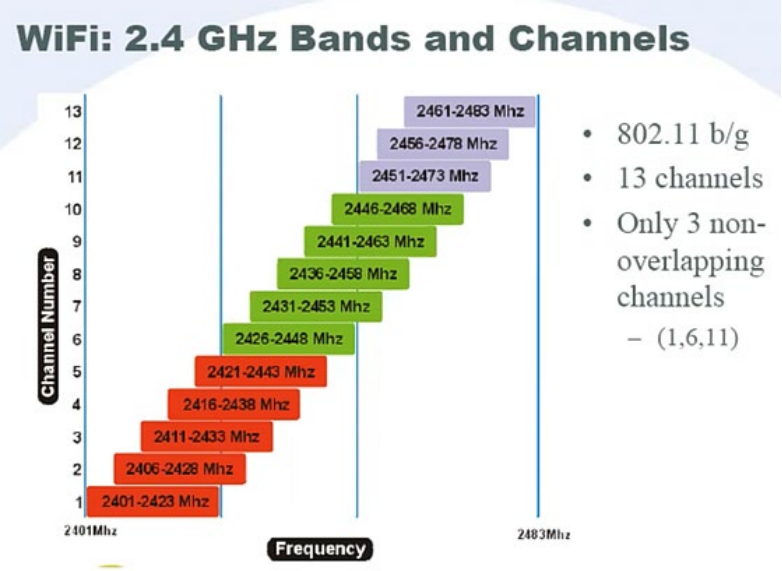
802.11:

```
v 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 נוסף שמתווסף לכל מסגרת 802.11 בעת לכידת מסגרות. רק כדי להיות ברור - אלה אינם חלק מפורמט הפריימים הסטנדרטי 802.11, אלא הם מידע שנוסף בזמן הלכידה כדי לספק עוד נתונים על הפריימים שנלכדו. לדוגמה, בלכידת תעבורה רגילה 802.11, אין מידע לגבי רמת אות הקבלה של המסגרת בזמן הלכידה אבל זה נמצא בהידר RadioTap, מה שיכול להיות שימושי מאוד. כדוגמה 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/

ככל שתדר יותר גבוה אז האורך גל יותר קטן, וככל שאורך גל יותר קטן אז החדירות שלו (חדירה דרך מכשולים) יותר קטנה
ערוצים הם תחומי תדרים (לדוגמה, 2.4 ג'יגה הרץ) או במילים אחרות, הקצאה של טווח תדרים



בשביל לנצל את **כל** רוחב הפס, מצופה שאף מכשיר אחר לא ישתמש בחלק מהתווך (לדוגמא, התווך בתמונה למעלה)

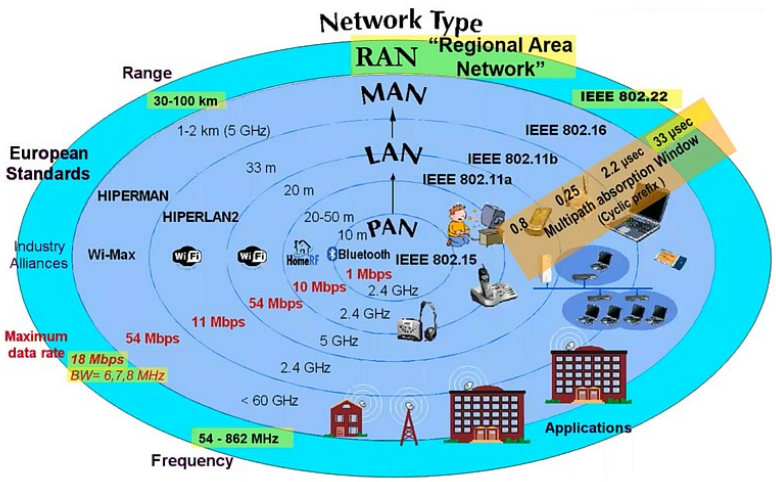
תזכורת מודל השכבות:

מספר השכבה	שם השכבה	מטרה (בקצרה)	פרוטוקול לדוגמה	שם של גוש מידע
1	השכבה הפיזית (Physical Layer)	העברת המידע ביט אחר ביט – 0 או 1 בכל פעם		**ביט** (bit, סיבית)
2	שכבת הקו (Data Link)	תקשורת בין ישויות סמוכות זו לזו	Ethernet	**מסגרת** (frame)
3	שכבת הרשת (Network Layer)	החלטה על המסלול שתעבור חבילת מידע בין המקור אל היעד	IP	**פקטה** (packet, חבילה)
4	שכבת התעבורה (Transport Layer)	ריבוב אפליקציות על אותה ישות (תמיד) + מתן אמינות לקישור (אופציונלי)	TCP	**סגמנט** (segment)
5	שכבת האפליקציה (Application Layer)	שימושים שונים בהתאם לאפליקציה	HTTP	* אין שם מיוחד *

תקן אומר שאיזה תדרים עובדים, ובאיזה צורה עובדים ואיך יוצרים את החבילות שעובדים איתם
תקן 802.11 זה wireless WLAN
תקן IEEE 802 נמצא בתפר בין Network Layer ל-Data Link (IEEE עובד ב3 השכבות התחתונות)
כלומר, אינו מדבר על Network Layer ומטה

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

802.11 זה תקן (גוף עסקי) וזה לא wifi

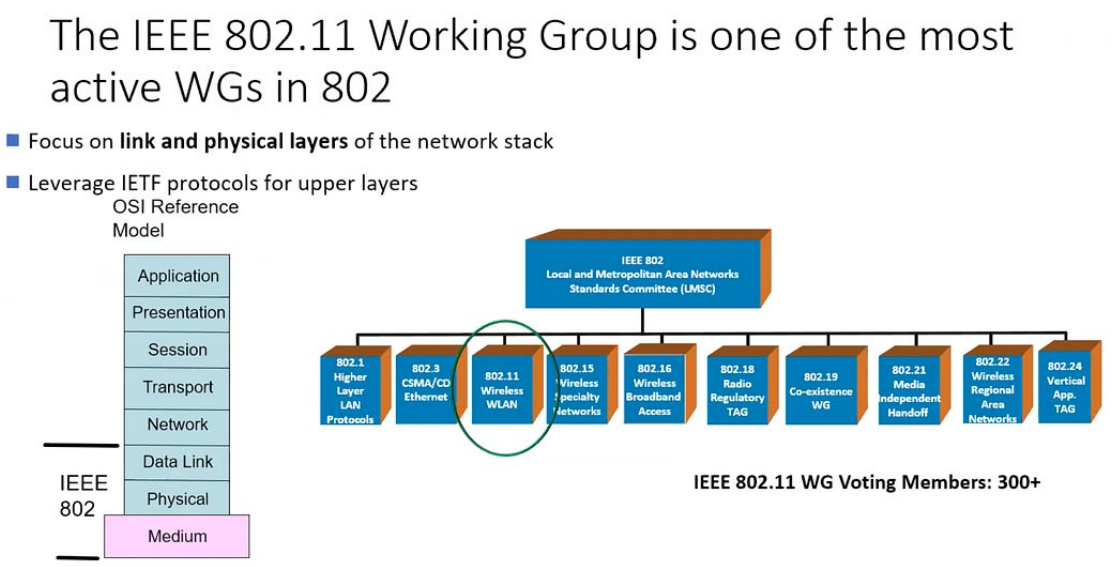


	Personal Area Network (PAN)	Local Area Network (LAN)	Metropolitan Area Network (MAN)	Wide Area Network (WAN)
Technology	• Bluetooth • Ultra-wideband (UWB)	• WiFi (802.11a/b/g/n/ac) • WiGig (802.11ad)	• WiMAX (802.16)	• GSM • GPRS • W-CDMA • HSPA • LTE
Data Transfer	Low data rates	High data rates	Medium 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 שהסכימו על דרך להעביר תקשורת אלחוטית. כלומר, יצרו מוצר ע"י כך שלקחו מה שטוב להם.
נקרא wifi alliance (alliance = ברית/שיתוף פעולה)

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

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



מבחינת בסיס הפרוטוקול כאשר נרצה להקים רשת אלחוטית נצטרך לשלוח אותות על מנת שמכשירים אחרים יזהו אותנו
הארכיטקטורה שלנו היא כזו שתמיד מנוהלת ולא מבוזרת (מבוזרת הכוונה שכל רכיב מנהל את עצמו אבל תלוי ברכיב אחר)
נשים לב כי בתקשורת קווית כי כל אחד מנהל את עצמו אך התקשורת מועברת בהסכמה

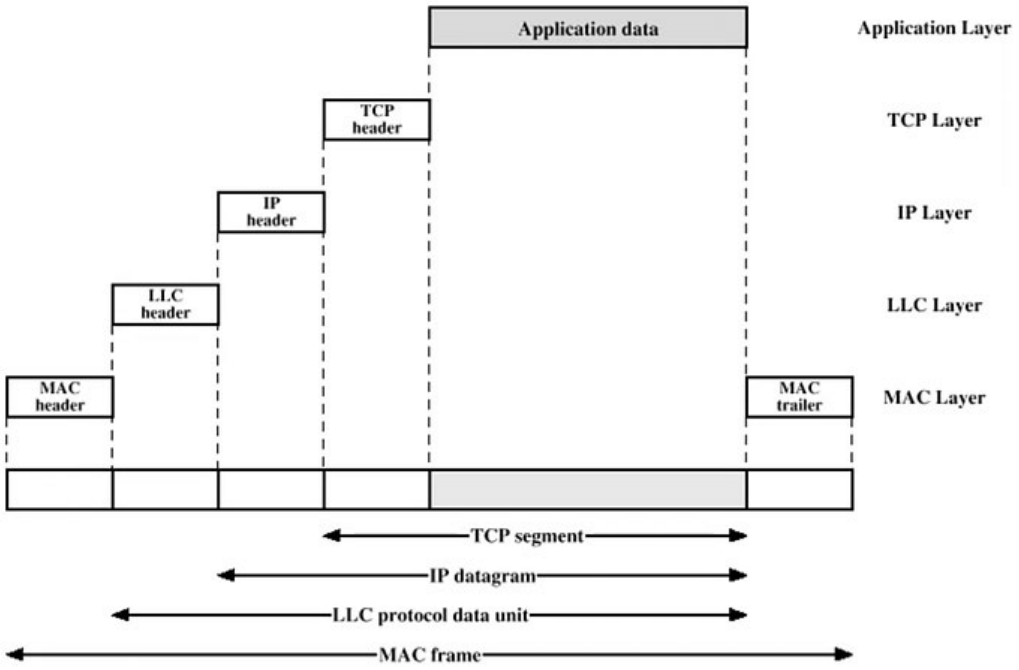
בארכיטקטורת 802.11 יש רכיב מרכזי שמנהל וכל השאר עוברים דרכו

ראוטר מנהל נקודת גישה. נקודת הגישה, בין היתר, מאפשרת תקשורת בין עמדות קצה שלא יכולות לתקשר בעצמם בגלל המרחק

בשלב זה של הקורס, אנחנו עוסקים בWLAN וwifi aliance. אנחנו צריכים לדעת ששילוב בניהם לבין GSM הייתה קיימת בתיאוריה אבל לא מתקיים כי אי אפשר לחייב בתשלום כשעוסקים בWLAN וכו'

שיעור 4:

נעסוק במבנה החבילות עצמן:



הידר הMAC הוא תחילת ההודעה
הידר הLLC מאפשר לדעת איזה חבילה חבויה בפנים
הידר הIP מאפשר לגעת איזה IP ואיזה גרסת IP (4 או 6) וכו'
הידר הTCP
הידר הApplication

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

מטרת חבילת Beacon היא ליידע שקיימת כאן רשת [חבילה כזו היא Management (מוגדר ברמת הMAC)] וכל אחד יכול לייצר אותה (גם למטרות לא טובות כמו Evil Twin)

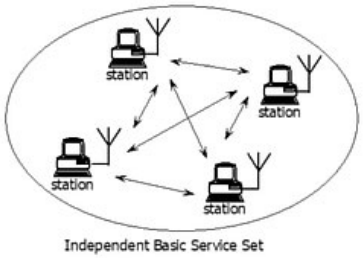
BSS היא סט שירותים בסיסיים (מקומיים) הניתנים ע"י נקודת AP
ESS היא סט שירותים מורחב, כמו שAP מאפשר גישה לשאר האינטרנט

בגדול AP מייצרת Distribution System שאפשר לקטלג כBSS או ESS שזה בעצם רעיון של מתן שירות לקבוצה של רכיבים

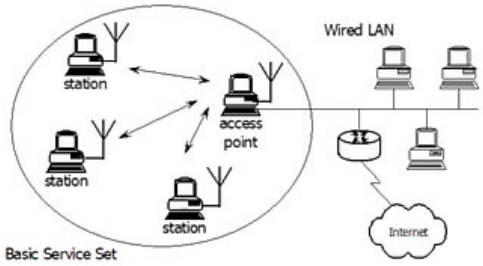
אצלנו הקופסה של הראוטר מכילה מגוון שירותים, היא **גם** AP **וגם** ראוטר **וגם** פורטל וגם מספקת שירותי אבטחה **ועוד**

ארכיטקטורות 802.11 (אלו בעצם מודים של הכרטיס רשת ברמת התקן):

- Ad hoc mode: Peer-To-Peer, מספק תקשורת לוקאלית, מאפשר Authentication וגם Registration (בפועל לא משתמשים באחרונים).



- Infrastructure Mode: מאפשר forwarding לתקשורת קווית, מאפשר ESS, **בדר"כ מי שנמצא במצב Infrastructure הוא הAP** (כי מצב זה מאפשר לו תקשורת עם נקודות קצה אחרות ויכול לעשות Authentication וגם Registration [בשביל לקשר (associate) בינו לבין עמדות קצה] ויכול לעשות forwarding לתקשורת קווית)



גם אם אנו נמצאים במצב Infrastructure אז נצטרך עוד רכיבים המאפשרים התמודדות עם דברים שאנו מצפים לקבל ברשת
בין היתר, הרכיבים: (רכיבים אלו מייצרים את הBSS או ESS)

- Distribution of messages within a DS, מאפשר לדעת מי שלח למי ולשלוח את זה הלאה
- Trasition typed based on mobility, מאפשר לדעת אם מעבירים לרשת נוספת או לאינטרנט. כלומר, היכולת לעבור בין DS (BSS או ESS או BSS אחר)
- Association related services, מאפשר לדעת אם מישהו חבר ברשת הזאת. Association או Reassociation או Diseassociation. עוזר להתחבר במהירות ולהתנתק כי אנו רוצים מצד אחד להיות תמיד בהאזנה אבל גם לא לבזבז אנרגיה.
- Access and privacy services, מאפשר פרטיות, Authentication או Deauthentication או Privacy. כלומר, אנו יודעים מי אתה ואנו רק מאבטחים אותך.

יכול לקרות מצב שעברנו את שלב הAssociation אך לא את הAuthentication ואז אנו יכולים להיות מחוברים ולקבל שירותים מהרשת אבל לא לקרוא הודעות כי הם מוצפנות. מצד שני, מצב זה יכול להיות מספיק בשביל לפרוץ את WEP.

- IEEE 802.11 Medium Access, הוא שימוש בMedium אחר ולכן זה אומר שהוא פגיע (ולא מוגן יותר כמו כבל חשמל) ולכן אנו בודקים בעזרת גישות שונות שיש גישה ואבטחה ושנעברת המידע תעשה בצורה מהימנה
- Reliable Data Delivery, מאפשר לשלוח את המידע בצורה מהימנה, לדוגמה אם יש חפיפת בין כמה AP אז צריך להגיד לכולם שמישהו הולך לשדר [כי אם לדוגמה יש לנו 3 תחנות ממסר אחת אחרי השנייה כך שכל אחת שומעת **רק** את הסמוכה לה, אז אם התחנה הראשונה תרצה לשלוח הודעה לתחנה השנייה יכול לקרות מצב שהשנייה לא תוכל לשמוע כי השלישית גם משדרת (כלומר, השנייה מקשיבה לשלישית וגם לראשונה ואז יש רעש) והתחנה הראשונה לא יודעת את זה. זה נקרא **hidden terminal**] ולכן יש CTS / RTS. כל זה ברמה פיזיקאית ויכול לקרות מצב של retransmit גם אם משתמשים בUDP (בתקן 802.11)

- Access control, אלו טכניקות ניהול
- Medium access control, מתבצע כאשר אין CTS / RTS ואנו צריכים לנהל את עצמנו **(ההסבר למטה)**
-

מצב מוניטור מאפשר לשמוע איזה חבילות שנרצה גם אם לא מופנות אלינו, ולכתוב איזה חבילות שנרצה (זה נקרא passive sniffing ו-packet injection).

הדרך בה מקבלים את המידע:
1. מקבלים מסר בינארי (מידע ספרתי)
2. הופכים אותו למידע באמצעות carrier signal
3. כמה זמן שאנו משדרים את הcarrier signal משמש אותנו כpreamble
4. משדרים את האות עם המידע

האות עם המידע היא המידע הספרתי

כשאנו רוצים לקבל מידע אנו שולחים Probe request
התשובה מהAP היא חבילת Probe response (מחזיר מידע, לדוגמה את הSSID)
החבילות הנ"ל הינם פרוטוקול של services

Probe response דומה לBeacon, כולל מידע על יכולת, מידע אימות וכו'. ההבדל הוא שbeacon נשלחת לעתים קרובות ותגובת Probe response רק בתגובה לProbe request.

אם נרצה להתחזות לAP נוכל בעצם לשלוח Beacon

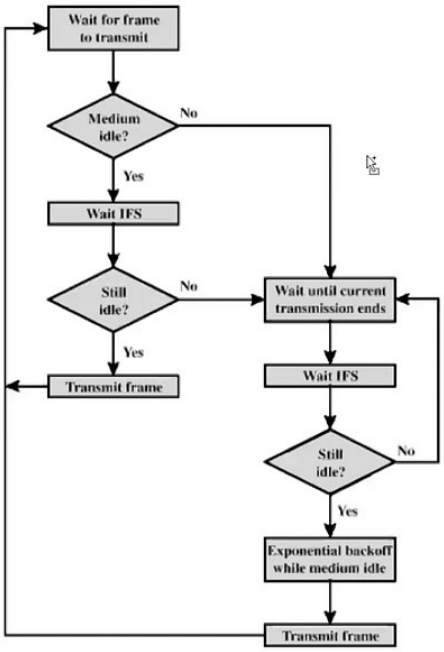
תחת 802.11 ישנם 3 סוגי מסגרות:
1. Management (לדוגמה, Beacon)
2. Data
3. Control

בשני הביטים הראשונים של ההודעה 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 התקשורת)
בסלולר יש מקור ניהול אחד בערוץ
לעומת זאת, ב802.11 wifi כל אחד מנהל את עצמו, לכן, מי שעומד בתקן תמיד יחכה בין השליחות של ההודעות כפי שניתן לראות בתמונה:



כאשר idle הוא הזמן שהתווך פנוי וכאשר IFS היא יחידת המתנה מסוימת (פרוסת אוויר)
ישנן כמה יחידות המתנה DIFS, PIFS, SIFS, כאשר האחרונה הקצרה ביותר ומשומשת כאשר עוסקים בהודעות עם עדיפות גבוהה ואז כשהתווך פנוי נחכה פחות זמן וככה נכנסים לשידור ראשונים.

גם לAP יש קדימות מבחינת IFS כמו לדוגמה אם מדובר בAssociation שהוא סוג Management

לפעמים זה בלתי נמנע ובגלל זה קורה מצב בו יש קושי ל4 אנשים לראות יוטיוב בו זמנית אם עושים זאת ברשתות פשוטות כמו 2.4, כי כולם רוצים להשתמש באותו תווך.

נשים לב כי אם נשתמש במכשיר שהוא אינו תחת התקן אז נוכל באמת לחסום תקשורת כי אנו לא מתחשבים באחרים

שיעור 5:

Subnetwork:

כשמדובר בכתובות לרשתות, אז מספרי הכתובות מחולקות כך שישנם טווחים שמיועדים לרשתות/חומרות שונות, כך בעצם מגדירים קבוצות של מחשבים בצורה לוגית
לדוגמה, בip4 נוכל להגדיר 256 קבוצות בצורה פשוטה (בip6 נקבל יותר קבוצות)
ולזה משתמשים ב-BSS

הגדרות בנוגע לחבילות:

- TX הוא הtransmitter (שולח)
- RX הוא הreceiver (מקבל)

כשנעביר חבילות תחת כמה תחנות ממסר אז הtx, rx משתנים אבל הsource, destination קבועים

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

כאשר נתקלים בבעיות אז הרכיב עובר לשדר במודולציה נמוכה (כמו 1.2 מגה ביט פר שניה)
וכשמשדרים במודולציה נמוכה אז תופסים יותר זמן אוויר וזה נקרא rate avalanche
הפתרון הוא שליחת ack על מנת לדעת מתי לבצע שליחה חוזרת

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

Mac Frame Format:

אינו שייך ספציפית ל802.11 אלא מגיע מEthernet (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 שכאן ב802.11 מה שעשוי להשתנות הוא המשמעות של הדברים

- נשים לב כי כתוב בשדה השני Duration או ID כי זה תלוי בסוג החבילה
- Address 1: מקבל (receiver)
- Address 2: שולח (transmitter)
- Address 3: יעד (destination)
- Address 4: מקור (source)

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

כאשר Frame Control 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	

Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Management	More data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

כאשר, אם נשלח מAP לAP אז שני הפלגים יהיו 1 (גם To DS וגם From DS)

<u>Control Frame Subtypes:</u>

כפי שהזכרנו לעיל את RTS / CTS, הם תתי סוגים והם שייכים לסוג Control
גם ack הוא תת סוג ושייך 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 מצוינים בתוך הFrame Control (FC) כפי שנראה בתמונות למטה

עד כאן הבנו באופן כללי את החבילות
מכאן והלאה נלמד איך נוצרת רשת ואיך מקבלים שירותי רשת

בשביל להבין איך נוצרת רשת נעבור לשכבת הLink
תמיד נצטרך תאימות לאחור עבור תקנים קודמים גם ברמת הLink כדי שיתאים גם לEthernet שהוא 802.3