WiFi

Outline

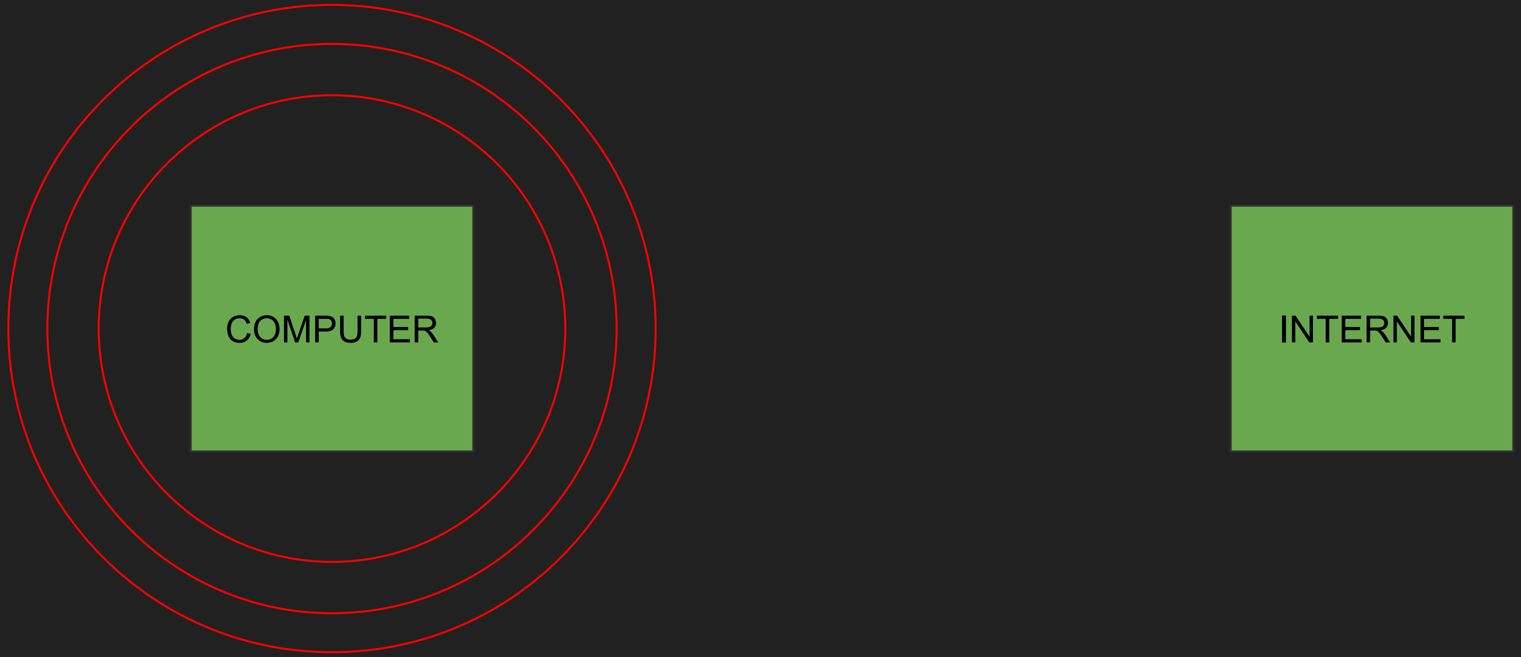
- Hardware and network configuration
- Software
- Authentication and Encryption
    - Open
    - WPA2
        - 4 way handshake
        - PSK
        - Enterprise
            - RADIUS and EAP
            - PEAPv0-MSCHAPv2

What is WiFi

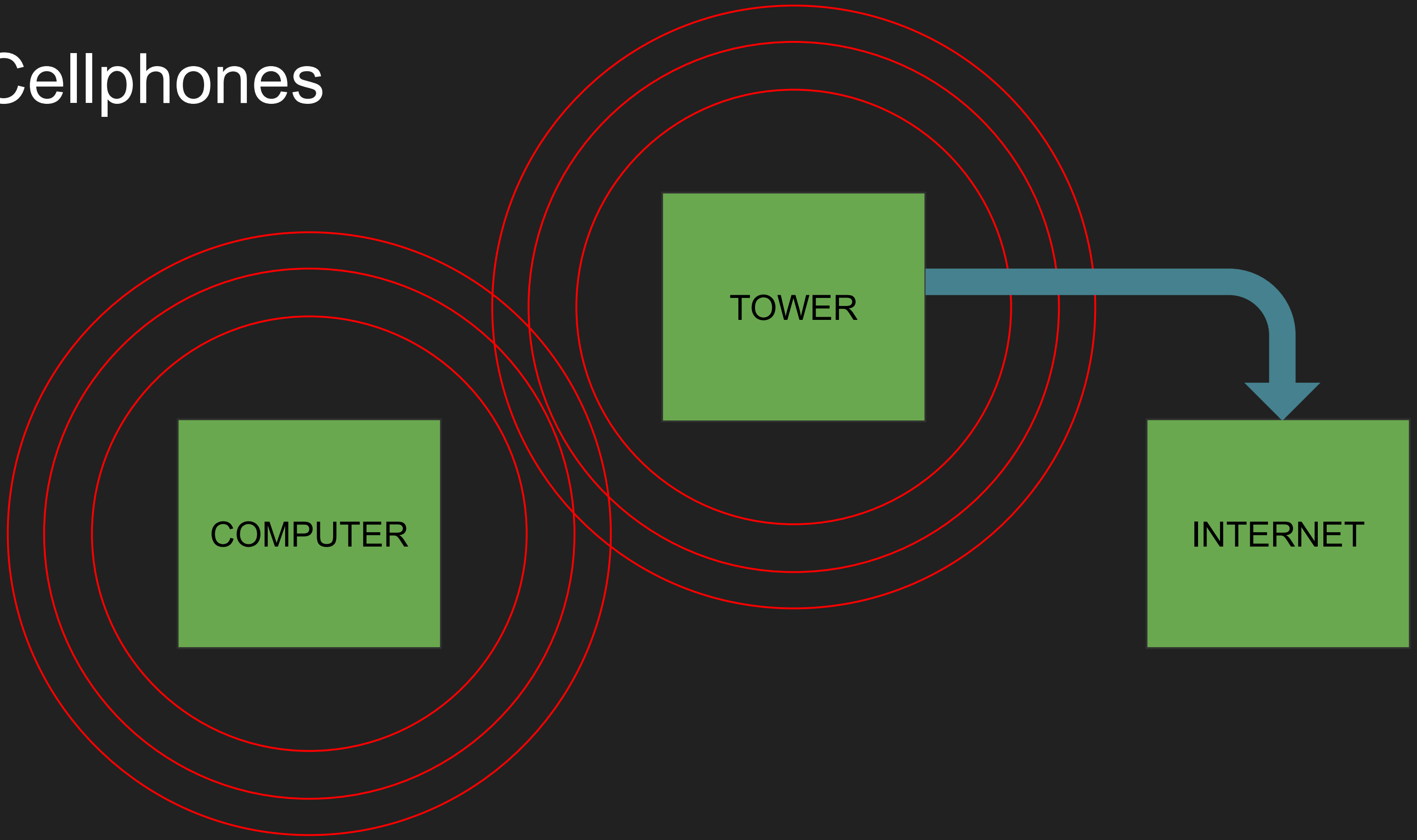
COMPUTER

INTERNET

What is WiFi



Cellphones

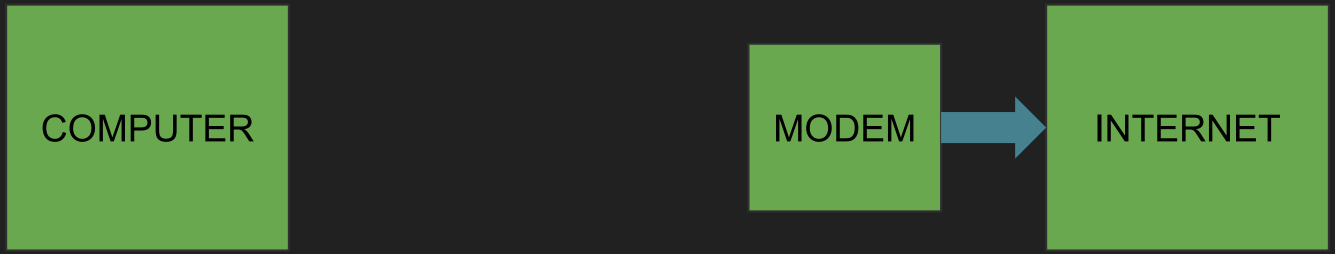


Typical Home Internet Setup

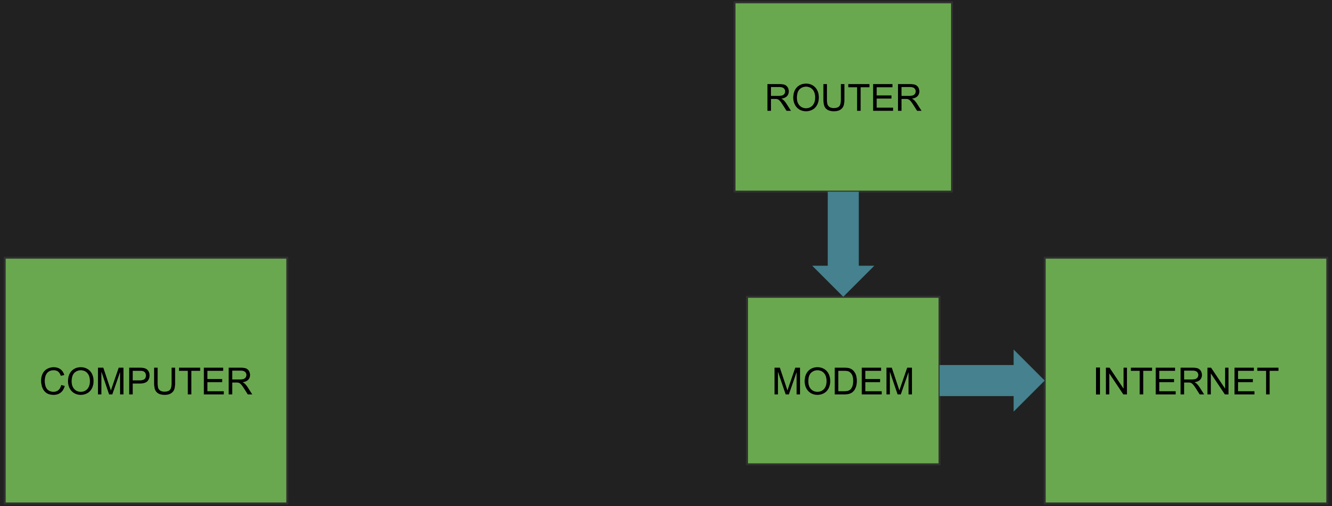
COMPUTER

INTERNET

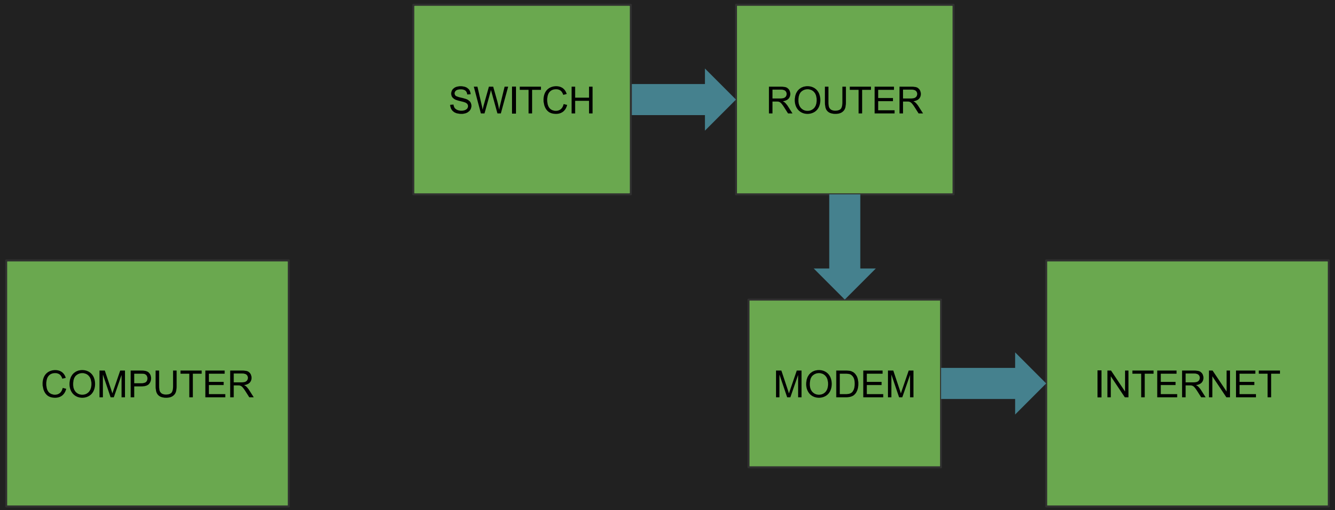
Typical Home Internet Setup



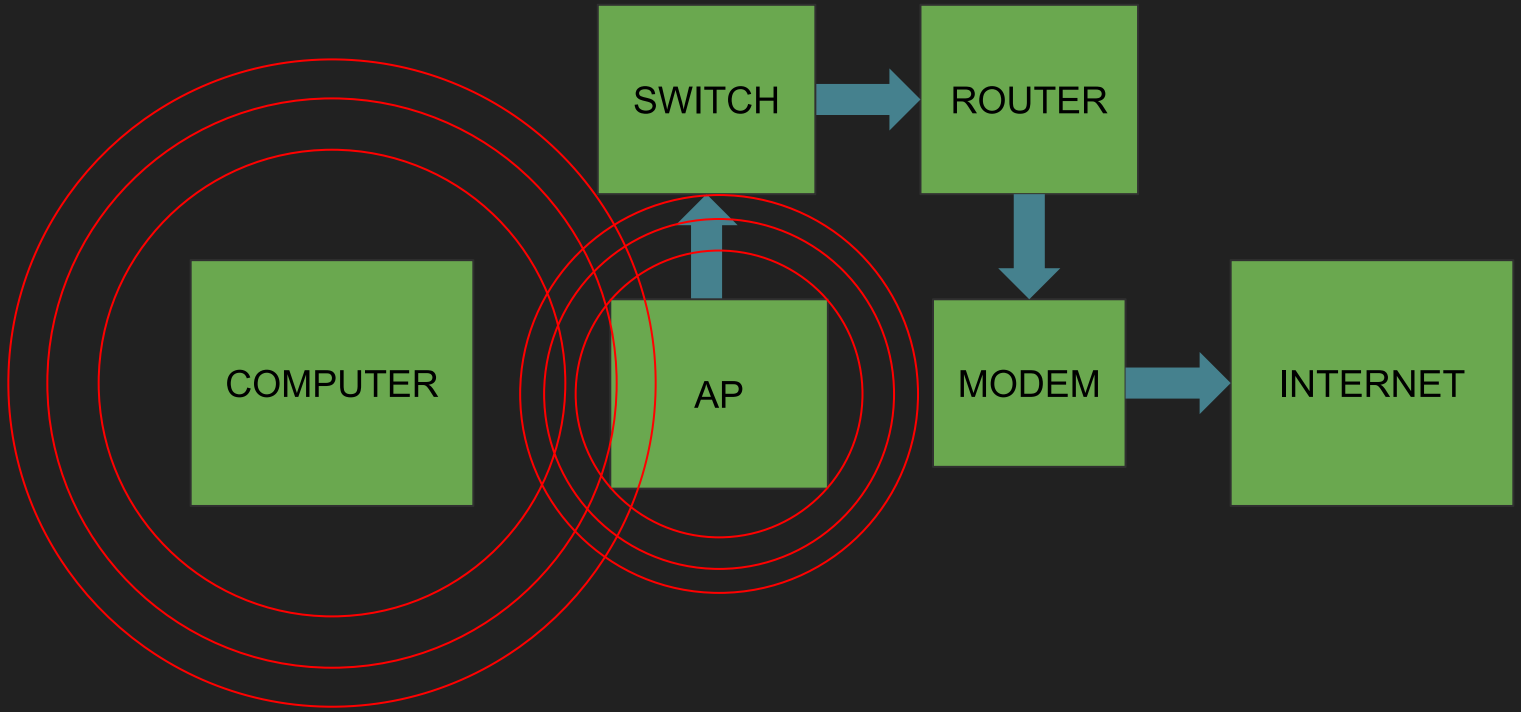
Typical Home Internet Setup



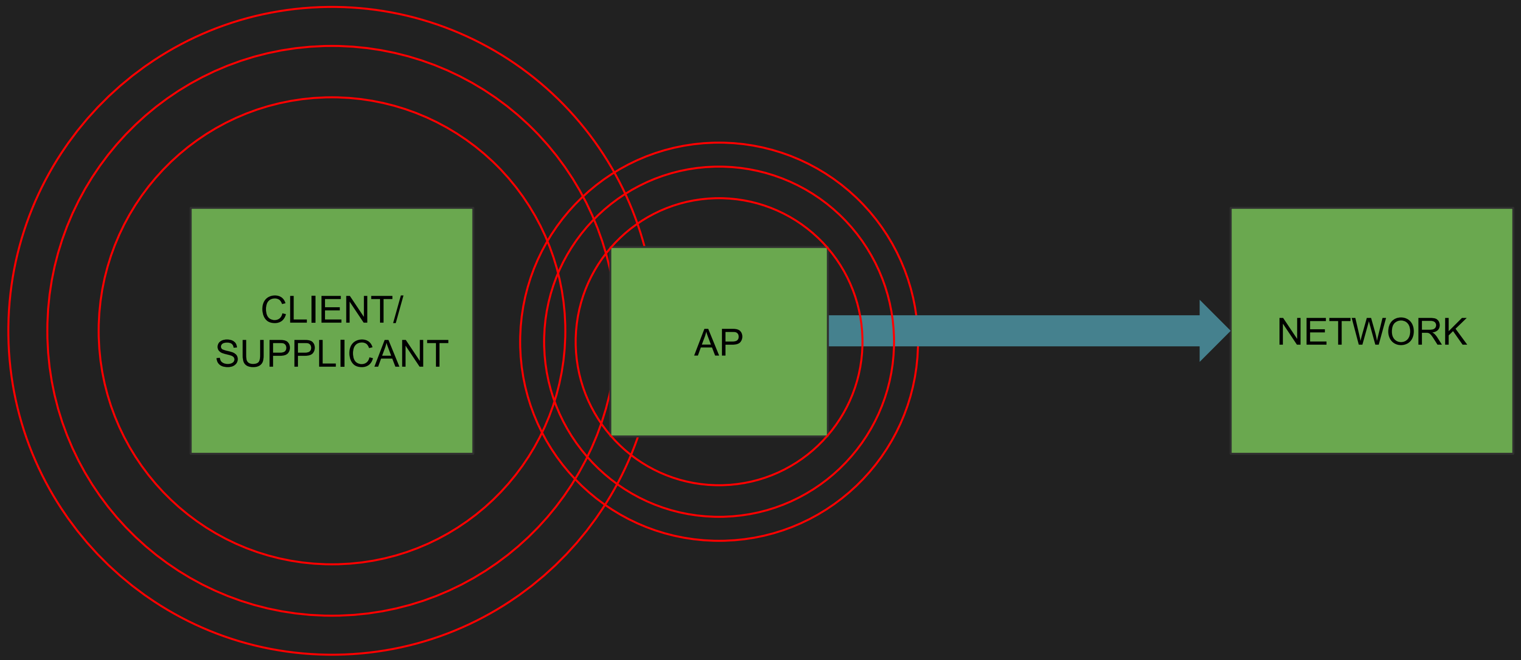
Typical Home Internet Setup



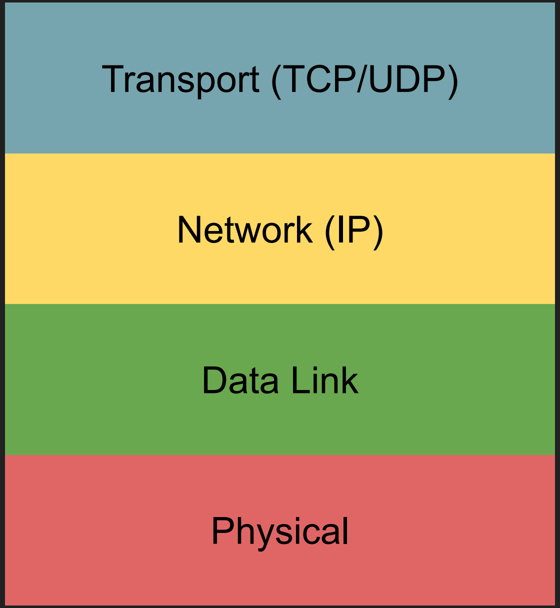
Typical Home Internet Setup



The Interesting Part



Layers



Transport (TCP/UDP)

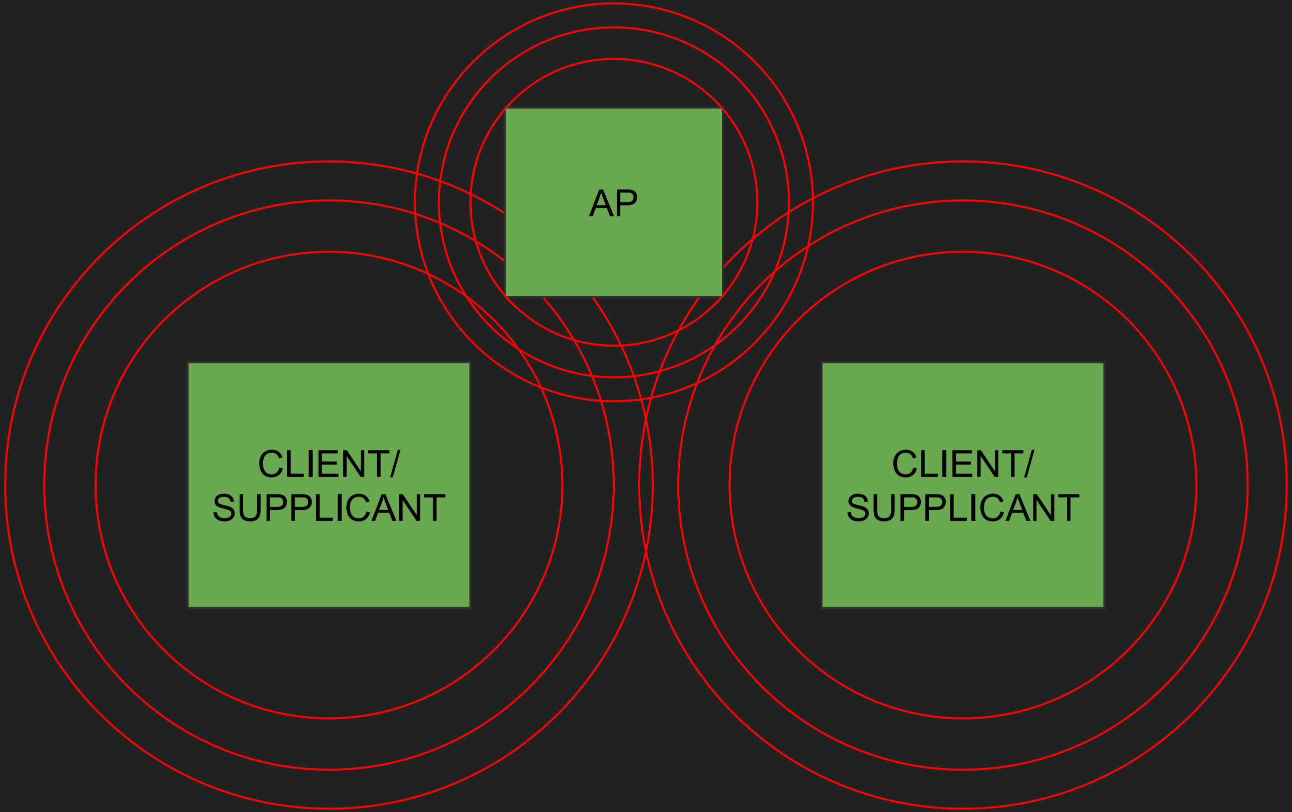
Network (IP)

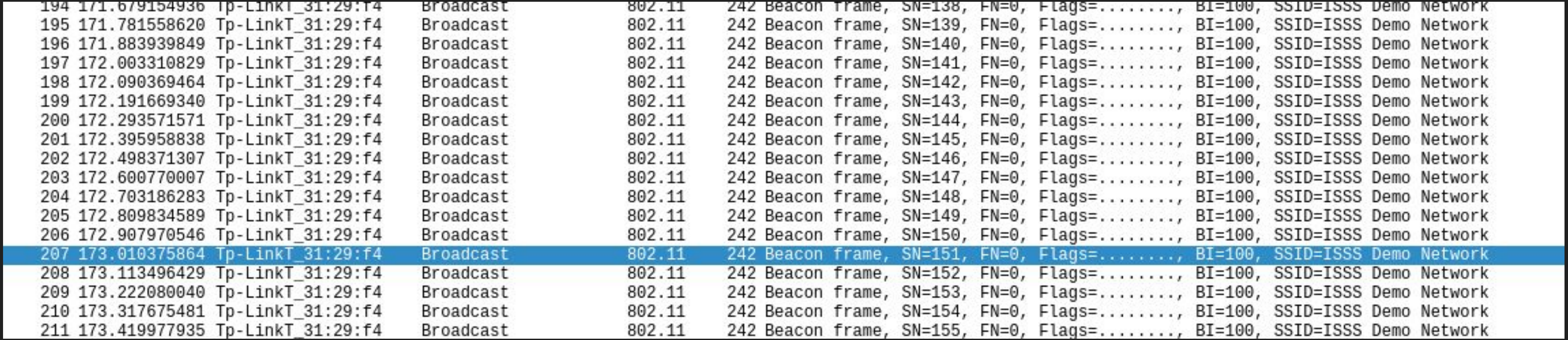
Data Link

Physical

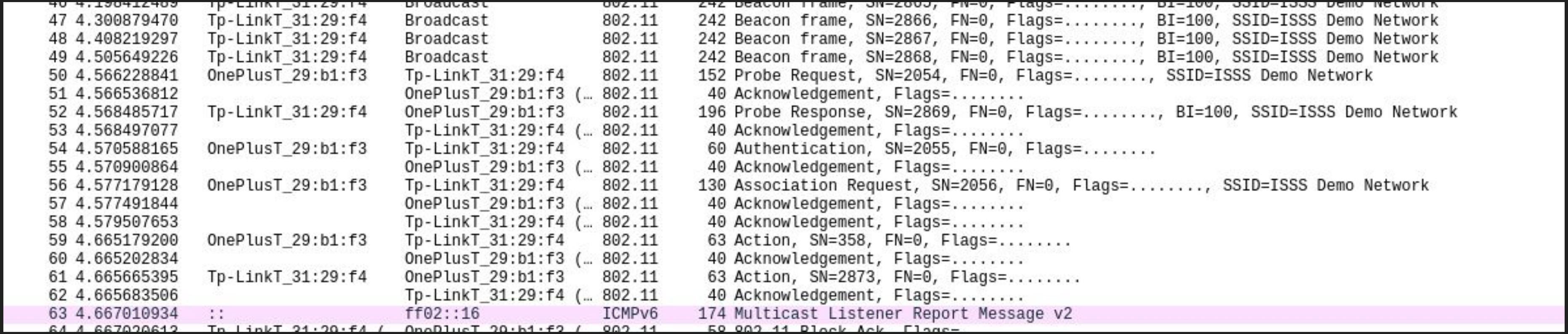
MAC Addresses

FC:FC:48:00:00:00


AP
CLIENT/ SUPPLICANT
CLIENT/ SUPPLICANT



```
194 171.679154936 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=138, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
195 171.781558620 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=139, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
196 171.883939849 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=140, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
197 172.003310829 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=141, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
198 172.090369464 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=142, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
199 172.191669340 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=143, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
200 172.293571571 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=144, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
201 172.395958838 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=145, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
202 172.498371307 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=146, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
203 172.600770007 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=147, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
204 172.703186283 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=148, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
205 172.809834589 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=149, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
206 172.907970546 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=150, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
207 173.010375864 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=151, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
208 173.113496429 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=152, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
209 173.222080040 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=153, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
210 173.317675481 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=154, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
211 173.419977935 Tp-LinkT_31:29:f4     Broadcast           802.11     242 Beacon frame, SN=155, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
```



```
 46 4.198412489   Tp-LinkT_31:29:f4    Broadcast             802.11     242 Beacon frame, SN=2865, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
 47 4.300879470   Tp-LinkT_31:29:f4    Broadcast             802.11     242 Beacon frame, SN=2866, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
 48 4.408219297   Tp-LinkT_31:29:f4    Broadcast             802.11     242 Beacon frame, SN=2867, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
 49 4.505649226   Tp-LinkT_31:29:f4    Broadcast             802.11     242 Beacon frame, SN=2868, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
 50 4.566228841   OnePlusT_29:b1:f3    Tp-LinkT_31:29:f4     802.11     152 Probe Request, SN=2054, FN=0, Flags=........, SSID=ISSS Demo Network
 51 4.566536812                        OnePlusT_29:b1:f3 (… 802.11      40 Acknowledgement, Flags=........
 52 4.568485717   Tp-LinkT_31:29:f4    OnePlusT_29:b1:f3     802.11     196 Probe Response, SN=2869, FN=0, Flags=........, BI=100, SSID=ISSS Demo Network
 53 4.568497077                        Tp-LinkT_31:29:f4 (… 802.11      40 Acknowledgement, Flags=........
 54 4.570588165   OnePlusT_29:b1:f3    Tp-LinkT_31:29:f4     802.11      60 Authentication, SN=2055, FN=0, Flags=........
 55 4.570900864                        OnePlusT_29:b1:f3 (… 802.11      40 Acknowledgement, Flags=........
 56 4.577179128   OnePlusT_29:b1:f3    Tp-LinkT_31:29:f4     802.11     130 Association Request, SN=2056, FN=0, Flags=........, SSID=ISSS Demo Network
 57 4.577491844                        OnePlusT_29:b1:f3 (… 802.11      40 Acknowledgement, Flags=........
 58 4.579507653                        Tp-LinkT_31:29:f4 (… 802.11      40 Acknowledgement, Flags=........
 59 4.665179200   OnePlusT_29:b1:f3    Tp-LinkT_31:29:f4     802.11      63 Action, SN=358, FN=0, Flags=........
 60 4.665202834                        OnePlusT_29:b1:f3 (… 802.11      40 Acknowledgement, Flags=........
 61 4.665665395   Tp-LinkT_31:29:f4    OnePlusT_29:b1:f3     802.11      63 Action, SN=2873, FN=0, Flags=........
 62 4.665683506                        Tp-LinkT_31:29:f4 (… 802.11      40 Acknowledgement, Flags=........
 63 4.667010934   ::                   ff02::16              ICMPv6     174 Multicast Listener Report Message v2
 64 4.667020613   Tp-LinkT_31:29:f4 (… OnePlusT_29:b1:f3 (… 802.11      58 802.11 Block Ack, Flags=
```

Crypto on WiFi

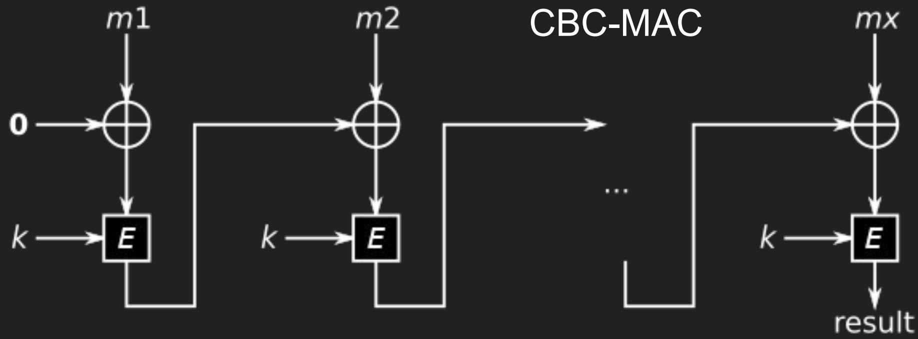
- Open network
- WEP
- WPA
- WPA2
  - PSK
  - Enterprise
- WPA3
  - PSK
  - Enterprise

WPA2

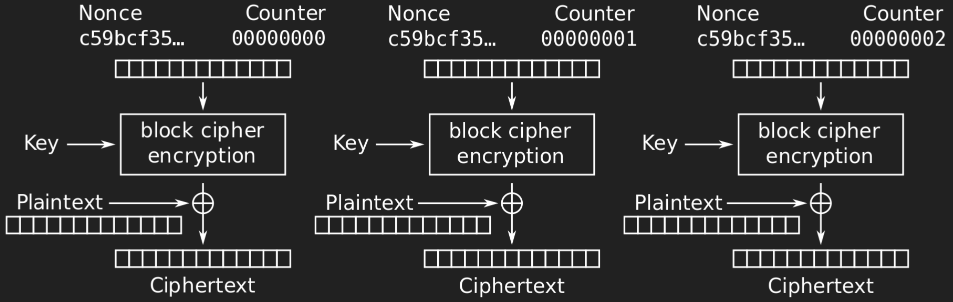
- PSK (pre-shared key)
    - Mostly used in homes
    - Password shared with everyone on the network
- Enterprise
    - Mostly used in businesses
    - Allows more flexible authentication
    - Authenticate via central database
    - Individual authentication tokens

Encrypting Data

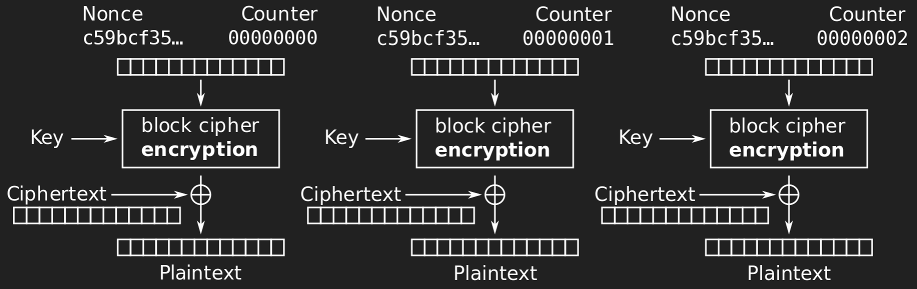
- Data is encrypted using AES CCM with 128 bit keys
  - AES in CTR mode
  - CBC-MAC associated data and ciphertext



CBC-MAC



Counter (CTR) mode encryption



Counter (CTR) mode decryption

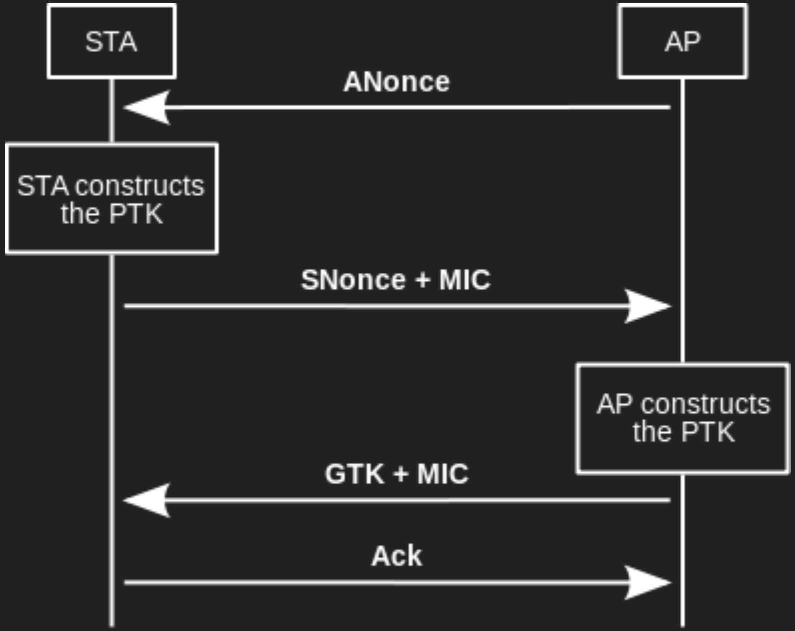
Encrypting Data

- Shared keys need to be established
- Unicast communication (supplicant to AP) requires PTK (pairwise transient key)
- Multicast communication (supplicant to supplicant) can use GTK (group temporal key)

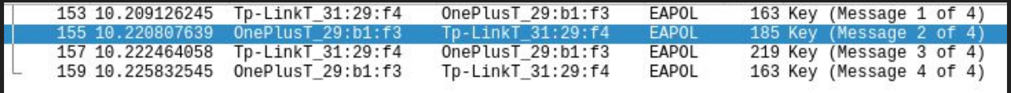
4 Way Handshake

- There is 4 message handshake to establish the PTK and GTK
- Assume there is a known and shared PMK (pairwise master key)
- Derive a PTK in a way that proves both the supplicant and the access point know the PMK
- Don’t transmit the PMK

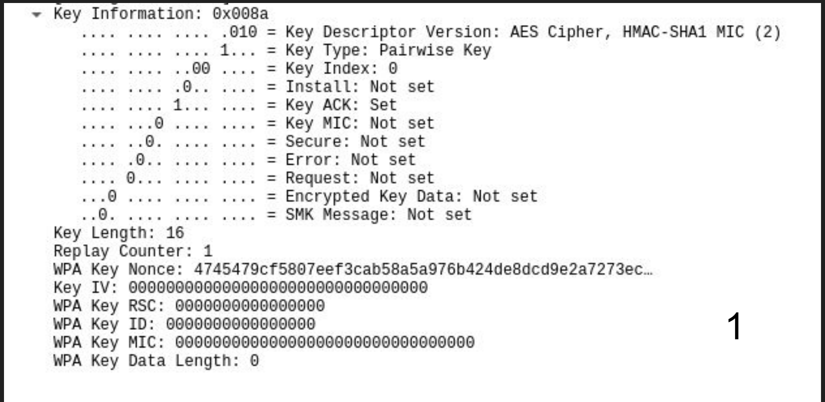
4 Way Handshake



4 Way Handshake

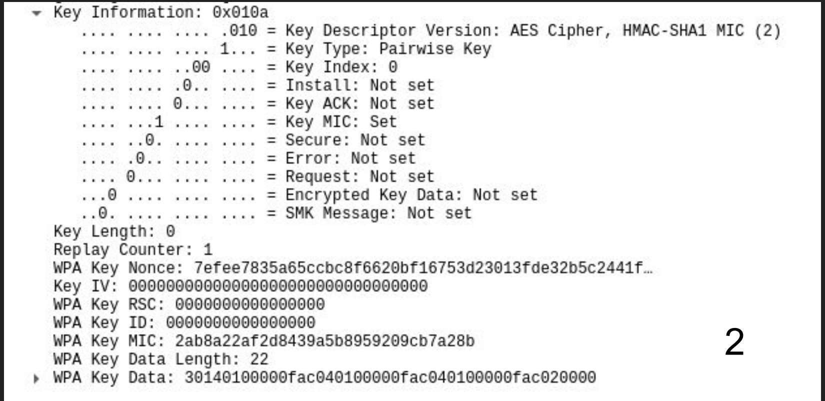


```
153 10.209126245  Tp-LinkT_31:29:f4    OnePlusT_29:b1:f3    EAPOL    163 Key (Message 1 of 4)
155 10.220807639  OnePlusT_29:b1:f3    Tp-LinkT_31:29:f4    EAPOL    185 Key (Message 2 of 4)
157 10.222464058  Tp-LinkT_31:29:f4    OnePlusT_29:b1:f3    EAPOL    219 Key (Message 3 of 4)
159 10.225832545  OnePlusT_29:b1:f3    Tp-LinkT_31:29:f4    EAPOL    163 Key (Message 4 of 4)
```



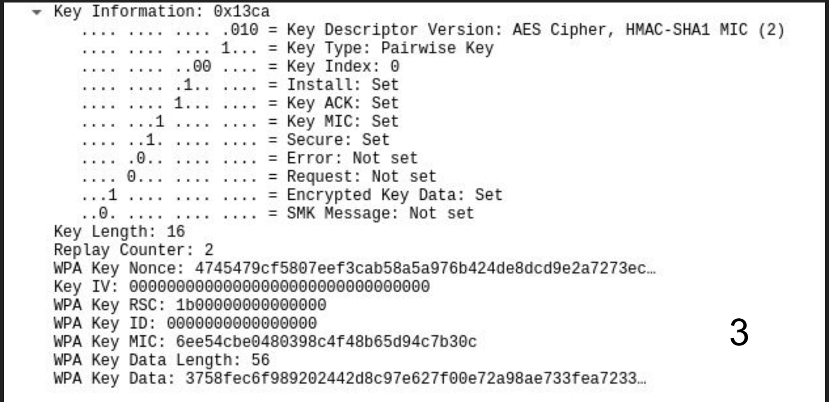
```
▾ Key Information: 0x008a
    .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
    .... .... .... 1... = Key Type: Pairwise Key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install: Not set
    .... .... 1... .... = Key ACK: Set
    .... ...0 .... .... = Key MIC: Not set
    .... ..0. .... .... = Secure: Not set
    .... .0.. .... .... = Error: Not set
    .... 0... .... .... = Request: Not set
    ...0 .... .... .... = Encrypted Key Data: Not set
    ..0. .... .... .... = SMK Message: Not set
  Key Length: 16
  Replay Counter: 1
  WPA Key Nonce: 4745479cf5807eef3cab58a5a976b424de8dcd9e2a7273ec…
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 00000000000000000000000000000000
  WPA Key Data Length: 0
```

1



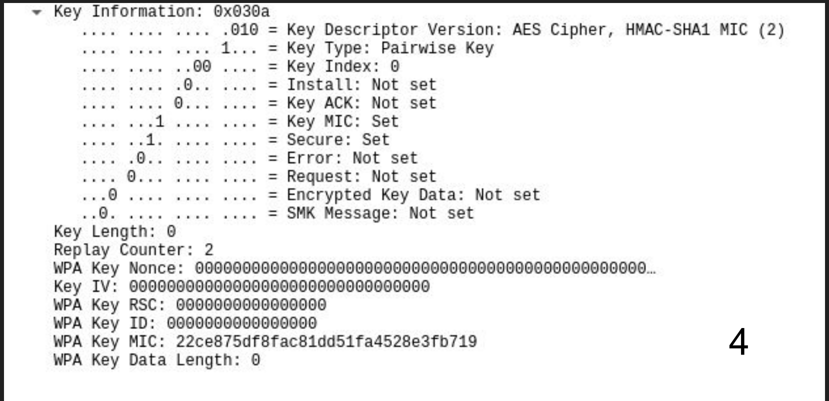
```
▾ Key Information: 0x010a
    .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
    .... .... .... 1... = Key Type: Pairwise Key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install: Not set
    .... .... 0... .... = Key ACK: Not set
    .... ...1 .... .... = Key MIC: Set
    .... ..0. .... .... = Secure: Not set
    .... .0.. .... .... = Error: Not set
    .... 0... .... .... = Request: Not set
    ...0 .... .... .... = Encrypted Key Data: Not set
    ..0. .... .... .... = SMK Message: Not set
  Key Length: 0
  Replay Counter: 1
  WPA Key Nonce: 7efee7835a65ccbc8f6620bf16753d23013fde32b5c2441f…
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 2ab8a22af2d8439a5b8959209cb7a28b
  WPA Key Data Length: 22
▸ WPA Key Data: 30140100000fac040100000fac040100000fac020000
```

2



```
▾ Key Information: 0x13ca
    .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
    .... .... .... 1... = Key Type: Pairwise Key
    .... .... ..00 .... = Key Index: 0
    .... .... .1.. .... = Install: Set
    .... .... 1... .... = Key ACK: Set
    .... ...1 .... .... = Key MIC: Set
    .... ..1. .... .... = Secure: Set
    .... .0.. .... .... = Error: Not set
    .... 0... .... .... = Request: Not set
    ...1 .... .... .... = Encrypted Key Data: Set
    ..0. .... .... .... = SMK Message: Not set
  Key Length: 16
  Replay Counter: 2
  WPA Key Nonce: 4745479cf5807eef3cab58a5a976b424de8dcd9e2a7273ec…
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 1b00000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 6ee54cbe0480398c4f48b65d94c7b30c
  WPA Key Data Length: 56
  WPA Key Data: 3758fec6f989202442d8c97e627f00e72a98ae733fea7233…
```

3



```
▾ Key Information: 0x030a
    .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
    .... .... .... 1... = Key Type: Pairwise Key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install: Not set
    .... .... 0... .... = Key ACK: Not set
    .... ...1 .... .... = Key MIC: Set
    .... ..1. .... .... = Secure: Set
    .... .0.. .... .... = Error: Not set
    .... 0... .... .... = Request: Not set
    ...0 .... .... .... = Encrypted Key Data: Not set
    ..0. .... .... .... = SMK Message: Not set
  Key Length: 0
  Replay Counter: 2
  WPA Key Nonce: 000000000000000000000000000000000000000000000000…
  Key IV: 00000000000000000000000000000000
  WPA Key RSC: 0000000000000000
  WPA Key ID: 0000000000000000
  WPA Key MIC: 22ce875df8fac81dd51fa4528e3fb719
  WPA Key Data Length: 0
```

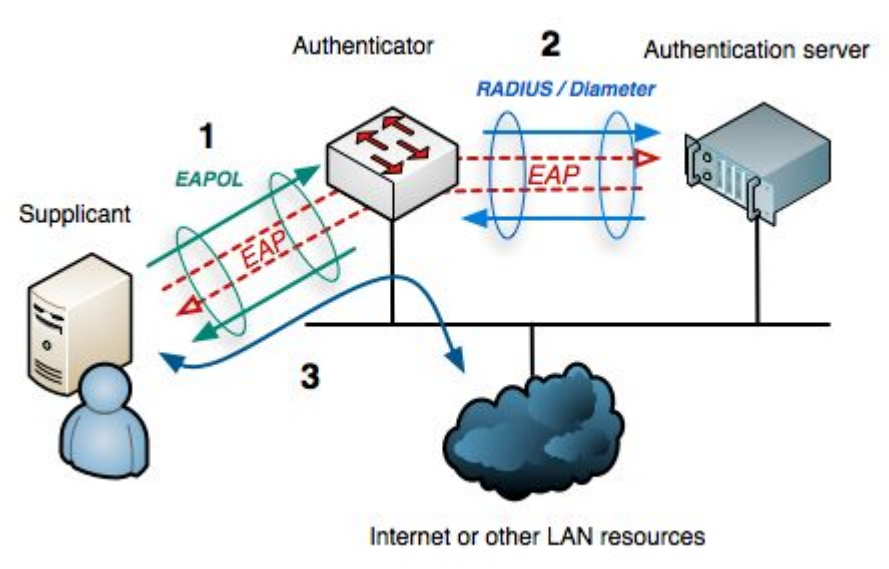
4

PSK

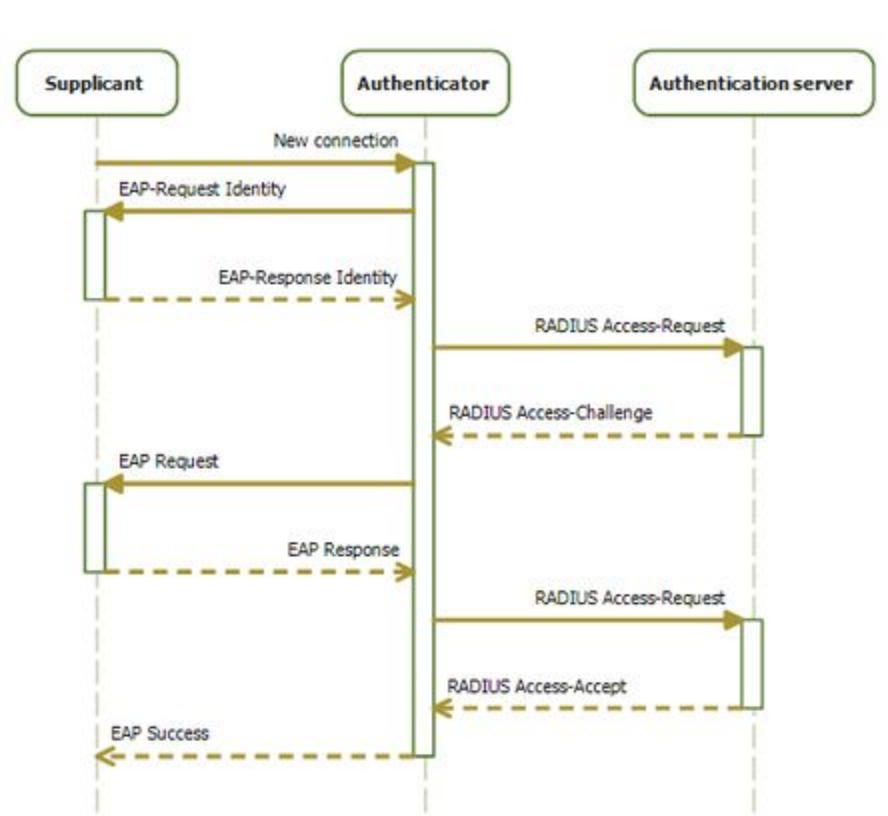
- Shared password between all supplicants
- PMK is the PSK
- PSK is derived from the passphrase
    - PBKDF2(HMAC−SHA1, passphrase, ssid, 4096, 256)
    - ssid is the salt
    - 256 bit output
    - 4096 iterations
    - HMAC-SHA1 as the PRF
- Weak PSKs can be guessed in an offline dictionary attack
- All supplicants can snoop on traffic

Enterprise

- Enterprise WiFi allows for more customized authentication
- 802.1X is the name of the standard
- PSK is derived during authentication
- An authentication server is needed
    - Can also do accounting (for billing)
    - Communicates via RADIUS



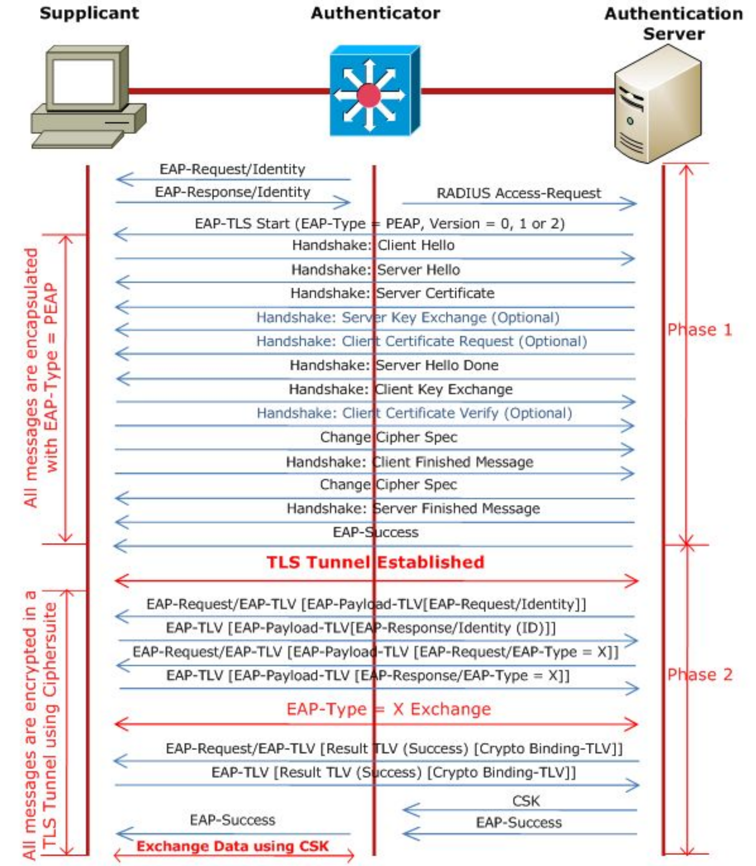
EAP (extensible authentication protocol)



PEAPv0-MSCHAPv2

- PEAP (protected extensible authentication protocol) wraps EAP in a TLS tunnel
  - Use certificates to verify the AP
- Another authentication protocol relying on EAP can run inside
- MSCHAPv2 (Microsoft challenge handshake authentication protocol version 2) takes a username and password
  - Mutual authentication
  - Both RADIUS server and supplicant must know the NTLM hash of the password
  - Severely broken (at most 2^56 DES encryption operations to find the NTLM hash of the password)

PEAP



Supplicant

Authenticator

Authentication Server

EAP-Request/Identity

EAP-Response/Identity

RADIUS Access-Request

EAP-TLS Start (EAP-Type = PEAP, Version = 0, 1 or 2)

Handshake: Client Hello

Handshake: Server Hello

Handshake: Server Certificate

Handshake: Server Key Exchange (Optional)

Handshake: Client Certificate Request (Optional)

Handshake: Server Hello Done

Handshake: Client Key Exchange

Handshake: Client Certificate Verify (Optional)

Change Cipher Spec

Handshake: Client Finished Message

Change Cipher Spec

Handshake: Server Finished Message

EAP-Success

TLS Tunnel Established

EAP-Request/EAP-TLV [EAP-Payload-TLV[EAP-Request/Identity]]

EAP-TLV [EAP-Payload-TLV[EAP-Response/Identity (ID)]]

EAP-Request/EAP-TLV [EAP-Payload-TLV [EAP-Request/EAP-Type = X]]

EAP-TLV [EAP-Payload-TLV [EAP-Response/EAP-Type = X]]

EAP-Type = X Exchange

EAP-Request/EAP-TLV [Result TLV (Success) [Crypto Binding-TLV]]

EAP-TLV [Result TLV (Success) [Crypto Binding-TLV]]

CSK

EAP-Success

EAP-Success

Exchange Data using CSK

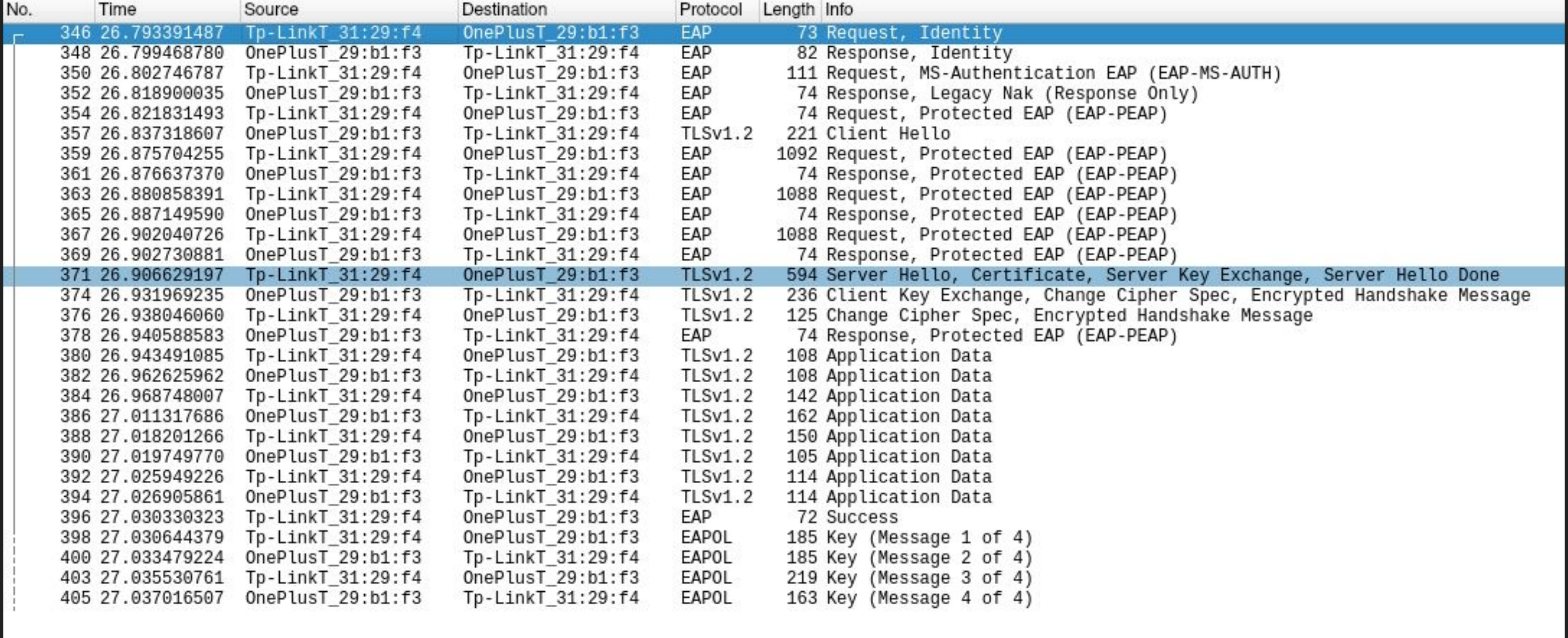
Phase 1

Phase 2

All messages are encapsulated with EAP-Type = PEAP

All messages are encrypted in a TLS Tunnel using Ciphersuite

Example



```
No.   Time          Source              Destination         Protocol  Length Info
  346 26.793391487  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   EAP          73 Request, Identity
  348 26.799468780  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   EAP          82 Response, Identity
  350 26.802746787  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   EAP         111 Request, MS-Authentication EAP (EAP-MS-AUTH)
  352 26.818900035  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   EAP          74 Response, Legacy Nak (Response Only)
  354 26.821831493  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   EAP          74 Request, Protected EAP (EAP-PEAP)
  357 26.837318607  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   TLSv1.2     221 Client Hello
  359 26.875704255  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   EAP        1092 Request, Protected EAP (EAP-PEAP)
  361 26.876637370  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   EAP          74 Response, Protected EAP (EAP-PEAP)
  363 26.880858391  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   EAP        1088 Request, Protected EAP (EAP-PEAP)
  365 26.887149590  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   EAP          74 Response, Protected EAP (EAP-PEAP)
  367 26.902040726  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   EAP        1088 Request, Protected EAP (EAP-PEAP)
  369 26.902730881  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   EAP          74 Response, Protected EAP (EAP-PEAP)
  371 26.906629197  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   TLSv1.2     594 Server Hello, Certificate, Server Key Exchange, Server Hello Done
  374 26.931969235  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   TLSv1.2     236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  376 26.938046060  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   TLSv1.2     125 Change Cipher Spec, Encrypted Handshake Message
  378 26.940588583  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   EAP          74 Response, Protected EAP (EAP-PEAP)
  380 26.943491085  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   TLSv1.2     108 Application Data
  382 26.962625962  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   TLSv1.2     108 Application Data
  384 26.968748007  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   TLSv1.2     142 Application Data
  386 27.011317686  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   TLSv1.2     162 Application Data
  388 27.018201266  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   TLSv1.2     150 Application Data
  390 27.019749770  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   TLSv1.2     105 Application Data
  392 27.025949226  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   TLSv1.2     114 Application Data
  394 27.026905861  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   TLSv1.2     114 Application Data
  396 27.030330323  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   EAP          72 Success
  398 27.030644379  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   EAPOL       185 Key (Message 1 of 4)
  400 27.033479224  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   EAPOL       185 Key (Message 2 of 4)
  403 27.035530761  Tp-LinkT_31:29:f4   OnePlusT_29:b1:f3   EAPOL       219 Key (Message 3 of 4)
  405 27.037016507  OnePlusT_29:b1:f3   Tp-LinkT_31:29:f4   EAPOL       163 Key (Message 4 of 4)
```

Breaking MSCHAPv2

https://youtu.be/gkPvZDcrLFk