# IEEE 802.11 Frames

## فريمات الشبكات اللاسلكية

### تقرأ في هذا الفصل عن

- دور فريمات الشبكات اللاسلكية في الإتصال
- كيف يعلن الأكسس بوينت عن نفسه
- كيف يبحث الجهاز غن الأكسس بوينت
- فريمات التحكم و القيلولة اللاسلكية
- رحلة فريم الوايرلس الي الإيثرنت
- دور الفريم في ضبط السرعة
- دور الفريم في التوافق بين معايير اللاسلكي
- استخدام VLAN لضبط مسار الفريم

م / نادر المنسي

http://itech4arab.wordpress.com

# كيفية التراسل في الشبكات اللاسلكية

كما عرفنا مسبقا أن الشبكات اللاسلكية هي شبكات ترسل البيانات half-duplex اي أنها لا ترسل أو تستقبل في نفس الوقت و لهذا فإنه عند ارسال أكثر من جهاز في نفس الوقت تكون البيانات قابلة للتصادم و هذا يؤثر علي مدي امكانية استقبالها أو قرائتها و هذا يضطرنا لإرسالها مرة أخري مما يزيد في وقت الإرسال و الإستقبال و لهذا فإن الشبكات اللاسلكية تستخدم طريقة لتجنب هذا التصادم و هي تحسس القناة لتفادي التصادم(CSMA/CA) carrier sense multiple access collision avoidance

ومعني carrier sense هو قدرة المرسل علي تحسس قناة الإرسال لإكتشاف ما إن كان هناك من يرسل في نفس الوقت و سيظل ينتظر حتي يتبين له خلو الوسط و تسمي هذه الفترة بـ IFS و هي الفترة التني علي المرسل انتظارها حتي يرسل مرة أخري

و هناك أنواع لـIFS

■ Short interframe space (SIFS):

فترة زمنية بسيطة تستخدم عند لزوم ارسال الفريم بشكل سريع و كأنه يستعجل خلو القناة

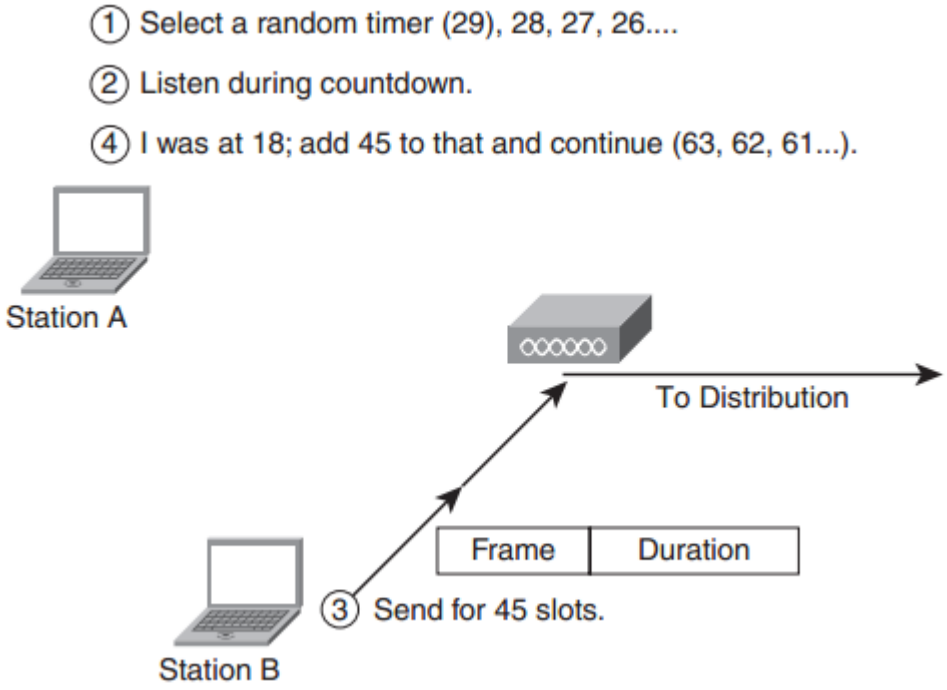
■ Point-coordination interframe space (PIFS):

فترة زمنية يستخدمها الأكسس بوينت لبدء التحكم في القناة

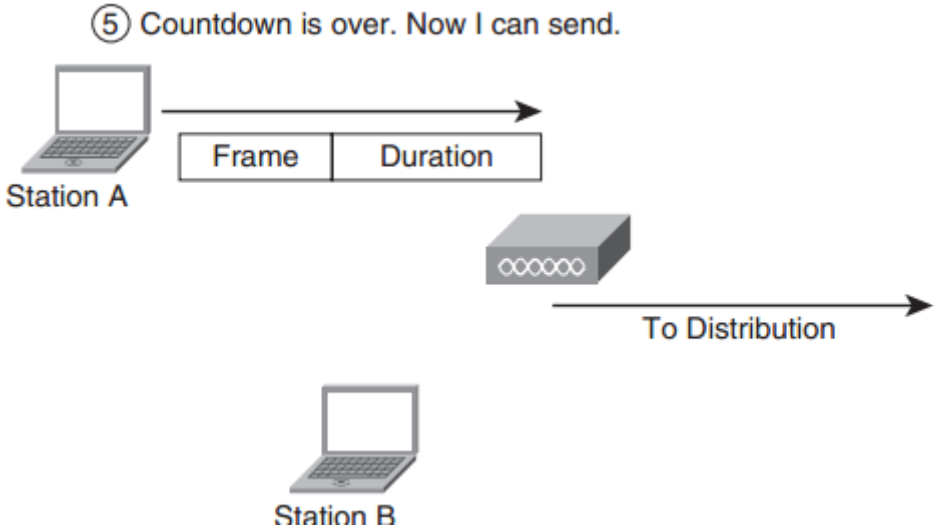
■ Distributed-coordination interframe space (DIFS):

تستخدم لإرسال البيانات أو بشكل اصح هي فترة زمنية بين كل فريم يرسل

و يبين الشكل التالي كيفية ارسال الفريم حيث يريد الجهاز A الإرسال و لهذا فيقوم بالإنصات للقناة و يتحسس خلوها في فترة زمنية تسمي backoff timer يقوم بما يشبه العد التنازلي بسرعة تسمي slottime و تختلف قيمها بيم معايير الوايرلس a, b, g.802.11
و دعونا نستخدم المثال التالي حيث لدينا جهاز A يريد الإتصال بالأكسس بوينت و هذا الشكل يبين خطوات هذا الإتصال




- يتخير الجهاز A توقيت رقمي عشوائي مثل 29
- يبدأ في العد التنازلي 29 – 28 – 27 – 26- 25 ... و هكذا و في أثناء العد يقوم بتحسس فيما ان كان هناك جهاز آخر يشغل القناة
- عندما يصل التايمر الي 18 يقوم الجهاز B بإرسال فريم برقم عددي 45 و ذلك حسب التعداد الذي ارتضاه عشوائيا
- يقوم الجهاز B بحجز القناة بواسطة مقدمة فريم Frame header تسمي network allocation vector (NAV)و من ثم ينتظر الجهاز A فترة زمنية SIF ليتأكد من خلو القناة يقوم الجهاز A بإضافة العدد45 الي الخاص بالجهاز B الي العدد 18 الذي بدأ العد به و يبدأ ي العد مرة أخري 63-6-61-.... و هكذا و تسمي الفترة الزمنية الكاملة التي ينتظرها بـ contention windowو عندما يصل الجهاز A الي العدد 0 هنا يتم التأكد من خلو القناة و يستطيع ارسال الفريم كما بالشكل التالي حيث



-عندما يفشل الجهاز من ارسال الفريم لأي سبب فإنه يقوم بإعادة العملية و اختيار تعداد عشوائي أكبر من سابقه

-عندما تنجح عملية الإرسال يتم ارسال رسالة تأكيد ACK بتوقيت SIFS timer حيث أنه أسرع التوقيتات المستخدمة

## أنواع فريمات الشبكات اللاسلكية

لا يتشابه ارسال الشبكات السلكية مع اللاسلكية الا من حيث استخدامها للعنوان الفيزيائي MAC address في الفريم Frame فالشبكات اللاسلكية تتراسل بطريقة مختلفةتماما عن الشبكات السلكية و لها ثلاثة أنواع من الفريم تستخدمهم للتراسل

■ Management frames:

و يستخدم عن الإتصال أو قطع الإتصال بالشبكة اللاسلكية

■ Control frames:

و يستخدم لمعرفة متي يتم استقبال فريم البيانات

■ Data frames:

و هو الفريم الحامل للبيانات

*Frame Types Table*

| Management | Control | Data |
|---|---|---|
| Beacon | Request to Send (RTS) | Simple data |
| Probe Request | Clear to Send (CTS) | Null function |
| Probe Response | Acknowledgment | Data+CF-ACK |
| Association Request | Power-Save-Poll (PS-Poll) | Data+CF-Poll |
| Association Response | Contention Free End (CF-End) | Data+CF-Ack |
| Authentication Request | Contention Free End + Acknowl-edgment (CF-End +ACK) | ACK+CF-Poll |
| Authentication Response | CF-ACK | |
| Deauthentication | CF-ACK+CF-Poll | |
| Reassociation request | | |
| Reassociation response | | |
| Announcement traffic indication message (ATIM) | | |
| Each frame type merits its own discussion to follow. | | |

## شكل فريم الشبكات اللاسلكية

يعتبر فريم الوايرلس أطول من فريم الشبكات الإيثرنت حيث يبلغ طوله 2346 بايت كحد أقصي فهو يبدأ

بمقدمة الفريم Preamble بطول 72 بت او 144 بت ثم يليها سبعة أجزاء

أولها fame control بطول 16 بت و يحدد الهدف من الفريم و سنشرح أجزاءه

ثانيها duration field بطول 16 بت مبينة المدة التي سينشغل الوسط بالفريم

ثالثهم ثلاثة عناوين فيزيائية MAC addresses بطول 18 بايت

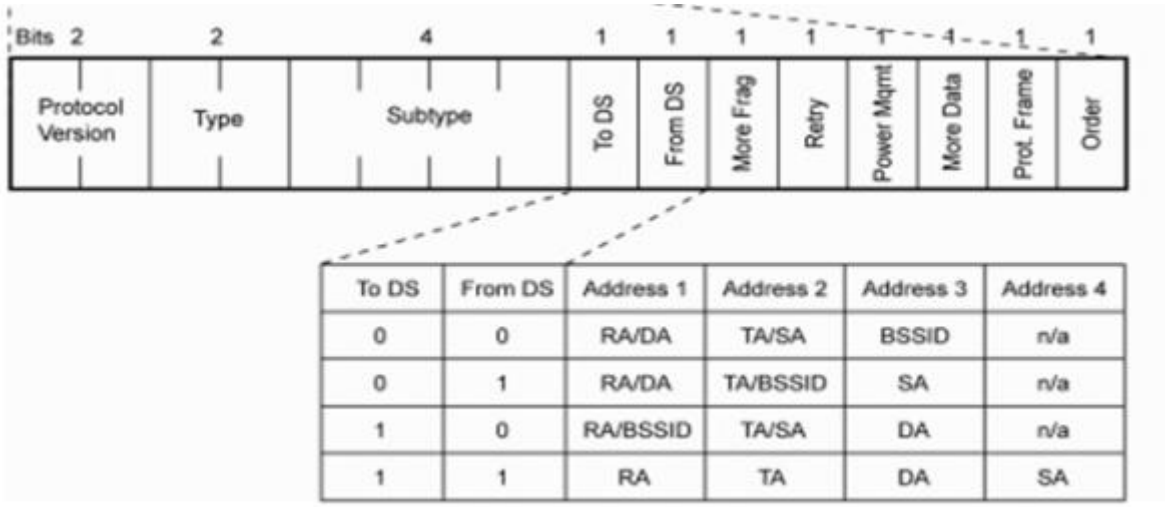
رابعهم sequence control field بطول 2بايت/16بت

خامسهم عنوان فيزيائي اضافي MAC address بطول 8بايت /64 بت

سادسهم frame body بطول 2304 بايت

سابعهم 4 بايت لجزء التحقق FCS) frame check sequence)

**الجزء الخاص بـ control.**




| To DS | From DS | Address 1 | Address 2 | Address 3 | Address 4 |
|---|---|---|---|---|---|
| 0 | 0 | RA/DA | TA/SA | BSSID | n/a |
| 0 | 1 | RA/DA | TA/BSSID | SA | n/a |
| 1 | 0 | RA/BSSID | TA/SA | DA | n/a |
| 1 | 1 | RA | TA | DA | SA |

يحدد هذا الجزء كما قلنا مهمة الفريم و يحتوي علي حقول فرعية أهمها حقل Type و يحدد نوع الفريم data او control أو management و بعض الحقول الباقية تبين اتجاه البيانات مرسلة أو مستقبلة طبقا للعناوين الفيزيائية

**الجزء الخاص بالعناوين الفيزيائية**

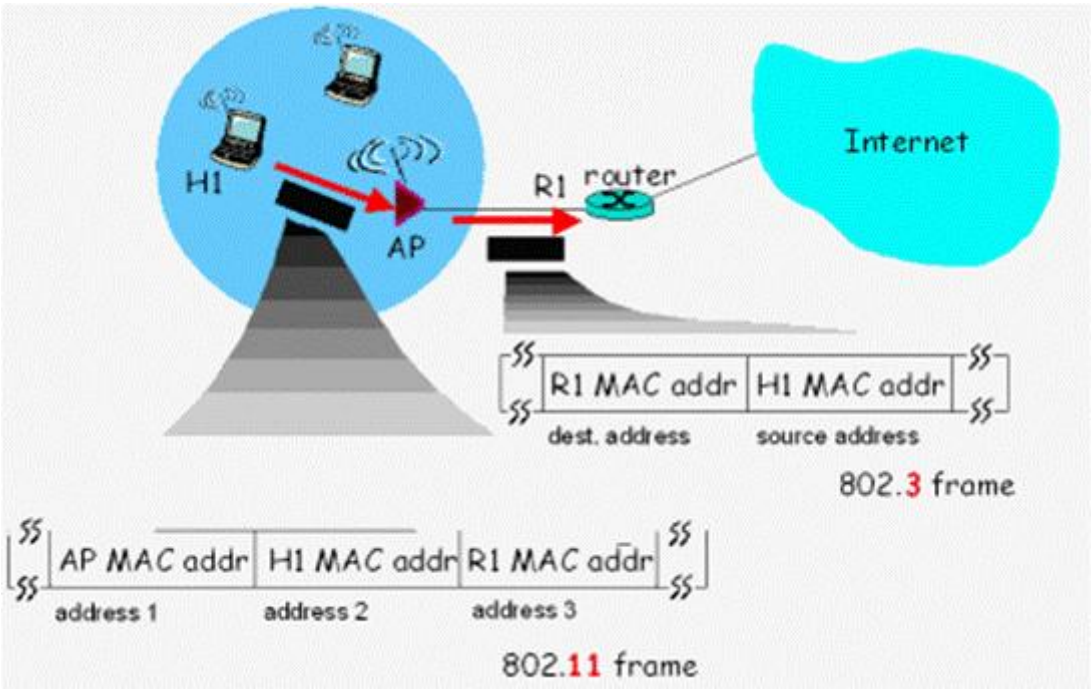
فريم الوايرلس يحتوي علي أربع عناوين فيزيائية بحد أقصي

عنوان المصدر SA source address هو عنوان الجهاز الذي يريد أن يرسل الفريم

عنوان المرسل TA transmitter address و هو عنوان المحطة التي ستستقبل القريم لإرسالها أو اعادة تكرارها مثل المكرر Repeater

عنوان الهدف DA destination address هو عنوان الجهاز الذي ترسل له الفريم

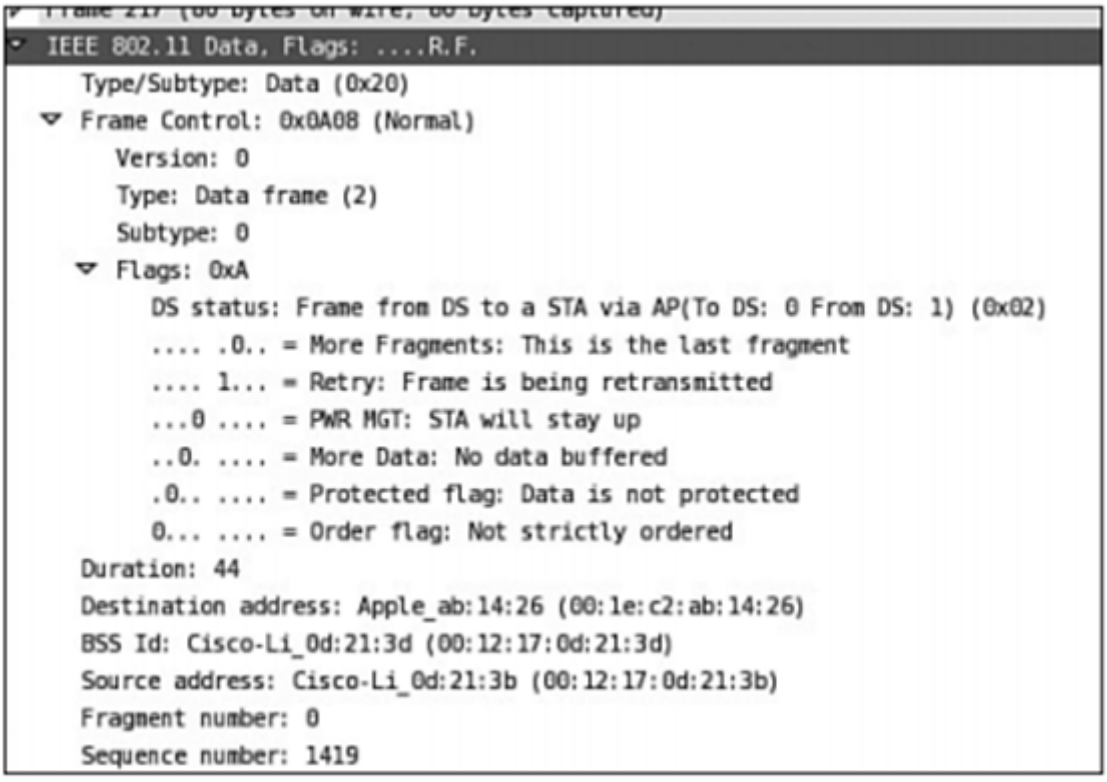
عنوان المستقبل RA receiving address و هو عنوان المحطة التي سترسل الفريم للجهاز الهدف



و لدينا اذن أربع سيناريوهات للإرسال

- السيناريو الأول هو أن يتم ارسال الفريم بين جهازين في شبكة AD-HOC و هنا سيكون العنوان الفيزيائي الأول الهدف أو المستقبل DA أو RA و سيكون العنوان الفيزيائي الثاني المصدر أو المرسل (TA/SA)
- السيناريو الثاني يتم ارسال الفريم بين جهاز الي أكسس بوينت وهنا سيكون العنوان الأول هو عنوان الجهاز و العنوان الثاني هو عنوان TA/SA و العنوان الثالث هو DA و لا يستخدم الرابع
- السيناريو الثالث هو ارجاع الفريم عكس المرحلة الثانية و هنا يكون العنوان الأول RA/DA و العنوان الثاني هو TA و الثالث هو SA و الرابع لا يستخدم
- السيناريو الرابع هو ارسال الفريم و تنقلها بين جهازي أكسس بوينت _جسور اومكررات – أو أكثر وهنا سنستخدم الأربع عناوين الأول RA و الثاني TA و الثالث DA و الرابع SA

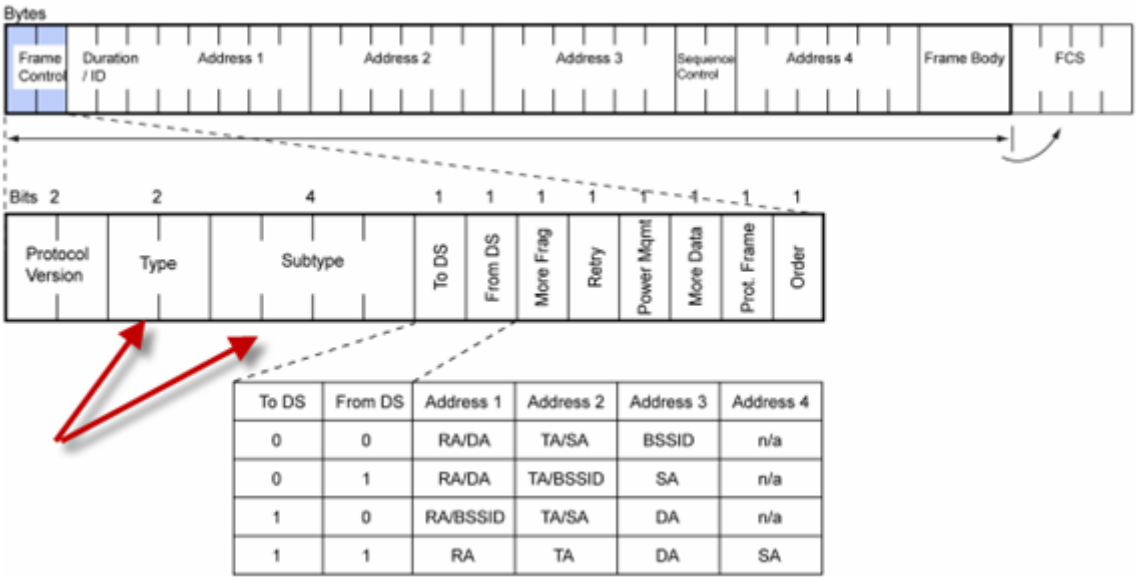
و الشكل التالي هو جزء من لقطة capture لفريم الوايرلس المرسل من جهاز الي آخر و تستطيع أن تتبين فيه أجزاء الفريم و طولها




هناك برمجيات كثيرة تستيطع التقاط فريم الشبكات السلكية و اللاسلكية و تحللها و هو ما يعتمد عليه الهكر كثيرا

## أعلان الأكسس بوينت عن نفسه بواسطة الفريمات الإدارية

كما قلنا فإن الشبكات اللاسلكية تستخدم ثلاث أنواع من الفريم و هي Management , Control , Data و هذه الثلاث أنواع يكون الفريم الخاص بهم متشابه بالشكل الذي شرحناه و الإختلاف الرئيسي هو في جزء Type من frame control و الذي يحدد طبيعة الفريم مثل management frames و جزء subtype الذي يحدد النوع الفرعي للفريم مثلBeacon frame في management frames




| To DS | From DS | Address 1 | Address 2 | Address 3 | Address 4 |
|---|---|---|---|---|---|
| 0 | 0 | RA/DA | TA/SA | BSSID | n/a |
| 0 | 1 | RA/DA | TA/BSSID | SA | n/a |
| 1 | 0 | RA/BSSID | TA/SA | DA | n/a |
| 1 | 1 | RA | TA | DA | SA |

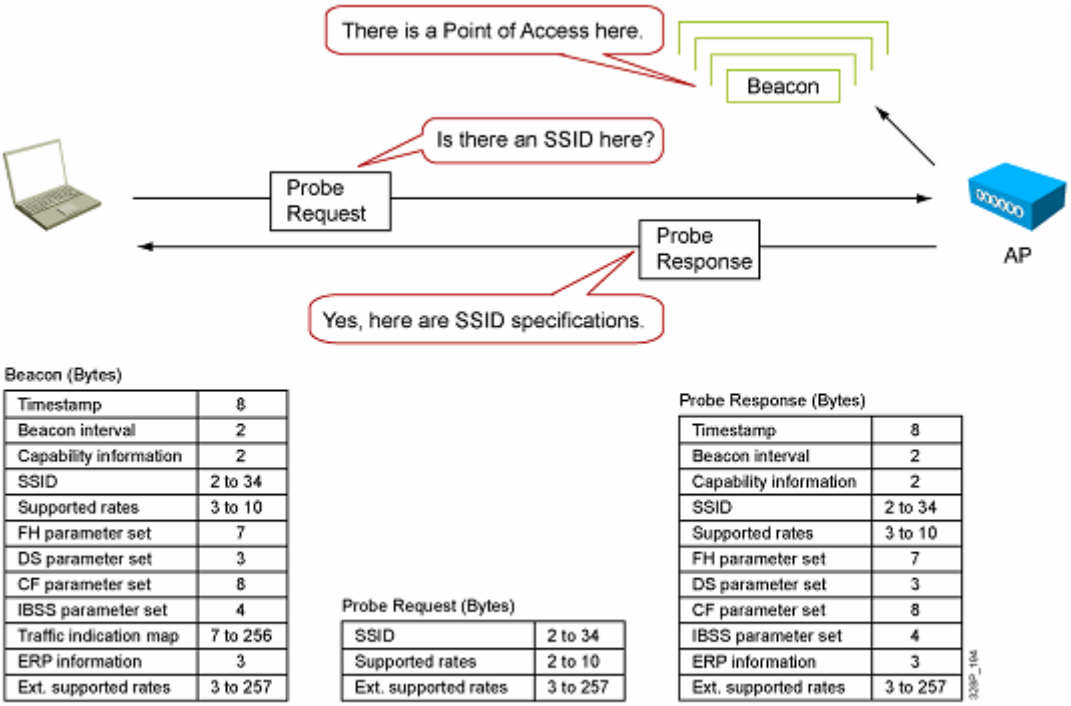
و الفريمات الإدارية Management Frames هي عدة فريمات تستخدم لإستكشاف الشبكات اللاسلكية و الإتصال بها و إدارة هذا الإتصال و ذلك عبر عدة فريمات فرعية مثل Probe و Beacon و فريمات التوثيق و الإرتباط و غيرها كما تري

- Management:
  - Beacon, probe request, probe response
  - Authentication request, authentication response
  - Association request, association response
  - Deauthentication, reassociation request, reassociation response
  - Announcement Traffic Indication Message (ATIM)

و تؤدي هذه الفريمات جميعا ثلاث أدوار

الدور الأول هو استكشاف الشبكة و الدور الثاني هو الإتصال بالشبكة و الدور الثالث هو إدارة هذا الإتصال

أما الدور الأول فيقوم باستكشاف أو الكشف عن الشبكة مستخدما فريمات Beacon كفريم للإعلان عن الأكسس بوينت و فريم Probe لبحث كيفية كيفية استخدام اعلان الأكسس للإتصال به كما تري




Beacon (Bytes)

| | |
|---|---|
| Timestamp | 8 |
| Beacon interval | 2 |
| Capability information | 2 |
| SSID | 2 to 34 |
| Supported rates | 3 to 10 |
| FH parameter set | 7 |
| DS parameter set | 3 |
| CF parameter set | 8 |
| IBSS parameter set | 4 |
| Traffic indication map | 7 to 256 |
| ERP information | 3 |
| Ext. supported rates | 3 to 257 |

Probe Request (Bytes)

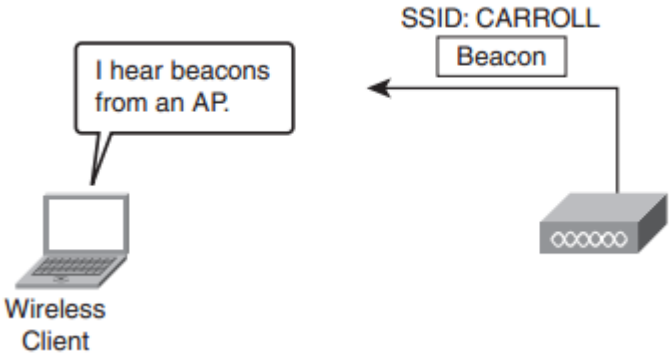
| | |
|---|---|
| SSID | 2 to 34 |
| Supported rates | 2 to 10 |
| Ext. supported rates | 3 to 257 |

Probe Response (Bytes)

| | |
|---|---|
| Timestamp | 8 |
| Beacon interval | 2 |
| Capability information | 2 |
| SSID | 2 to 34 |
| Supported rates | 3 to 10 |
| FH parameter set | 7 |
| DS parameter set | 3 |
| CF parameter set | 8 |
| IBSS parameter set | 4 |
| ERP information | 3 |
| Ext. supported rates | 3 to 257 |

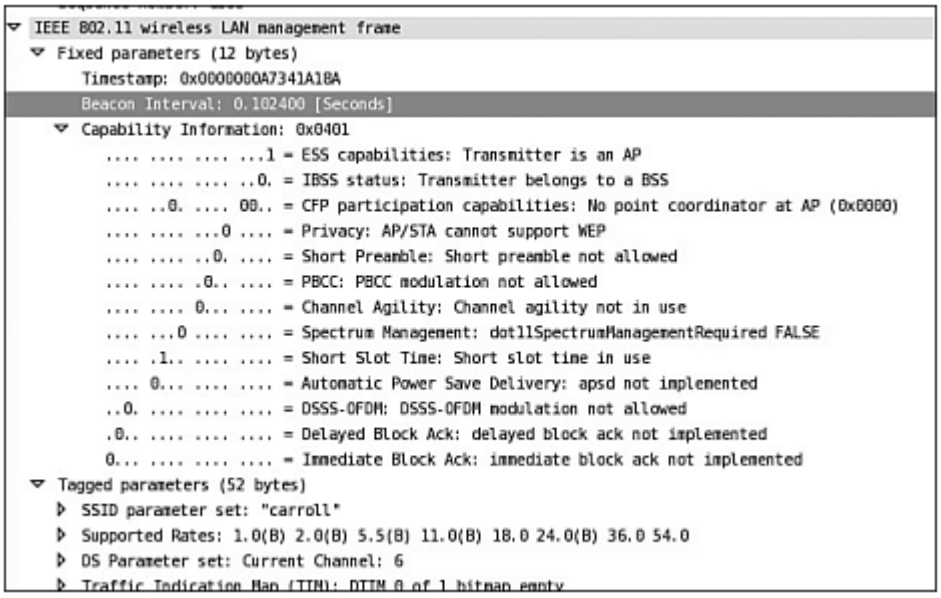
## فريم beacon و البحث الخامل

فعندما تريد الإتصال بشبكة الإيثرنت العادية فإنك بمجرد أن تري منفذ الإتصال بالحائط أو في السويتش تقوم بقبس الكابل فيه ، و هذا الأمر لا يتوفر في الشبكات اللاسلكية و لذلك وجب علي الأكسس بوينت أو أي جهاز لاسلكي معد للإتصال به أن يقوم بالإعلان عن نفسه ليعرفه من يريد الإتصال به و اشارة هذا الإعلان هو فريم البيكون Beacon frame و هو فريم يطلقه الأكسس بوينت كل 100 ميللي ثانية للإعلان عن تواجده




و يحمل Beacon frame عدة معلومات تجعل الأجهزة قادرة علي رؤيته و تحديد متطلبات الإتصال به مثل نوع الشبكة و هل هي Ad Hoc أو Infrastructure و سرعة الإتصال و عنوان الشبكة SSID

و نوع التعديل الرايديوي المستخدم Modulation مثل FHSS أو DSSS أو OFDM أو غيرها و يمثلهم في الشكل السابق اختصاراتFH, DS, CF, IBSS, ERP




و يوجد جزء من الفريم يسمي Traffic Indication Map (TIM) وظيفته تحديد ما ان كان الأكسس بوينت يتصل بأجهزة في وضع الخمول الكهربي power-save mode و تستخدم الأجهزة فريم ATIMلنفس الغرض و لكن عند الإتصال في وضعAd Hoc

و تسمي عملية استخدام beacon بالشكف الخامل Passive Scanning حيث أن جهاز الكمبيوتر لا يعاني في البحث عن الإشارة بل كل ما عليه هو ان يتسمع الإشارة التي تصله و يستنتج منها بيانات الإتصال , لكن ماذا لو أراد الجهاز أن يقوم بنفسه بطلب بيانات الأكسس بوينت أي أنه يقوم بنفسه بالكشف عن إشارة الأكسس بوينت

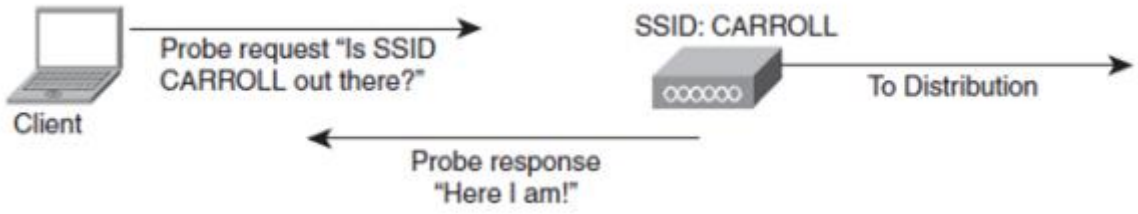
هنا تسمي هذه العملية Active Scanning و هي طريقة أكثر سرعة حيث أن الجهاز يقوم مباشرة بطلب الإتصال بجهة معينة بناء علي معلومات سابقة مثل SSID ,و لكي تعمل هذه الطريقة فإننا نلجأ الي استخدام إحدي الفريمات الإدارية Management Frames و تسميProbe frames

## فريم Probe و البحث النشط

تبدأ عملية البحث برسالة استكشافية Probe Rquest و يحتوي هذا الفريم علي جزئين

- أحدهما يختص بعنوان الشبكة SSID فتستطيع أن تبحث عن شبكة معينة أو البحث العام عن أي شبكة
- و الثاني هو الجزء الخاص بالمعيار المستخدم و المعوم من قبل الجهاز a, b , g , n802.11

ثم يقوم الأكسس بوينت بالرد علي probe Request بفريم Probe Response حاملا معلومات عن الأكسس بوينت تتضمن كل ما يحتاجه الجهاز لـلإتصال بالأكسس بوينت و يحتوي علي نفس النوعين الموجودين في فريم الطلب Probe Request و هما SSID و Rate و الذي تحدده إحدي معيار الإتصالa, b , g , n




و يرسل الأكسس بوينت إحدي ثلاث خيارات تبين مدي امكانية الجهاز لـلإتصال عبر هذه المعايير و هم mandatory, supported, disabled

فأما Disabled فتعني أن الجهاز لا يستطيع الإتصال بالكشش بوينت لعدم دعمه معايير الإتصال به

و أما Supported فتعني أن الجهاز يدعم معايير الإتصال بالأكسس بوينت و يستطيع الإتصال علي إحدي هذه المعايير

و اما Mandatory فهنا يجبر الأكسس بوينت الجهاز علي الإتصال فقط بإحدي المعايير لأنه لا يدعم سواها، و هذا لا يعني أن الجهاز مجبر علي الإتصال بالأكسس بوينت بنفس سرعة المعيار الذي يدعمه a , b , g , n بل انهما يتفقان علي المعيار المستخدم ثم يقوم الجهاز بالإصتال بالأكسس بوينت حسب السرعة التي يستطيع الإتصال بها حسب بعده أو قربه من الأكسس بوينت و حسب عوامل الإتصال الأخري

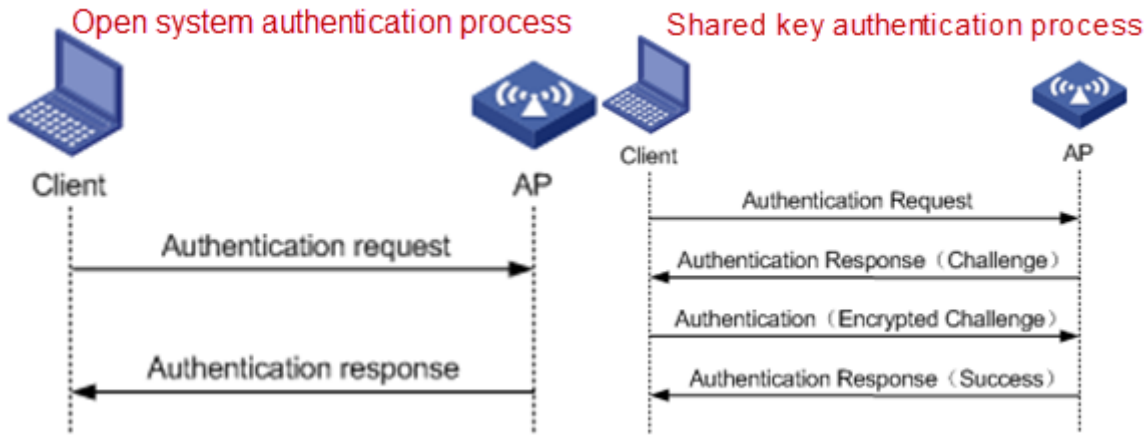
**استخدام الفريمات الإدارية في التوثيق و الربط**

أولا التوثيق authentication

بمجرد أن يعرف الجهاز بيانات الأكسس بونيت بواسطة probe أو beacon فإنه يحاول الإتصال به و يتم ذلك بواسطة فريم التوثيق AUTHENTICATION FRAME و الذي يتكون من الأجزاء التالية

- authentication algorithmبطول 2 بايت لعملية challenge عند وجود باسورد
- Authentication transactionبطول 2 بايت لطلب و و الإستجابة للتوثيق
- Status codeبطول 2 بايت لبيان مدي نجاح أو فشل التوثيق
- Challenge textبطول 3 الي 255 بايت

و يتغير طول و محتويات هذه الأجزاء طبقا لحالة التوثيق و نوعها فقد تكون عملية التوثيق هذه تتطلب باسورد و ذلك في حالة حماية الشبكة بـ WEP Wired equivalent privacy أو لا تحتاج باسورد اذا كان مستوي الحماية في الشبكةopen

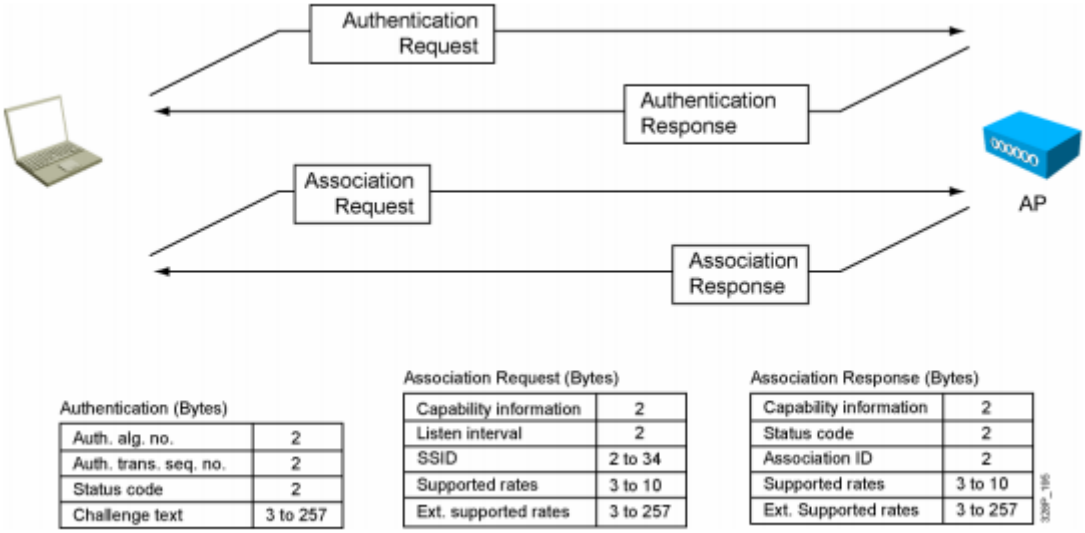



و في حالة كون درجة الحماية open يتم التأكد من تمكن الإتصال فيزيائيا بالأكسس بوينت أي أن الإتصال اللاسلكي متحقق ثم يرسل الجهاز فريم توثيق و لكن يكون authentication algorithm خالي لعدم وجود باسورد و يكون Authentication transaction بطول 1 بايت و ليس 2 و باقي أجزاء الفريم خالية ، ثم يقوم الأكسس بوينت بالرد بواسطة فريم authentication response يحتوي علي 2 بايت من Authentication transaction و يكون الجزء الخاص بالحالة status هوsuccess

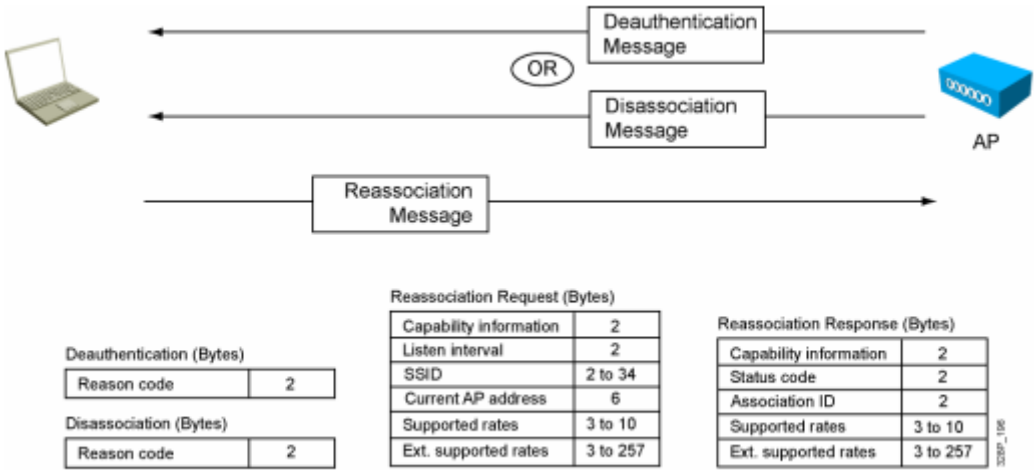
### ثانيا مرحلة الربط Association

بمجرد أن يقوم الأكسس بوينت بتوثيق طلب الجهاز يقوم الجهاز بطلب الإنضمام لشبكة ألأكسس بوينت و ذلك بواسطة فريم طلب ربط association frame request و الذي يحتوي علي التالي

- 2بايت لبيان مدي امكانية الجهاز علي الربط
- 2بايت لبيان مدي امكانية الجهاز للإستماع للأكسس بوينت في حالة وجوده في وضع الخمول الكهربيpower save
- 2الي 34 بايت لعنوان الشبكة SSID
- معدل نقل البيانات الذي يدعمه الجهاز و ذلك بطول من 3 الي 257 بايت




يقوم الأكسس بوينت بعدها بالرد بواسطة فريم association response لبيان مدي قابلية الجهاز للربط او لا ثم يقوم الأكسس بوينت بالرد بواسطة assosciation response frame مع بيان وضع الربط هل نجح أم لا مع بيان رقم الجهاز في الشبكة التي يربطها الأكسس بوينت



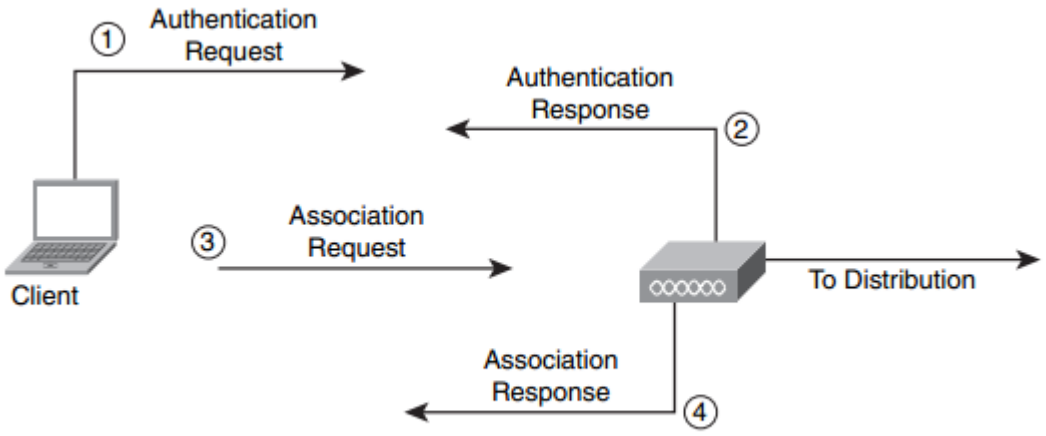

اثناء الإتصال بالأكسس بوينت يقوم الجهاز بمراقبة اتصاله و طبيعي جدا ان يقوم بقطع اتصاله و ذلك بإرسال deauthentication messageأو disassociation messag e

و الفرق بينهما هو أنه لو تم التأكيد علي deauthentication فإنه سيحتاج الي مرحلتي authenticationو association لأنه قام بالغاء الأصل و هو توثيق نفسه في الأكسس بوينت

أما لو تم الغاء ربطه association فإنه يستطيع أن يقوم بطلب الربط مرة أخري Reassociation بدون مرحلة authentication

و أعتقد أن لديكم الخبرة الكافية لفهم ذلك لتدرك الفرق بين اتصالك بشبكة لاسلكية جديدة أو أخري مخزنة مسبقا علي جهازك

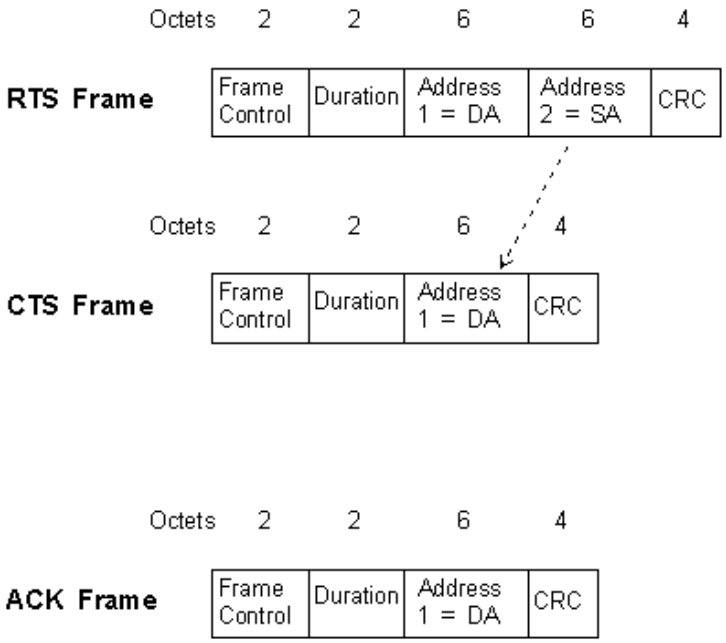
وهذا هو ملخص لعمليات التوثيق و الربط




*Authentications and Association*

## Control Frames

الآن جاء دور فريمات التحكم Control frames و هي فريمات خاصة تستخدم لضبط فاعلية الإتصال و الإرسال و الإستقبال و تنقسم لنوعين نوع يعمل في وضع DCF و يكون كل جهاز مسؤل عن الإرسال و الإستقبال مثل فريمات request to send (RTS) و clear to send (CTS) و Acknowledgment (ACK) و أنواع تعمل تحت وضع PCF الذي يقوم فيه الأكسس بوينت بإدارة هذه العمليات



## RTS and CTS

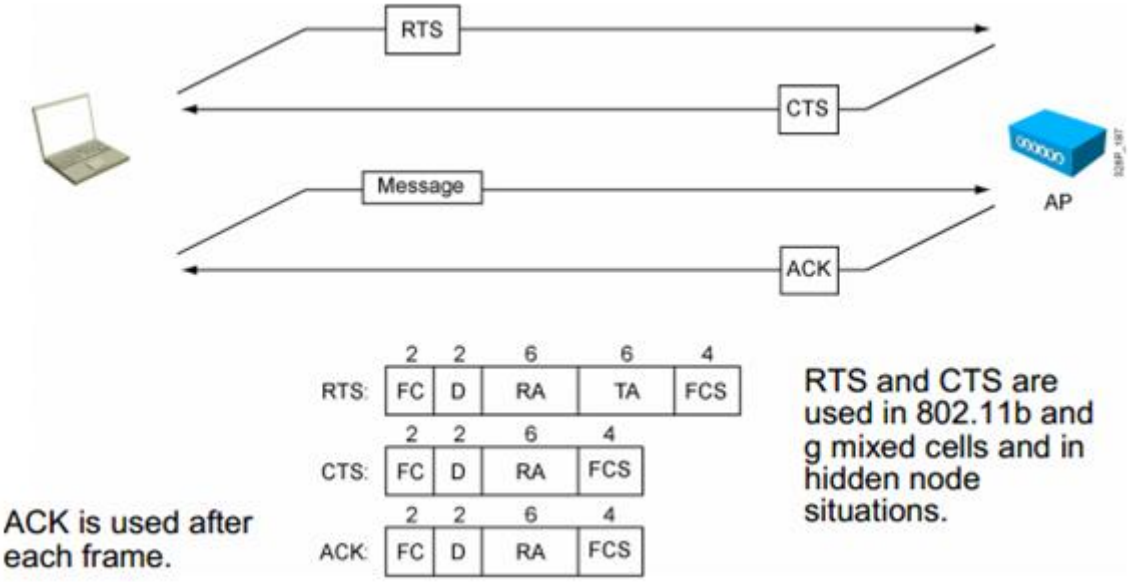
RTS/CTSيستخدمان لحماية الإتصال من عمليات التصادم بحجز الوسط اللاسلكي حيث يقوم المرسل بإستخدامهم عندما يريد أن يرسل للأكسس بيونت

بعد ان يستقبل فريم Clear-to-Send (CTS) لإعلامه بخلو الوسط يقوم بإرسال فريمRequest-to-Send (RTS)للإعلان عن الرغبة في الإرسال

بعض المصادر تعكس العملية أي يقوم الجهاز بإرسال RTS عندما يريد الإتصال و يرسل بعدها CTS لإعلامهم بجعل القناة خالية حتي يتم الإتصال

## ACK

Acknowledgment (ACK)فريم تحكم يبين مدي نجاح مهمة الإرسال و التأخر في استقبال او ارسال هذا الفريم يحدث تصادم في الوسط




## فريم PS-Poll

PS-Poll (Power-Save Poll)فريم تحكم يستخدم عندما يدخل الجهاز في وضع الخمول و ذلك لحفظ الطاقة فيقوم الأكسس بوينت بحفظ البيانات التي ترسل اليه حتي ''يقوم من النوم'' و عندما يصحو الجهاز يقوم بطلب بياناته بواسطة فريم **PS-Poll**

أما فريمات التحكم التي تستخدم في وضع PCF فهي

■ Contention Free End (CF+End)

■ Contention Free End Ack (CF +end_ack_)

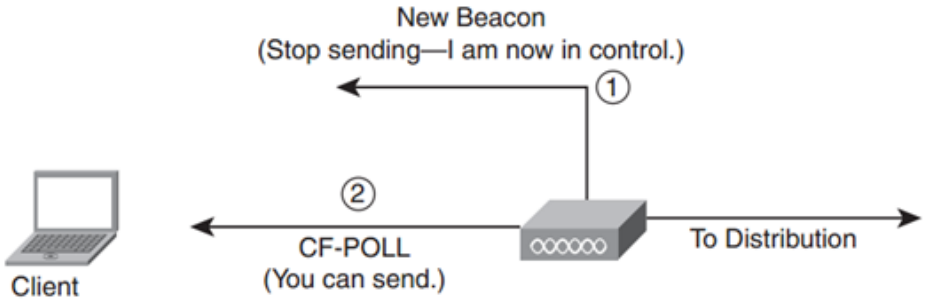
■ CF-Ack

■ CF Ack+CF Poll

■ CF-Poll

عندما يأخذ الأكسس بوينت دور المتحكم في الإرسال و الإستقبال يتحول من وضع DCF الي وضع PCFو يجعل الأجهزة تنتهي عن الإرسال لفترة ما و تسمي هذه الفترة contention free window (CFW)و ذلك لإدارة عملية الإرسال و الإستقبال

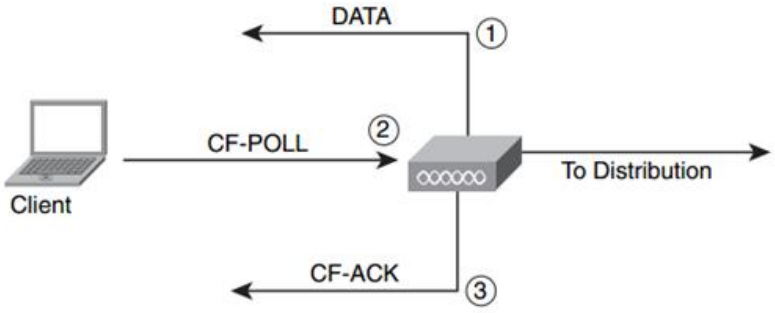
و عندما يحدث ذلك و تلتزم الأجهزة بمنع الإرسال يقوم الأكسس بوينت بإرسال رسالة استطلاع CF-Poll لمعرفة من يريد الإرسال




*CF-Poll in PCF Mode*

يقوم أحد الأجهزة بإرسال رسالة رد لهذا الإستطلاع ليتمكن من الإرسال فيقوم الأكسس بيونت بإعطائه المجال

يقوم الأكسس بوينت بالسماح للجهاز بتلقي البيانات بواسطة فريمات تحكم CF-Poll وCF-ACK



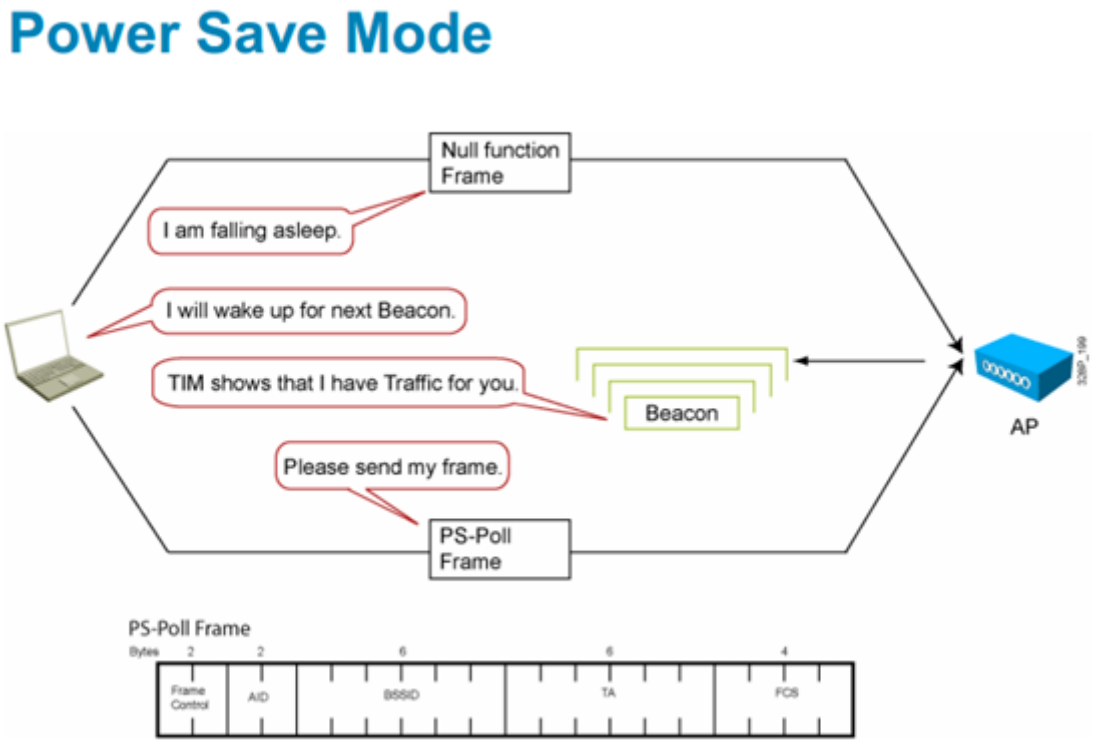

*Data + CF-Poll + CF-ACK*

# القيلولة اللاسلكية

حيث اننا نعول في كل حياتنا تقريبا علي الطاقة المستمدة من البترول والي ان نستطيع جديا ان نعتمد اعتماد كلي علي الطاقات الدائمة والنظيفة فإنه لابد ان نحافظ ونقلل استهلاكنا لهذ الطاقات المستنفذة تستطيع أن تطفيء الأجهزة الكهربية المصابيح الغير مستعملة او تستبدلها بأخري ذات استهلاك أقل و تضبط المكيف علي درجات أقل و تستخدم سيارات اقتصادية في استهلاك الوقودو أيضا تستطيع أن تضبط الكثير من اجهزتك الإلكترونية علي وضع يسمي وضع "توفير الطاقة power saving " مثل أجهزة الحاسوب و الموبايل و البلوتوث وغيرها و يسمي احيانا وضع الإسبات أو القيلولة اللاسلكية sleeping معظم كروت الشبكات اللاسلكية تستهلك الكثير من الطاقة ولهذا نستخدم خاصية توفير الطاقة لمنع او لتقليل استخدام الطاقة في اوقات عدم الإرسال او الإستقبال

وضع التوفير هذا قد لا يعتبره البعض خدمة قومية بقدر ما نعتبره توفير لحظي في بطارية الجهاز في اماكن و أوقات لا نستطيع شحن البطارية

فعندما يدخل الجهاز الي هذا الوضع فإنه يقوم بعمل "قيلولة لاسلكية Wireless Snoozing "و يقوم بتعطيل بعض من خصائص التراسل حفظا للطاقة ، و عندما يصحو الجهاز من قيلولته فإنه يتسمع الي رسائل الأكسس بوينت



وفكرة عمل هذا الوضع تنبني علي فريمات التحكم التي عرفناها في الحلقة السابقة

في البداية يقوم الجهاز بإرسال فريم فارغ empty frame يسمي null function الي الأكسس بوينت ليخبرها أن الجهاز سيدخل في قيلولة لاسلكية و لا يريد من أحد ازعاجه و بعدها سيقوم الجهاز بإطفاء مخارجه اللاسلكية و يعطل بعض من اشائه الأخري و يبقي علي ''الساعة'' فخباره كم مضي من وقت اثنا قيلولته

و هنا يبدأ الأكسس بوينت في تخزين buffer كل الرسائل و الأحداث التي تخص هذا الجهاز الي ان يقوم من قيلولته

بمجرد أن يصحو الجهاز يبدأ في الإستماع الي beacon الخاص بالأكسس بوينت و يحتوي هذا البيكون علي جزء يسمي (Traffic Indication Map (TIM يبين قائمة بالأجهزة التي أرادت الإتصال به أثناء نومه

بعدها يقوم الجهاز بإرسال فريم تحكم (Power Save Poll (PS-Poll ليخبر الأكسس بوينت أنه كان نائما و قد استيقظ الآن و يطلب منه رسائله المخزنة لديه

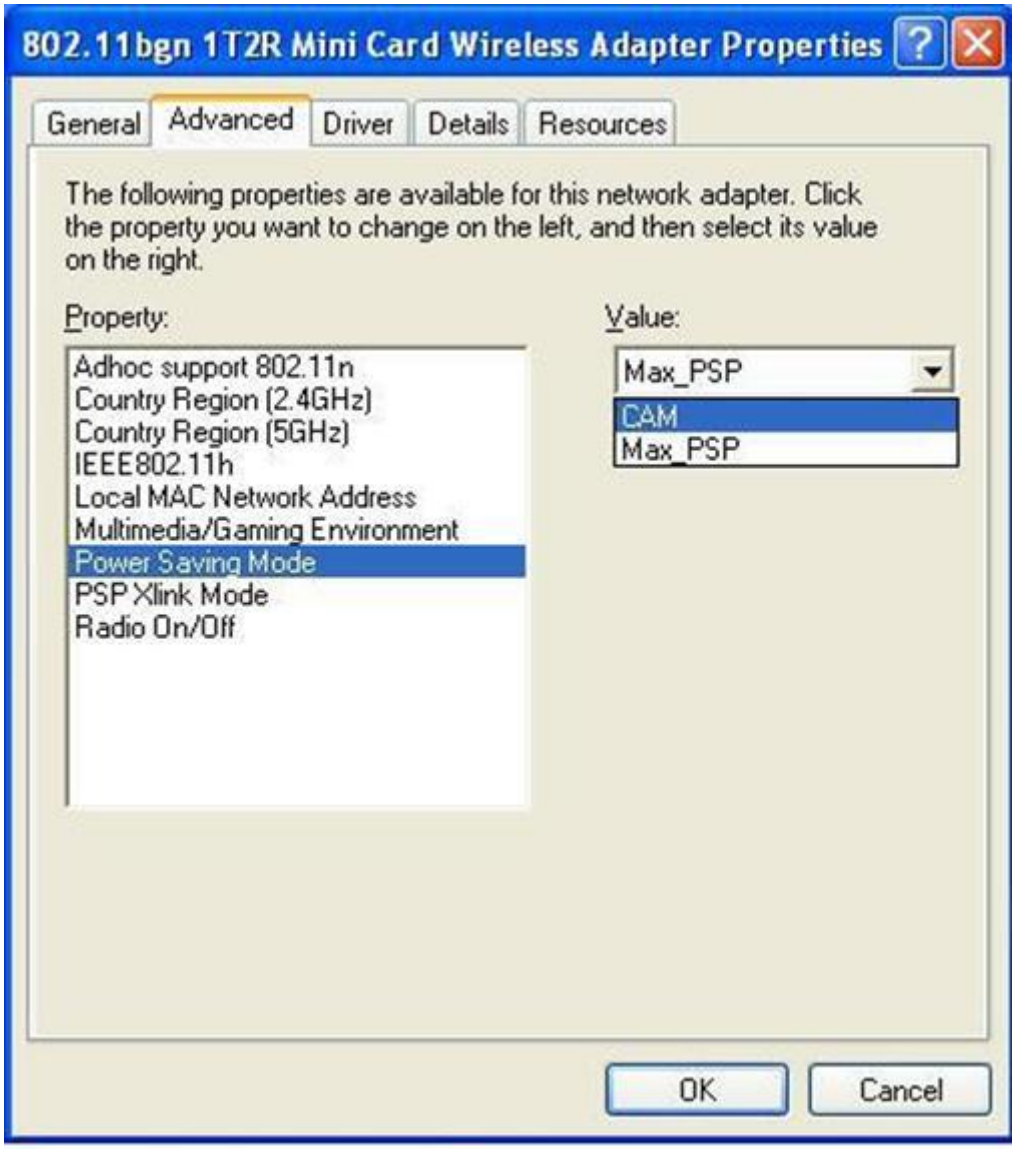
يقوم الأكسس بوينت بإرسال البيانات اليه عند تأكده من أنه هو الجهاز الذي رسائله مخزنة لديه

بعض البيكون الخاصة بالأكسس بوينت تسمي Delivery Traffic Indication Map (DTIM)تبين طبيعة البينات المخزنة من حيث كونها عامة broadcast أومخصصة لبعض الجهات multicastأو لجهاز ماunicast

بعض المصنعين يرون أن وضع power saving mode بهذا الشكل غير فعال و غير مجدي لهذين السببين

- هذا الوضع يعتبر عبئا علي الشبكة بسبب تداول الكثير من الرسائل المخزنة بعد وضع القيلولة هذا
- وضع القيلولة غالبا لا يستمر اكثر من 10 الي 15 دقيقة خلال مدة عمل بطارية عمرها التشغيلي ساعتين و هو أمر لا يدعو الي تحميل الشبكة هذا الكم من تداول الرسائل من اجله

و لهذا فالكثير من المصنعون دعموا هذا الوضع و لكن بخيارات أكثر مرونة فسيسكو مثلا و غيرها ادخلوا وضع في كروتهم اللاسلكية يسمي(Constant Awake Mode (CAM

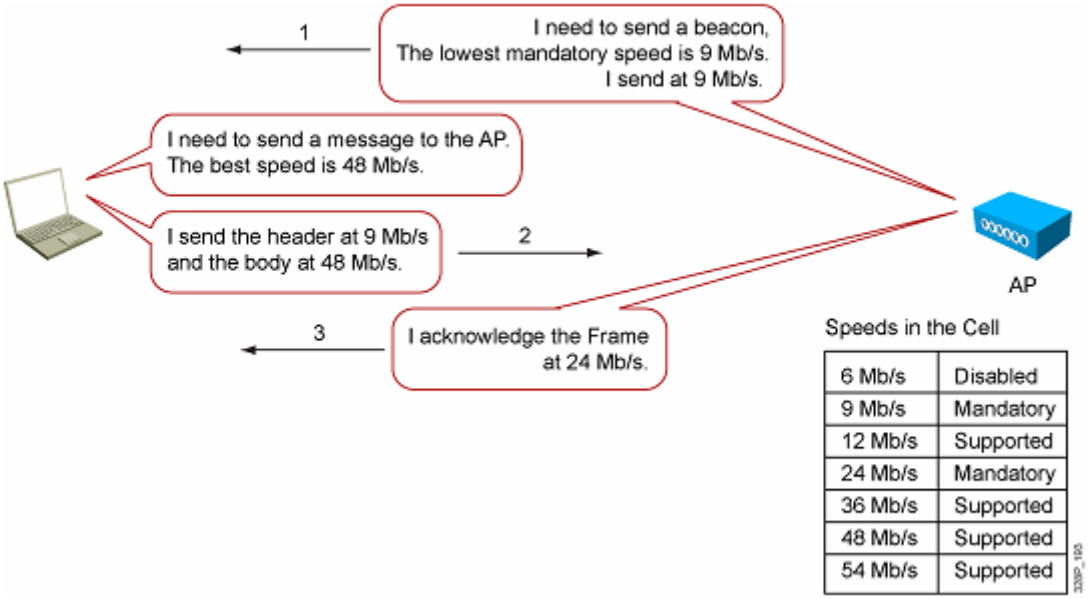



## دور الفريم في موائمة السرعة بين الجهاز و الأكسس بوينت

يقوم الأكسس بوينت بإقتراح سرعات تدفق بيانات data rate للأجهزة التي تريد الربط به كي يستطيعوا اكمال الإتصال و يستطيع الهاز العمل بتلك النصيحة او الإتصال عبر سرعات أخري مدعمة من قب الكسس بوينت

فمن الممكن مثلا أن يتعامل الأكسس بوينت مع سرعة تدفق البيانات ذات القيمة 24 mbps و لكنه يستطيع دعم ربط أجهزة تتعامل بسرعات mbps54

و يتم معرفة السرعات المدعومة من الأكسس بوينت من خلال فريمات البيكون beacon التي يطلقها في عملية البحث الخامل passive scan ثم تتم عدة عمليات تشبه المحادثة بين الجهاز و الأكسس بوينت لإختيار سرعة الربط الأمثل كما بالشكل




و قبل ان يتم ارسال الإشارات يقوم كل جهاز بتحديد السرعة المثلي للإستخدام و يتم هذا اعتمادا علي معاملات الإشارة التي عفناها مسبقا مثل RSSI و SNR و كذلك معدل الفقد

و لذلك يقوم الأكسس بوينت بوضع كل الإحتمالات التي يدعمها في سرعاته في فريم البيكون مع وضع افضليات بينها فمنها ما يكون السرعة الإفتراضية mandatory و تسميها بعض المصادر basic rates أو سرعة مدعومة supported أو معطلة لا يستطيع الإتصال عبرهاdisabled

هكذا مثلا

- 6 Mb/s: disabled
- 9 Mb/s: mandatory
- 12 Mb/s: supported
- 24 Mb/s: mandatory
- 36 Mb/s: supported
- 48 Mb/s: supported
- 54 Mb/s: supported

اذن ليستطيع الجهاز الإتصال بالأكسس بوينت فإنه لابد أن يكون قادرا علي ارسال الفريمات بسرعة 9 و 24 ميجابت لكل ثانية و السرعة الدني 9 هي المستخدمة من قبل الأكسس بوينت لإرسال الفريمات الإدارية مثل البيكون كما تري في الشكل السابق "سهم 1"

و السرعة الأعلي و هي 24 يستدمها الأكسس بوينت لإرسال البيانات "سهم 3"

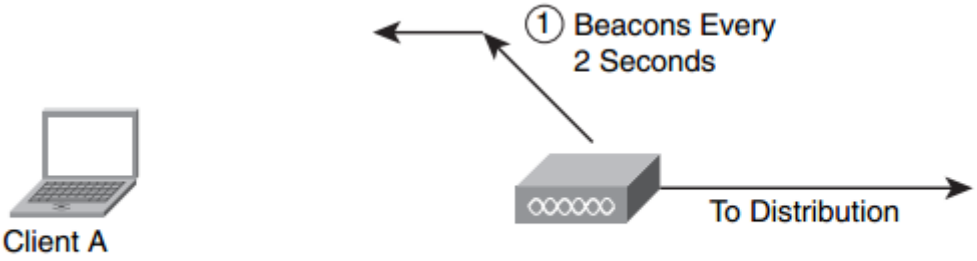
كذلك يرسل و يستقبل الأكسس بوينت فريم ACK الذي يبين نجاح أو فشل وصول الفريمات الأخري علي سرعات أقل من التي تم ارسال تلك الفريمات ،، فلو تم ارسال الفريمات علي سرعة 48 فإن ACK يتخير السرعة الأقل المدعومة أو الإفتراضية و هي مثلا 24

كذلك فإن الجهاز عندما يريد ارسال بيانات الي الأكسس بيونت فإنه يرسل البيانات نفسها data body بالسرعة الأعلي مثلا 48 و يرسل header بالسرعة الأقل 9 mbps

## رحلة الفريم في الشبكات اللاسلكية

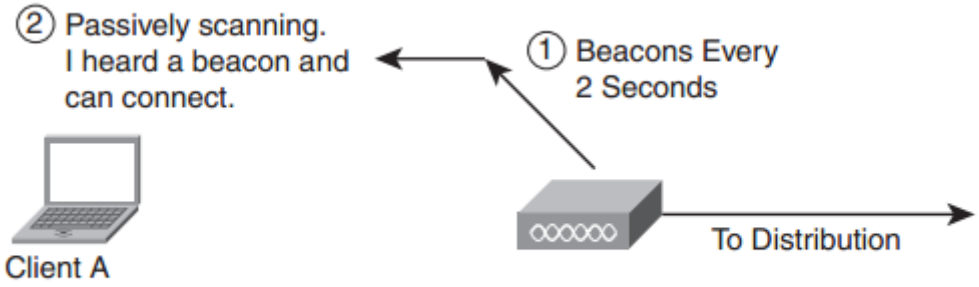
تعالو نبسط موضوع الفريمات الخاصة بالوايرلس IEEE 802.11 Frames بمثال حواري كامل يبين كيفية استخدام كافة أنواع فريمات الوايرلس في الإتصال بين الأكسس بوينت و الأجهزة

أولا و في بداية الحوار اللاسلكي يبدأ بإعلان الأكسس بوينت عن نفسه بواسطة فريم بيكون beacon frame كل ثانيتين




*AP Beacons*

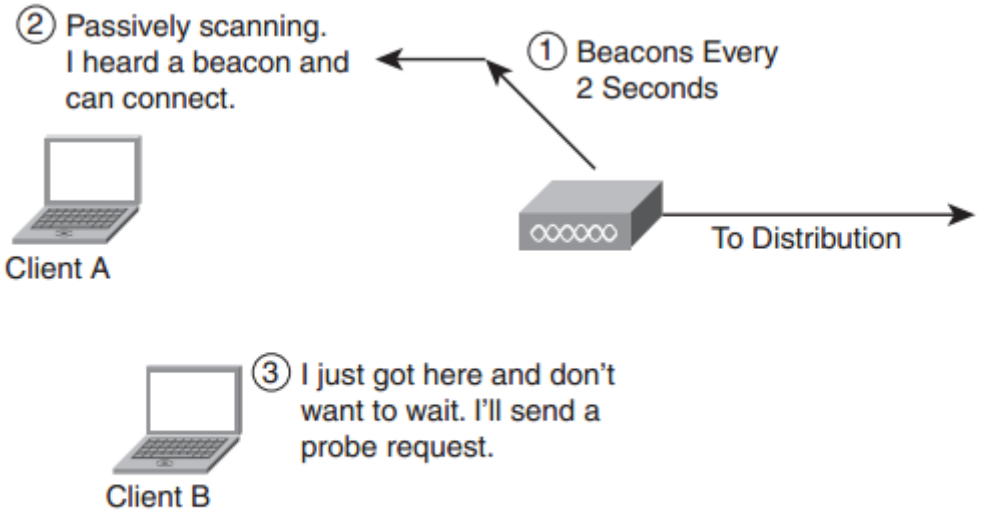
ثانيا و من جانبه يقوم الجهاز client A بعمل مسح خامل – passive scanning اي بدون بيانات مسبقة – وتبين نتيجة المسح عن وجود جهاز أكسس بوينت – الذي أعلن عن نفسه سابقا- و يستطيع بعد تفحص فريم البيكون beacon frame للأكسس بوينت من تبين الشروط التي تجعله قادرا علي الإتصال به




*Passive Scanning*

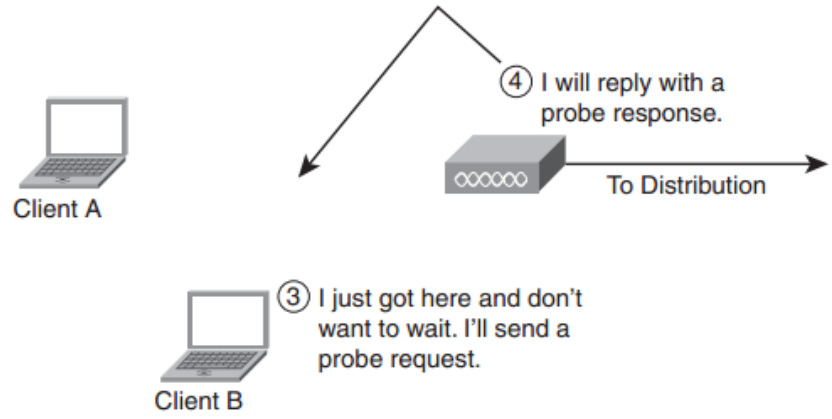
ثالثا يوجد جهاز جديد Client B في حيز اشارة الأكسس بوينت و له معرفة مسبقة بالأكسس بوينت و لا ينتظر وجود اشارة فريم البيكون فهو يقوم بإرسال طلب بواسطة فريم بروب probe request frame ليستكشف بها الأكسس بوينت و هو ما يسمي بالكشف النشطActive Scanning

في حين يقوم الجهاز A بمحاولة الإتصال بالأكسس بوينت طبقا لبيانات البيكون التي وصلته



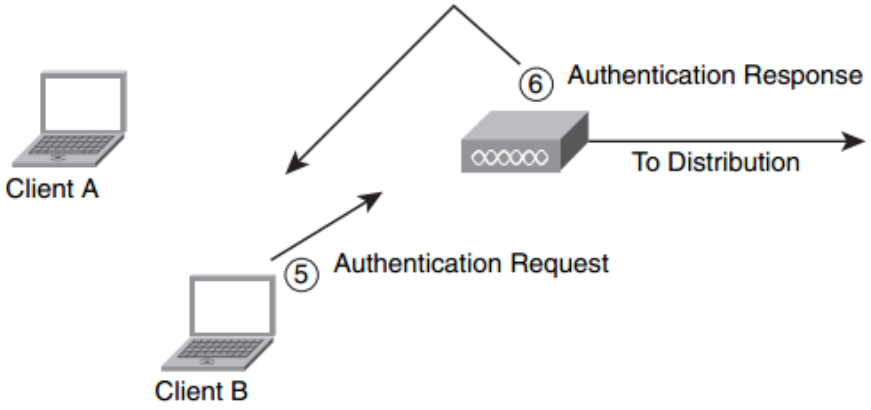

*Active Scanning Probe Request*

رابعا يتعرف الأكسس بوينت علي الجهاز B و يقوم بإرسال رد لطلبه علي هيئة فريم بروب Probe response frameليمكن الجهاز من الإتصال به فإن تأخر في الرد يقوم الجهاز B بمعاودة ارسال فريم probe request frame



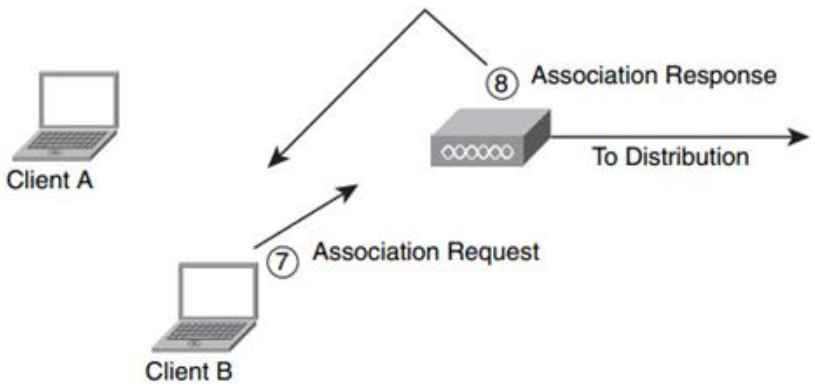

*Probe Response*

خامسا يبدأ الأكسس بوينت بتوثيق طلبات الإتصال للجهازين A و B بواسطة فريمات رد طلب التوثيق authentication responseحيث قاما الجهازان بعد أن تيقنا من قدرتهما علي الإتصال بالأكسس بوينت بطلب توثيق الإتصال بواسطة فريم طلب توثيقauthentication request



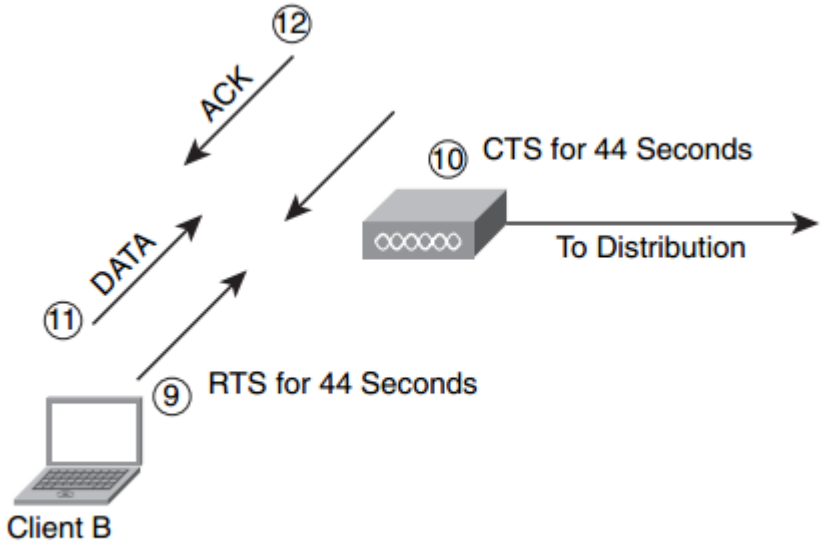

*Association Request and Response*

سادسا بعد أن تأكدا الجهازان من عدم ممانعة الأكسس بوينت لطلب الإتصال به يقومان بطلب الدخول الي شبكته فعليا بواسطة فريم طلب الربط Association Request و يتم التأكيد من قبل الأكسس بوينت بواسطة فريم الموافقة علي الربطAssociation Response



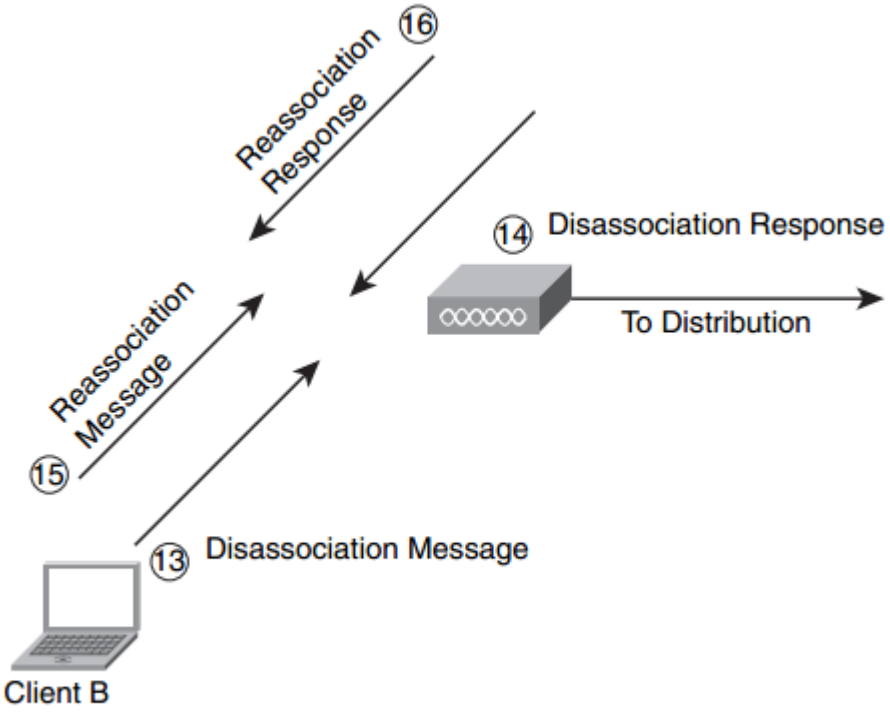

*Association Request and Response*

سابعا يبدأ الجهاز الذي اتصل بالأكسس بوينت بطلب ارسال بيانات و ذلك بواسطة فريم RTS فيقوم الأكسس بوينت بقبول الطلب و يفرغ القناة بفريم CTS فيرسل بعدها الجهاز البيانات و خلال كل فريم تم ذكره في هذه الفقرة يتم ارسال فريم ACK للتأكيد علي وصول اي من هذه الفريمات




*RTS/CTS*

ثامنا و أخيرا انتهت طلبات الجهاز و انتهي الغرض الذي اتصل من أجله بالأكسس بوينت فيقوم بطلب فك ارتباط disassociation message فيقوم الأكسس بوينت بالإستجابه له و يقطع الإتصال به بواسطة فريمdisassociation response




*Reassociation*

و يظل الجهاز قادرا علي الإتصال به ما دام موثقا لدي الأكسس بوينت و كل ما عليه لطلب الإتصال مرة اخري هو ارسال اعادة طلب ولوج لشبكة الأكسس بوينت كفريم reassociation message ليقوم الأكسس بوينت بقبول الطلب بفريمreassociation response

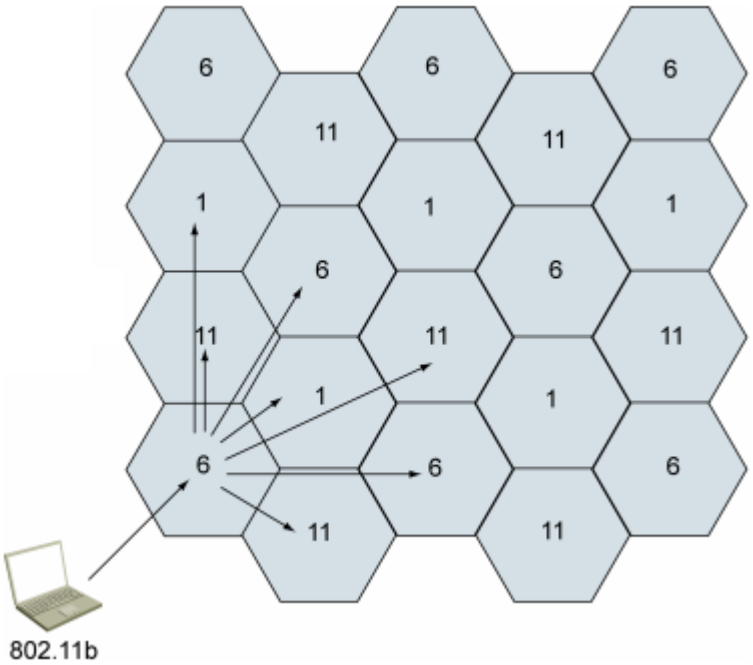
## دور الفريم في موائمة السرعة بين ieee 802.11 b و ieee 802.11 g

من أحد الأشياء الجميلة في معيار 802.11g أنه متوافق مع المعيار الأقدم 802.11b و هذا يعطي امكانية للأجهزة التي تعمل علي المعيار القديم b أن تستخدم الأكسس بوينت الذي يتعامل مع المعيار

من الطبيعي أن لا يفهم جهازان يتعاملان بمعيارين مختلفين بعضهما فعندما تضع جهاز يعمل بمعيار 802.11b وسط شبكة لاسلكية تعمل بمعيار 802.11g تشبه وضعك لشخص صيني وسط أشخاص عرب

لأن المعيار b يتعامل مع تكنولوجيا تعديل DSSS و غير مهيء للتفاهم مع تكنولوجيا OFDM التي يتعامل بها 802.11g و لذلك فلن يوجود تفاهم بين الأجهزة التي تتعارض في المعايير في نفس الخلية حين الإرسال و لن يوجد تنسيق مما يؤدي الي وجود تصادمات لظنه أن القناة فارغة في حين أنها مشغولة ببيانات أجهزة 802.11g

و لذلك احتيج الي طريقة لعمل توافقية بين هذه المعايير و هذا هو ما تؤديه خدمة أو تكنولوجيا Protection Mechanism التي توائم بين الأجهزة التي تختلف معاييرها في نفس الخلية

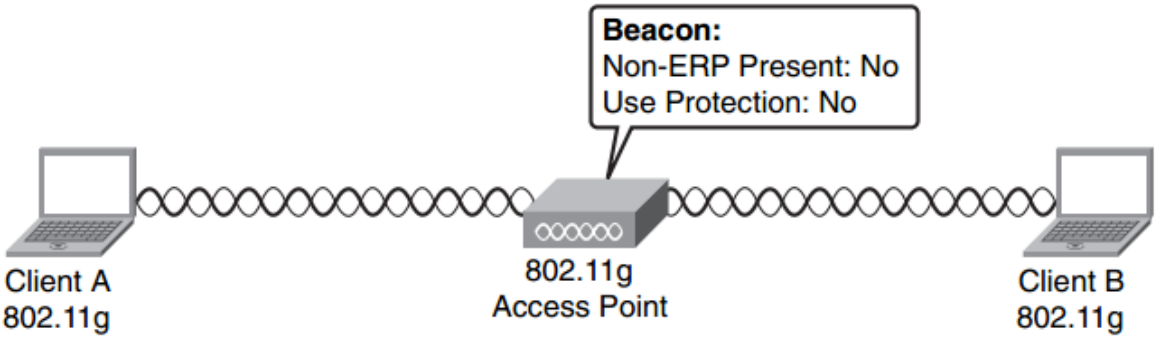



في البداية هيا نتصور عدم وجود أجهزة تعمل بالمعيار 802.11b في حيز أكسس بوينت يعمل بالمعيار 802.11g ، هنا سيكون الرد الإفتراضي للأكسس بوينت هو ارسال فريم بيكون beacon frames تحتوي علي المعلومات الخاصة به و التي منها التالي

NON_ERP present: no

Use Protection: no

و ERP أو Extended Rate Physical هي معلومة تعطي من خلال البيكون تبين مدي الاحتياج لوجود دعم ترددي لمعيار 802.11b و هي علاقة عكسية تعني أنه في حالة عدم وجود أجهزة 802.11b فإنه لا حاجة الي وجود أو استخدام protection mechanism أو بشكل مبسط القيمة المعطاه منها تبين هل يوجد أجهزة من معيار 802.11b أم لا



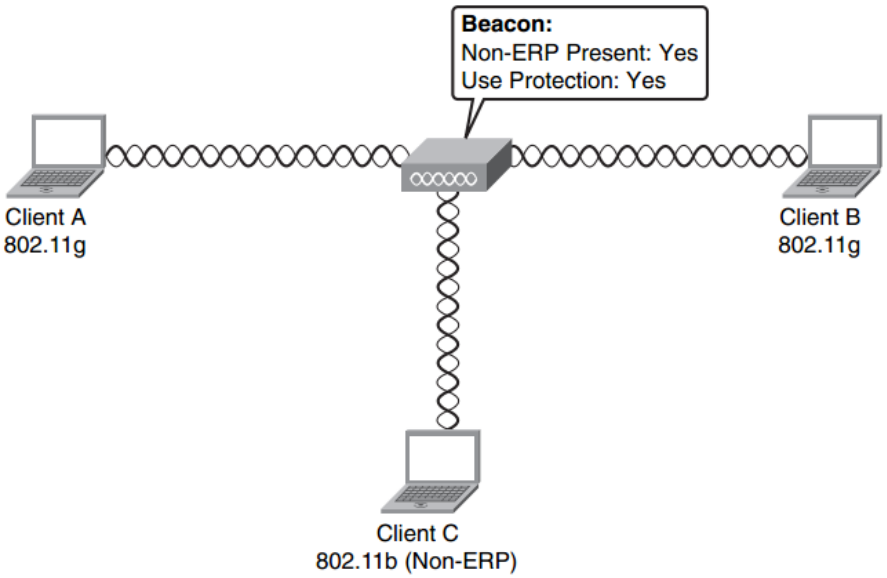

*802.11g Cell with No 802.11b Clients*

أما في حالة وجود أجهزة من المعيار 802.11b فإن فريمات البيكون تقوم علي الفور بإعلامهم بأنهم قادرون علي الولوج الي شبكة الأكسس بوينت كما تري في الشكل

لاحظ تغير حالة

NON_ERP present: yes

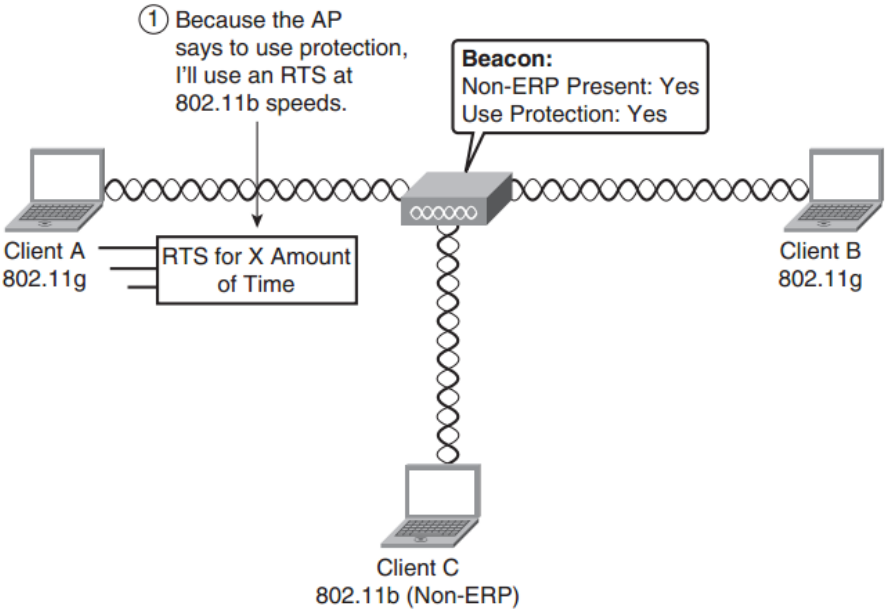
Use Protection: yes




*802.11g Cell with an 802.11b Client*

الآن الأكسس بوينت يعلم بوجود أجهزة 802.11b و لهذا تتغير طريقة الإرسال ، فعندما ترسل اجهزة 802.11g فريم فإنها لابد أن تقوم بإرسال رسائل تنبيهية كفريمات request to send (RTS) لأجهزة 802.11b و بنفس سرعتها كي تستطيع الأجهزة التي تتعامل مع معيار 802.11b سماعها و فهمها و بعدها تقوم أجهزة 802.11b بالتجاوب و ارسال فريم clear to send (CTS) علي نفس سرعة 802.11b

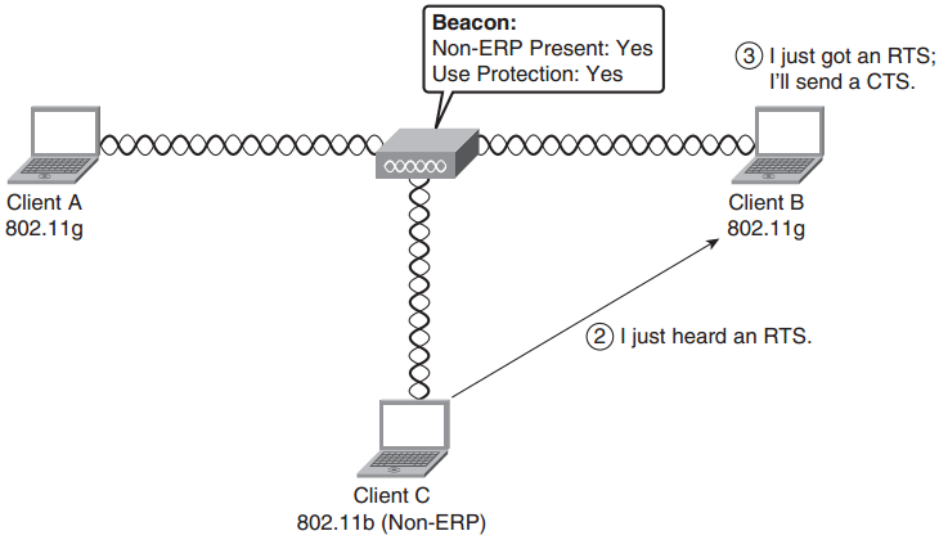
فريمات RTS ليست عامة broadcast ترسل لكل الأجهزة و لكنها محددة unicast و مرسلة فقط للأجهزة ذات المعيار b




*802.11g Cell Using Protection: Part 1*

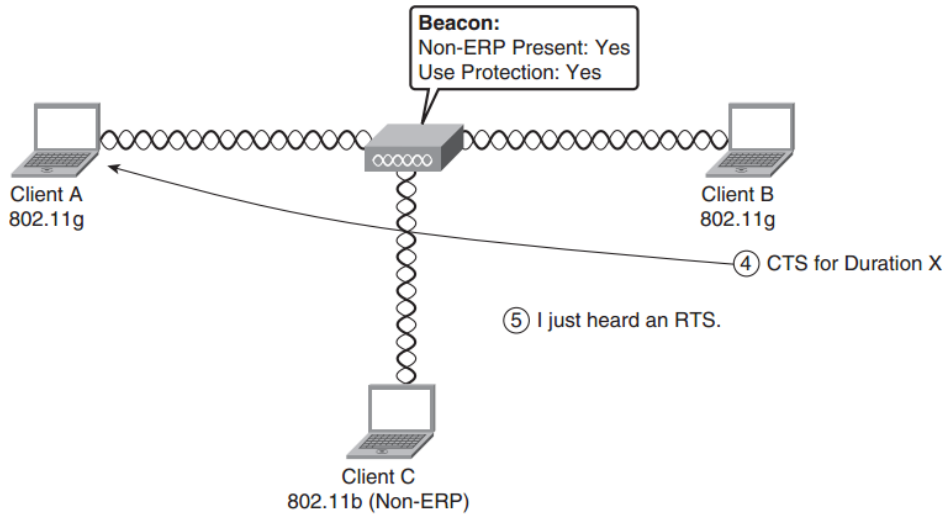
الخطوة الثانية تقوم أجهزة 802.11b بسماع RTS و التي تحتوي علي فترة توقيتية ملزمة للسماع بدون ارسال تسمي duration و خلال هذه المدة لا يستطيع الإرسال و لا يستطيع أيضا سماع بيانات 802.11g المرسلة خلال هذه الفترة

يفكر الآن 80.211b في ارسال CTS ليتأكد من خلو القناة




*802.11g Cell Using Protection: Part 2*

الخطوة الثانية يقوم الجهاز B المتعامل بالمعيار 802.11g بإرسال CTS الي الجهاز A المتعامل بنفس المعيار و يظل الجهاز C المتعامل بالمعيار 80.211b يسمع فقط CTS

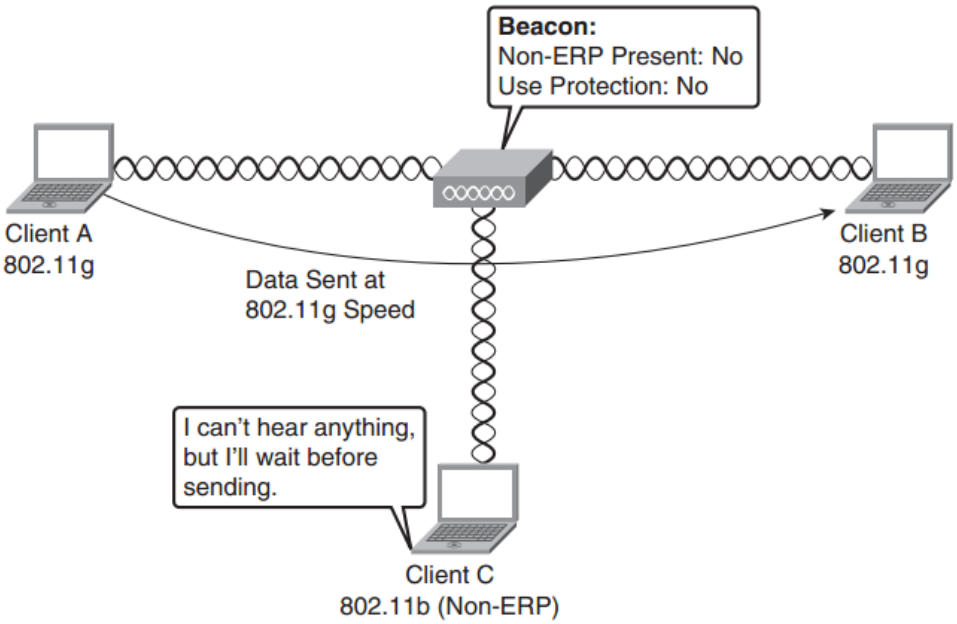



*802.11g Cell Using Protection: Part 3*

.

الخطوة الثالثة يقوم الجهاز A المتعامل بالمعيار 802.11g بإرسال بيانات الي الجهاز B الذي يتعامل بنفس المعيار و لا يستطيع الجهاز C الذي يتعامل بالمعيار 802.11b سماع تلك البيانات و يراها كأنها شوشرة noise و يظل ينتظر انتهاء مدة الإنتظار الموجودة في رسائل RTS/CTS

و هذا دليل علي عمل protection mechanism




*802.11g Cell Using Protection: Part 4*

.

كل هذا لا يعني خلو هذا التوافق من مشاكل قد تحدث فوجود المعيرين في نفس المكان قد يؤدي الي ظاهرة تسمي تأثير الدومينو domino effect و هي تنشأن نتيجة وجود جهازي أكسس بوينت متجاورين أحدهما يتواجد فيه خليط من أجهزة 802.11b و 802.11g فيعلن عن بيكون بهذه المعلومات

NON_ERP present: yes

،Use Protection: yes

و الآخر القريب من هذا الأكسس بوينت لا يتواجد فيه هذا الخليط و لكنه يري البيكون الخاص بالأكسس بوينت القريب منه فيحتاط لذلك فيعلن عن بيكون يدل علي عدم وجود أجهزة 802.11b لديه و لكنه سيأخذ احتياطاته لقربها منه هكذا

NON_ERP present: no

Use Protection: yes

هذا الأمر يحمل علي الأكسس بوينت احتياطات قد لا يحتاجها أسوأها هو تقليل السرعة من سرعة المعيار 802.11g ذو 22 ميجابت لكل ثانية الي سرعة المعيار 802.11b ذو 9 ميجا بت لكل ثانية و هذا أحد عيوب هذا الأمر و لذلك ينصح بتوحيد معايير الأجهزة في نفس الشبكة

## رحلة الفريم بين شبكات الإيثرنت والشبكات اللاسلكية

عرفنا مما سبق رحلة الفريم في الشبكات اللاسلكية ، لكن ماذا يحدث للفريم عند انتقاله بين شبكة سلكية و أخري لاسلكية فمن المعروف أن شبكات سيسكو التي تعتمدها كحلول لاسلكية يستخدم فيها جهاز كنترولر يقوم بالتحكم في الأكسس بوينت و هذا الجهاز يتصل بالشبكة اللاسلكية بواسطة سويتش سيسكو يقوم بدوره بربط الأكسس بوينت بواسطة أسلك UTP و لا يقف الأمر هكذا فربما تحتاج أجهزة مراقبة و تأمين للشبكة اللاسلكية و كلها سترتبط بشبكتك اللاسلكية سلكيا كما تري

اذن فسينتقل الفريم من شبكة سلكية الي لاسلكية و العكس فهل سيتغير أم سيتم المحافظة علي شكله أم ماذا بالضبط و هذا ما سنتعرف عليه حالا و سنستخدم الشبكة التالية كمثال لما سنتكلم عنه

و سيستخدم الأكسس بوينت عنواني شبكة SSID لكل منهم شبكتهم الخاصة Subnet أحدهما يختص بالضيوف و الثاني بالمستخدمين و سيكونان معزولان شبكيا رغم استخدامهما لنفس معيار الراديو a , b , g , n و ستكون بياناتهما هكذا

الضيوف

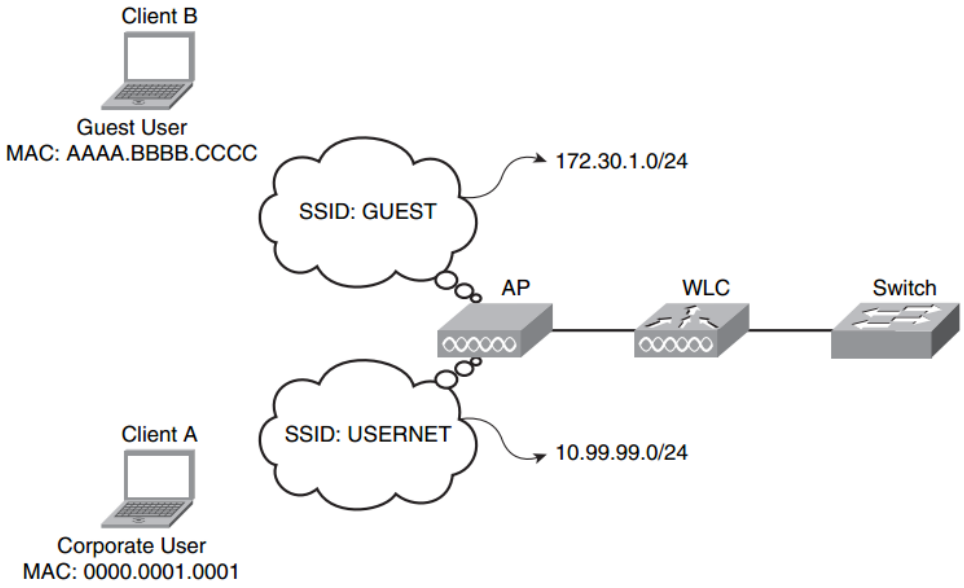
SSID : Guest

Network : 172.30.1.0/24

المستخدمون

SSID : UserNet

Network : 10.99.99.0/24




*A Simple Wireless Network*

ستقوم الأجهزة الموجودة ضمن شبكة guset البحث الخامل Passive Scanning عن الأكسس بوينت و معني ذلك أنه لن يتم اخفاء عنوان الشبكة الخاص بها Guest=SSID

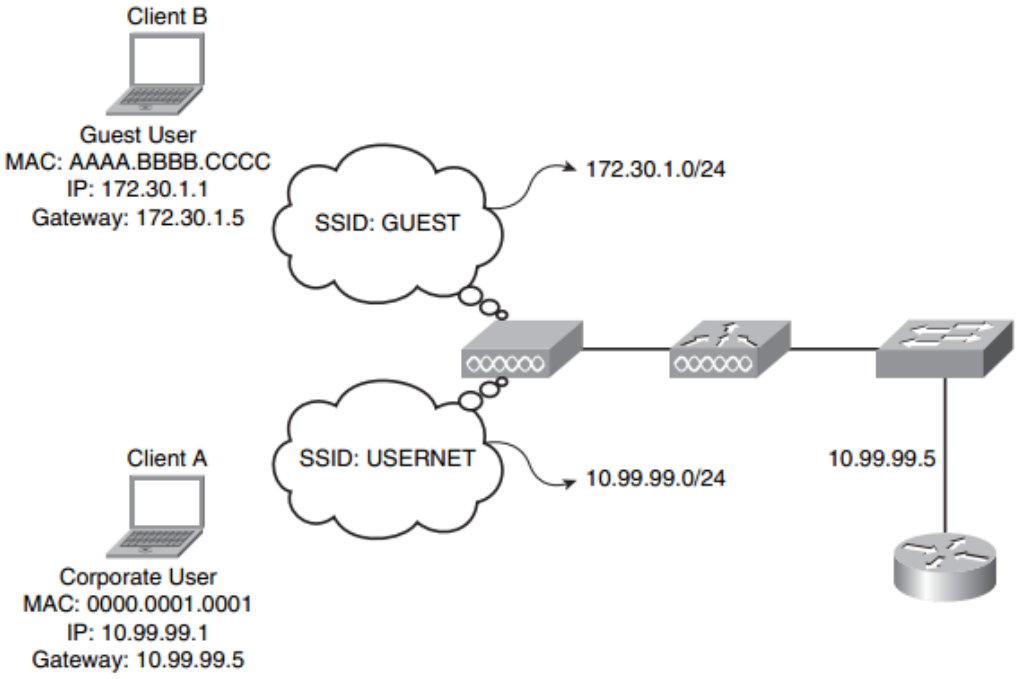
و علي العكس فسيتم اخفاء عنوان البشكة الخاصة بالمستخدمين SSID=UserNet و سيكون علي المستخدمين بها البحث النشط عنها Active Scanning

و في الحالتين سيتم تداول الفريمات بين الأكسس بوينت و الأجهزة من مرحلة authentication طلبا و ردا الي مرحلة Association طلبا و ردا و سيتم خلال هذه المراحل تعرف الأجهزة علي data rate و

speed المستخدمة أو المتاحة من قبل الأكسس بوينت باستخدام Received Signal Strength Indicator (RSSI) and signal-to-noise ratio (SNR)

اذن فلدينا شبكتين مختلفتين فماذا سيحدث ان أراد جهاز في أي من هاتين الشبكتين مراسلة الآخر

طبقا لما نعرفه فإن الجهازين معزولين لأنهما ينتميان الي شبكتين مختلفتين و لذلك كي يستطيع أن يراسل كل منهما الآخر فلابد أن يستخدم طرق أخري منها استخدام الراوتر default gateway ذو العنوان 10.99.99. و هنا سيقوم الجهاز A بإنشاء طلب Resolution Protocol (ARP) و يرسله الي الأكسس بوينت و ذلك لترجمة عنوان الأيبي الخاص بالراوتر الي عوان فيزيائي




*Client A Communicating with Client B*

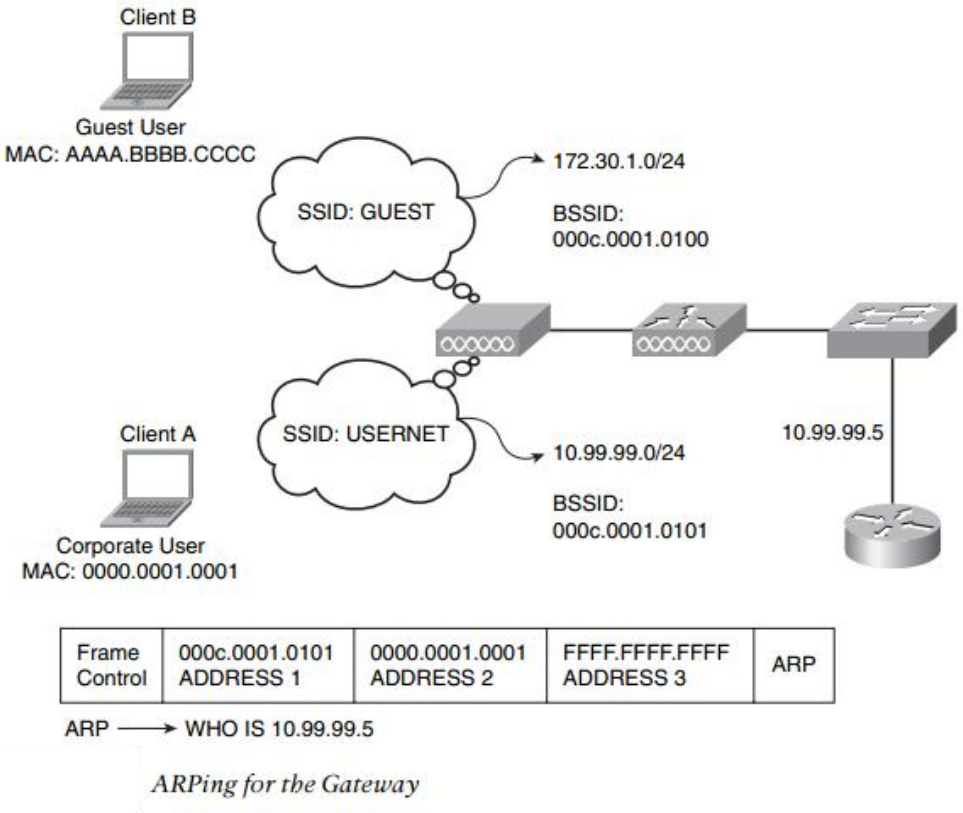
عندما يرسل الجهاز طلب Resolution Protocol (ARP) الي الأكسس بوينت فإن الأمر يختلف عن الشبكات السلكية فالشبكة السلكية يتعامل الفريم الخاص بها مع عنواني MAC هما المرسل source address و المستقبل destination address أما الشبكات اللاسلكية فقد يكون الفريم الخاص بها يتكون من أربع عنواين فيزيائية تمثل المحطات التي يمر بها في طريقه بدءا من المرسل و حتي المستقبل هكذا

source address (SA) = و هو الماك الخاص للجهاز المرسل لطلب ARP و هو العنوان الثاني في الفريم

destination address (DA) : الماك أدرس الذي سينشر broadcast طلب ARP و هو FFFF.FFFF.FFFF.FFFF

receiving address (RA) : هو الأكسس بوينت و هو العنوان الأول في الفريم

transmitter address (TA) : الماك أدرس لأكسس بوينت آخر في طريق الفريم و هو غير موجود لدينا هنا




*ARPing for the Gateway*

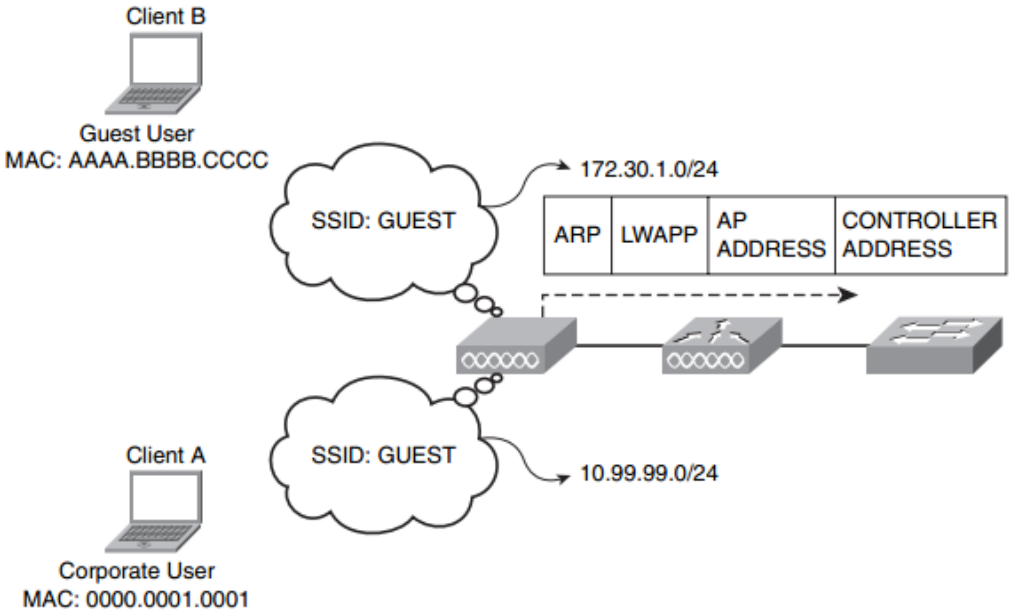
و الشكل التالي يبين فريم وايرلس به ثلاث عناوين و لا يوجد به عنوان TA لوجود أكسس بوينت واحد فقط

| Frame Control | ADDRESS 1 000c.0001.0101 | ADDRESS 2 0000.0001.0001 | ADDRESS 3 FFFF.FFFF.FFFF | ARP REQUEST |
|---|---|---|---|---|

*ARP Request*

الأكسس بوينت يستقبل ARP ويفحص محتوياتها و يتحقق من FCS frame check sequence في الفريم و ينتظر فترة تسمي short interframe space (SIFS) ثم يرسل ACK الي الجهاز الذي أرسل ARP ليطمئنه علي وصول الفريم

يقوم بعدها الأكسس بوينت بإرسال الطلب الي جهاز الكنترولر WLC Wireless Controller و ذلك بإستخدام بروتوكول خاص من سيسكو لتبادل البيانات بين الأكسس بوينت و الكنترولر يسمي Lightweight Access Point Protocol LWAPP



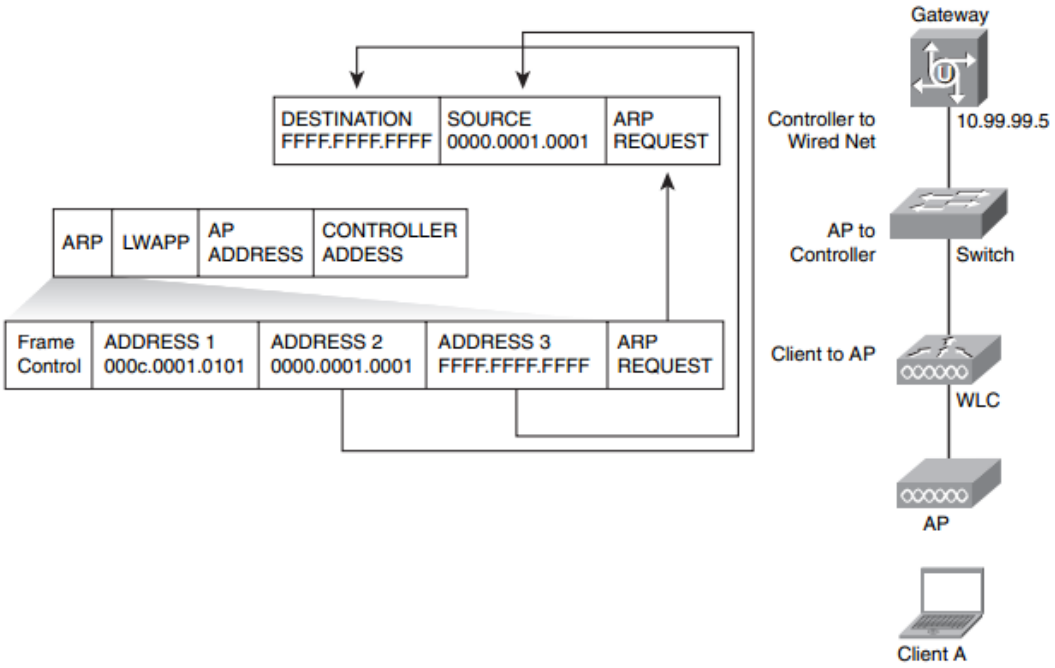

*ARP Forwarded in LWAPP Frame*

يسافر فريم LWAPP بين الأكسس بوينت و الكنترولر عبر كابل utp و ليس لاسلكيا حيث أن وسيلة الإتصال المدعومة من سيسكو بينهما هي الكابلات و هنا يطغي سؤال

ما هو موقف فريم الوايرلس و كيف سيتم التعامل معه

بروتوكول LWAPP يقوم بعمل تغليف encapsulate الفريم داخل header بطول 6 بايت و هذا الهيدر يحتوي علي IP و MAC للأكسس بوينت كمصدر source و عنوان IP و MAC لـ WLC كهدف Destination

و يتم وضع فريم الوايرلس بكل ما فيه داخل هذا header و عندما يصل فريم LWAPP الي WLC يقوم بإعادة صياغة طلب ARP القادم بصيغة الوايرلس 802.11الي صيغة ايثرنت 802.3 ليتم ارسالها عبر كابلات الإيثرنت بالشكل الذي تراه



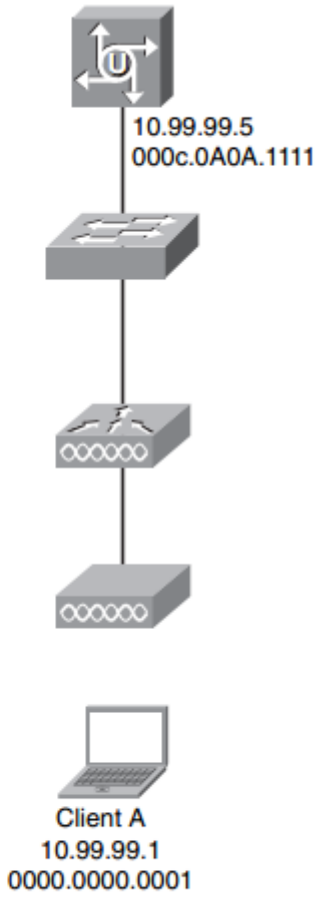

*WLC Forwarding the ARP Toward the Gateway*

عندما يتسلم السويتش طلب ARP يقوم بقراءة عنوان الجهة المستهدفة destination MAC address في الفريم و قد قلنا أنها عنوان broadcast فيقوم بنشر flood الفريم الي كل البورتات التي لديه عدا البورت الذي جاء منه

عند وجود VLAN سيقوم السويتش بنشر طلب ARP عبر البورتات التي تنتمي لنفس VLAN المنتمي له البورت الداخلة منه طلب ARP

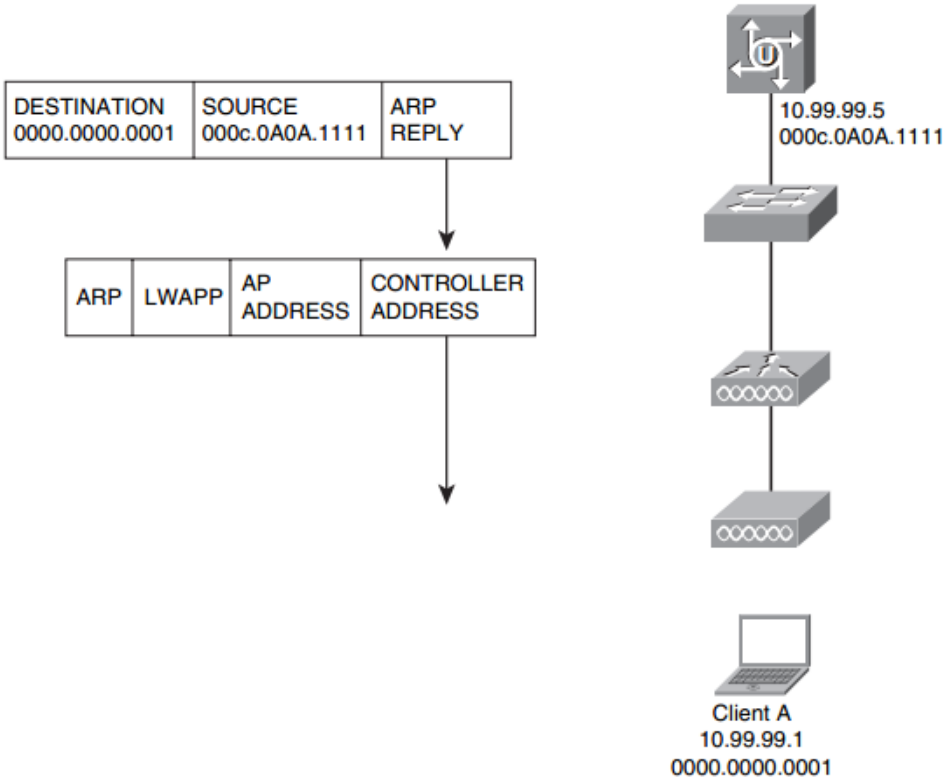
بعد ذلك سيصل الفريم الي الراوتر default gateway و سيقوم بالرد علي طلب ARP بالعنوان الفيزايئي MAC الحاص به و هنا تبدأ مرحلة الرد ARP response علي ARP request و لكن سيكون انتشار هذا الرد أو مساره عبر Unicast لأنه تم معرفة الجهة التي تطلب ARP و يكون عنوان مصدر ARP response هو عنوان الراوتر و عنوان الهدف اي البورت القادم منه فريم ARP request في السويتش

| DESTINATION | SOURCE | ARP |
|---|---|---|
| 0000.0000.0001 | 000c.0A0A.1111 | REQUEST |




*Gateway Responds to ARP*

سيذهب الفريم الي الكنترولر و يقوم بإعادة صياغته عكسية من ايثرنت الي فريم وايرلس صالح للتخاطب بين الكنترولر و الأكسس بوينت أي LWAPP ثم يقوم بإرساله الي الأكسس بوينت الذي يقوم بدوره بحذف LWAPP header مبقيا علي فريم الوايرلس 802.11 frame




*WLC Receives ARP Reply from GW and Converts It to LWAPP*

بعدها يقوم الأكسس بوينت بعمل عد تنازلي بقيمة معينة و عند انتهائها يرسل البيانات الي الجهاز A الذي بدوره يرسل فريم تأكيد ACK بعد فترة SIFS

و الآن استطاع الجهاز معرفة طريقه الي جهاز آخر في الشبكة مع عمل mapping لعوان الراوتر و ذلك عبر مسار تخلله أوساط سلكية و لاسلكية و أجهزة أكسس بوينت و كنرولر و سويتش و راوتر

## استخدام VLAN لضبط مسار فريم الشبكات اللاسلكية

بعد معرفتنا لرحلة فريم الشبكات اللاسلكية عبر شبكات الإيثرنت لابد أن يتبادر الي ذهننا تساؤل هو كيف تحافظ الشبكات الاسلكية علي الفصل بين البيانات ذات SSID المختلفة عند مرورها من خلال سويتش واحد و أكسس بوينت واحد و كنترولر واحد

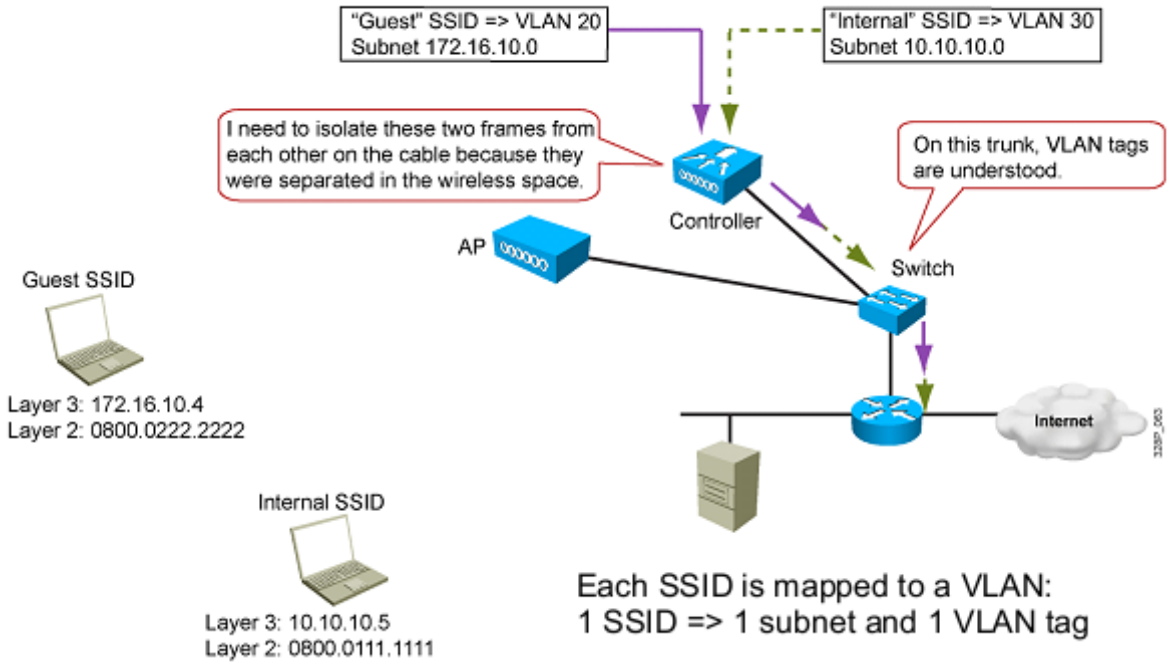
هنا يأتي دور VLAN في الشبكات اللاسلكية حيث نقوم بربط كل subnet مع SSID ليكون شبكة خاصة بكل منهم معزولة سلكيا بال vlan كما كانت معزولة لاسلكيا بواسطة SSID و ذلك لأن البيانات

ستمر من خلالل الكنترولر الي السويتش و من ثم الي الراوتر و هذه أجزاء سلكية من الشبكة و نحتاج الي عزل بيانات الشبكتين كما عزلناهم لاسلكيا بواسطة SSID

و في جهاز الكنترولر نقوم بضبط اعداداته لربط كل SSID مع VLAN ID و عندما يصل فريم الوايرلس الي جهاز الكنترولر فإنه يقوم بتحويل فريم الوايرلس الي فريم ايثرنت و ربط كل SSID مع VLAN الخاصة به ثم يطلقها الي السويتش عبر خط trunk فيقوم السويتش بقراءة tag لكل vlan و تحديد طريقها

اذن ففي الشبكات اللاسلكية تستطيع تجميع المستخدمين الذين يستخدمون نفس SSID في شبكة VLAN واحدة و تعزل المستخدمين الذين يتعاملون مع SSID أخري عنهم و ذلك لأن البيانات اللاسلكية في أنظمة سيسكو تمر جميعها علي سويتش واحد و تحتاج الي عزل البيانات طبقا للشبكات الموجودة

أو يكون هناك تفاضل بين صلاحيات المستخدمين طبقا لنوع SSID المستخدم فتحتاج لعزل المستخدمين المؤقتين guests عن الدائمين users




الشبكات الظاهرية هي شبكات تستطيع تقسيم الشبكات المحلية الي مناطق معزولة صانعة ما يسمي logical broadcast domain لتجميع الأجهزة التي تستخدم خدمات متشابهة أو توجد في مكان

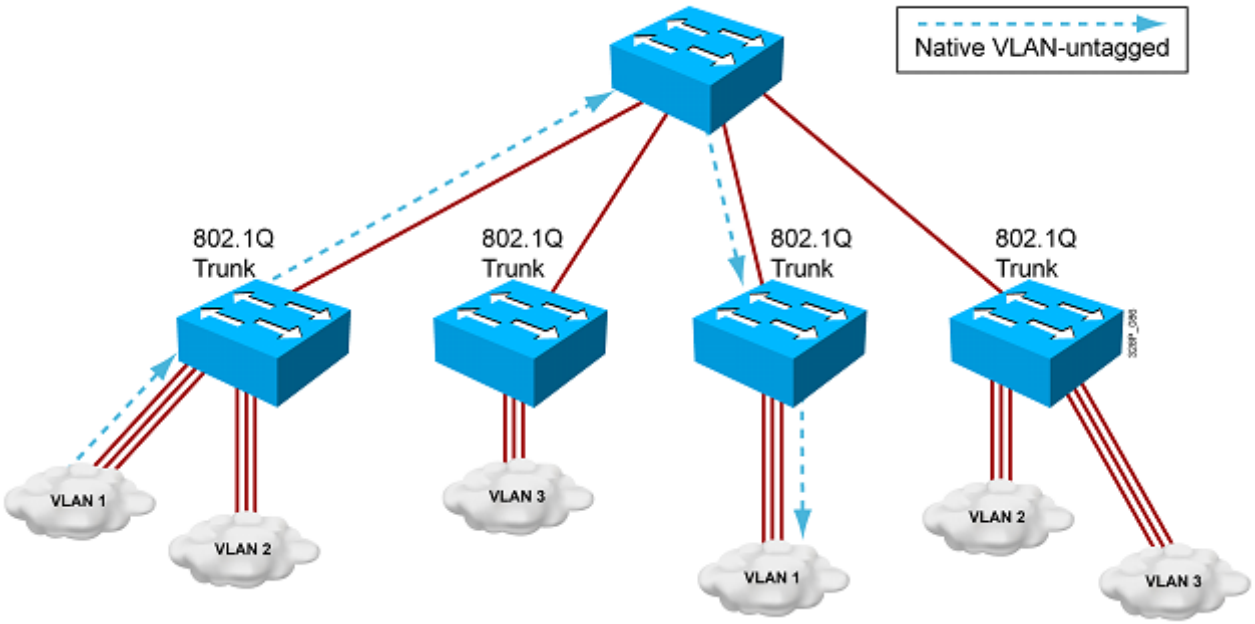
واحد في شبكة واحدة معزولة بغض النظر عن أماكن تواجدها و يكون كل بورت من السويتش مرتبطا بأحد هذه VLAN مما يمكنك بتطبيق سياسة أمنية عليها

فتستطيع أن يتبادل الأجهزة المشتركة في نفس VLAN البيانات حتي و ان كانت موجودة في أكثر من مكان بل و علي شبكة WAN و تكون معزولة عن الأخري حتي و ان كانت علي نفس السويتش

سويتشات سيسكو التي تم اعداد VLAN عليها تقوم بتقييد نقل البيانات القادمة من أحد البورتات بنقله الي البورت الذي ينتمي فقط الي نفس VLAN القادمة منه هذه البيانات لتخرج البيانات أيضا للتصل ببورت في سويتش آخر ينتمي الي نفس VLAN

هذا التقييد يجعل البيانات معزولة مما يمكنك من توزيع المهام عليها طبقا لنوعها و هذا مفيد عند عمل شبكات بها بيانات خاصة مثل الصوت و الفيديو و نقل البيانات عبر الوايرلس

عنند انتقال هذه البيانات المختلفة بين السويتشات تحتاج لضبط اعدادات بورت علي الأقل بين كل سويتشين له صلاحيات حمل كل أنواع VLAN علي السويتش و هذا البورت يكون غالبا uplink و يكون الإتصال بين السويتشات التي تم ضبط هذه البورتات بينها يسمي trunk



و يعتبر trunk هو خط اتصال بين بورت أو أكثر بين سويتشين أو سويتش و راوتر لحمل بيانات أكثر من شبكة VLAN و لهذا فإن لهذا الخط مواصفات و بروتوكولات خاصة فسيسكو قدمت لدعمه بروتوكول IEEE 802.1Q و يقوم Trunk بإضافة 4 بايت علي header التنقل بين بورتي السويتش

كل بورت تم اعداده ليكون trunk عبر بروتوكول 802.1Q قادر علي نقل شبكة VLAN واحدة خاصة تسمي Native Vlan لها رقم (VID) VLAN ID و الرقم الإفتراضي لها هو VLAN 1 تقوم هذه البشكة الخاصة بنقل البيانات الغير منتمية الي اي VLAN من التي تم اعدادها علي السويتش

و يفضل أن تقوم بتغيير أي إعدادات افتراضية في السويتش لضمان السيكيوريتي

و يتم معرفة كل VLAN من قبل السويتشات بواسطة tag يضاف بواسطة Q802.1 لكل vlan يبين رقمها عدا native و الذي يستطيع أي بورت تقبلها مثل بروتوكول سيسكو Cisco Discovery Protocolو لإدارة سويتشات سيسكو remotely يتم وضع Ip للسويتش و هذا الأي بي هو في الأصل خاص بـ Native vlan لتضمن وصول للسويتش عبر trunks و لهذا تسمي management VLAN

سيسكو في شبكاتها اللاسلكية دائما مغرمة بالتعامل مع السويتش 3750X و هو ما سنتعامل معه هنا أيضا

يتم عمل vlan في وضع global configuration في عدة خطوات

أولا انشاء VLAN

يتم عمل vlan في وضع global configuration بواسطة الأمر Vlan x حيث x هي رقم من 1 الي 1001 بعدها تقوم بوضع اسم بواسطة الأمر name y حيث y هي الإسم الذي اخترته و في حال لو لم تقم بعمل اسم له فإن الجهاز يقوم بعمل اسم مثل VLAN0004 للشبكة التي رقمتها بـ vlan 4

```
wlanvlan(config)#vlan 5

wlanvlan(config-vlan)#name guest
```

ثانيا ربط vlan مع بورت لسويتش

في وضع global configuration تقوم بالدخول علي وضع اعداد اي من البورتات بالأمر مثلا interface f0/0 أو مجموعة منها مثل interface range f0/0 - 5 ثم تضع الأمر switchport access vlan x حيث x هو رقم vlan الذي تريد ربطه بهذا البورت أو بهذه البورتات

```
wlanvlan(config)#interface range gigabitEthernet 1/0/1-5
wlanvlan(config-if-range)#switchport access vlan 5
```

قمنا بجعل البورتات من 1 الي 5 من نوع جيجا ايثرنت ضمن الشبكة guest و تظل باقي البورتات ضمن native vlan

تستطيع ب معرفة مختصر لما قمت بعمله و ستجد الشبكة guest و البورتات الموضوعه فيها بهذا الأمر

```
wlanvlan#sh vlan br
```

```
wlanvlan#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/6, Gi1/0/7, Gi1/0/8
                                                Gi1/0/9, Gi1/0/10, Gi1/0/11
                                                Gi1/0/12, Gi1/0/13, Gi1/0/14
                                                Gi1/0/15, Gi1/0/16, Gi1/0/17
                                                Gi1/0/18, Gi1/0/19, Gi1/0/20
                                                Gi1/0/21, Gi1/0/22, Gi1/0/23
                                                Gi1/0/24, Gi1/1/1, Gi1/1/2
                                                Gi1/1/3, Gi1/1/4, Te1/1/1
                                                Te1/1/2
2    VLAN0002                         active
5    guest                            active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
wlanvlan#
```

كذلك تستطيع التأكد من حالة بورت معين و الشبكة التي يوجد بها بهذا الأمر

```
wlanvlan#show interfaces gigabitEthernet 1/0/1 switchport
```

```
wlanvlan#show interfaces gigabitEthernet 1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: On
Access Mode VLAN: 5 (guest)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
wlanvlan#
```

ثالثا ضبط اعدادات trunk

في خطوتين مكررتين تستطيع عمل اعداد لمسار trunk علي السويتشين المتصلين به علي أن تكون اعدادات native vlan أيضا متشابهة

في البداية تختار رقم البورت ثم تقوم بعدها بعمل trunk و لكن قد تظهر هذه الرسالة و التي تخبرك بعدم امكانيةعمل trunk و ذلك بسبب عدم تفعيل بروتوكول سيسكو dot1Q

```
wlanvlan(config)#interface tenGigabitEthernet 1/1/2
wlanvlan(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be co
nfigured to "trunk" mode.
wlanvlan(config-if)#switchport trunk encapsulation dot1q
wlanvlan(config-if)#switchport mode trunk
wlanvlan(config-if)#
```

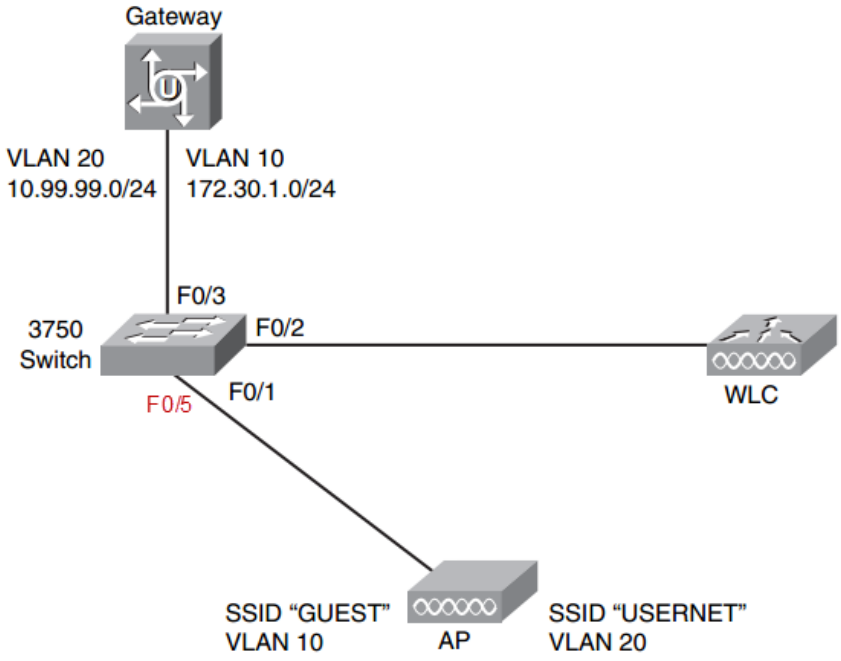
بعدها قم بالتأكد مما عملت بواسطة الأمر show interfaces tenGigabitEthernet 1/1/2 switchport

```
wlanvlan#SHow interfaces tenGigabitEthernet 1/1/2 switchport
Name: Te1/1/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
wlanvlan#
```

أو بواسطة الأمر show interfaces tenGigabitEthernet 1/1/2 trunk

```
wlanvlan#SHow interfaces tenGigabitEthernet 1/1/2 trunk

Port        Mode             Encapsulation  Status        Native vlan
Te1/1/2     on               802.1q         other         1

Port        Vlans allowed on trunk
Te1/1/2     none

Port        Vlans allowed and active in management domain
Te1/1/2     none

Port        Vlans in spanning tree forwarding state and not pruned
Te1/1/2     none
wlanvlan#
```

و هذا تطبيق عملي في شبكة لاسلكية




عمل vlan

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 10
Switch(config-vlan)#exit

Switch(config)#vlan 20
Switch(config-vlan)#exit

Switch(config)#end
Switch#
00:01:07: %SYS-5-CONFIG_I: Configured from console by consol

Switch#show vlan brief

VLAN Name                Status  Ports
---- ------------------- ------- -------------------
1   default              active  Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                 Fa0/21, Fa0/22, Gi0/1, Gi0/2

10   VLAN0010             active

20   VLAN0020             active
1002 fddi-default            act/unsup
1003 token-ring-default         act/unsup
1004 fddinet-default          act/unsup
1005 trnet-default           act/unsup
```

## ربط كل بورت بالشبكة الظاهرية vlan

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#int f0/5

Switch(config-if)#switchport mode access

Switch(config-if)#switchport access vlan 10
Switch(config-if)#

Switch#show interface status
00:13:00: %SYS-5-CONFIG_I: Configured from console by consoleerface status

Port    Name         Status     Vlan     Duplex Speed Type
Fa0/1               connected  1      a-full a-100 10/100BaseTX
Fa0/2               connected  1      a-full a-100 10/100BaseTX
Fa0/3               connected  1      a-full a-100 10/100BaseTX
Fa0/4               connected  1      a-full a-100 10/100BaseTX

Fa0/5               connected  10      a-full a-100 10/100BaseTX
Fa0/6               connected  1      a-full a-100 10/100BaseTX
Fa0/7               connected  1      a-full a-100 10/100BaseTX
Fa0/8               connected  1      a-full a-100 10/100BaseTX
<text omitted>
```

## اعداد Trunk

```
Switch#enable
! To simplify configuration, you can set the parameters on a range of interfaces
rather than one at a time

Switch(config)#interface range f0/1 - 3

Switch(config-if-range)#switchport trunk encapsulation dot1q

Switch(config-if-range)#switchport mode trunk
Switch(config-if-range)#
00:15:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
  state to down
00:15:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
  state to down
00:15:42: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
  state to downswitchpoer
00:15:45: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
  state to up
00:15:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed
  state to up
00:15:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed
  state to up

Switch(config-if-range)#switchport nonegotiate

Switch(config-if-range)#switchport trunk native vlan 1
Switch(config-if-range)#
! Exit Back to Priviledge EXEC to verify

Switch(config-if-range)#end
!Use the following command to verify what interfaces are enabled for trunking
Switch#show interface trunk
00:19:55: %SYS-5-CONFIG_I: Configured from console by consoleow interface trunk

Port     Mode      Encapsulation Status     Native vlan

Fa0/1    on        802.1q      trunking    1

Fa0/2    on        802.1q      trunking    1

Fa0/3    on        802.1q      trunking    1
Fa0/23   desirable  802.1q      trunking    1
Fa0/24   desirable  802.1q      trunking    1
! Output omitted for brevity
```

للمراسلات و النقد و التعقيب

naderelmansi@gmail.com