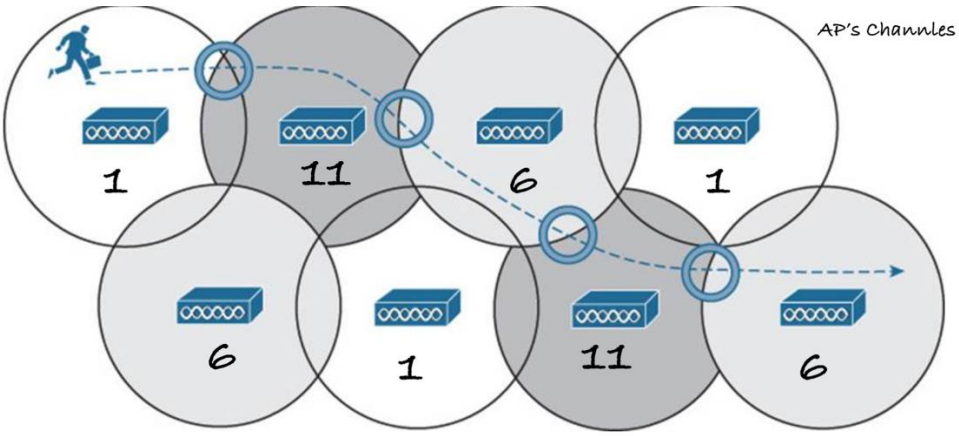
Wireless Signals and Modulation-2

Wireless Roam and Location Services

İstemcilerin bir AP üzerinde bulunan bağlantısının bir diğer AP'e aktarılması sürecidir. Normal şartlarda ek bir konfigürasyon yapılmadığı takdirde istemci tarafında bağlı olunan AP'in kapsama alanından çıkış yapılmadığı sürece bir diğer AP'e bağlanılmaz (Bu duru istemciden istemciye farklılık gösterebilir). SSID değerleri aynı verildiği taktirde WLC veya AP tarafında ek bir konfigürasyona gerek kalmadan bu süreç sağlanabiliyor.

İki AP'in kesiştiği noktada istemciler networke bağlanmak istediğinde WLC üzerinden AP'ler arasında istemciye gönderilen paketlerde AP'lerden birinin dönmemesi veya daha geç dönüş yapması sağlanabiliyor. Bu sayede iki AP'in kapsama alanının kesiştiği konumlarda hangi istemcinin hangi AP'e bağlanılacağı (ilk mesajı dönen AP'e) belirlenebiliyor (Aynı zamanda istemciler AP'ler arasında paylaştırılabiliyor).



İstemci bir hücreden diğer bir hücreye (Cell) geçiş yapacağı esnada yeniden kimlik denetimi sürecine girer. Bu işlem çok kısa sürelerde gerçekleşse de geçiş sırasına isteğe bağlı istemcinin her AP geçişinde yeni ip adresi talep etmeye zorlanması gibi farklı konfigürasyonlar da uygulanabiliyor. Bu gibi uygulamalar geçiş sürecinin uzamasına neden olacaktır.

Kablosuz IP telefon gibi en küçük kesintilerden dahi etkilenecek sistemler kullanılıyorsa geçiş sürecindeki kimlik denetiminde harcana süre önem kazanabiliyor. Bu nedenle geçiş sürecindeki kimlik denetim sürecini istemci tarafında hızlandıracak çözümler kullanılabiliyor (Bunun için istemci NIC kartının sürücü yazılımı bu özellikleri desteklemesi gerekiyor). Bu çözümlere bakıldığında;

- **CCKM** (Cisco Centralized Key Management), bir WLC CCKM sunucusu olarak ayarlanıyor. İstemcilerin AP'e yani networke bağlanırken kimlik denetiminden geçtikten sonra güvenli iletişim kurabilmek için şifreleme sürecinde kullanılacak anahtar bilgileri (anahtar oluştururken kullanılacak bilgiler) paylaşılır. CCKM çözümü ise bu anahtarların depolanmasını temel alan çözümdür (Anahtarı oluşturmak için çok fazla zaman ve kaynak harcanıyor). İstemci kimlik denetimini geçtikten sonra her AP geçişinde yeniden anahtar oluşturmasına gerek kalmasın diye bu bilgileri WLC zerinde

oluşturduğu CCKM sunucusunda depoluyor. Bu sayede şifreleme süreci için yeniden anahtar oluşturma gibi işlemlere zaman harcanmasına gerek kalmıyor.
    - Bu çözümün ilk çıktığı zamanlarda CCKM sunucusu bir AP üzerinde tanımlanabiliyordu. CCKM sunucusu olan AP, anahtar bilgilerini istemcinin geçiş yaptığı AP'e de öğreterek anahtar üretme süreci elemine edilebiliyordu.
- **Key Caching**, kimlik denetimi gerçekleştirildikten sonra AP'lerin istemci bilgilerini önbellek alanına kaydederek istemcinin farklı AP'ler üzerinden yeniden aynı AP'e geldiklerinde önbelleklerine kaydedilen bilgiler doğrultusunda istemcilerin bağlantılarının devam edilmesini temel alan çözümdür.
    - Autonomous topoloji kullanıldığında AP'ler aynı SSID değeriyle yayın yapabiliyorlar. İstemciler ise AP'lere kayıt olma sürecinde SSID değeriyle beraber AP'in MAC adres bilgisini de kayıt altına alırlar. Bu sayede AP'leri birbirinden ayırt edebiliyor. Yani AP'leri MAC adreslerine göre ayırt ederek daha önce bağlandığı AP olup olmadığını tespit edip daha önce bağlandığı AP'lerden biriyse istemci de daha önce kaydettiği (kayıtlı) anahtar bilgilerini kullanarak bağlantısına devam edebiliyor.
- **802.11r**, CCKM çözümünün Open Standart karşılığıdır.
    - Her üç çözümde de AP değişiminde kimlik denetimi gerçekleştiriliyor. Sadece şifreleme sürecinde kullanılan anahtar bilgileri üzerinde tasarruf sağlanmaya çalışılıyor.
    - Açıklamalardan da anlaşılacağı gibi istemcilerin de bu özellikleri destekleyen sürücü yazılımlarına sahip olması/desteklemesi gerekiyor.

Multi Controller

Kapsama alanının geniş olduğu veya AP sayısının yüksek olduğu durumlarda birden fazla WLC kullanılması gerekebiliyor. Aynı kapsama alanı altında (WLC'lere bağlı AP'lerin kesiştiği yerler bulunuyorsa) birden fazla WLC kullanılması durumunda WLC'ler arası haberleşme süreci de önem taşıyor. Bu durumda WLC'ler aynı/tek bir ip adresi üzerinde tek bir SSID ile yayın yapıyorlarsa aralarında bilgi paylaşımı yapılarak roaming gibi özelliklerin desteklenmesi sağlanabiliyor.

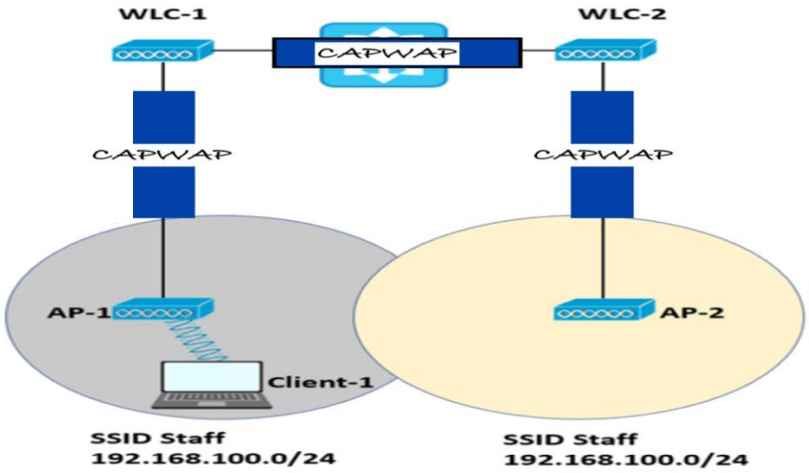
- Kapsama alanları kesişmediği/farklı konumlarda bulunduğu durumda WLC'ler farklı ip adresiyle de farklı SSID değeriyle de yayın yapmaları sorun yaşatmayacaktır. İstemci bir WLC'ye bağlı AP'lerin kapsama alanı bittiği yerde farklı bir WLC'nin kapsama alanındaki AP'lere bağlanırken yeniden kimlik doğrulama, ip bilgisi alma gibi işlemleri yapması gerekecektir.

Birden fazla WLC kullanılan topolojilerde WLC'lerin farklı konumlarda (birbirinden çok uzak) bulunmasına rağmen kullanıcıların her iki konumda da aynı ip adresiyle yapılan yayına bağlanması istendiğinde ek çözümler gerekebiliyor. Bir örnek üzerinden açıklamak istendiğinde;
*** Bir kurumun dört farklı şehirde şubeleri olduğunu düşünelim. Kullanıcıların hangi şehirdeki şubeye giderse gitsin cihallarının kablosuz yayına otomatik olarak bağlanması isteniyor. Bunu sağlamak normal şartlarda mümkün değildir. Nedenine bakıldığında farkı WLC'lere bağlı AP'lerin aynı SSID ve ip adresiyle yayın yapması gerekecektir. WLC'ler farklı networklerde bulunduğundan farklı ip blokları kullanmak zorunda kalacak (bir routerun iki

arayüzü aynı networke dahil edilemez. Bu mümkün olsaydı bile ip adresleri aynı network içerisinde görüneceği için paketler routera/default gateway'e gönderilmezdi), dolayısıyla farklı ip adresleri atanması gerekecektir. Böyle bir durumda WLC'ler arası iletişimi sağlayabilmek ve aynı ip adresi ve SSID kullanılarak yayın yapılabilmesi için **Mobility Group Hierarchy** çözümü kullanılıyor.

Mobility Group Hierarchy, aralarında haberlşemesi istenen WLC'leri bir Mobility Group adında gruplara ekliyor. Bu gruplara eklenen WLC'ler aralarında CAPWAP tünel kurup haberleşme sürecini bu tünel üzerinden gerçekleştiriyorlar. CAPWAP tünel sayesinde paketlere WLC'lerin ip adres bilgileri ekleniyor ve network üzerinde herhangi bir sorun yaşamadan iletim süreci gerçekleştiriliyor. Paket kaynak WLC'den hedef WLC'ye ulaştığında kapsülden çıkarılarak yeniden kapsüllenip ilgili AP'e iletiliyor (Yani tek bir paket iletilirken 3 kez kapsüllenip dekapsüle ediliyor.). Bu sayede farklı WLC'ler üzerinden farklı konumlarda tek bir yayın yapılabiliyor.

Bu gibi durumlara daha çok kaynaklara sadece belirli ip adreslerinden erişim sağlanabilmesi için kısıtlamalar tanımlandığında ihtiyaç duyulabiliyor.



- Bu şekilde WLC'ler arasında roaming işlemi gerçekleştiriliyorsa istemcinin asıl bağlı olduğu WLC'ye **Anchor Controller** denirken, uzaktan asıl roaming sürecin yöneten WLC'ye **Foreign Controller** denilmektedir.

Location Devices in a Wireless Network

Sık karşılaşılacak durumlardan biri olmasa networke bağlı cihazları konumlarının tespit edilmesi istenebilir. Bunu sağlayabilmek için çeşitli yazılımlar kullanılarak (Cisco Wireless Location Appliances gibi) AP'lerin konumları manuel olarak tanımlanıp AP'lerin GPS mekanizması gibi (en az 3 AP'in gücüne göre cihazın konumuna referansı alınarak hesaplamalar yapılıyor) çalışarak cihaz konumlarını yaklaşık olarak tespit etmesi sağlanabiliyor.

- Sık kaybolan cihazlar takip edilebileceği gibi tehdit aktörlerinin de konumlarını tespit etmek için kullanılabilir.
- RFID Tags eklenerek networke bağlı cihazlar dışında insan, hayvan gibi nesnelerin de internete bağlanmaksızın takip edilmesi/konumlarının tespit edilmesi sağlanabiliyor.

Authentication Wireless Clients

Güvenlik konusu kablolu ortama kıyasla kablosuz ortamda çok daha dikkat edilmesi gereken konulardan biridir. Kablosuz ortamda güvenlik konusunu, networke bağlanma (kimlik denetimi) ve veri iletimi (şifreleme) olarak iki kısımda incelenebilir. Bu süreçte kullanılan tekniklere bakıldığında (Bir istemcini AP'e bağlanırken gerçekleştirdiği trafik akışı için https[:]//documentation.meraki.com/General_Administration/Tools_and_Troubleshooting/Analyzing_Wireless_Packet_Captures yazısını inceleyebilirsin. Kablosuz sürecinin kurulum ve konfigürasyonu CCNA notlarında bulunduğu için burada ayrıca açıklanmamıştır);

- **Open Authentication**, istemcilerin hiçbir kimlik denetiminden geçirilmeden networke bağlanabildikleri yöntemdir.
    - Günümüzde kafe, üniversite gibi ortamlarda yaygın olarak kullanılmaktadır.
    - Kimlik doğrulama işlemi daha çok Web Authentication (Captive Portal, Hotspot olarak da biliniyor) olarak bilinen sayfalar aracılığıyla gerçekleştiriliyor. Güvenli bir teknik değildir. Üzerine çeşitli saldırılar geliştirilebilir.
- **WEP (Wireless Encryption Protocol)**, kimlik denetimi yapılmamaktadır. Verileri şifreli iletmek için kullanılan anahtar bilgisi bulunmaktadır. Bu anahtar bağlantı süresince hiç değiştirilmeden kullanıldığı için bir istemcinin veri trafiği belirli bir süre dinlenerek kırılabildiği için günümüzde güvenli kabul edilmemektedir. Bu nedenle günümüzde kullanılmamaktadır.

- **Wi-Fi Protected Access (WPA) Pre-Shared Key (PSK)**, normalde bu teknikte de kimlik denetim mekanizması bulunmamaktadır (bağlantı sürecinde dikkat edilirse kullanıcı adı-parola bilgisi yerine sadece parola bilgisi soruluyor. Kimlik denetiminde kullanıcı adı ve parola bilgisi kontrol edilir). Kullanıcıların networke bağlanabilmeleri için bu anahtar (Master Key) bilgisini bilmesi gerekiyor. Master Key kullanılarak kullanıcı ve AP arasında gerçekleşen haberleşme sürecindeki şifreleme algoritmasında kullanılacak anahtarların oluşturulması sağlanıyor. Bu nedenle Master Key bilinmediği sürece kullanıcıya şifreleme algoritması için özel anahtar oluşturamayacak ve gönderdiği hiçbir trafik AP tarafından çözümlenemeyecektir. Dolayısıyla gönderdiği paketler de kablolu ortama aktarılamayacaktır.
    - **WPA1, Wi-Fi Alliance** adı verilen özel bir topluluk tarafından geliştirilmiştir. WEP tekniğinden farklı olarak belirli bir süre sonrasında şifreleme anahtarında kullanılan anahtarın değiştirilmesi sağlandı(TKIP-Temporal Key Integrity Protocol). Her ne kadar belirli bir noktaya kadar güvenli görünse de zaman içinde kırılmıştır.
    - **WPA2,** 802.11i olarak da bilinmektedir. IEEE tarafından çıkarılmıştır. WPA1'den farklı olarak WEP şifreleme algoritması yerine AES şifreleme algoritması kullanılmaya başlandı.
        - AES şifreleme algoritmasında kullanıcıya özel anahtar oluşturma (**Four-way Handshake** olarak biliniyor) sürecinde bir zafiyet keşfedildi. Yaması yayınlandı. Güncelleme üzerine bu zafiyet giderilebiliyor.
    - **WPA3**, WPA1 ve WPA2'ye kıyasla daha çok güvenlik önlemi içeren sürümüdür.
        - WPA1 ve WPA 2 versiyonlarında olduğu gibi ev kullanıcıları için Personal, kurumlar için Enterprise versiyonu bulunmaktadır.

- **EAP**, WPA Enterprise olarak da bilinir. L2 başlık bilgisinin önüne ek başlık bilgileri eklenerek kimlik denetimi gerçekleştiren teknolojiye verilen isimdir. Başlangıçta PAP (Password Authentication – Two-Way Authentication), CHAP (Challenge-Handshake Authentication Protocol) gibi çeşitli çözümler geliştirilse de kimlik denetim sürecini daha güvenli kılabilmek için çeşitli EAP çözümleri geliştirilmiştir (**EAP-MD5**, **Peap**, **EAP-TTLS** …). Kimlik denetimi sürecinde kullanılan terimlere bakıldığında;
    - **Supplicant**, kimlik denetiminden geçirilecek istemciye verilen isimdir.
    - **Authenticator**, kimlik denetiminden geçirecek cihaza verilen isimdir (Bu cihaz topolojiye göre bir WLC veya AP olabilir).
    - **Authentication Server**, kimlik denetimi sürecinde üzerinde kimlik denetim bilgilerinin tutulduğu sunucu/veritabanına verilen isimdir (RADIUS gibi).
        - RADIUS sunucusu desteklendiği taktirde WLC üzerinde oluşturulabileceği gibi farklı bir kaynak üzerinden de kullanılabilir.
        - Duruma göre yedekleme amacıyla birden fazla RADIUS sunucusu tanımı da yapılabiliyor.
        - RADIUS sunucusunun için iki farklı port numarası kullanılabiliyor (eski port numarası UDP 1645, yeni port numarası UDP 1812). WLC üzerinde konfigürasyon yaparken dikkat edilmesi gerekiyor.

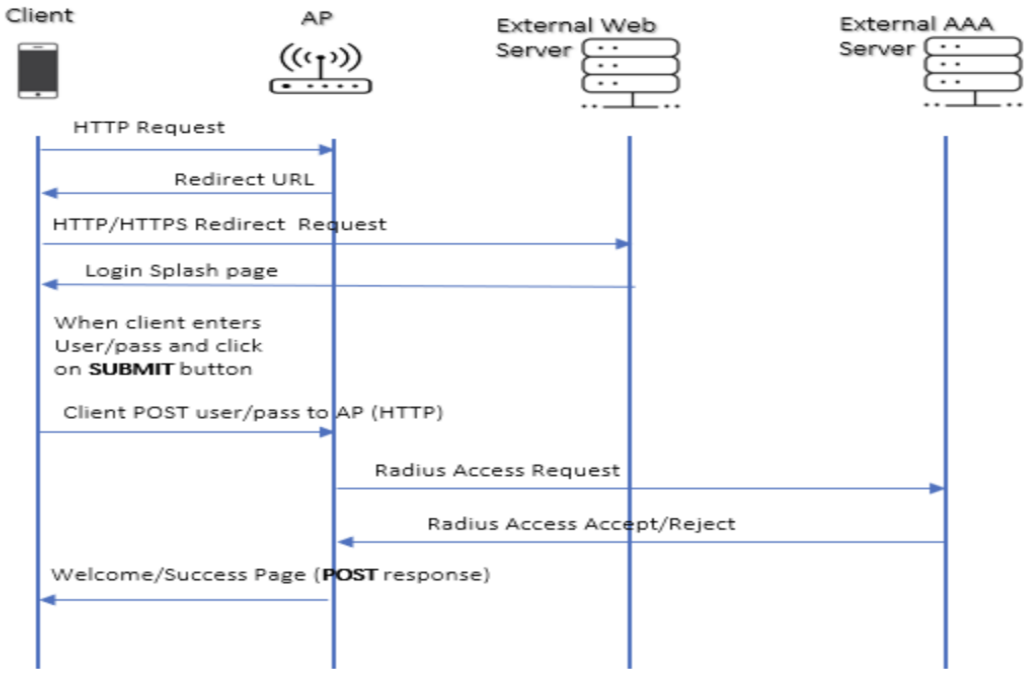
Authentication with WebAuth

Kimlik doğrulama işleminin network üzerinde (L2'de) yapmak yerine Web sayfası üzerinden gerçekleştirildiği tekniktir. Kimlik denetim süreci bu şekilde gerçekleştirilmek istendiğinde genelde network üzerinden (L2) Open Authentication kullanılıyor. Yani kimlik denetimi yapılmadan kullanıcıların networke bağlanması sağlanıyor. Network üzerinde Open Authentication kullanılabildiği gibi WPA-PSK veya EAP gibi çözümlerle birlikte kullanılarak da bu süreç işletilebiliyor.

WebAuth ile kimlik denetimi aslında network üzerinde L3 seviyesinde paketlerin bir kimlik denetimi sunucusuna yönlendirilmesiyle gerçekleşiyor. Kullanıcı bu sayede kimlik denetimi sayfasına ulaşabiliyor.
WebAuth tekniğinde kimlik denetimi gerçekleştirilmek istendiğinde bunu gerçekleştirebilmek için çeşitli seçenekler bulunuyor. Bu seçeneklere bakıldığında (Detaylı bilgi içi https[:]//www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/71881-ext-web-auth-wlc.html ve https[:]//mrncciew.com/2013/03/21/wlc-web-authentication/ adreslerini ziyaret edebilirsin);

- WLC üzerinde bir veritabanı tanımlanıp kimlik denetiminin bu veritabanı üzerinden gerçekleştirilmesi sağlanabiliyor.
- RADIUS, LDAP gibi harici sunucular üzerinden gerçekleştirilmesi sağlanabiliyor.
- Web sayfası harici bir kaynağa yönlendirilerek kimlik denetiminin orada yapılması sağlanabiliyor.
- Kullanıcıya bir web sayfası çıkarılarak sadece bilgilendirme yapılıp geçiş yapması sağlanabiliyor (Kimlik denetimi yapılmıyor. Bu seçenek **Passthrough** olarak de biliniyor).
    - İsteğe bağlı olarak kullanıcının e-mail bilgisi girmesi de istenebiliyor.

- MAC adres bazında kimlik denetimi de yaptırılabiliyor. Kayıtlı olmayan MAC adresine sahip kullanıcı networke bağlanmak istediğinde kullanıcı Web Portal arayüzüne yönlendirilerek kimlik doğrulaması istenebiliyor (MAC adresleri değiştirilerek kimlik doğrulama süreci atlatılabilir).
- 802.1x ile birlikte (L2'de EAP veya WPA-PSK) kullanılarak kimlik denetimi gerçekleştiriliyor. L2 üzerinde kimlik doğrulama işlemi gerçekleştirildikten sonra bir AS (Authentication Server) üzerinden giriş yapan kullanıcı bilgilerine göre bir farklı WebAuth sayfaları kullanıcı cihazına gönderiyor. Kimlik doğrulama sürecinin bu şekilde uygulanmasına **Splash Page Web Redirect** deniliyor.



|→ Görselde önce web sayfasının gönderildiği görünüyor ama External Web Server ile External AAA Server trafik sırasının farklı olması gerektiğini düşünüyorum (internet üzerindeki görsellerde genel olarak durum böyleydi). Böyle düşünmemin nedeni L2'de kimlik denetimi yapılmadan istemci networke dahil olamayacak, dolayısıyla L3 üzerinden bir WebAuth sunucusuna yönlendiremeyecek olmasıdır.

- Splash Page Web Redirect tekniğine benzer olarak **Conditional Web Redirect** tekniği de uygulanabiliyor. Conditional Web Redirect tekniğinde isimden de anlaşılacağı üzere istemciye bir koşul karşılığında erişim izni veriliyor. Bu koşul sadece bilgilendirme yapmak için çıkarılan bir web sayfası olabileceği gibi networke bağlı kalabileceği süreyi sınırlandırmak gibi çeşitli politikaları uygulamak için de kullanılıyor.

PEAP, EAP-TTLS gibi tekniklerin kurulumu, konfigürasyonu ve çalışma mekanizması üzerine ayrıca bir doküman hazırlandığında aynı dizin altında bulabilirsin (23.v son 20m önemli).

NOTLAR:

- WPA2 sürümünde kullanılan AES şifreleme algoritması çalışırken çok yüksek kaynak harcamaktadır. Her kullanıcı için ayrı ayrı çalıştırılmaktadır. Bu nedenle ev kullanıcılarında Wifi üzerinden belirli bir kullanıcı sayısından fazla kullanıcı bağlandığında ADSL üzerindeki kaynaklar yetersiz kalacağı için çatlayacaktır.
- Cisco'nun RADIUS sunucusuna ISE (Cisco Identity Services Engine) denilmektedir.
- Kimlik denetimi merkezi bir sunucu üzerinden yaptırılıyorsa buna CWA (Central Web Authentication) da denilmektedir.