Jonas, Tobias og Steffen
H4 – Mobile og trådløse systemer
Whitepaper

# Wi-Fi og sikkerhed

## Historie

Wi-Fi står for Wireless Fidelity og er en teknologi der bruger radio bølger til at give internetforbindelse.

Wi-Fi blev skabt da United states FCC åbnede for at de trådløse frekvenser 900 Mhz, 2.4 Ghz og 5.8 Ghz kunne bruges uden licens. For at gøre det muligt at kommunikere med disse frekvenser blev der brugt spread spectrum som gør det muligt at sende over flere frekvenser for at undgå interferens, men enheder fra forskellige mærker kunne ikke kommunikere og derfor blev standarten 802.11 sat under udvikling og efter 9 år i år 1997 blev standarten offentlig.

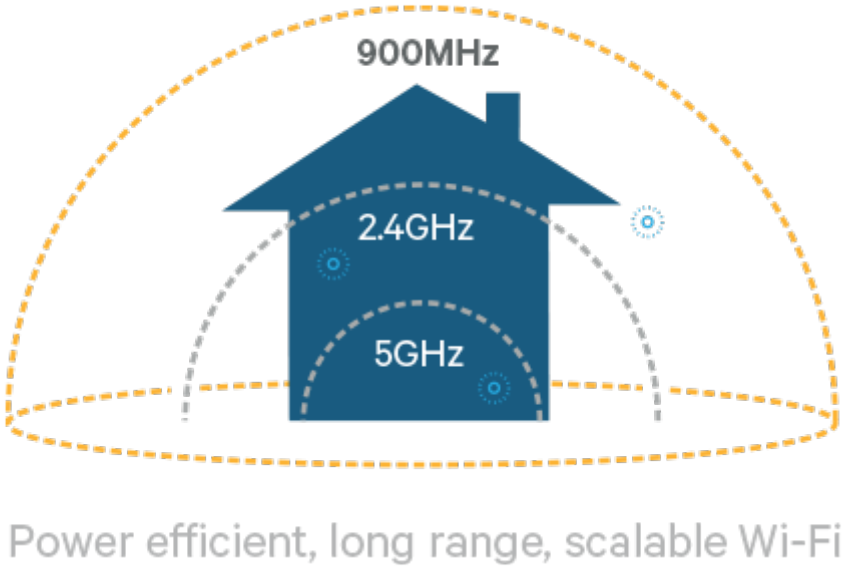
Da standarten udkom var det mulig at sende data med 2 megabits per sekunder, men 2 år senere kom 802.11a som gjorde det muligt at sende op til 45 megabits per sekund, men havde en begrænset rækkevide og var dyrt at producere, og derfor kom 802.11b året efter som var billigt og havde en bedre rækkevidde, som gjorde at Wi-Fi begynde at blive mainstream.

I dag er de 2 mest brugte Wi-Fi typer N og AC. N kører 2.4 Ghz og 5 Ghz og MIMO blev introduceret sammen med denne udgave som gør at der kan bruges flere indgange og udgange og på den måde kan der sendes mere data. AC bruger også MIMO og supportere op til 8 antenner.

Fremtidens versioner af 802.11 er bl.a. ah og ax

Ah er bl.a. udviklet til IoT, da den kører 900 MHz og derfor har lang rækkevidde.

Ax bliver højhastigheds med op til 10.53 Gbps og kommer som 2.4 Ghz og 5.0 Ghz



Jonas, Tobias og Steffen
H4 – Mobile og trådløse systemer
Whitepaper

# Wi-Fi setup

Når man opsætter Wi-Fi kan man konfigurer det på to måder:

WPS(Wifi Protected Setup): Er noget the Wi-Fi Alliance har lavet for at simpelt gøre Wi-Fi opsætningen.
WPS laver SSID og encryption automatisk med WPA2/AES.
WPS fungere på den måde at man skrive en pin kode for at komme på nettet eller trykker på en fysisk knap for at give en enhed adgang.

Devices skal understøtte WPS med mindre det er Win7

Manuel:

Man kan også konfigurere det manuelt. Der vil man typisk gøre følgende:

**SSID:**

Service Set Identifier(SSID) Det er en streng, som identificerer og navngiver en trådløst netværk, og det er en del af IEEE 802.11 WLAN-standarden, som er den der bliver brugt idag.

SSID anbefales at blive skjult i nogle omstændigheder, da det kan være et sikkerhedsbrud.

**WPA:**

Sikkerhedsnøgle og hvilken kryptering der skal bruges

**Mode:**

Man vælger IEEE standart så som 802.11ac

**Channel Width:**

Her kan det konfigureres om der skal bruges 20 Mhz hvor det anbefales at bruge kanal 1,6 eller 11

Ved 40 Mhz er det bedst at bruge kanal 3 og 11

Grunden til dette er at kanalerne ikke interferere med hinanden.

Jonas, Tobias og Steffen
H4 – Mobile og trådløse systemer
Whitepaper

# Wi-Fi Sikkerhed

## Security modes

Der findes fire former for Security modes som Wi-Fi kan køre:
1. WEP
2. WPA-Personal
3. WPA-Enterprise
4. No Security

WPA2 Personal er hvor du har en pre-shared key som kan bruges til at logge på netvæket med. Dette bruges typisk i husstande.

WPA2 Enterprise kræver en RADIUS server, som kan tage sige af godkendende adgang og en database hvori separate klient legitimationsoplysninger ligger. Dette gør at der er større sikkerhed og er nemmere for virksomheder at administrere. En netværksadministrator kan nemt slå en bruger eller klient fra i tilfælde af tyveri eller at en medarbejder forlader virksomheden. Hvis der blot skulle bruges en Pre-shared key var virksomheden nødt til at ændre passwordet hver gang der opstod en situation hvor en bruger eller pc skulle udelukkes.

RADIUS serveren er det centrale i et WPA2 enterprise setup. Serveren styre forbindelser og adgange og koordinere altid imellem routere, databasen og klienten.

Derudover skal der også laves en EAP som definere hvilke oplysninger og hvilken godkendelse der skal bruges. LEAP er bland andet en type, som bruger brugernavn og kodeord til at godkende med.

## Krypterings former

Der findes tre krypterings metoder for WiFi: WEP, WPA og WPA2

WEP(Wired Equilevant Privacy): er den ældste og mest bugte krypterings protocol i verden da den er bagudkompatibel til mange systemer. WEP kom i 1999 og tilbød 64 bit kryptering, hvorefter de opgraderet det til 128 bit. Problemet med WEP kom efter 2001, hvor computer software kunne knække den 128 bit kode. Derfor blev WEP introduceret. The WiFi-Aliance fjernet WEP i 2004 af sikkerhedsmæssige årsager.

WPA(WiFi protected access): var the WiFi alliance' svar på at komme med en ny og forbedret kryptering. WPA kom i 2003. WPA-PSK(Pre Shared key) tilbyder en 256 bit kryptering, hvilket er dobbelt så meget som WEP 128. Dette tilbyder en helt anden sikkerhed til WiFI. WPA tilbyder også besked integritet, hvilket gjorde at man kunne finde ud af om en hacker havde fanget eller ændret pakker mellem en klient og en access point.

WPA2: Kom 2006. Forskellen på WPA og WPA2 er AES algoritmen og CCMP som erstattet TKIP. Med WPA2 er det meget sværere at hacke et netværk. Det kræver nemlig at hackeren skal ind på netværket for at fange data. Stadig kan WiFi være et security breach i virksomheder. Derfor skal man stadig tænke over det.

Jonas, Tobias og Steffen
H4 – Mobile og trådløse systemer
Whitepaper

Sikkerheds listen over kryptering fra meste sikker til meste usikker:

1.WPA2+AES
2.WPA+AES
3.WPA+TKIP/AES
4.WPA+TKIP
5.WEP
6.Open network

AES vs TKIP

AES og TKIP er to forskellige krypterings former. TKIP blev introduceret til WPA og er en gammel krypteringsform som er blevet erstattet af AES.

## AES (Advanced Encryption Standard):

For at forklare algoritmen simpelt så tager den plain text og konvetere det til ciphertext. Ciphertext ligner en tilfældig string af karaktere til en person der ikke har en nøgle til at decryptere det med.

Personen på den anden side har en nøgle der kan decryptere den sendte data. Hvis vi tog et senarie hvor vi har en router og en klient, har routeren den første nøgle og kryptere data før den bliver broadcastet. Computeren har den anden nøgle der decryptere transmisionen så man kan se det på skærmen i forståeligt format.

Der findes 128, 192 og 256 bits kryptering. Det bestemmer hvor mange potentielle kombinationer det tager for at bryde krypteringen. Selv med 128 bits kryptering er det umuligt at finde frem til nøglen. Det vil tage mange millioner år.

## TKIP (Temporal Key Integrity Protocol)

Det var en sikkerhedsprotokol som blev brugt i IEEE 802.11 trådløst netværk. Den er udviklet af Wi-Fi Alliance. Det var meningen at TKIP skulle overtage WEP uden at man skulle have nyt hardware. TKIP er ikke længere betegnet som sikker, og er ikke rigtig blevet brugt siden 2012.

TKIP er relateret til WPA, men der er 3 nye sikkerhedsfeatures i TKIP.

I TKIP er der key mixing function som samlinger secret root key med initialization vector før den sender den til RC4 initialization. Anden ting er en sequence counter som sikrere mod replay angreb. Hvilket betyder pakker som bliver modtaget ude af rækkefølge vil blive afvist af access pointet. Og den sidste ting som er blevet tilføjet er en 64-bit Message integrity Check (MIC)

For at TKIP skulle kunne køre på gammel udstyr, så bruger den RC4 som chip. TKIP sender hver pakke med en unik Krypteringsnøgle.

Key mixing øger sikkerheden ved at gøre det svære at afkode de nøgler som der skal bruges, ved at give angriberen mindre data som er krypteret med en nøgle.

TKIP er sårbar imod MIC key recovery angreb, hvis det er rigtig gjort som giver det crackeren adgang til at sende og Dekryptere vilkårlig pakker på det netværk som er blevet angrebet.